tufin The Security Policy Company.

Hybrid Network Security

6 Essential Automations for Modern Enterprises

Enterprise networks have become increasingly fragmented and diverse, as organizations continue to adopt new cloud resources, virtualization technologies, and agile processes. As a result, security teams confront new network security challenges. To ensure both secure and efficient operations, security professionals should consider deploying intelligent automation to support their network security programs. In this paper, we will highlight the six critical processes organizations should look to automate, and detail the essential capabilities needed for scalable success.

By deploying the right automations, security teams can more accurately identify and quantify risk, reduce the time it takes to address network access requests, streamline compliance and audit responses, and make microsegmentation and zero-trust objectives achievable.

When leveraged successfully, automation can help bridge the communication and process gaps that often exist between network security, cloud security, and DevOps teams.

There are no silver bullets, but **well-designed network security automation can help valuable technical resources work smarter and faster.**

Automation is a broad concept, and security teams have many options. Working with the world's largest and most innovative enterprises, we have identified those that are essential to scalable and successful network security. Though each automation delivers unique capabilities, they all either...

- support secure network design
- facilitate secure network changes, or
- integrate network security into DevOps processes.

Let's dive in.

Automating Network Design

Modern enterprise networks are a collection of diverse technologies – typically from a variety of vendors. Large organizations may utilize a broad variety of network security devices (e.g. firewalls), on-prem compute and storage technologies, private clouds, and public cloud infrastructures and services. Complicating the matter, these resources often ship with their own security controls, and have characteristics that make a cohesive security strategy challenging. (For example, many cloud assets and resources do not have an IP-address, making IP-based traffic management impossible.)

In such a heterogenous network environment, the ability to control "who can talk to whom, and what can talk to what" can prove very challenging. To address this, a policy-based approach to network access and isolation is essential. A policy-based approach enables organizations to establish and enforce a collection of rules that dictate who and what can access network resources, and in what manner.

1 **AUTOMATION:**

Network Security Policy Design

Network security pros need the ability to design and deploy security policies that dictate access and connectivity across the network. Due to the complexity of modern hybrid networks, and the fact that enterprise workloads and apps often leverage both on-prem and cloud resources to operate—it has become necessary to automate the design of these policies.

Business Impact of Automation

- Enables a consistent, policy-based approach to network security
- Ensures policies are optimized for your network & processes
- Avoids errors and burden of manual security policy creation

2 **AUTOMATION:**

Network Segmentation Design

Closely related to policy design, network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. Mature organizations often isolate with greater granularity, including workload-level microsegmentation. This not only facilitates a zero-trust architecture, it improves the organization's ability to mitigate damage in the event of a cyber attack by creating smaller areas of containment and reducing an attacker's options for lateral movement.

In modern networks, automation is now essential for successful segmentation. Specifically, security pros should look to automate the development of isolation rules, based on analysis of the entire network, and auto-identification of all assets and services and their related workload dependencies.

Business Impact of Automation

- Enables segmentation across hybrid & multi-cloud networks
- Supports zero-trust architecture
- Mitigates risk of movement by bad actors

When evaluating approaches to enable both network security policy design & segmentation, be sure to select a solution that...

Delivers end-to-end network visibility

In order to develop effective security policies, you must first have complete awareness and visibility across the network. This requires technology that can "look through the firewalls" and "look into the cloud" to fully understand access. Leverage a solution that supports visibility across all brands of firewall, router, network asset, private cloud instances, and public cloud platforms.

Supports tags and labels

Given the dynamic nature of the cloud and containerized workloads, many assets and services utilize tags (or labels for K8s) for identification and organization. Successful policy automation & segmentation demands a solution that supports tags, can enforce policies based on both IP-address and tag, and can automatically segment new network resources in compliance with those policies.

Identifies and alerts on risk

Given the scope and complexity of modern networks, it is effectively impossible to manually identify all risk. By leveraging a solution that automatically identifies risk (based upon industry best practices and any regulatory standards the org must meet), security teams can ensure that the risk is not memorialized in the policies and isolation strategies they design and deploy. This requires a solution that supports a broad variety of regulatory standards, and alerts when any network configuration violates those standards.

Recommends policies based upon existing traffic and least-privilege principles

Modern networks have so many workloads, apps, and users – all interacting in myriad ways - it can prove challenging for security teams to develop policies that provide the access needed by all stakeholders. The ideal solution automatically evaluates the existing access and connectivity across the network, quantifies the risk associated with that access (as described above), and then recommends policies appropriate for the organization.

3 AUTOMATION:
Access & Change Requests

Network access and change requests can come from a broad variety of stakeholders. A department head may request network access for a new tool they've procured; managers may need to provision access for third-party contractors or remote workers; and developers may need to enable access for their new applications. Using automation, organizations should provide all stakeholders with a single workflow through which they can submit access requests, and track the status of that request over time. Whether this automation integrates with an organization's existing ticketing system (e.g. ServiceNow or Remedy) or is a "stand-alone" workflow, it must be flexible enough to support the specific business processes of the organization, including any business approvals and notifications required. When done right, it provides the entire organization a single, transparent, trackable process that minimizes confusion, reduces manual effort, and streamlines audit responses.

Business Impact of Automation

- Centralizes, accelerates, and de-risks network change process
- Accelerates network change SLAs
- Provides "line-of-site" to all stakeholders

4 AUTOMATION:
Path & Risk Analysis

Once a network access/change request is submitted, it must be evaluated in terms of risk. To calculate this risk, security teams must identify all of the implications of the access, and how that changes the organization's attack surface. A new application built by the engineering team may need access to the internet, but enabling that access (or doing it in the wrong manner) may have "follow on" effects the security team is not aware of (e.g. exposing a sensitive database to outsider threat.)

