Proposed Framework for Automating Network Infrastructure Hardening Audits Based on CIS Benchmarks and Vendor Security Standards

by Faizal Alfiana Sakti

Submission date: 06-Nov-2026 02:15PM (UTC+0700)
Submission ID: 3081705417
File name: 51_Artikel_JTIK_V12N2_Faizal_3560.pdf (658.01K)
Word count: 6199
Character count: 39595

Jurnal Teknlogi Informatika dan Komputer MH. Thamrin p-ISSN 2656-9957; e-ISSN 2622-8475
Volume 12 No 2; September 2026 Hal 1875-1894

Proposed Framework for Automating Network Infrastructure Hardening Audits Based on CIS Benchmarks and Vendor Security Standards

Faizal Alfiana Sakti[1)*)], Ferhat Aziz[2)], Tukiyat[3)]

[1)2)3)]Program Studi Magister Teknik Informatika, Program Pascasarjana, Universitas Pamulang
[*)]**Correspondence author**: faizal.sakti01@gmail.com, Tangerang Selatan, Indonesia
DOI: https://doi.org/10.37012/jtik.v12i2.3560

Abstract

The complexity of multi-vendor network infrastructure demands configuration hardening audits that are consistent, measurable, and repeatable. Differences in operating systems, command syntax, output formats, and security references across Cisco, MikroTik, and Ruijie devices make auditing difficult using a single uniform approach. This study designs, implements, and evaluates an automated network infrastructure hardening audit framework based on CIS Benchmarks and vendor-specific security standards. Using an applied experimental approach, an audit-only workflow was developed comprising Collector, Evaluator, and Report modules. The Collector retrieves actual device configurations via SSH and stores them as raw JSON; the Evaluator compares device outputs against vendor-specific YAML baselines; and the Report module generates audit artifacts in HTML, PDF, CSV, chart, and audit-log formats. Evaluation was conducted on 50 production devices (25 Cisco, 10 MikroTik, and 15 Ruijie), using a 68-rule baseline that produced 1,135 evaluated controls. Results showed 626 Pass controls (55.15%) and 509 Fail controls (44.85%). A complete audit session finished in 206 seconds, with all devices successfully processed. CIA Impact mapping revealed Integrity as the dominant aspect associated with non-compliant controls. Findings indicate the framework offers a structured, adaptive, and well-documented audit-only approach for evaluating multi-vendor configuration hardening compliance without modifying production configurations.

Keywords: *Configuration Audit, Network Hardening, CIS Benchmarks, Multi-Vendor, CIA Impact*

Abstrak

Kompleksitas infrastruktur jaringan multi-vendor menuntut adanya audit penguatan konfigurasi hardening yang konsisten, terukur, dan dapat diulang. Perbedaan dalam sistem operasi, sintaksis perintah, format keluaran, dan referensi keamanan pada perangkat Cisco, MikroTik, dan Ruijie menyulitkan pelaksanaan audit dengan pendekatan tunggal yang seragam. Penelitian ini merancang, mengimplementasikan, dan mengevaluasi kerangka kerja audit penguatan infrastruktur jaringan otomatis yang berbasis pada CIS Benchmarks dan standar keamanan spesifik vendor. Dengan menggunakan pendekatan eksperimental terapan, dikembangkan alur kerja khusus audit yang terdiri dari modul Collector, Evaluator, dan Report. Modul Collector mengambil konfigurasi aktual perangkat melalui SSH dan menyimpannya dalam format JSON mentah; modul Evaluator membandingkan keluaran perangkat dengan baseline YAML spesifik vendor; dan modul Report menghasilkan artefak audit dalam format HTML, PDF, CSV, grafik, serta log audit. Evaluasi dilakukan terhadap 50 perangkat produksi (25 Cisco, 10 MikroTik, dan 15 Ruijie) menggunakan baseline berisi 68 aturan yang menghasilkan 1.135 kontrol yang dievaluasi. Hasilnya menunjukkan 626 kontrol berstatus Lulus (Pass) (55,15%) dan 509 kontrol berstatus Gagal (Fail) (44,85%). Sesi audit lengkap diselesaikan dalam waktu 206 detik, dengan seluruh perangkat berhasil diproses. Pemetaan dampak CIA menunjukkan bahwa integritas merupakan aspek dominan yang terkait dengan kontrol yang tidak memenuhi standar. Temuan ini mengindikasikan bahwa kerangka kerja tersebut menawarkan pendekatan audit yang terstruktur, adaptif, dan terdokumentasi dengan baik untuk mengevaluasi kepatuhan penguatan konfigurasi multi-vendor tanpa mengubah konfigurasi produksi.

