

# Solving Security Challenges with Automation to Reduce Risk and Increase Efficiency across the Hybrid Network

## Success story



As the largest multimedia operator in Slovakia, Slovak Telekom operates a very complex network. To keep pace with business demands, they were in the process of adopting new cloud platforms and DevOps methodologies, but they struggled to incorporate new practices into their traditional processes. With an increased volume of requests, it became necessary to make some changes to prevent loss of control over their firewalls. At the same time, Slovak Telekom wanted to reduce the high number of resources dedicated to ensuring compliance with internal and external mandates, like ISO 27001 and the looming GDPR requirements. To select the right solution that would best address their challenges, Slovak Telekom reached out to Dimension Data for their experience and expertise with network security.

## The Basics: A Complex Network

Slovak Telekom operates a large number of firewalls from multiple vendors, making the change process difficult to manage at best. The existing methods to adhere to security policy were inefficient and included the use of Excel spreadsheets, which were difficult to maintain and prone to error. In addition, they faced a large project to migrate a quantity of firewalls to Next Generation Firewalls (NGFWs), and the pressure from the C-suite and compliance officers to ensure continuous compliance and pass the next audit was at an all-time high.

## The Need: Visibility and Control

Slovak Telekom could not continue using the same processes; it was only a matter of time before serious trouble would affect the network. An IT executive expressed concern that their manual change management process was slow and cumbersome and not the best use of the talented network security engineers on his staff. "The manual change process was prone to error and bad requests, which meant having to do things more than once – not to mention making the network less secure."

Slovak Telekom began the search for a firewall management solution that would simplify their change process, eliminate spreadsheet management, reduce error-prone manual tasks and enable the company to improve their overall network security.

## Why Now? Change Was Needed

The main drivers behind Slovak Telekom's decision to seek a solution included:

### *Driver #1: rules were not effectively managed*

With over 10,000 rules to manage, the Slovak Telekom staff did not have the necessary visibility to understand why many rules existed and had no way to make sense of the environment to understand which rules were required for business connectivity and which rules could be deleted. Manually tracking and removing rules was very complicated and time consuming for a team that had many other priorities to address. Without an efficient process, changes resulted in redundant, shadowed and obsolete rules, leaving the network vulnerable.

## The Benefits

- Increased the rate of change implementation by 80% with higher accuracy
- Improved productivity, reduced manual tasks, and eliminated email and spreadsheet tracking by automating change processes
- Gained visibility and control over configuration of multi-vendor firewalls, devices and routers
- Reduced risk through automated decommissioning of overly permissive and unused rules
- Ensured compliance with ISO 27001 and GDPR with fewer resources
- Automatically documented changes and rule recertification to continuously fulfill audit requirements
- Recertification workflow leveraged to automate the processing of expired rules
- Migrated to NGFW with full confidence that policies are transferred accurately

### *Driver #2: firewall migration*

Because of a project to migrate from traditional to NGFWs, it was necessary for Slovak Telekom to ensure that all firewall rules were properly transferred and implemented. At the end of the migration, the company planned for approximately 90% of their existing firewall environment to be NGFW.

### *Driver #3: passing internal audit*

Slovak Telekom required a more effective solution to ease the burden of passing internal and external security audits and needed an auditable change process to replace emails and Excel files. They also had a compliance requirement to manage and track the expiration for all access rules.

## The Solution: Visibility and Automation

Slovak Telekom made a decision to adopt a Network Security Policy Management (NSPM) solution to track and monitor the rule change process. The goal was to provide the simplicity that comes with a single network view to gain visibility across their entire network. With a multi-vendor firewall infrastructure, using each individual firewall vendor management tool to solve their challenges would not have provided the relief needed to streamline operations.

With the help of Dimension Data, Slovak Telekom launched a review process to select a vendor.

