Confronting Configuration

The misconfiguration of network devices like firewalls and routers represents a much overlooked but serious threat to enterprise security. Can automation help reduce the burden placed on network and security managers? Jody Brazil answers this question in the affirmative.

In October last year, long-time security guru HD Moore disclosed a problem relating to the misconfiguration of Palo Alto Networks firewalls that resulted in Windows accounts credentials being leaked on to the Internet, exposing underlying services such as VPN and webmail. That incident alone illustrates how an inability to properly configure existing network defences arguably remains one of the most significant security challenges facing today’s enterprises, increasing the risk of compromise and often resulting in breach scenarios.

According to Gartner's analyst Greg Young: “Through to 2018, more than 95% of firewall breaches will be caused by firewall misconfigurations rather than firewall flaws.”

The problem of network security device misconfiguration still lies largely under the radar. Moreover, with growing network complexity intensified by emerging technologies including – among many others – virtualisation, cloud computing and software-defined networking, the problem of firewall misconfiguration is only going to intensify.

At the same time this is an issue that, upon identification, can be easily addressed and leveraged to provide greater insight into network operations. Let’s flesh out the detail to understand this clear paradox.

No such thing as a ‘Magic Box’

Historically, to fix a network security problem the attitude has been that you should just ‘buy a better box’. Companies have spent billions on firewalls and other network security devices in the genuine hope that adding expanded capabilities via this next generation of ‘Magic Boxes’ would address related challenges.

The fact is that, without proper management, network access risk is never truly improved and this issue of perception lives on. It's no coincidence that related breaches remain prevalent. More often than not, such breaches arise due to poor visibility of firewall configuration on a network-wide scale.

It may sound obvious but leaving device settings on default – whether related to configuration, passwords or any other services – automatically places the network at risk.

In most cases, configuration issues arise due to an explicit action – or lack of action – taken by network administrators in setting firewall access rules and creating overly permissive configurations. This is largely due to the involved complexity and a lack of visibility into the impact that a new rule may have across the entire company network.

Unfortunately, there’s no big flashing warning sign that pops up whenever a mistake has been made to help prevent administrators from implementing problematic rules, with such mistakes only discovered – if indeed they are unearthed – when a resulting breach occurs.

That being so, a broader and more holistic view of the network is required in order to minimise risk and empower greater efficiencies in network security management.

New technology: easing the burden?

Another widespread misconception among today’s companies is that emerging security technologies – or that next generation of ‘Magic Boxes’ – are going to make device and policy management simpler. That’s not quite right.

In some cases this may in fact be possible, but only once the configurations, access policies and associated rule sets have been correctly implemented and allow devices to function as promised.

The obvious example here is the next generation firewall. These encompass both traditional firewall functions such as packet filtering and inspection along with other
advanced capabilities for preventing attacks and filtering traffic based on specific applications or users. While these devices offer to provide more comprehensive, actionable security intelligence, they also introduce a range of added management challenges and related risks that could result in exposure. Fundamentally, next generation firewalls need to be appropriately configured and integrated within the larger infrastructure. Otherwise, and despite any extended security capabilities, they will only serve to make the environment even more complex and harder to manage – resulting in greater inefficiency.

The complexity of networks and their inherent speed of change is set to intensify with the rise in adoption of technology paradigms including cloud computing, hybrid cloud, virtualisation, Software-Defined Networking, Bring Your Own Device and The Internet of Things. Each of these paradigms comes with its own set of challenges and complexities that need to be managed on an effective and efficient footing.

Without applicable security methodologies and solutions in place, the adoption of these technologies will only create a never-ending mountain to climb for practising network administrators.

Automation is the key
Managing network devices effectively demands significant time and effort from security and network teams. Importantly, it also requires that aforementioned wider view of the network infrastructure. This is where automation comes into its own. Specifically, automation can help reduce the burden on network managers and lessen the risks associated with network security device misconfiguration.

The problem of managing configurations is most pressing for network administrators as they deal with a barrage of change requests requiring them to update or create new rules and access policies. On a weekly basis, teams might face an onslaught of hundreds of such requests to amend current access policies, support the introduction of new applications or integrate with new partners. Pushed by stakeholders to enable these business requirements as quickly as possible, this is where errors most often occur driven by complexity and a lack of visibility.

By leveraging automation, responsibility for the management of firewalls and other network security device infrastructure can be more equitably and comprehensively addressed across both the security and network teams. What has grown into a relationship of increasing discontent can become far more harmonious with teams working towards one core goal – securing the business and ensuring that the network runs as it should when enabled by a common set of automated tools.

Rather than hoping that the new ‘Magic Box’ is working correctly and blaming each other when it’s not, a clear and shared workflow can be embraced that’s empowered and underpinned by detailed visibility and relevant intelligence.

This is also an area where automation is clearly preferable to manual, hands-on methodologies. In a typical enterprise, firewall management involves the ongoing evaluation of tens of thousands of rules distributed across hundreds of firewalls. Using humans to complete this work is impractical as it involves documenting each rule, evaluating them against a policy and then reviewing this data with relevant business owners – which can take many hours... And that’s per rule! Using manual processes would result in the need for dozens of full-time staff members within a typical host enterprise.

Automation is helpful in addressing firewall rules and policy management because the involved review process must be carried out continually to prevent emerging risk exposures driven by ongoing change.

By automating processes directly related to the assessment and oversight of network security device infrastructure along with related compliance and risk management factors, and presenting teams with the ability to make more informed decisions, mistakes – and resulting breach incidents – can be avoided.

Replacing time-consuming manual processes with automation, key members of the team can focus on other strategic risk reduction efforts.

"The complexity of networks and their inherent speed of change is set to intensify with the rise in adoption of technology paradigms including cloud computing, hybrid cloud, virtualisation, Software-Defined Networking, Bring Your Own Device and The Internet of Things"