Kata Kunci: Audit Konfigurasi, Pengerasan Jaringan, CIS Benchmarks, Multi-Vendor, Dampak CIA

PENDAHULUAN

Infrastruktur modern berkembang ke arah lingkungan yang semakin kompleks, heterogen, dan terhubung dengan berbagai layanan digital organisasi. Kompleksitas tersebut tidak hanya muncul dari meningkatnya jumlah perangkat, tetapi juga dari keberagaman sistem operasi perangkat jaringan, sintaks konfigurasi, protokol manajemen, serta kebutuhan keamanan yang berbeda pada setiap vendor. Dalam konteks ini, perangkat jaringan seperti router, switch, dan gateway tidak lagi hanya berperan sebagai penghubung lalu lintas data, tetapi juga menjadi titik kendali keamanan yang menentukan kerahasiaan, integritas, ketersediaan, dan kesinambungan layanan digital. Perangkat tersebut mengatur berbagai fungsi penting, mulai dari akses manajemen, autentikasi administrator, segmentasi jaringan, proteksi Layer 2, logging, sinkronisasi waktu, hingga layanan monitoring. Oleh karena itu, kelemahan konfigurasi pada perangkat jaringan dapat membuka peluang akses tidak sah, penyalahgunaan layanan manajemen, manipulasi trafik, gangguan ketersediaan layanan, serta hilangnya jejak audit ketika terjadi insiden keamanan. Tantangan audit konfigurasi semakin kompleks pada lingkungan multi-vendor. Perangkat Cisco, MikroTik, dan Ruijie memiliki sistem operasi, perintah, struktur konfigurasi, dan format output yang berbeda. Perintah yang relevan untuk memeriksa SSH pada Cisco IOS tidak selalu sama dengan MikroTik RouterOS atau Ruijie RGOS. Demikian pula mekanisme pengamanan SNMP, AAA, logging, DHCP Snooping, Dynamic ARP Inspection, dan port security tidak selalu memiliki bentuk konfigurasi yang identik pada setiap vendor. Kondisi tersebut membuat audit manual berpotensi menghasilkan interpretasi yang tidak konsisten, terutama ketika jumlah perangkat dan kontrol keamanan yang dievaluasi semakin meningkat.

Otomasi jaringan telah banyak dibahas sebagai pendekatan untuk meningkatkan konsistensi manajemen konfigurasi dan mengurangi ketergantungan pada proses manual. Babaei et al. (2022) menempatkan otomasi sebagai bagian penting dari kontrol dan manajemen jaringan modern, sedangkan Banerjee et al. (2023) menekankan pentingnya otomasi pada jaringan terbuka dan multi-vendor. Dalam konteks keamanan, Bringhenti et al. (2024) menunjukkan bahwa konfigurasi keamanan jaringan semakin kompleks sehingga membutuhkan mekanisme yang mampu menghubungkan kebijakan keamanan dengan implementasi teknis. Aslan et al. (2023) menegaskan bahwa keragaman ancaman siber kontemporer menuntut kontrol keamanan yang dapat diverifikasi secara sistematis, bukan hanya diterapkan secara ad hoc. CIS Benchmarks menyediakan acuan konfigurasi aman yang dapat digunakan

sebagai dasar hardening, dan Govindappa Venkatesha dan Singh (2024) menunjukkan bahwa acuan tersebut juga efektif diadaptasi pada infrastruktur multi-cloud. Namun, tidak seluruh vendor perangkat jaringan memiliki acuan CIS dengan tingkat kelengkapan yang sama. Cisco IOS memiliki benchmark yang lebih mapan, sedangkan MikroTik dan Ruijie memerlukan pemanfaatan standar keamanan vendor serta adaptasi kontrol umum yang sesuai dengan karakteristik masing-masing perangkat.

Penelitian terdahulu telah membahas otomasi administrasi jaringan, hardening berbasis CIS, dan otomasi konfigurasi lintas vendor. Santyadiputra et al. (2021) membahas otomasi administrasi jaringan berbasis Python dan SSH; Ortiz-Garces et al. (2021) membahas otomasi untuk meningkatkan hardening pada jaringan kampus; Perera et al. (2021) mengembangkan NetBot untuk hardening router Cisco berbasis CIS Benchmark; sedangkan Muhammad dan Munir (2023) serta Thati (2025) menekankan pentingnya konfigurasi dan compliance automation berbasis REST API. Imoukhuede et al. (2025) mengoptimalkan hardening perangkat pada lingkungan multivendor, dan Martino et al. (2025) mengulas pendekatan policy-as-code untuk mengelola kondisi keamanan dan privasi pada ekosistem edge dan cloud computing. Meskipun demikian, sebagian besar penelitian tersebut masih berorientasi pada provisioning, deployment, remediation, atau enforcement. Masih diperlukan penelitian yang secara spesifik memisahkan proses audit dari perubahan konfigurasi perangkat, menerjemahkan acuan keamanan menjadi baseline yang dapat dieksekusi, dan menguji framework audit pada perangkat produksi dari beberapa vendor secara seragam.

Tabel 1.

Posisi penelitian dan gap penelitian

Penelitian	Otomasi jaringan	Baseline keamanan	Multi-vendor	Perangkat produksi	CIA Impact
Santyadiputra et al. (2021)	✓	×	△	×	×
Ortiz-Garces et al. (2021)	✓	✓	△	△	×
Perera et al. (2021)	✓	✓	×	×	×
Muhammad & Munir (2023)	✓	×	✓	×	×
Imoukhuede et al. (2025)	✓	✓	✓	×	×
Thati (2025)	✓	✓	△	×	×
Penelitian ini	**✓**	**✓**	**✓**	**✓**	**✓**

Keterangan: ✓ = dibahas/diimplementasikan; △ = sebagian dibahas atau bukan fokus utama; × = tidak dibahas atau tidak menjadi fokus penelitian.

