tufin

Achieving Compliance Across VMware NSX and the Physical Network

About the Customer

This Tufin client is a Fortune 500 United States-based global financial investment management leader that offers a wide range of financial products and services including retirement, asset management, and insurance. For the purposes of this case study, this Tufin customer's user will be referred to as Brian. Brian is part of the network operations team and works closely with the security team to successfully manage a complex network containing over 100 firewalls, which in part consists of Check Point R80.10 firewalls and management, as well as VMware NSX. Both platforms are proven technical integrations of the Tufin Orchestration Suite.

About the User

Brian is a Senior Network Analyst at one of the largest global financial investment managers, and he has over 10 years of experience across network management and information security. Before deploying Tufin Brian was neck deep in manual firewall operations, such as daily change requests, audit preparations and routine maintenance. Now that Tufin is successfully deployed, Brian has the bandwidth to research ways to further improve his team's overall efficiency and introduce policy-driven automation across the enterprise.

The Challenges of Home Grown Change Management

Brian's team had considered purchasing a solution for rule change tracking in the past, but faced a lack of funding and corporate support for the purchase. As a result, Brian's security and network teams were bound to using existing tools for change request and access management, which ultimately was at the expense of his team's time. "Even though we had a good internal process documented for approving changes, that didn't necessarily stop someone from making a change, so we really needed a solution for processing, visualizing, and tracking changes," Brian shared. "The manual methods that we were employing were creating time sinks for troubleshooting connectivity issues, and our ability to tackle strategic projects was being hindered."

The network team faced difficulty in getting funding until an external audit concluded with some outstanding requirements, necessitating a solution for rule change tracking and validation. "Once we had an external audit that detailed the requirements for both post-change validation and tracking, achieving compliancy required us to pursue a network security policy management solution," reflected Brian.

Meeting Compliance and Simplifying Audit Readiness

To improve compliance with industry regulations and security standards Brian's team developed a proactive ongoing internal review of firewall rule changes. The Tufin Orchestration Suite simplified the new process by providing a central console to review changes across the multi-vendor next generation network. "We've implemented a check so that when we receive IT-submitted changes, they're living documents that we retain and can reference," commented Brian. "Once a quarter we'll have our change approver go through a small random sample of the change requests across vendors and platforms and validate that each person who said they were going to change something actually did it."

Reducing Manual Effort While Emphasizing Policy Health

Brian's team had previously spent too much of their time reviewing and understanding their network policy, ultimately detracting from the ability to undertake strategic projects. With Tufin's Automatic Policy Generator (APG), Brian's team was able to automate the search for risky rules and the traffic analysis, and to streamline the process of tightening the rules. "Before the APG, we would go through the logs and look at the traffic, build rules based on the traffic,

Customer Benefits

- Ensured readiness for external and internal network security audits

- Reduced costs and time to resolution through simplified connectivity troubleshooting

- Consistent network security policy health across the enterprise

- Increased security and efficiency for data center migrations

- Simplified NSX firewall administration

- Successful delegation to end users with a secure, custom interface that was built with Tufin REST API

refresh the logs, review the traffic again, and then build some new rules again… it was an overly-iterative, repetitive, and inexact process," described Brian. "The APG suggests rules based on how permissive you think that they should be, and we simply approve and apply them – We've tightened a lot of access rules with Tufin while significantly reducing the team's time spent on the process."

Securing Datacenter Migration

With a large and changing enterprise network, Tufin has played a critical role in determining new rules for greenfield environments and ensuring policy health in new networks. "We've had two decent-sized migrations to new environments, and since no one knew what rules were required, we started off with open rules and used Tufin to monitor and analyze the traffic and establish firewall access rules to support it" noted Brian. "We took one of our larger datacenter LAN sites and migrated it to a segregated network zone protected by a firewall, and without anyone knowing what the access policy should be, we used the APG to lock down those firewall rules."

Expediting Time-to-Resolution

Brian's team now spends significantly less time on troubleshooting connectivity issues and more time on ensuring the health of their policy. "Previously when we received connectivity issues, we would need to dig through the firewall's audit logs searching for the right audit log, and then try to manually compare changes," Brian recalled. "Now when we find issues we can immediately go to Tufin, identify the changes during the window of access disruption, and compare the historical changes during that window – you select the two different rules and boom, it's all visualized."

Simplifying NSX Firewall Administration

Brian and his team found the auditing and management of VMware NSX micro segmentation complex and time consuming. Tufin risk management made the private cloud security policies easier to monitor, analyze and audit. "We're using Tufin for tracking firewall security policy within NSX for audit purposes and proactively identifying risky services for policy health improvement," stated Brian. "Tufin has been very helpful in complementing the IP grouping of NSX through individual IP searching, which makes our job of designing and ensuring access even easier. As we get further into our usage, we're looking to use Tufin to automate and provision changes within NSX."

Finding New Solutions Through APIs

Brian found that he could use the Tufin REST API to develop some unique internal solutions that met business requirements without violating security policies. "Some employees need to view whether objects are used within firewall policy during their day-to-day operations, but they shouldn't be able to see the actual firewall policies," described Brian. "I built an internal web page that calls the Tufin API that triggers a search for objects through the Tufin object lookup and returns the results of whether or not those objects are used within firewall policy – this has reduced our overall requests and increased our overall efficiency in change provisioning."

As with any open API, the opportunity to further integrate Tufin enables Brian's team to consistently improve their efficiency. "As we start to automate more things, I want to have requests make an API call to Tufin and have Tufin start the workflow process," shared Brian. "Whether it's decommissioning a server, giving access to a server, or duplicating access for an existing server, we can use Tufin to improve our operations while ensuring the consistent application of security policies across the network."

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. Find out more at www.tufin.com.