TITANIA | Use Case

Identifying network compromise and prioritizing remediation

Network devices such as firewalls, switches and routers are a vital part of cyber defenses. But while network operations teams regularly carry out software updates and apply patches to their network devices, misconfigurations are often overlooked, resulting in a persistent, and potentially critical, risk to network security. For high-profile targets like federal government organizations that need to secure their networks against nation state attacks, having full visibility of misconfigurations and the risk they pose to network security is essential to understanding the organization's exposure to cyber-attack and in planning and prioritizing remediation action.

US Government Advisory

In June 2022, the NSA, CISA and FBI issued a US government advisory discussing how state sponsored cyber actors exploited publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. Added to this in October, the organizations publicized a list of the top common vulnerabilities (CVEs) that are being actively exploited by state sponsored actors.

Although the focus of these documents is on how the state sponsored cyber attackers exploit common vulnerabilities to compromise unpatched network devices, they also provide useful insight into how these attacks were carried out.

The advisory highlights that these state-sponsored attacks are targeting and manipulating devices that are often overlooked by network and security teams, such as switches and routers which, unlike firewalls, are often not assessed on a regular basis.

Recent research has shown that 96% of organizations only assess their firewalls when validating network device configuration settings, relying on perimeter-only defenses for their network.

Although the findings showed that the firewalls are not sampled, suggesting that there is cross-sector agreement that sampling is not best practice for these devices, the omission of switches and routers means that misconfigured switches and routers remain exposed to potentially significant and unidentified risks that undermine network security. In effect, organizations are only sampling their fleet of network devices.

This is an inherently risky approach to configuration security and runs counter to Zero Trust best practice, where all devices should be assessed as an essential part of preventing lateral movement across networks.

How previous attacks have worked

The advisory goes into specific detail about how one known method works, describing how the cyber actors accessed a network, specifically focusing on accessing and manipulating router configurations. Firstly, by scanning for vulnerabilities, the cyber actors gained access to the network and used this access to change the configuration of routers for their own purposes, before then manipulating or removing the logfiles to hide the evidence of what they had done.

> "After establishing the tunnel, the cyber actors configured the local interface on the device and updated the routing table to route traffic to actor-controlled infrastructure… PRC state-sponsored cyber actors then configured port mirroring to copy all traffic to the local interface, which was subsequently forwarded through the tunnel out of the network to actor controlled infrastructure… Having completed their configuration changes, the cyber actors often modified and/or removed local log files to destroy evidence of their activity to further obfuscate their presence and evade detection."
>
> **Source:** US Cybersecurity Advisory: State-Sponsored Cyber Actors Exploit Network Providers and Devices, June 2022.

The value of prevention

The advisory highlights four best practice actions to take to defend against such attack.

- **Apply patches as soon as possible**
- **Disable unnecessary ports and protocols**
- **Replace end-of-life infrastructure**
- **Implement a centralized patch management system**

Although ensuring that all devices are patched and up to date is part of best practice security, this doesn't help mitigate against misconfigurations. Unlike software vulnerabilities, poor or insecure device configurations cannot be 'patched away'. This is why verifying that devices are securely configured is critical to minimizing an organization's attack surface and why ongoing configuration validation is a key tenet of Zero Trust.

But it is important that organizations assess all of their network devices, including switches and routers and not just firewalls. Switches and routers play an equally vital role in effective network segmentation, which is a fundamental mitigating control to reduce the attack surface by stopping lateral movement across networks. Segmentation is especially important to defend the network from less sophisticated attacks like ransomware, which can impact service availability, but also more targeted and expert attacks.

> **"Firewalls can't solve today's most urgent security priorities. After all, more than 80 percent of network traffic is inside the perimeter."**
>
> **Source:** Guardicore Centra / Forrester

Segmentation policies will help ensure that if a host gets infected or compromised, the incident will remain contained within a small segment of the network.