Berdasarkan Tabel 1, penelitian terdahulu telah memberikan kontribusi pada otomasi jaringan, penerapan baseline keamanan, dan otomasi konfigurasi lintas vendor. Namun, masih terdapat gap pada penelitian yang secara bersamaan menggabungkan otomasi audit hardening, baseline keamanan, dukungan multi-vendor, pengujian pada perangkat produksi, dan pemetaan CIA Impact. Sebagian penelitian masih berfokus pada provisioning, deployment, remediation, atau enforcement, sedangkan penelitian ini menekankan pendekatan audit-only yang memisahkan proses evaluasi konfigurasi dari perubahan konfigurasi perangkat. Dengan demikian, framework yang diusulkan lebih sesuai untuk lingkungan produksi karena hanya melakukan pengumpulan data, evaluasi terhadap baseline, dan pelaporan hasil tanpa melakukan perubahan konfigurasi secara otomatis. Secara teoretis, penelitian ini juga memberikan kontribusi berupa model penerjemahan acuan keamanan multi-sumber CIS Benchmarks dan dokumentasi keamanan vendor ke dalam representasi baseline yang dapat dieksekusi dan dipetakan terhadap dimensi Confidentiality, Integrity, dan Availability (CIA), sehingga hasil audit tidak hanya bersifat biner (Pass/Fail) tetapi juga dapat diinterpretasikan dari perspektif dampak keamanan.

Berdasarkan gap tersebut, penelitian ini bertujuan merancang, mengimplementasikan, dan mengevaluasi framework otomatisasi audit hardening infrastruktur jaringan berbasis CIS Benchmarks dan standar keamanan vendor. Kontribusi penelitian ini meliputi: (1) rancangan arsitektur audit-only yang memisahkan proses pengumpulan data, evaluasi konfigurasi, dan pelaporan; (2) penerjemahan CIS Benchmarks dan standar keamanan vendor ke dalam baseline YAML spesifik vendor; (3) pengujian framework pada 50 perangkat produksi Cisco, MikroTik, dan Ruijie; serta (4) penyajian hasil audit dalam bentuk Pass/Fail, artifact laporan, dan pemetaan CIA Impact terhadap kontrol yang belum memenuhi baseline.

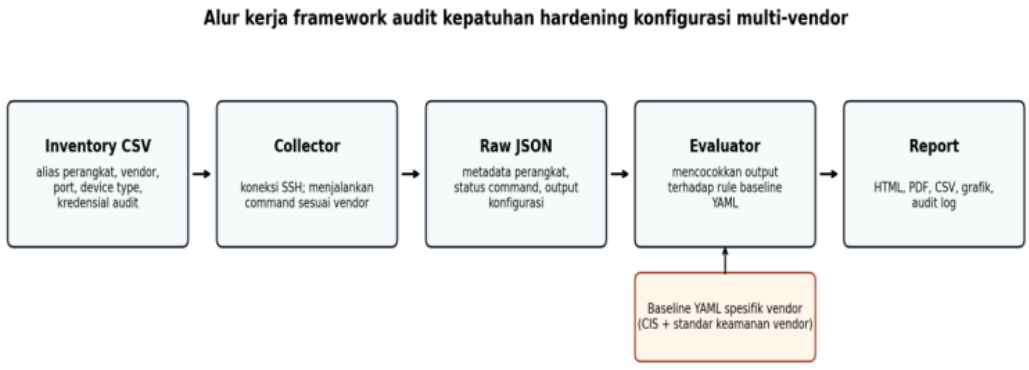
METODE PENELITIAN

Penelitian ini menggunakan pendekatan terapan eksperimental. Pendekatan ini dipilih karena penelitian tidak hanya menyusun konsep, tetapi juga membangun framework audit yang dijalankan pada lingkungan jaringan produksi. Eksperimen dilakukan dalam bentuk satu sesi audit otomatis yang mencakup proses pembacaan inventory, pengambilan

konfigurasi aktual, evaluasi terhadap baseline, dan penyusunan laporan. Pengujian tidak menggunakan audit manual sebagai ground truth independen, sehingga hasil Pass dan Fail diinterpretasikan sebagai keluaran kepatuhan konfigurasi terhadap baseline yang didefinisikan, bukan sebagai sertifikasi kepatuhan eksternal atau pengukuran akurasi terhadap auditor manual.

Ruang lingkup penelitian dibatasi pada audit hardening konfigurasi perangkat jaringan. Framework tidak melakukan remediasi otomatis, tidak menjalankan penetration testing, tidak melakukan vulnerability scanning, dan tidak menganalisis trafik jaringan. Pembatasan ini penting karena objek pengujian merupakan perangkat produksi. Dengan mode audit-only, framework hanya membaca konfigurasi dan menghasilkan rekomendasi berbasis baseline tanpa mengubah konfigurasi perangkat secara langsung. Keputusan tindak lanjut hardening tetap dilakukan oleh administrator setelah meninjau hasil audit.

