How Drut helps in Firewall Review

A case study for a large telcom company.

By
ANB Professional Services Team

Summary

One of India's leading telecom providers, implemented drut., a robotics-based automation platform for Governance, Risk, and Compliance (GRC), to streamline firewall rule configuration reviews across its large-scale telecom infrastructure.

The Challenge

The Company operates firewalls from seven major vendors (Cisco, Fortinet, Juniper, Nokia, F5, ZTE, Huawei) totaling over 630+ devices with heterogeneous platforms and architectures. Manual firewall rule reviews across this diverse environment are time-consuming, error-prone, and inefficient, creating risks of non-compliance, security misconfigurations, unauthorized access, and potential regulatory penalties.

Solution : Three-Pillar Approach

1

Automated Data Collection

drut. uses native SSH/API integrations to securely extract and standardize firewall configuration data across all integrated platforms simultaneously, eliminating manual exports and ensuring audit-ready data consistency.

2

Automated Analysis and Risk Identification

drut. performs rule-level analysis identifying seven key security risks:

1. Rules with source/destination/service set to "ANY" or "ALL".

2. Insecure services or vulnerable ports.

3. Excessive IP addresses or ports in single rules.

4. Missing logging configurations.

5. Disabled rules (legacy or incomplete implementation).

6. Unused rules retained for extended periods.

7. Overly permissive access policies.

3

Dashboard and Exception Reporting

Results are displayed at three aggregation levels: individual firewall analysis (specific rule IDs and IPs), OEM/vendor-level patterns, and enterprise-wide risk dashboards showing severity-wise non-compliance counts.

Detailed Comparison Overview

Feature	drut.	Tufin	Skybox
Supported Firewall Vendor	Paloalto, Cico, Fortinet, Juniper, Checkpoint Nokia, Huawei, ZTE, F5, Mavenier.	Paloalto, Cico, Fortinet, Checkpoint	Paloalto, Cico, Fortinet, Juniper, Checkpoint
Monitoring Type	Scheduled / Batch	Near Real-Time (Polling)	Scheduled / Batch
Default Frequency	Typically, hourly/daily	5–15 min configurable pulls	Typically, hourly/daily
Connection type	SSH, HTTPS API's, RPA	SSH, HTTPS API's	SSH, HTTPS, Syslog
Centralized Policy review	Yes	Yes	Yes
Rule Optimization	Yes	Yes	Yes
Continuous Compliance Monitoring	Yes	Yes	Yes

Return on Investment with Drut

Benefit	Impact
Efficiency	60–80% reduction in review time; analysis completed in minutes instead of weeks
Accuracy	Standardized logic eliminates human error and inconsistent policy interpretation
Compliance	Faster audit preparation and regulatory readiness; reduced audit findings
Security	Continuous identification of high-risk rules and misconfigurations
Multi-Vendor Support	Eliminates need for vendor-specific expertise training
Continuous Monitoring	On-demand assessments maintain optimized firewall policy over time
Cost Savings	High ROI typically achieved within first year of deployment

drut.
ROBOTICS GRC

For any queries or feedback reach out to us on

SANJIV.VANKER@DRUT.COM