Why Network Complexity Kills Security

The increasing complexity of networks is a growing concern for most enterprises. Networks are built with a raft of diverse solutions, starting with switches, routers, servers, and firewalls, all procured from different vendors. Over time, other hardware and software systems are layered on, such as software-defined networking, virtual machines, cloud resources, and new applications. Every vendor has its own vocabulary, terminology, and help line, and its solutions have their own distinct command line interfaces. As Gartner observed, “Digital diversity management is not about people, but rather about the managing the explosion of diverse assets and technologies used in today’s modern digital enterprise.”[1] The problem is network management.

Vendors offer a single pane of glass to manage their products. Cisco has a management console for its switches, for example, and Fortinet has a console for its firewalls. Vendors’ management consoles, however, support only their products. With such disparate administrative tools, how can IT departments holistically manage multiple vendors, devices, and platforms? Most critically, how can changes be made in the network without introducing security risks?

The short answer: not too easily.

Security teams, already hard-pressed to stay on top of network security operations, are hamstrung by a paucity of cybersecurity pros. According to ESG, “the percentage of organizations reporting a problematic shortage of cybersecurity skills continues to increase.”[2] If networks never needed to change, this wouldn’t be an issue, but they do, all the time. Access to the network must be granted, for example, and other times, limited or removed. If access is too permissive, the attack surface increases; if too restricted, the business suffers. Implementing network change involves individually configuring multiple components, each in different ways. So, how can security staff, already spread thin, know the administration, unique CLIs, and nuances of every solution?

In most cases, not so fast…

Today, misconfigurations can be as high as 70 percent. Misconfigurations can open breachable tunnels into the business that can be exploited. The most common occur with databases in AWS or other clouds, which by default, are accessible to everyone and daunting to lock down. Access to the network must be limited to only those who need it. If access is too permissive, the attack surface increases. Yet if access is too restricted, the business may suffer.

To manually configure changes to switches, firewalls, and other resources, security pros need to grasp how everything connects, despite network complexity. This demands a near impossible familiarity with a myriad of products from multiple vendors. If an access request requires modifications to a Cisco switch and a Palo Alto firewall, they must master multiple security technologies to implement it. They need to determine what needs to be changed and what constitutes risk.

Suppose there's a Wannacry malware attack using port 445? The security team must determine all the possible compromises in that network zone and the security devices and datasets in it. They must then ensure the attack doesn't spread elsewhere in the environment, and be quick about it. Malware attacks are usually automated. They scan ports on devices to determine which are open, and then seek vulnerabilities deeper into the environment. The longer security teams take to identify and close a vulnerability, the longer the attack executes inside the network.

And that's the rub.

It takes time to manually make configurations. Many organizations have SLAs that require three- to five-days or more for approval of network changes. Security teams, short-staffed, swamped, and struggling to manage their diverse networks, can take days to respond to an incident or change request that could be done in minutes with greater know-how. Access requests, as a result, take longer, which can impede business. Meanwhile, the network is vulnerable to intrusion, and attack mitigation is delayed.

As such, the success of each network security operation is only as effective as the skills of the security pros assigned to it. Some may be well versed in Cisco solutions. Others may be familiar with Fortinet products. Vendor/solution knowledge is so compartmentalized that staff are often asked to manage systems outside of their bailiwicks. This contributes to mistakes.

"Managing security configurations across vendors and platforms, on-prem and hybrid cloud, from a single pane of glass will reduce efforts and better control risks," stated Tufin.[3] With fragmented management consoles, it is extremely difficult to understand an environment's topology, how everything in it connects, and what changes will achieve acceptable security.

Instead, security teams need to centrally manage large deployments of firewalls and other solutions. With growing network complexity and heterogeneity, enterprises must consolidate security device and platform management. They need an all-encompassing system that doesn't require much manpower to operate or specialized knowledge of any one vendor's systems. To improve efficiencies, reduce risks, and empower the business, organizations need end-to-end policy management.

With cohesive policy management across the entire environment, network security operations can do a lot more with a lot less, and do it much faster and more efficiently. Security will then realize its full value to the business.

[1] https://www.gartner.com/smarterwithgartner/top-10-trends-impacting-infrastructure-and-operations-for-2019/
[2] https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html
[3] https://www.tufin.com/blog/4-inventive-ways-combat-cybersecurity-skills-shortage

----