Framework dirancang secara modular agar setiap tahap audit dapat dipisahkan dengan jelas. Modul Collector bertanggung jawab mengambil data konfigurasi aktual perangkat melalui koneksi SSH berdasarkan daftar perangkat pada inventory CSV. Modul Evaluator bertugas membaca raw output JSON dan baseline YAML, kemudian menentukan status Pass atau Fail berdasarkan pola evaluasi pada setiap rule. Modul Report menyusun hasil evaluasi menjadi artifact laporan yang dapat dibaca administrator, meliputi HTML, PDF, CSV, grafik, dan audit log. Pemisahan ini memudahkan pengembangan rule baru, perluasan vendor, serta penelusuran ulang hasil audit karena setiap status evaluasi dapat dilacak dari rule, command, raw output, dan alasan evaluasinya.



Gambar 1. Alur kerja framework audit kepatuhan hardening konfigurasi multi-vendor

Tabel 2.

Komponen framework dan fungsi utama

Komponen	Fungsi	Keluaran
Inventory CSV	Menyimpan daftar perangkat, alias, vendor, port, dan parameter koneksi SSH yang digunakan sebagai input audit.	Target audit per perangkat
Collector	Membuka koneksi SSH, menjalankan command berdasarkan vendor, dan menyimpan output konfigurasi aktual.	Raw output JSON dan status output command
Evaluator	Membaca raw JSON dan baseline YAML untuk menentukan kesesuaian konfigurasi terhadap rule hardening.	Detail hasil Pass/Fail, reason, dan CIA Impact
Report	Menyusun hasil evaluasi menjadi laporan yang dapat ditinjau administrator.	HTML, PDF, CSV, grafik, dan audit log

Baseline keamanan disusun dalam format YAML dan dipisahkan berdasarkan vendor karena setiap vendor memiliki command dan pola output yang berbeda. Baseline Cisco disusun dengan mengacu pada CIS Cisco IOS Benchmark, baseline MikroTik disusun berdasarkan panduan keamanan vendor MikroTik, sedangkan baseline Ruijie disusun melalui adaptasi kontrol CIS dan pedoman keamanan vendor. Secara keseluruhan terdapat 68 rule baseline, yaitu 23 rule Cisco, 23 rule MikroTik, dan 22 rule Ruijie.

Setiap rule memuat identitas kontrol, deskripsi, referensi standar, rasional keamanan, command yang dijalankan, pola evaluasi, dan CIA Impact. Evaluator membaca pola tersebut untuk menentukan status kontrol. Jika konfigurasi aktual memenuhi pola wajib dan tidak memuat pola yang dilarang, kontrol diberi status Pass. Sebaliknya, jika pola wajib tidak ditemukan, pola alternatif tidak terpenuhi, atau pola terlarang ditemukan, kontrol diberi status Fail. Status Fail tidak dimaknai sebagai skor risiko absolut, melainkan sebagai indikasi bahwa konfigurasi belum sesuai dengan baseline yang dipilih.

Tabel 3.

Platform perangkat, versi software, dan acuan baseline

Vendor	Platform/Perangkat	Versi software	Jumlah perangkat	Acuan baseline
Cisco	Cisco Catalyst C3560E, C3560E-UNIVERSALK9-M	Cisco IOS Software Version 12.2(55)SE3	25	CIS Cisco IOS Benchmark
MikroTik	Perangkat berbasis MikroTik RouterOS	RouterOS 6.47.8 stable	10	Panduan keamanan vendor MikroTik
Ruijie	Ruijie 10G Ethernet Switch S5350-48GT4XS-P-E	S5350E_RGOS 12.6(3)B0708	15	Adaptasi CIS dan panduan keamanan vendor Ruijie

Tabel 4.

Struktur elemen rule baseline YAML

Elemen	Fungsi dalam evaluasi
id	Identitas unik rule yang digunakan sebagai penanda kontrol audit.
title/description	Nama dan uraian kontrol hardening yang dievaluasi.
ref/cis_ref	Acuan standar atau panduan keamanan yang menjadi dasar penyusunan rule.
rationale	Alasan keamanan mengapa kontrol tersebut perlu diterapkan.
commands	Daftar command yang dijalankan oleh Collector pada perangkat sesuai vendor.
expect_regex	Pola konfigurasi yang wajib ditemukan agar kontrol dapat dinyatakan sesuai.
expect_all_regex	Kumpulan pola yang seluruhnya harus ditemukan.
expect_any_regex	Kumpulan pola alternatif; minimal satu pola harus ditemukan.
none_match_regex	Pola konfigurasi yang tidak boleh ditemukan karena menunjukkan konfigurasi tidak sesuai baseline.
cia_impact	Klasifikasi aspek Confidentiality, Integrity, dan/atau Availability yang berkaitan dengan kontrol.

```yaml
- id: CISCO_DISABLE_TELNET
  title: "Disable Telnet on all VTY lines (SSH-only)"
  cis_ref: "1.2.1"
  cia_impact:
    - Confidentiality
    - Integrity
  rationale: >
    Memastikan seluruh akses manajemen melalui VTY tidak menggunakan Telnet
    dan hanya mengizinkan SSH untuk mencegah akses manajemen tanpa enkripsi.
  commands:
    - cmd: "show running-config | section line vty"
      expect_regex:
        - "(?is)line\\s+vty\\s+0\\s+4[\\s\\S]*?transport\\s+input\\s+ssh"
        - "(?is)line\\s+vty\\s+5\\s+15[\\s\\S]*?transport\\s+input\\s+ssh"
      none_match_regex:
        - "(?im)^\\s*transport\\s+input\\s+telnet\\s*$"
        - "(?im)^\\s*transport\\s+input\\s+all\\s*$"
        - "(?im)^\\s*transport\\s+input\\s+telnet\\s+ssh\\s*$"
```

Gambar 2. Contoh rule baseline YAML CISCO_DISABLE_TELNET

Tabel 5.

