TITANIA
Assured Accuracy

Establishing a Defendable Core Network and Automating RMF Compliance

Combining continuous misconfiguration detection and auto-mitigation with risk-focused compliance analysis

Keith Driver | CTO

Table of Contents

Abstract

Core network devices (firewall, routers and switches) are pivotal to the security of all networks. Each device is managed through a complex configuration. Errors arising in the configuration can result in critical security risks to the network, its data, applications and the mission.

It's why DISA ACAS augments its scanning capabilities by incorporating vulnerability and configuration assessment modules in its solution as well as traffic monitoring and reporting modules. The vulnerability scanning module provides information on vulnerabilities associated with the software/firmware version whilst the configuration module looks at the device configuration.

However, the ACAS configuration module is designed to look at each device setting individually, not in conjunction with other settings, leading to well-known accuracy issues and reports of significant time being wasted investigating false-positives findings. As a result, since 2013, elite cyber teams across Department of Defense and Fourth Estate have complemented their core network vulnerability analysis with Titania's highly accurate configuration auditing software, Nipper – resulting in time savings of up to 80% for a base configuration assessment compared to using ACAS.

This whitepaper summarizes how Nipper is able to achieve unrivalled accuracy in configuration assessment by virtually modelling the entire configuration as a single entity to consider interdependencies and suppress irrelevant findings. It will also demonstrate how this approach to detecting misconfigurations is enabling cyber teams to prioritize remediation workflows for firewalls, routers and switches, based on network risk criticality – viewed through either Nipper's security and/or compliance lenses, such as NIST 800-53 or CMMC.

Moreover, as configurations change daily and these advanced cyber teams have a need for continuous assessment as a foundational component of establishing a defendable core network and meeting the DoD's zero trust architecture objectives – this whitepaper focuses on how Titania will provide them with continuous detection and remediation capabilities with Nipper Enterprise.

Comparison: Core Network Security Assessment Methodologies

Penetration Testing

The expert process of using a variety of tools to probe and examine, in detail, how the network has been configured. In the case of firewalls, switches, routers and other infrastructure devices, this involves reviewing the configuration file, line-by-line, and comparing it to a secure configuration. Pentesters typically provide independent audits of systems installed and maintained by experienced people who apply their own methods and technologies for protecting their networks.

Vulnerability Scanning

Vulnerability scanning includes the assessment of a device by probing its external interface (scanning it). This process only provides a subset of the security checking required. The scans also retrieve the version number of the firmware and look it up in publicly available tables from NIST or the manufacturer to list known Common Vulnerabilities and Exposures (CVE) against the firmware version. Neither of these techniques reveal risks in the device configuration, which can result in undetected misconfigurations in the core network that pose critical risks.

Configuration Assessment

Configuration assessment is sometimes referred to as a 'build review' by penetration testers. It involves a line-by-line granular assessment of the internal system instructions (configuration or O/S) of a physical or virtual device. As these instruction sets determine a system's actual security response, it is regarded as the least intrusive, most accurate and detailed way of determining the system's security and compliance status. There are two types of configuration assessment technologies:

» 'Find and match' text string analysis (grep) tools (e.g. Tenable Nessus)

» Solutions with built-in virtual modelling of device configurations and interactions (e.g. Titania Nipper)

Grep configuration auditing is prone to false positives and false negatives, whereas virtual modelling provides the high levels of granular auditing accuracy needed for SIEM solutions and Security Orchestration Automation and Response (SOAR) enabled playbook-controlled risk prioritization and auto-mitigation.

Complementary features	Nipper	Scanners
Authentication & Authorization Configuration	√	-
Account & Logging Configuration	√	-
IDS & IPS Configuration	√	-
Password Strength & Encryption Analysis	√	-
Timeout Configuration	√	-
Physical Port Audit	√	-
Routing Configuration	√	-
VLAN Configuration	√	-
Network Address Translation	√	-
Network Protocols	√	-
Device Specific Options	√	-
Time Synchronization	√	-
Network Filtering (ACL) Audit	√	√
Wireless Networking	√	√
Warning Messages (Banners)	√	√
Network Administration Services	√	√
Network Service Analysis	√	√
Software Vulnerability Analysis	√	√
VPN Configuration	√	√
Network Discovery and Topology	-	√
Availability Monitoring	-	√

The challenge: accurately auditing and assuring every device, every day

Modern military and federal networks contain hundreds of thousands of devices and potentially millions of endpoints. This represents an enormous attack surface to defend. Therefore, all the devices must maintain a secure configuration. In addition, the configurations in each device must match both network policy and functional intent. Over time, configurations can change. A range of people may alter the configuration for differing purposes, leading to configuration drift.