## The Decision: Why Tufin?

Dimension Data understood Slovak Telekom's needs from the beginning. "It is a high priority for Dimension Data to develop a close relationship with the key influencers on any project to gain a deep understanding of their goals," said Vladimír Ružička, Managing Director of Dimension Data Slovakia.

Following six months of research, evaluation and due diligence, and a thorough proof of concept (POC) with the corporate security and operations teams, Slovak Telekom selected Tufin Orchestration Suite™ because it had the best workflow solution and could be fully deployed within a couple of months.

## The Deployment: Instant Value with a Phased Approach

Slovak Telekom had a tight timeline, and Dimension Data was enlisted to help the company deploy Tufin SecureTrack and Tufin SecureChange. Only a month later, the solution was in production managing 34 of their multi-vendor firewalls. Step by step, they added more firewalls to Tufin Orchestration Suite until they connected Slovak Telekom's entire estate.

By taking a phased approach to adding firewalls, Slovak Telekom was able to open access for all technicians to submit change requests. All the users were fully trained and now use Tufin Orchestration Suite directly for all change requests.

## The Results: Improved Productivity, Security and Compliance

Slovak Telekom fully integrated Tufin Orchestration Suite into their everyday processes, and close to 80% of their technicians use the solution daily to request changes. Through the implementation of Tufin Orchestration Suite, the company has achieved the following:

**Automated processing of expired rules:** Engineers can add a one-year expiration for each access request and leverage the recertification workflow to automate the processing of expired rules.

**Reduced time to implement changes:** Productivity gains were experienced immediately as they reduced the time it takes to implement a change from 1 week to 1-2 days, eliciting positive feedback across the company.

**Increased productivity:** After the ramp-up time, the operations team now handles approximately 200 requests per month.

*"A firewall without a guard to manage it is a security concern."*

*Slovak Telekom senior IT executive*

*"In the case of Slovak Telekom, we were confident that Tufin was the right choice to meet their needs,"*

*Vladimir Ruzicka,*

*Managing Director Dimension Data Slovakia*

**Immediate productivity gains:** “Already implemented” requests were eliminated which improved productivity by 20%-30% immediately.

**Streamlined processes:** It is now much faster to approve or reject requests with the streamlined approval processes.

**Simplified compliance:** With changes automatically documented, Slovak Telekom effectively fulfills not only the defined internal security requirements, but also the requirements of ISO 27001 and GDPR.

**Validated firewall migration:** Throughout the process of migrating firewalls to virtual platforms, many firewall rules were decommissioned. Tufin Orchestration Suite tracked the rule base during the migration and verified that the policy remained intact after the migration.

## The Future: Automating, Unifying Security Policy and Integrating Third Parties

Slovak Telekom achieved baseline visibility, increased productivity and improved security. The company intends to delve deeper into the Tufin Orchestration Suite automation capabilities to remove manual processes and expand the usage to other areas of the network. The next step is to define security zones and configure the Unified Security Policy (USP) in partnership with the IT team to tighten controls and reduce the attack surface. They will also use Tufin APIs to integrate with third party tools to address additional use cases.

### About Slovak Telekom

Slovak Telekom has long been a leader in technological innovations on the Slovak Telecommunication market. The company is the biggest provider of wired broadband internet through optical and metallic networks (FTTX, ADSL, VDSL). Slovak Telekom also provides digital television via the latest IPTV and DVB-S2 satellite technology. In the field of mobile communication, the company provides internet access using several technologies of high-speed data transmission - GPRS/EDGE, UMTS FDD/HSDPA/H SUPA, Flash-OFDM and LTE.

Slovak Telekom is a member of the multinational Deutsche Telekom Group.

### About Dimension Data

Dimension Data is a global systems integrator and managed services provider that designs, manages, and optimizes today's evolving technology environments to enable our clients to leverage data in a digital age. We employ over 28,000 employees across 47 countries on five continents and we invest heavily in innovation to bring together the world's best technologies, from consulting, technical and support services to a fully managed service.

### About Tufin

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,000 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