Cakupan area hardening pada baseline

Area hardening	Contoh kontrol yang dievaluasi	Tujuan keamanan
Remote management	Disable Telnet, enforce SSH version 2, VTY ACL	Membatasi akses manajemen jarak jauh pada kanal yang lebih aman dan terkendali.
Autentikasi dan privilege	AAA, enable secret, local privilege control	Mengurangi risiko akses administratif yang tidak sah.
Layanan manajemen	Disable HTTP/HTTPS management, disable MAC server, SNMPv3 only	Mengurangi permukaan serangan dari layanan yang tidak diperlukan atau lemah.
Logging dan waktu	Syslog server, log timestamp, NTP/timezone	Mendukung akuntabilitas, korelasi kejadian, dan audit trail.
Proteksi Layer 2	BPDU Guard, DHCP Snooping, DAI, port security, storm control	Mencegah gangguan switching, spoofing, dan manipulasi trafik lokal.
Firewall/filtering	Input firewall baseline, brute-force protection, DoS rate limit	Membatasi akses ke layanan perangkat dan menekan trafik tidak sah.

Prosedur audit dimulai dari pembuatan audit session melalui antarmuka web. Pengguna mengunggah inventory CSV yang berisi daftar perangkat. Setelah inventory valid, Collector menjalankan command sesuai vendor dan menyimpan hasilnya dalam raw JSON. Evaluator kemudian memproses setiap raw output terhadap baseline YAML. Setiap pasangan perangkat dan rule menghasilkan satu kontrol evaluasi dengan status Pass atau Fail. Report menyusun ringkasan per vendor, ringkasan per perangkat, daftar kontrol yang gagal, distribusi CIA Impact, grafik, serta audit log.

Metrik yang digunakan meliputi jumlah perangkat, jumlah rule baseline, jumlah kontrol evaluasi, jumlah Pass, jumlah Fail, Pass rate, Fail rate, runtime audit, ketersediaan output hasil collection, dan distribusi CIA Impact. Pass rate dihitung sebagai jumlah kontrol Pass dibagi total kontrol evaluasi, sedangkan Fail rate dihitung sebagai jumlah kontrol Fail dibagi total kontrol evaluasi. Untuk CIA Impact, satu kontrol dapat berkontribusi pada lebih dari satu aspek karena satu rule dapat dipetakan ke Confidentiality dan Integrity sekaligus, atau Integrity dan Availability sekaligus. Oleh karena itu, frekuensi CIA Impact tidak harus sama dengan jumlah kontrol Fail.

HASIL DAN PEMBAHASAN

Eksekusi Audit Otomatis dan Runtime

Pengujian dilakukan pada 50 perangkat produksi yang terdiri atas 25 Cisco, 10 MikroTik, dan 15 Ruijie. Seluruh perangkat berhasil diproses pada level perangkat, yang berarti framework mampu menjalankan alur audit mulai dari collection, evaluation, hingga report tanpa perangkat yang gagal diproses secara keseluruhan. Satu sesi audit membutuhkan 206 detik, dengan tahap Collector menjadi bagian paling dominan karena proses ini melakukan koneksi SSH dan pengambilan output command dari seluruh perangkat.

Tabel 6.

Runtime satu sesi audit otomatis

Tahap	Waktu mulai	Waktu selesai	Durasi	Keterangan
Collector	15:14:14	15:17:15	181 detik	Pengambilan output command melalui SSH
Evaluator	15:17:15	15:17:30	15 detik	Evaluasi raw JSON terhadap baseline YAML
Report	15:17:30	15:17:40	10 detik	Penyusunan CSV, grafik, HTML, PDF, dan log
Total	15:14:14	15:17:40	206 detik	Workflow audit otomatis end-to-end

Durasi 206 detik untuk 50 perangkat menunjukkan bahwa framework dapat menjalankan audit konfigurasi dalam waktu yang relatif singkat untuk satu sesi pengujian. Penelitian ini

tidak membandingkan runtime tersebut dengan audit manual sehingga hasil ini tidak digunakan untuk menyatakan persentase efisiensi dibanding auditor manusia; angka runtime hanya digunakan untuk menunjukkan kelayakan eksekusi workflow otomatis pada lingkungan produksi.