Configuration drift is where the device configuration drifts out of compliance with policy, resulting in unintended security risks. Most of this activity is not malicious in intent but results in potentially critical security and operational problems nevertheless, largely through the unwitting interaction of configurable items – for example, routing changes or firewall rules.

"Human error creates the biggest threat. Technicians can inadvertently misconfigure devices, opening up holes. We need to go back and validate configs."

DISA Emerging Technologies Directorate, Steve Wallace

Traditional approaches to assessing the security status of the network involves personnel penetration testing the devices. This is a skilled and time-consuming job. The combination of network scale and the number of trained penetration testers available – even when using best of breed configuration on demand assessment software to automate the process – means that only a sample of devices can be tested and/or the cadence of testing reduces to testing the devices once per year. This can result in any security risks, including critical risks, persisting in the network and exposing the mission to unnecessary risk.

Indeed, military and federal security risk management programs, such as RMF for DoD and DHS CDM, (both based on NIST 800-53) for the agencies and CMMC and, NIST 800-171for their supply chains , reflect that sampling is insufficient to protect the networks, and continuous assessment must be implemented for the agencies and increasingly for their critical vendors.

If regulatory and mandated compliance was not enough of a driver already, recent events have emphasized how easily network security can be breached, and the far-reaching consequences of those breaches. It has long been recognised that a determined attacker will gain access to a network eventually using one of a variety of techniques. Once in the network, it is important that their progress to their goal is made as difficult as possible, inhibiting lateral movement. This means that security within the network perimeter is as important as the security on devices forming the perimeter.

Network architects are adopting a zero trust architecture to mitigate breaches. Indeed, DISA recently released their Zero Trust Reference Architecture, emphasizing its importance, and the recent Presidential Executive Order from May 2021 specifically calls out the adoption of zero trust paradigms to mitigate the risks.

There are many aspects to zero trust, but at its heart lies the principle that no entity should be implicitly trusted due to the application, device or location that they appear to be using. The second principle is to understand your estate and ensure every node in the network is configured correctly and has no security holes. As networks mature towards higher levels of zero trust implementation, it becomes necessary to perform continuous assessments to assure the network remains secure and that any inadvertent or deliberate acts are discovered quickly and the risk remediated.

This is why network and security teams need a solution with the capability to accurately assess the security configuration and compliance status of every device in a network, preferably on a continuous basis, ensuring that any misconfigurations are identified quickly and remediated as soon as practicable.

Core network security challenges


Large complex networks


Insufficient resource


Ad hoc audits and sampling


Unmonitored configuration drift


Exposure due to critical risks


Incomplete compliance reports


Remediation not prioritized by risk


Excessive mean time to remediate


Low confidence in core network security

Current solution for accurately assessing configuration security and compliance

Used by all four arms of US Department of Defense since 2013, Nipper offers unrivalled accuracy in detecting security and compliance issues in the core network, and is used for configuration analysis over and above ACAS. In this environment, Nipper has been proven to deliver higher accuracy and to reduce false-positive findings significantly, providing a superior, network-centric risk score, and offering detailed remediation instructions. It is reported that using Nipper instead of ACAS to assess the core network reduced base audits from 10 working days to 2, through not wasting time investigating false-positive findings generated by ACAS.

Nipper achieves this superior accuracy through its virtual modelling of the entire configuration as a single entity. By adopting this approach, the analysis can consider the interdependencies of the configuration settings and supress findings that are irrelevant, for example, because they are not enabled elsewhere in the configuration. The same is true for complex configurations within firewall devices, where overlapping rules can cause security issues, but all of the rules must be ingested and analysed simultaneously to discover them.

Not only does Nipper provide accuracy, it also provides a network risk context for any issues it finds. Competitor products use CVSS severity rather than risk scoring, but Nipper also takes into account other factors representing risk to the network, not just to the device. This includes:

» The impact of an exploitation of the misconfiguration

» How easy it is to exploit it, i.e.to assess risk likelihood

» How easy it is to remediate.

The Nipper findings report then automatically prirortizes the risks identified by criticality to the network.

Alternatively, the risk can be viewed through a compliance lens. For example, by assessing the 34 automatable NIST 800-53 controls across 10 control families, Nipper categorizes any misconfigurations found, prioritized by risk for remediation against the 800-53 control and control family to accurately prioritize RMF remediation by risk criticality.

In addition to scoring risk by security and/or compliance, Titania also provides detailed remediation advice, with command line syntax instructions, allowing network professionals to remediate issues quickly.

