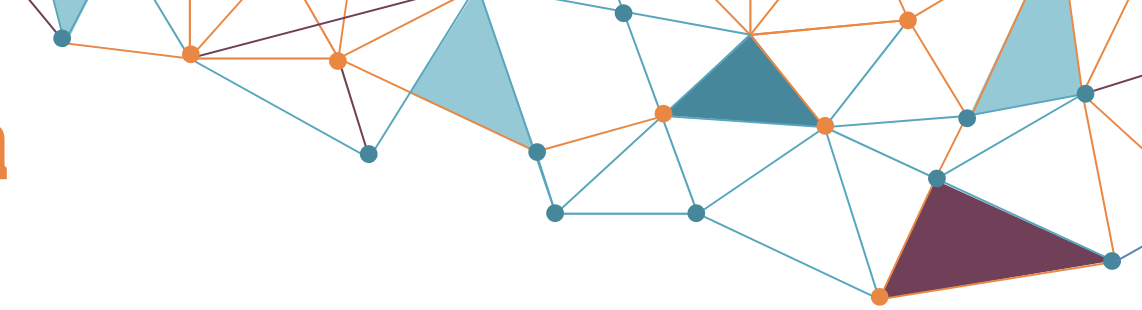

Automating Your Enterprise Network Security Policy Management to Gain Agility with Compliance

The Five Critical Steps

www.tufin.com

Executive Summary

Network security continues to be the top-priority investment for enterprise IT. A majority of the CIOs (82%) surveyed by the investment analyst firm Piper Jaffray are increasing their security budgets in 2016.[1] According to TechTarget.com, "security took center-stage" as a result of recent high-level breaches. This increased spending reflects the recognition by executives that investing in network security and getting it right is still far less expensive than the cost of having a major breach.

Not only does network security need to be "right" but it also must keep pace with business needs. Companies want – *need* – to have business agility—to get products and services to market faster, to address customers' needs better, to change their business models and the underlying applications on a dime, and above all, to be competitive. To properly enable the business, enterprise networks must be agile and their related security devices must be in lock-step. Waiting for firewall changes can't be the factor that holds business back.

The discipline of network security management has a number of challenges today. Enterprise networks have grown very complex, and manually making policy changes in hundreds of firewalls and other security devices can be harrowing. A misstep can stop business in its tracks or be too permissive and allow a data breach to happen. But making changes is a daily event, and security operations (SecOps) teams feel the pressure to quickly enable connections for business applications while still minimizing risk and maintaining compliance with regulatory mandates. Companies must find a way to overcome these challenges and finally balance security with agility.

Security management automation is the logical answer. Automation is already heavily used in other aspects of IT operations. When it is orchestrated on network security, the SecOps team can analyze and implement the appropriate network changes in minutes instead of days. Gartner research[2] has noted the benefits of effective network orchestration and automation which can improve management capabilities and operational efficiency, as well as increase availability, robustness and stability.

This paper looks at the five critical steps of network security automation and how to addresses the challenges in order to turn network security into a business enabler rather than a bottleneck:

1. Gain visibility into the business requirements
2. Model the network topology that enables the business
3. Define the organizational security policy
4. Create a well-defined, documented change process
5. Allow informed decisions based on the correlation between the business requirements, the organizational policy and the available network

[1] Piper Jaffray industry note, *2016 Piper Jaffray CIO Survey*, January 2016

[2] Simon Richard, Gartner research, *Effective Network Orchestration Starts by Automating Provisioning*, 31 August 2015

Network Security Management Needs Automation

The challenges outlined above are compounded by the lack of integrated data and automation. Too many organizations still keep track of network configurations and security rule sets on manually updated spreadsheets. The process of risk analysis (i.e., understanding if proposed changes will lead to security risks or break compliance mandates) is done manually. Such procedures are fraught with opportunities for mistakes and they slow the response time for access requests. As a result, security becomes a bottleneck for service delivery change and hinders business agility.