Ketersediaan Output Hasil Collection

Selama proses collection, framework menjalankan 1.050 command pada 50 perangkat. Dari jumlah tersebut, 954 command menghasilkan output yang tersedia, sedangkan 96 command menghasilkan output kosong atau tidak ditemukan. Kolom output kosong/tidak ditemukan bukan menunjukkan kegagalan eksekusi command, melainkan menunjukkan bahwa command berhasil dijalankan tetapi konfigurasi, fitur, atau parameter yang dicari tidak ditemukan pada perangkat. Output kosong ini tetap digunakan oleh Evaluator sebagai bukti kondisi konfigurasi untuk menentukan status Pass atau Fail sesuai logika rule baseline.

Tabel 7.

Ringkasan ketersediaan output hasil collection per vendor

Vendor	Perangkat	Total command	Output ada	Output kosong/tidak ditemukan	Output ada (%)
Cisco	25	525	497	28	94.67%
MikroTik	10	210	200	10	95.24%
Ruijie	15	315	257	58	81.59%
Total	50	1050	954	96	90.86%

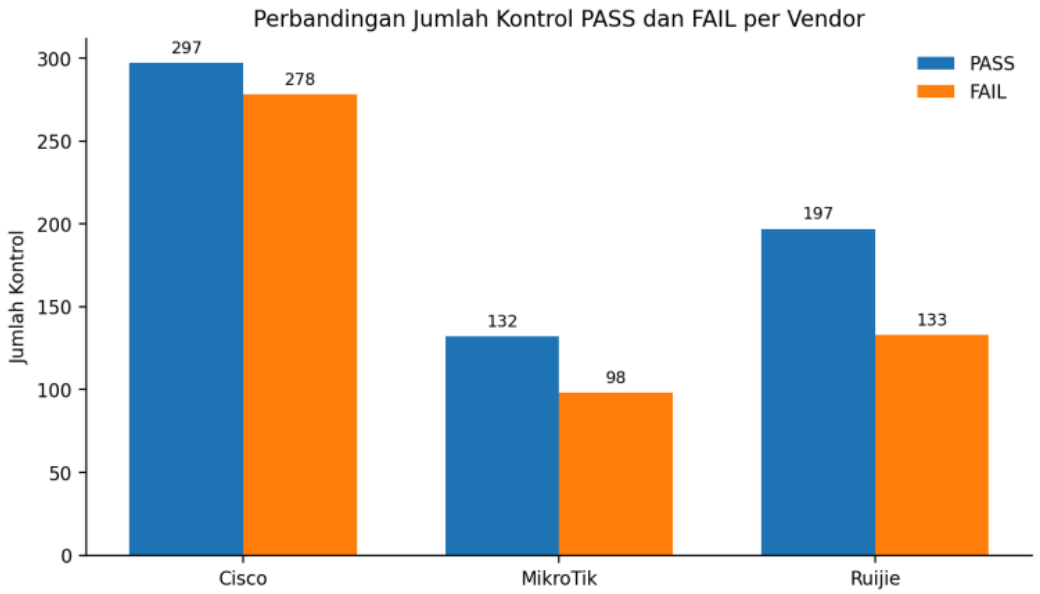
Hasil Pass dan Fail per Vendor

Baseline 68 rule menghasilkan 1.135 kontrol evaluasi karena setiap rule dijalankan pada perangkat sesuai vendor. Secara keseluruhan terdapat 626 kontrol Pass dan 509 kontrol Fail, sehingga tingkat kesesuaian terhadap baseline adalah 55,15% dan tingkat ketidaksesuaian adalah 44,85%. Hasil per vendor memperlihatkan bahwa Ruijie memiliki Pass rate tertinggi, yaitu 59,70%, diikuti MikroTik 57,39% dan Cisco 51,65%.

Tabel 8.

Hasil evaluasi Pass dan Fail per vendor

Vendor	Perangkat	Total kontrol	Pass	Fail	Pass rate	Fail rate
Cisco	25	575	297	278	51.65%	48.35%
MikroTik	10	230	132	98	57.39%	42.61%
Ruijie	15	330	197	133	59.70%	40.30%
Total	50	1135	626	509	55.15%	44.85%



Gambar 3. Perbandingan jumlah kontrol Pass dan Fail per vendor

Analisis Tingkat Kepatuhan per Perangkat

Ringkasan per perangkat digunakan untuk melihat variasi hasil audit di dalam masing-masing vendor. Pada Cisco, sebagian besar perangkat memiliki 12 Pass dan 11 Fail dari 23 kontrol, sedangkan satu perangkat menunjukkan jumlah Fail lebih tinggi. Pada MikroTik, variasi lebih lebar karena Pass rate perangkat berada pada rentang 47,83% sampai 73,91%. Pada Ruijie, Pass rate berada pada rentang 45,45% sampai 68,18%. Variasi ini menunjukkan bahwa meskipun perangkat berada pada vendor yang sama, kondisi konfigurasi aktual dapat berbeda akibat perbedaan peran perangkat, riwayat konfigurasi, atau kebijakan operasional lokal.

Tabel 9.

