BACKBOX

WHITE PAPER

Transforming Network Configuration Management: Challenges and Solutions

Introduction

Network Configuration Management (NCM) has been a cornerstone of network operations for over two decades. However, as network environments have evolved, traditional NCM solutions have struggled to keep pace with the increasing complexity and demands for automation. This whitepaper explores the evolution of NCM, the contemporary challenges faced by network teams, and the innovative solutions offered by BackBox to address these challenges and maintain secure, efficient networks.

Evolution of Network Configuration Management

Legacy Network Configuration Management tools have focused primarily on text-based configuration backups and manual configuration changes. However, as Gartner highlighted in their market guide for network automation, NCM is now a crucial subset of network automation platforms.

> **TRADITIONAL NCM PRACTICES**
> Traditional NCM solutions have focused on:

- **Backing Up Configurations:** Ensuring nightly backups and pre-change backups to enable rollbacks in case of errors.
- **Configuration Rollbacks:** Allowing network administrators to revert to previous configurations to correct mistakes.
- **Bulk Configuration Changes:** Managing large-scale changes across multiple devices, such as adding an access list to hundreds of switches.
- **OS Upgrades:** Keeping systems up to date on the latest versions, which historically has been infrequent but now increasingly necessary and urgent due to security vulnerabilities.
- **Compliance Assessment:** Checking to see if configurations meet internal best practices and external standards and reporting the difference.

Contemporary Challenges in Network Configuration Management

Despite the advancements in NCM tools over the years, network teams face several new challenges that traditional solutions often cannot address effectively.

Manual Intervention and Human Errors

Traditional NCM solutions rely heavily on manual intervention, which is time-consuming and prone to human error. Engineers spend significant time monitoring configuration changes and implementing updates manually, leading to inefficiencies and potential mistakes, not to mention that manual intervention doesn't scale.

Hybrid Network Environments

The shift to hybrid networks, combining on-premises and cloud-based devices, complicates NCM. Legacy NCM tools often struggle to manage configurations across these diverse environments effectively, which exposes the organization to security risk.

Limited Security Device Support

Traditional NCM tools are generally optimized for network devices like routers and switches but offer limited support for security devices such as firewalls. This gap can lead to inconsistent device administration and increased vulnerability.

Need for Continuous Compliance

Maintaining compliance with industry standards and internal policies is a continuous process. Legacy NCM tools typically lack the automation needed to perform real-time compliance assessments and adjustments in a timely manner to mitigate drift.

45%

of all major network-related outages are caused by configuration management failures.

The Consequences of These Shortcomings

Organizations are feeling the pain of not being able to keep up with the needs of the organization and evolving infrastructure. According to Uptime Institute's 2023 Annual Outage Analysis, configuration management failure is the most common cause (45%) of major network-related outages, with human error and management failures contributing to a considerable number of outages. Additionally, digital infrastructure outages are becoming more expensive with more than two-thirds of all outages costing more than $100,000.

AUTOMATION IN MODERN NCM

Modern NCM solutions integrate automation to enhance these traditional practices, improving scalability and performance while making them more efficient and less prone to human error. Automation in NCM includes:

- **Automated Backups and Rollbacks:** Reducing the manual effort required to maintain configuration integrity.
- **Smart Bulk Configuration Changes:** Minimizing the time and errors associated with large-scale changes.
- **Automated Complex OS Upgrades:** Streamlining the upgrade process to address vulnerabilities quickly. Automating updates to limit downtime and reduce after-hours work for an already overloaded team.
- **Dynamic Compliance Checks:** Continuously assessing configurations against best practices and compliance standards, like CIS benchmarks, DISA STIGs, and PCI DSS, and offering optional remediation should devices drift out of compliance.

BackBox: A Modern Approach to NCM

BackBox addresses the shortcomings of traditional NCM solutions by providing a comprehensive, automated approach to network configuration management.

Enhanced NCM Performance and Scalability

BackBox supports a wide range of devices, from a handful to thousands, offering scalable solutions that improve NCM performance through automation. With a distributed automation engine, we eliminate device polling allowing automations to execute independently across the network increasing scalability and performance.

API-First Integration

BackBox's API-first approach allows seamless integration with third-party ticketing systems, inventory systems, and CMDBs, while enhancing network operations through integration with CI/CD workflows. The intent is to help network teams manage their hybrid, multi-cloud environment as one ecosystem at scale with insights across their entire environment.

No-Code Automation

Automation Builder simplifies automation by enabling network administrators to create automations without having to write any code. Administrators can create and customize automation tasks through a user-friendly interface without needing complex scripting knowledge.

Extensive Multi-Vendor Support

BackBox supports over 180 vendors out of the box, including major network and security device manufacturers. This extensive support ensures comprehensive coverage for diverse network environments with a single tool and eliminates complexity for network teams.

CASE STUDY:

Automation in Action

A customer needed to update licenses to 92 firewalls in their network. Using BackBox, they automated the bulk configuration change in 20 minutes. Running the resulting automation took another 10 minutes reducing the time required from about 10 hours to 30 minutes and eliminating potential human errors.

Read more about this case study

Key Features of BackBox NCM

1 Automated Backups and Verification

Ensures all configurations are backed up and verified for integrity, enabling 1-click restores, even when restoring to bare metal.

2 Configuration Comparison and Drift Detection

Automatically compares current configurations with previous versions to detect changes and potential issues. Can optionally automatically groom configurations back into compliance.

3 Automated OS Upgrades

Streamlines the process of upgrading device firmware to address vulnerabilities and maintain security compliance. Complex upgrades like multi-step upgrades or upgrades of high-availability pairs are seamlessly supported.

4 Compliance and Vulnerability Management

Integrates compliance assessments and vulnerability management to ensure configurations meet industry standards and are secure from known threats.

5 ServiceNow Integration

Syncs devices with ServiceNow for discovery, and automates ticket creation/updates/closing, ensuring issues are tracked and resolved efficiently.

Conclusion

Network Configuration Management has evolved significantly, driven by the need for automation, hybrid environments, and enhanced security. Traditional NCM solutions are no longer sufficient to address the complex challenges of modern networks, nor do they scale to the performance needs of today's networks.

BackBox offers a robust, automated NCM solution that improves efficiency, reduces errors, and enhances network security. By adopting BackBox, network teams can deliver the performance and scalability demanded by today's network operations requirements, while maintaining secure, compliant, and efficient networks.

About BackBox

BackBox powers The BackBox Automation Platform for Network Teams, which supports network and security device automation of over 180 vendors, with thousands of security-centric pre-built automations and a scripting-free way to build new ones. Enterprises and managed service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance and vulnerability management, BackBox gives administrators the confidence that automations will deliver the expected outcome every time.

To learn more, visit **backbox.com**