This information is invaluable to the SOC and NOC to inform remediation strategies and workflows, and in order to reduce the risk in the network to the greatest extent as quickly as possible, as well as proving RMF assurance.

Whilst its valuable results can be aggregated and analysed in SIEM and GRC solutions to provide in-depth, on-demand analysis, until recently Nipper could not provide continuous configuration assessments, as it relied on a human to drive the process. Titania's Nipper Enterprise product now solves this problem, by automating the whole security and compliance assessment process for the core network.

The unique features and properties of Nipper have now been embedded and encapsulated in an enterprise-ready solution.

RMF/800-53 compliance assessment prioritized by network risk

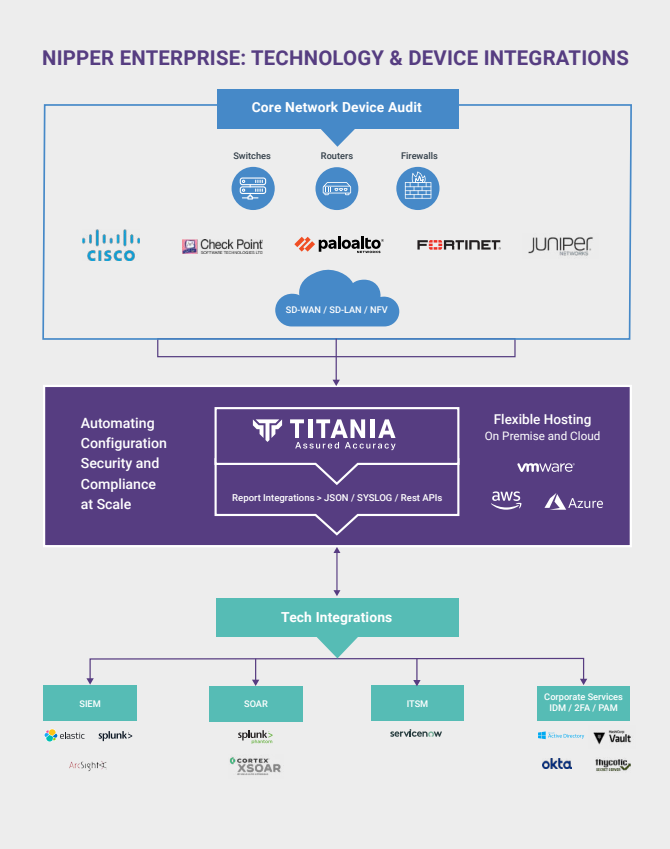
The shift from ad hoc to continuous assessment with Nipper Enterprise

Nipper Enterprise is a web application using a set of containerised Nipper instances that scale up and automate the assessment of the configuration of every core network device, every day. This brings the power and accuracy of Nipper to the whole network and enables the continuous audit and compliance assessment against mandataed risk frameworks, such as RMF and CMMC, that advanced cyber teams need.

Nipper Enterprise is capable of directly connecting to network devices to access the configuration file or ingesting previously extracted configurations. The analysis performed is identical regardless of the configuration source.

By ingesting configuration files, this means Nipper Enterprise can be used in situations where security professionals or auditors do not have direct access to the devices but are provided with the configurations or they are available from a configuration management database (CMDB). While this reduces the opportunity for continuous assessment, this file-based Nipper Enterprise mode facilitates auditing every device in the network at a single point in time, so as to produce and compare RMF posture assessments for the core network. Nipper Enterprise's connected mode fully integrates into the enterprise network and can connect directly and securely to devices offering the opportunity to schedule auditing, up to hourly, if required. Nipper Enterprise is not tethered to external cloud systems in any way, so no security or compliance data leaves the product, except through explicit secure integrations, to for example trusted existing SIEM, SOAR, GRC or ITSM systems.

Nipper Enterprise integrates with SIEM systems, such as Splunk and Elastic. The findings are shipped to these products as JSON records, either directly or via data lakes using SYSLOG as a transport. SIEM systems have powerful analysis and visualisation capabilities, and Titania has built dashboards in these products, demonstrating the ability to offer on-demand and continuous network compliance and risk views for the NOC and SOC professional respectively.



Technical Specifications

Titania Nipper Enterprise is a horizontally scalable application and can be applied to the largest networks, operating at an hourly audit cadence if required.

The application can be hosted in a VMWare environment as a virtual appliance, or within an AWS VPC. The application does not ship data to any cloud services, and can be deployed in air-gapped environments.