Statistik tingkat kepatuhan per perangkat

Vendor	Perangkat	Pass rate minimum	Pass rate maksimum	Rerata Pass rate	Fail minimum	Fail maksimum	Rerata Fail
Cisco	25	39.13%	52.17%	51.65%	11	14	11.12
MikroTik	10	47.83%	73.91%	57.39%	6	12	9.80
Ruijie	15	45.45%	68.18%	59.70%	7	12	8.87

Kontrol Dominan yang Berstatus Fail

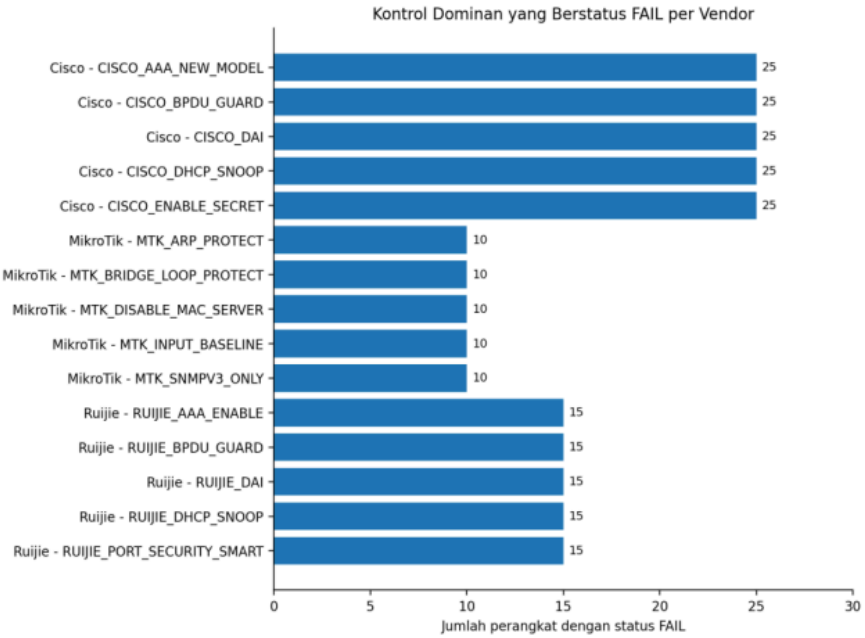
Analisis kontrol dominan dilakukan untuk mengetahui area hardening yang paling sering belum memenuhi baseline. Pada Cisco, beberapa kontrol mengalami Fail pada seluruh 25

perangkat, terutama AAA, BPDU Guard, Dynamic ARP Inspection, DHCP Snooping, enable secret, local privilege, login banner, port security, SNMPv3 only, storm control, dan VTY ACL. Pada MikroTik, kontrol yang gagal pada seluruh perangkat meliputi ARP protection, bridge loop protection, disable MAC server, input firewall baseline, SNMPv3 only, dan stateful firewall baseline. Pada Ruijie, kontrol yang gagal pada seluruh perangkat meliputi AAA framework, BPDU Guard, DAI, DHCP Snooping, port security/flood control, storm control, dan VTY ACL.

Tabel 10.

Kontrol dominan yang berstatus Fail per vendor

Vendor	Rule ID	Deskripsi kontrol	CIA Impact	Perangkat Fail
Cisco	CISCO_AAA_NEW_MODEL	AAA new-model enabled	Confidentiality, Integrity	25
Cisco	CISCO_BPDU_GUARD	BPDU Guard enabled (default or per-port)	Availability, Integrity	25
Cisco	CISCO_DAI	Dynamic ARP Inspection enabled	Integrity, Availability	25
Cisco	CISCO_DHCP_SNOOP	DHCP Snooping enabled	Integrity, Availability	25
Cisco	CISCO_ENABLE_SECRET	Enable secret configured (not enable password)	Confidentiality, Integrity	25
MikroTik	MTK_ARP_PROTECT	ARP protection (reply-only) on critical interfaces	Integrity	10
MikroTik	MTK_BRIDGE_LOOP_PROTECT	Bridge loop protection (RSTP enabled + bpdu-guard/edge on access ports)	Availability	10
MikroTik	MTK_DISABLE_MAC_SERVER	Disable MAC server (mac-telnet/mac-winbox) on WAN/All	Confidentiality, Integrity	10
MikroTik	MTK_INPUT_BASELINE	Baseline input firewall (established/related, invalid drop, final drop)	Integrity, Availability	10
MikroTik	MTK_SNMPV3_ONLY	SNMPv3 enabled; SNMPv1/v2 communities disabled	Confidentiality, Integrity	10
Ruijie	RUIJIE_AAA_ENABLE	AAA framework enabled	Confidentiality, Integrity	15
Ruijie	RUIJIE_BPDU_GUARD	BPDU Guard enabled (Global Default)	Availability, Integrity	15
Ruijie	RUIJIE_DAI	Dynamic ARP Inspection enabled	Integrity, Availability	15