Most other processes in the IT world are automated; for example, provisioning and de-provisioning user accounts and access to applications; creating and configuring virtual servers and even virtual security devices; applying patches to systems; performing data backups and recovering from equipment failures. Repetitive IT processes are done more quickly and with fewer errors when they are automated, thus helping to manage business risk. Clearly there is a need to adopt automation for network security management because, with automation, it's possible to have both agility and security without compromises.

In the article *Security Think Tank: Automation requires management, monitoring, governance*, Information Security Forum research analyst Indy Dhami points out, "The benefits of [security] automation include less manual intervention, reduced overheads in managing applications and faster identification of vulnerabilities, threats and incidents."[3]

> *"The benefits of [security] automation include less manual intervention, reduced overheads in managing applications and faster identification of vulnerabilities, threats and incidents."* – Indy Dhami, Information Security Forum

Automation requires that you have routine tasks and activities that are well defined and repeatable. This is quite a challenge in a complex networking environment, with diverse security devices from multiple vendors, across physical and virtual realms, extending into the cloud. There can be hundreds of devices with rule sets containing hundreds of policies. In short, the challenges of security automation are as great as the need for security automation—but that doesn't mean it can't be done.

We've identified five steps that are critical to answering the security automation challenge:

1. Gain visibility into the business requirements
2. Model the network topology that enables the business
3. Define the organizational security policy
4. Create a well-defined, documented change process
5. Allow informed decisions based on the correlation between the business requirements, the organizational policy and the available network

[3] Indy Dhami, ComputerWeekly.com, *Security Think Tank: Automation requires management, monitoring, governance*

Let's have a look at each and why it is a critical element of automation.

Step 1: Gain Visibility into the Business Requirements

Applications exist to support what a business needs to do. Depending on the size and nature of the enterprise there can be tens, hundreds or even thousands of applications in use all across the network (including in the cloud). To manage the security and connectivity around these applications, the IT teams need good visibility into what the applications are, what the business priority of each application is, what platforms or servers the applications are on, what databases and other services they need to access, what other dependencies the applications have, who owns each application, what policies must govern each application, and so on. Without this information, it's impossible to create repeatable tasks to automate any sort of change processes.

Step 2: Model the Network Topology

The next step is to have a very clear model of the network topology—what the devices are, where they are (i.e., specific IP addresses), the options for routing traffic throughout this network, how it's possible to connect various points, and so on. This model must be dynamic because, as we mentioned earlier, the network is in a state of constant change. All of this information is critical because without it, how would anyone know how or where to make changes?

Step 3: Define the Organizational Security Policy

The organization needs to define a single unified security policy baseline aligned with the external regulatory mandates and industry standards (e.g., PCI DSS, SOX, NERC CIP, etc.) that the organization must follow; internal enterprise-wide governance requirements; and general best practices that the enterprise observes. Ideally, this unified security policy would define what is and isn't allowed for security devices. For example, PCI DSS specifies that network segments that payment-process data must be isolated from all other network segments. This, then, dictates what connections and traffic are permitted into and out of the payments segment of the network.

Step 4: Create a Well-defined, Documented Change Process

Most enterprise organizations already have some sort of IT service management (ITSM) process or workflow process, in many cases based on the ITIL best practice framework. There are many products on the market that help organizations manage their changes across their IT environment and control everything that happens with the workflow. In many organizations the network changes aren't part of this process, but even network changes have a full workflow to them that needs to be done. In order to automate security change management, this process needs to be brought into the regular ITSM umbrella that controls most other aspects of IT management.

Furthermore, this change control process needs to include creating documentation with full accountability of precisely what changes are made, for what business purpose, and at whose request. The documentation needs to include sufficient comments so that auditors know what happened and why. This documentation is critically important for audits and if problems arise and the origin of changes needs to be traced, for example, for troubleshooting or cyber-attack investigations.