Because networks have grown so complex, it has become essential to automate the process of calculating the ideal path that should be enabled. This automates and enforces risk-based networking. When done right, this automation can empower organizations to rapidly calculate the risk associated with a given access request, and identify the most secure network path through which that traffic should travel.

Business Impact of Automation

- Minimizes risk associated with network access requests
- Enforces principles of least privilege
- Eliminates burdensome and error-prone manual processes

5 AUTOMATION: Firewall Rule Design & Management

Once an access request has been approved, and the most secure means of delivering it has been calculated (i.e. path and risk analysis), the actual enablement of that access requires a myriad of changes to the network. Virtually every network device through which traffic will pass maintains its own rulesets that govern its operation, and these rules need to be revised to enable the requested access.

Given the size and complexity of modern networks, attempting to manually provision these rule changes across every network device (e.g. firewalls, routers, security groups, etc.) is cumbersome and time-consuming. Making matters worse, over time the individual rulesets within these network security devices can become unwieldy, filled with duplicative, conflicting, overly-permissive, and shadowed rules.

Automating the design of network security device rules — and the ongoing curation of those rulesets – helps security teams streamline and de-risk the network change process. When done right, it empowers organizations to apply the principle of least privilege in their network operations and makes firewall audits far less burdensome.

Business Impact of Automation

- Accelerates access requests
- Enforces least privilege
- Streamlines audit response and reporting

When evaluating approaches to automate network changes, be sure to select a solution that...

Supports customizable stand-alone and integrated workflows:

In order to standardize network access requests, first and foremost the process needs to meet the needs of the business. Successful automation demands a solution that allows security pros to configure the precise steps that need to be taken throughout the workflow, and how that information is communicated to all stakeholders. The ideal solution should integrate seamlessly with an organization's existing workflow tool (e.g. ServiceNow or Remedy) and provide its own stand-alone workflow engine and UI.

Enables end-to-end risk analysis across hybrid networks:

Provisioning network access without fully understanding the security implications has become unacceptable in modern business. But in order to securely automate path and risk analysis, a solution must be able to evaluate the access and connectivity configurations of every asset and service across the network. The ideal solution provides full awareness across the network's on-prem, private cloud, and public cloud resources, calculating risk based upon this awareness.

Support for all network security products and devices:

Most organizations utilize a variety of network security devices from an array of vendors. (e.g. Cisco, Fortinet, Palo Alto, Azure Firewall, etc.) In order to efficiently provision and manage the rulesets associated with each of these devices, the solution must be "vendor-agnostic", and provide support for any and all devices being utilized in the network. Such a solution also empowers security teams to adopt the ideal technologies for their network going forward, confident that their network security automation solution will be able to support them.

Automating Network Security within CI/CD

Now that we've discussed how automation can drive successful network design and change management, we turn to the challenge of ensuring network security in the context of continuous integration, continuous delivery (CI/CD.)

One of the many virtues of cloud computing is the ability to streamline the provisioning of resources and workloads via automated DevOps processes and tools. But with so many stakeholders having the ability to create and configure cloud resources (with just a few clicks or lines of code), security teams are often not aware of what is happening in the cloud. If cloud teams are forced to wait for approval from network security engineers to do their work, productivity is slowed and the agility the cloud promises can be lost. On the other hand, if cloud teams are provisioning resources without oversight from network security, the organization can be exposed to increased risk.

AUTOMATION:

CI/CD Security Validation

Automation is a core principle of cloud computing, and cloud operations are largely automated. DevOps and CI/CD tools enable architects and developers to provision resources via code and orchestrate this work via both popular open source and proprietary tools (e.g. Jenkins, Terraform, Ansible.) But to ensure secure operations, organizations must have the ability to "verify" that the resources being provisioned adhere to the organization's policies.

Automatically validating CI/CD builds, in order to enforce secure configuration, has become essential. It makes it possible for organizations to gain agility without compromising security. The ideal solution integrates via API with an organization's DevOps tools, automatically and continually evaluates the proposed build against security policy, and approves or suspends the build depending on whether it meets policy.

Business Impact of Automation

- **Ensures proactive network security throughout agile cloud operations**
- **Synchronizes network security and DevOps processes and teams**
- **Empowers teams to adopt new processes and technologies with confidence**

When evaluating approaches to integrate policy-based network security into CI/CD, be sure to select a solution that...

Supports policy-based security:

It may be obvious, but it's worth stating that in order to integrate network security into DevOps processes, the underlying solution needs to support the design and enforcement of network security policies. So, in short, don't select a solution that promises to enable network security within CI/CD if it can't support security policies in the first place. (So first, make sure it delivers on automations #1 and #2.)

Supports your DevOps tools:

There are hundreds of tools available to support DevOps processes, and most organizations use a combination of tooling appropriate to their business. When selecting an automation solution, be sure it fully supports the tools you use — or better yet, a vendor agnostic solution able to support every CI/CD tool in the space via a published, well documented API.

Intelligent Automation = Security + Agility

As enterprise networks are becoming more diverse and fragmented, the business environment is demanding ever-greater agility and speed to market. To assume an aggressive security posture and remain agile, organizations are automating key network security processes. When part of a comprehensive security strategy, the six automations discussed above can help organizations minimize their attack surface, accelerate network management SLAs, unburden high-value staff from menial tasks, streamline the reporting and audit response process, and embrace agile processes without sacrificing security.

Want to know more about advanced automation? Visit...

https://www.tufin.com/solutions/automate-visibility-and-provisioning

About Tufin

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.

www.tufin.com

tufin
The Security Policy Company.

DP20220510