> **"Effective segmentation strategy has been proven to save an average of $20.1 million in application downtime and deflect five cyber disasters per year."**
>
> Source: Venture Beat, Everything you need to know about zero-trust architecture, June 2022

Baseline segmentation and policy/compliance enforcement are Zero Trust foundational capabilities, which DISA and US Department of Defense leaders agree will mitigate and/or identify and remediate critical mission and operational risks resulting from Privilege Escalation or Lateral Movement.

Identifying compromise and prioritizing remediation

Validating that firewalls, switches and routers are maintaining a secure configuration, and are not being subjected to configuration drift – either accidentally or nefariously – will help network security teams to understand where the risks are in their increasingly complex networks.

As attacks are on the rise, it is now a case of when, rather than if, an organization will be attacked. So detecting the early stages of exploitation is key to limiting the resultant damage. Continuously monitoring for misconfigurations, therefore, is a requisite capability, as is understanding the impact to the network, if the vulnerability was exploited.

For example, in the attack described above, a crucial factor in detecting the attack would have been to identify the unwanted changes to the router configuration. Intercepted early enough, it could very well have allowed the SOC to shut down the attack before malware was planted in target devices. Continuously monitoring for configuration drift and prioritizing remediation workflows based on impact to the network, along with robust network segmentation, could therefore close-down an attack before it impacts the network more widely. These proactive security measures are thus key to protecting critical networks from preventable and/or hidden attacks.

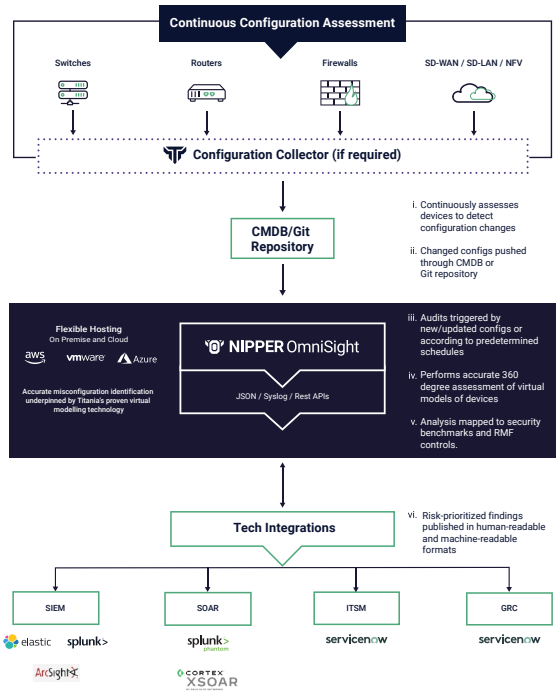
How Nipper OmniSight can help: Delivering accurate security assessment and RMF assurance at scale

Nipper OmniSight accurately assesses the security risk posture of up to 300,000 firewalls, routers and switches on an up-to-hourly basis. Findings are prioritized by risk criticality – based on ease of exploitation and network impact – and are reported with device specific remediation advice to improve MTTR.

In addition to being able to identify any known vulnerabilities (CVEs) in a network device, Nipper OmniSight is also capable of identifying when a device's configuration has changed. Once Nipper OmniSight detects change in a CMDB or git repository, an audit of the device's configuration is automatically triggered – as opposed to waiting until that device's next scheduled audit

This provides network teams with assurance that planned changes have not introduced new vulnerabilities to the network and audits of unplanned changes can alert network defenders to potential indicators of compromise (IOC) that require further investigation.

In the case of the example discussed, the attackers executed commands on a router and configured its local interface, enabling data exfiltration and routing traffic to actor-controlled infrastructure. Nipper OmniSight could have immediately identified these configuration changes within the config repository as a potential IOC and flagged for automatic assessment.



About Titania

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally. Whether organizations need real-time visibility and analysis of every network change to get ahead of threats, segmentation violations, and potential network disruptions. Or scheduled network posture and device vulnerability assessments to enhance attack surface security and demonstrate compliance. We have a solution for every stage of the journey to network readiness and resilience.