Step 5: Allow Informed Decisions

Automation can help humans make better decisions. There can be automated processes to simulate the planned security changes and determine how well the expected results fit into the overall environment before allowing the change to take place. For example, by making a requested change to a series of firewalls, will it break anything like a regulatory compliance mandate or a company policy? If so, this is the time to pause and allow the security team to talk to the change requestor to discuss the business need. They can jointly decide to allow the risk despite the current policy, or they can find an alternate means of doing what the requestor wants to accomplish. In any event, the actual change implemented and its business justification are fully documented as part of the security automation process.

Ready, Set, Automate!

Once the organization understands its business needs, and it has a dynamic but accurate model of the network topology, and it knows what the precise security policies must be, and there is a formal process for orchestrating the changes, and people are informed and confident about the decisions to make changes to the network security, *then* it's possible to wrap the security change requests into an automation tool.

What's needed is a comprehensive tool that bridges the gap between the network infrastructure layer –the different devices and cloud services – and the business applications and services, as shown in Figure 2. The tool must be driven by the organizational security policy and provide the ability to make the security changes in an automated way – preferably through the ITSM system already in place – to serve the different business applications and services, no matter where they reside. And, the tool must help ensure the security and compliance of the network environment.

The Tufin Orchestration Suite Fills the Gap for Network Security Automation

The Tufin Orchestration Suite fills this gap by automating the network security change process end-to-end for enterprise environments. The suite abstracts the network infrastructure and the business applications to analyze the risk of changes and then provisions them once approved. The suite also supports APIs to communicate with other important elements of the computing environment, such as an IT service management system. The architecture of this suite is illustrated in Figure 2.

Figure 2: The architecture of the Tufin Orchestration Suite

Briefly, here's a description of what each of these components does.

- The ***Application Connectivity*** component allows an organization to model its business applications and services, defining the connectivity requirements in order to work.

- The ***Security & Compliance*** component holds the organization's Unified Security Policy™. Unified Security Policy defines the desired (or required) security policies that must be enforced in the organization. These include segmentation policies, best practices policies, regulatory compliance policies, and any other security policies the organization wants to comply with internally.

- The ***Network & Security Automation*** component enables change automation in the network. This component performs the actual security automation activities, while checking with the *Security & Compliance* component that these automated changes are not breaking or violating the desired security and compliance policies.

- The ***Network Abstraction*** component hides the network complexities from the other components. It maps and holds the network topology and interacts with the different networking and security technologies running in the network.

- The ***RESTful APIs*** component enables full programmability to any of the suite's components, allowing easy integration with other enterprise systems and technologies.

Fulfilling All Steps Critical for Enterprise Network Security Automation

The Tufin Orchestration Suite meets the five critical steps for automation. The suite provides visibility into all of the applications on the network and their relationships to each other and to the security devices. It then builds and maintains a dynamic model of the network topology. The suite's Unified Security Policy provides the ability to centrally manage all of the organizational security policies in a single place. An analytics engine thoroughly explores

the possibilities of risk and ensures that all future changes in the network are aligned with the centralized policies, and any new violations introduced to the network are alerted on.

The Tufin Orchestration Suite's flexible, customizable workflows can plug into any ITSM or process workflow solution so that security change management activities follow a prescribed process, with complete documentation for future reference and audit purposes. And Tufin provides risk information to the enterprise IT teams so they can make informed decisions about the business requirements and organizational policy.

Through security automation and risk analytics, Tufin enables an organization to implement network changes in minutes instead of weeks, all with increased accuracy and security.

Conclusion

CIOs are increasing their investment in network security because of the vital role it plays in reducing risk to the business. Network security management is too complex – and too important – to be done manually; it must be automated to maintain business agility and ensure a secure and compliant environment. At the same time, automation itself is a complex undertaking for enterprise networks that are heterogeneous in multiple dimensions.

The Tufin Orchestration Suite is built to deliver the five critical steps of network security automation: visibility into business requirements; modeling the network topology; defining a Unified Security Policy; creating a well-defined change process; and allowing informed decisions. Through automation, enterprise IT teams can meet the business needs of analyzing and implementing the appropriate changes in minutes instead of days with built-in controls for security and compliance. Now network security can be a business enabler instead of a business bottleneck.

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 1,800 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.