tufin The Security Policy Company.

CASE STUDY

Large U.S. Utilities Company Cuts Network Change Time, Automates Compliance Tracking, and Reduces Downtime

A network outage at a major US utility company can mean a power outage for millions of customers. Massive power outages put people's lives in danger — think hospitals, traffic lights, emergency communications. Therefore, the mission of this network security team comes with the burden of maintaining public safety.

In order to secure this utility company's complex and fragmented network, the team must adeptly deploy and manage firewall rules across 2500+ devices, controlling access to critical assets in the company's infrastructure. Manual processes and lack of visibility resulted in months-long SLAs and an ineffective use of highly skilled resources. Tufin SecureChange and SecureTrack have vastly improved their SLAs and the company's overall security posture.

Challenge I: Accelerating Network Access Changes

Managing network changes in a large, highly regulated environment is a complex undertaking, especially when relying on manual processes to implement changes across 2,500 firewalls and thousands of routers and switches. Previously, nearly 40 people managed change requests. There was a two-month lead time and a tremendous backlog. This is because each change requires an impact analysis to check any proposed changes against security policy, vulnerability management tools, DNS servers and more. "Security was seen as a bottleneck and blocker instead of a business enabler," explains the Cybersecurity Manager.

Challenge II: Automating and Streamlining Compliance Tasks

With an obligation to comply with many federal and regional regulations, such as NERC CIP, this company's network security team must track every change across all infrastructure assets and validate that firewall rules are current and accurate. Identifying and eliminating all shadowed rules was impossible, because they had no way to automatically track all rules across their hybrid architecture. An inability to keep with up network permissions across firewalls greatly increases an organization's cyber risk exposure.

Challenge III: Faster root cause identification to handle network outages

When outages or other service interruptions occurred, the network security team had to manually research and review past changes because they lacked a solution to provide comprehensive path analysis to find the blockage.

Why Tufin

BUSINESS IMPACT

- Rule change SLAs are < 1 week – down from 2+ months
- 50% reduction in time to resolve outages
- 80% reduction in time to identify and remediate shadowed rules.
- Reduced number of people focused on change requests from 40 to 5
- Reduced time to prepare for compliance audits from weeks to 2 hours

> *"The more efficiently we manage the thousands of firewalls and other critical devices in our environment, the better we enable the business to move quickly in service of our customers. Tufin helps us deliver on that mission."*
>
> — Cybersecurity Manager, Large U.S. Utilities Company

> *The value becomes apparent when a workload that took 40 people, now takes about 5 people."*
>
> — Senior Cybersecurity IT Solutions Engineer, Large U.S. Utilities Company

The cybersecurity team evaluated options for best managing its firewall environment. Flexible automation, scalability and breadth of integrations were top of mind. They needed the ability to check the company's security policy against every rule exception request. Moreover, they wanted a solution that could implement and track changes in a single location for all the firewalls, routers, switches, and F5 and NSX devices in their environment. "Tufin checked all the boxes," commented the Senior Cybersecurity IT Solutions Engineer.

The Results

Network Changes in Days, Not Months

With Tufin network security solutions in place, the network security team has dramatically reduced the time and effort required to manage firewall rules and change requests. "The value becomes apparent," commented the Solutions Engineer, "when a workload that took 40 people, now takes about 5 people."

Automated, Streamlined Compliance Efforts

"We save countless hours on rule cleanup and compliance reporting, and we can give management visibility without pulling one of our valuable team members from critical tasks," explained the Cybersecurity Manager.

Tufin SecureTrack automatically identifies shadowed rules. Plus, it automatically reviews and tests every access change against the company's security policy. The company is also planning to leverage its ability to check against security intelligence from third-party solutions, such as the company's vulnerability management tool and its SIEM.

With immediate visibility into partial and fully shadowed rules, the team has reduced its time to identify and remediate these issues by 80%.

Ensuring Uninterrupted Business

With such a large deployment of firewalls in regulated and internal domains, being able to determine the cause for outages that may be the result of firewall policies or rules is essential to the network security team providing rapid resolution. During outages, Tufin's path analysis tool streamlined the process of identifying where the blockage is, reducing time to resolution by 50%.

> *We save countless hours on rule cleanup and compliance reporting, and we can give management visibility without pulling one of our valuable team members from critical tasks."*
>
> — Cybersecurity Manager, Large U.S. Utilities Company

Future Plans

Going forward, the network security team plans to take greater advantage of Tufin's market leading workflow automation, such as automatically permitting firewall rule changes that meet standard policies. "We want to continually reduce our SLAs, explained the Manager.

In addition, the team is piloting SecureCloud, Tufin's SaaS solution, which allows the team to integrate NetSec and DevOps processes and apply a security policy in the provisioning of cloud resources. They are also test driving various Tufin marketplace apps, to better leverage intelligence from their vulnerability management platform and to get more advanced in automated rule lifecycle management.

DP20220716