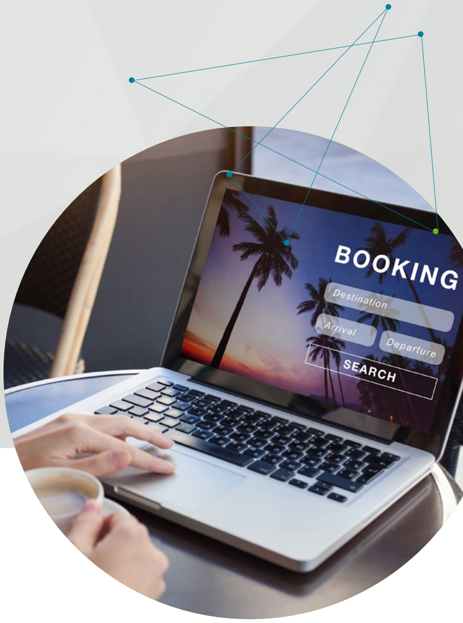
tufin The Security Policy Company.

Case Study

Automated Policy Management and Audit Reporting for Fortune 500 Travel Company



With 25,000 employees across 15+ countries, this e-commerce travel company is behind some of the world's most trusted online travel brands. Known for delivering the ultimate user experience for consumers and partners, they turned to Tufin to help expedite the secure delivery of new service launches while effectively managing security policies across its heterogeneous IT environment.

The Challenge

To succeed in the highly competitive online global travel industry, this Fortune 500 company must launch new services on time, apply access changes quickly, and successfully pass quarterly security audits. They lacked centralized visibility and management of security policies across their hybrid, multi-vendor environment. Manual processes were often error-prone with significant time spent on networking operations, the tracking of changes, and creation of audit trails.

To succeed in their dynamic market, the online travel company's network and security teams wanted to rapidly detect, analyze, and resolve security and operational network access issues. They had to log into various network security management consoles to determine which rules blocked traffic or were misconfigured, which could take hours. Lacking a holistic view of the heterogeneous environment forced the company to quickly correlate insights from multiple network resources for effective response. Meeting or exceeding defined SLAs, as well as security and compliance mandates, was critical for their teams.

The online travel company required a centralized solution to enhance visibility into its fragmented network which included disparate platforms and technologies. They also needed to expedite service delivery and quickly troubleshoot issues with any of its 50+ multi-vendor firewalls (e.g. Palo Alto Networks, Check Point, Juniper, Cisco) deployed across on-premises, public, and private cloud.

Why Tufin

With the Tufin Orchestration Suite, they began to automate and track access changes across their multi-vendor, heterogenous environment. They can quickly troubleshoot access issues for faster resolution and apply segmentation policies for enhanced security. They successfully lowered the number of firewall incidents and reduced SLA times, and can now meet compliance requirements.

With Tufin on board, the teams benefit from end-to-end visibility across their fragmented network dashboard and alerts to help them detect and resolve network security and operational issues.

Business Impact

- Automated compliance reporting across multiple vendors
- Significantly reduced number of resources required to make firewall changes
- Gained efficiency and drove consistency across integrated security tools

Key Success Metrics

- Reduced SLA from 5 days to just a few minutes or hours
- Thousands of rules were cleaned in one week, resulting in decreased CPU consumption
- Reduction in firewall incidents
- Greater collaboration between security, network, SOC, and NOC teams due to joint visibility and unified processes

The Results

With enhanced visibility of their security posture, security and network teams can prioritize and turn their attention to higher value tasks. They now have instant visibility into network security and operational issues for fast detection and remediation, for example, unusual spikes in a rule that could indicate an attack or network outage. This data can then be correlated with IPS/EDS data to help verify true /false positives. By integrating Tufin with their SIEM solution, they also receive real-time alerts on overly permissive rules and unused rules. The SIEM integration ensures up-to-date policy information to bring enhanced context and the accelerated resolution of incidents, where they can see the full path for any event, what devices might be impacted, and which policy is allowing traffic. These alerts help them to not only effectively mitigate risk, but also to ensure their segmentation policy is accurate enough to enable daily operation that meets Zero Trust objectives.