Nipper Enterprise accesses device configurations in two ways. Firstly, device details can be provisioned into the application, and then Nipper Enterprise will reach out securely to the device over the client network to retrieve the configuration for analysis. The configuration is retrieved either as a single action, or on a regular scheduled cadence from every hour, to quarterly. Nipper Enterprise has successfully assessed and reported on over 300,000 device configurations daily, and, due to its horizontally scalable nature, this can be increased further as required. If direct network access is not possible, then configuration files extracted separately can be deposited in an application directory, and Nipper Enterprise will audit those files. This too is scalable allowing for hundreds of thousands of devices to be assessed quickly at a single point in time.

All Nipper reports produce tagged security findings that Titania has mapped to Risk Management Frameworks; for example, NIST 800-53 dashboards have been developed in Splunk to visualize the RMF compliance across the network, applying a risk lens through which to prioritize actions.

Nipper Enterprise is also future proof, supporting a wide range of enterprise integrations, including SIEM and SOAR systems, to facilitate automatic remediation where this is appropriate.

Significantly reducing MTTR and playbook controlled auto-mitigation

Virtually modelling and analysing the entire configuration as a single entity, in the way that Nipper and Nipper Enterprise do, provides accuracy and granular detail about where the actual configuration differs from the desired secure configuration. This means that the findings can be reported with remediation recommendations and where possible complete with command line syntax instructions to remediate any misconfiguration risks found.

This means that Nipper Enterprise can produce reports suitable for ingest by workflow tools, such as ServiceNow, or automatic playbook controlled remediation tools, such as SOAR, incluing Splunk Phantom and Cortex XSOAR.

Integrating Nipper Enterprise's detailed findings with SOAR systems not only allows configuration security and compliance data to be visualized and prioritized in those products, it can also be used in playbooks that step through the remediation processes, enabling playbook controlled automatic remediation capability for a variety of risk classes.

So Titania's software is not only proven to reduce the mean time to detect (MTTD) core network misconfigurations, it also addresses the mean time to repair (MTTR) and remediate risks, supporting users in their missions to establish a defendable network.

Conclusion

Increasingly sophisticated methods of attack, the sheer size of networks, and the volume of interdependent configurations that need to be checked daily, means core network security is no longer considered a case of 'finding and fixing' every vulnerability. Rather, best practice is to find and fix the misconfigurations that pose any critical risk first and to inform remediation workflows, ensuring the prioritization of the work that is required to most significantly improve the security and compliance posture of the network.

Reducing the mean time to remediate a vulnerability that has low impact on the network if exploited cannot be considered an effective benchmark of security. In order to prioritize remediation effectively, network owners need to be able to:

» Accurately identify misconfigurations and interdependencies between core network settings

» Analyze the impact if it is exploited

» Understand how easy it is to exploit the misconfiguration

» Assess the risk in terms of both security and compliance

» Calculate how easy it is to remediate (with a time to fix)

» Determine and advise the remediation recommendation

Only then, equipped with the accurate data they need, can network teams implement considered remediation workflows that provide a roadmap to security compliance and configuration confidence.

So whilst on the surface, vulnerability detection software for the core network might appear equal – in reality, the way in which the software detects vulnerabilities has a significant impact on the efficacy of the findings and on a network team's ability to remediate critical misconfigurations and reduce risk.

Vulnerability scanners with configuration management modules that use GREP analysis can find firmware and software quality issues, but cannot accurately identify and prioritize network misconfigurations based on risk.

Complementary to their analysis, Titania's Nipper solutions provide:

» Audit accuracy – saving significant time not investigating false positives and identifying misconfigurations others don't to improve MTTD

» Risk scoring and prioritization – with a security and/or compliance lens

» Remediation advice – with exact technical fixes that can be used in playbook-controlled auto-mitigation, reducing MTTR

Furthermore, Titania has augmented Nipper software and associated visualizations to specifically address the DoD network and report against the RMF compliance framework. By generating a unique network risk assessment, Nipper's NIST 800-53 compliance report is prioritized to help network owners decide what actions to take first to reduce RMF risk as soon as possible.

These are the primary reasons that the DoD and approximately 30 other federal agencies complement their DISA ACAS (Tenable Nessus) analysis with Nipper configuration analysis for core network devices. It's also the reason that Titania has developed Nipper Enterprise, to deliver the market-leading configuration assessment accuracy that the DoD depends on, at scale, every day.

About Titania

World leaders in accurate configuration audit automation, with over 10 years supporting US government security and compliance missions, Titania's proven software is trusted to secure the world's most critical core networks against preventable attacks.

For more information on any of our products or services please visit:

www.titania.com

TITANIA
Assured Accuracy