Streamlined service delivery via automation

Prior to adopting Tufin, the company's network team had to manually access individual management consoles (e.g., Panorama, FortiManager, etc.) for tasks like rule changes, enabling new access for an app, or decommissioning a server. This was a laborious and error-prone process. On average, it took the team five days to complete a firewall change, while also handling an average of 10–20 firewall rule changes per day. These changes are rather lengthy, or required a unique skill set where each change might contain up to 500 lines of firewall rules and ultimately resulted in the creation of team dedicated solely to firewall changes. Implementing manual changes across multiple management consoles comes at a cost—outages, risky access, and compliance issues.

With Tufin's change automation, their network team was able to automate policy management and implement access changes within minutes or hours, and significantly reduce firewall misconfigurations. Reducing the network change times from 5 days to just minutes or hours, lowered the number of escalation cases.

> “*With Tufin, we only have to add source, destination, port, and services, and Tufin finds the optimal route, implements the change, and validates the change was deployed as planned. We saved a tremendous amount of time, especially during COVID, when we needed to implement access changes overnight to enable our remote workforce. Now, we have almost zero incidents deploying firewall changes, and everything is automated with zero impact on our production environment. Tufin's solution enables our developers to immediately test and deploy their apps faster than ever before.*” — Company's Security Engineer

The Security Engineer added, “We also integrate Tufin SecureChange with our ITSM ticketing system, ServiceNow, where a ticket triggers a workflow within SecureChange, and an implementation notification is sent back to ServiceNow, facilitating easy and centralized tracking. Tufin Designer can run across multi-vendor firewalls and highlight rules and interfaces. Because Tufin integrates with most network security devices, it helps us to achieve accurate topology which enables us to automatically implement changes quickly that also comply with our policy.”

Continuous compliance

Auditing has always been a critical issue for the online travel company, especially for its firewalls. The auditors sought to remove overly permissive, unused, and non-compliant rules. When done manually, every line in a firewall rule had to be reviewed and checked for compliance. The travel company came to rely on the customizable workflows offered through SecureChange and deploys them for numerous use cases, such as access changes, and modifying/deploying object groups.

Using Tufin, the company's security team automated firewall rule audits. They now have compliance templates created in Tufin that run on any firewall in any zone, with just one click. Unused rules and shadowed rules, for example, are quickly and automatically removed, and an email with the results is sent to the auditors. Manual processes were no longer required, and after deploying Tufin, thousands of rules were cleaned in one week.

> *"There are numerous shadowed rules and redundant rules, and it's not easy to just remove rules from firewalls. If you're saying you have to remove a rule, everyone jumps, and asks, 'What are you going to break?' This is what Tufin helps us with."*

With Tufin reporting packs, every change is documented, and the teams easily prepared for audits. The company conducts quarterly PCI-DSS audits on firewalls, ensuring there are no firewall rules that violate the PCI-DSS security policy; specifically blocking any traffic between production and non-production environments. This is where Tufin reporting capabilities are extremely helpful when it comes to monitoring and proving compliance.

Securing the Future

Thanks to the enhanced visibility and automation offered by Tufin, this online travel giant bolstered its security posture, improved operational productivity, and enhanced its position in the market. In the future, they plan to use the Tufin Vulnerability Management App (VMA) to prioritize vulnerability remediation efforts, and automatically apply mitigating controls. They further plan to deploy Tufin IPAM Security Policy Application (ISPA), to automatically synchronize their segmentation matrix with the network addresses of its IPAM.

One thing is certain: they can make these technology choices with the confidence that their centralized security policies will continue to reduce risk and enhance overall security.

Tufin (NYSE: TUFN) 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 company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2,000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.

tufin
The Security Policy Company.