Gambar 4. Kontrol dominan yang berstatus Fail per vendor

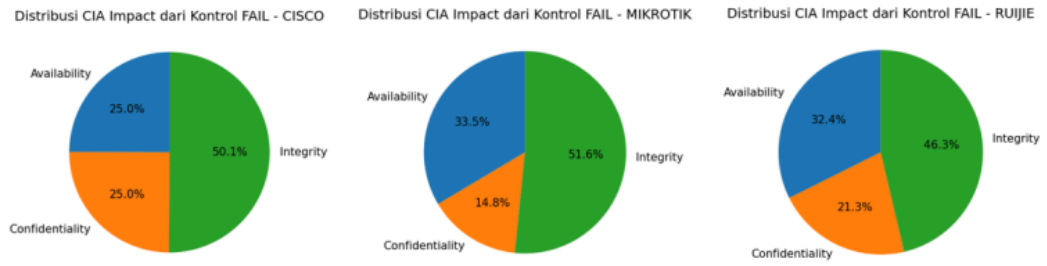
Distribusi CIA Impact

Pemetaan CIA Impact dilakukan pada kontrol yang berstatus Fail. Hasilnya menunjukkan bahwa Integrity merupakan aspek paling dominan pada seluruh vendor. Pada Cisco, Integrity muncul 253 kali atau 50,10% dari total frekuensi CIA Impact vendor tersebut. Pada MikroTik, Integrity muncul 80 kali atau 51,61%, sedangkan pada Ruijie Integrity muncul 111 kali atau 45,87%. Dominasi Integrity menunjukkan bahwa banyak kontrol yang belum memenuhi baseline berkaitan dengan keutuhan konfigurasi, validitas mekanisme jaringan, autentikasi, otorisasi, logging, serta pencegahan manipulasi trafik.

Tabel 11.

Distribusi CIA Impact pada kontrol Fail

Vendor	Confidentiality	Integrity	Availability	Total frekuensi CIA
Cisco	126	253	126	505
MikroTik	23	80	52	155
Ruijie	52	111	79	242
Total	201	444	257	902



Gambar 5. CIA Impact dari kontrol Fail per vendor

Frekuensi CIA Impact pada Tabel 11 tidak sama dengan jumlah kontrol Fail karena satu kontrol dapat dikaitkan dengan lebih dari satu aspek CIA. Sebagai contoh, kontrol SNMPv3 only dapat dipetakan ke Confidentiality dan Integrity karena berkaitan dengan kerahasiaan akses monitoring serta integritas konfigurasi manajemen. Oleh karena itu, CIA Impact diposisikan sebagai klasifikasi dampak keamanan, bukan sebagai skor risiko.

Ketercapaian Rancangan Framework

Hasil pengujian menunjukkan bahwa rancangan framework mampu menjalankan proses audit hardening konfigurasi secara end-to-end. Seluruh perangkat berhasil diproses pada level perangkat, raw output dapat dikumpulkan, baseline YAML dapat dieksekusi oleh Evaluator, dan laporan audit dapat dihasilkan dalam beberapa format. Hal ini menunjukkan bahwa pemisahan modul Collector, Evaluator, dan Report memberikan struktur yang cukup jelas untuk kebutuhan audit konfigurasi. Collector berfokus pada akuisisi data, Evaluator berfokus pada interpretasi baseline, sedangkan Report berfokus pada penyajian hasil. Pemisahan tanggung jawab ini konsisten dengan argumen Bringhenti et al. (2024) bahwa otomasi konfigurasi keamanan memerlukan mekanisme yang memisahkan kebijakan keamanan dari implementasi teknis, sehingga perubahan command vendor atau penambahan rule baru dapat dilakukan pada baseline tanpa harus mengubah keseluruhan sistem.

Pendekatan audit-only menjadi karakteristik penting penelitian ini. Dalam jaringan produksi, otomatisasi yang langsung melakukan perubahan konfigurasi berpotensi menimbulkan gangguan layanan apabila rule belum tervalidasi secara operasional. Dengan membatasi framework pada fungsi audit dan pelaporan, administrator memperoleh informasi ketidaksesuaian konfigurasi terlebih dahulu sebelum menentukan tindakan remediasi. Model ini berbeda dari pendekatan Ortiz-Garces et al. (2021) dan Perera et al. (2021) yang

mengarahkan otomasi langsung pada peningkatan level hardening; penelitian ini justru memisahkan tahap observasi dari tahap remediasi, sehingga lebih aman untuk tahap awal penerapan compliance automation karena memprioritaskan observasi, dokumentasi, dan pengambilan keputusan berbasis bukti.

Interpretasi Hasil per Vendor

Pada Cisco, jumlah Fail yang relatif tinggi terutama disebabkan oleh kontrol yang gagal pada seluruh perangkat, seperti AAA new-model, BPDU Guard, Dynamic ARP Inspection, DHCP Snooping, enable secret, local privilege, login banner, port security, SNMPv3 only, storm control, dan VTY ACL. Pola ini menunjukkan bahwa beberapa praktik hardening dasar belum diterapkan secara seragam pada seluruh perangkat Cisco, meskipun Cisco IOS memiliki CIS Benchmark yang paling mapan di antara ketiga vendor. Temuan ini memperkuat pengamatan Athauda (2023) bahwa ketersediaan benchmark keamanan yang lengkap tidak secara otomatis menjamin penerapannya secara konsisten pada perangkat operasional. Dari sudut pandang operasional, kontrol tersebut berkaitan dengan dua area penting, yaitu pengamanan akses administratif dan proteksi Layer 2. Ketidaksesuaian pada area ini perlu diprioritaskan karena dapat berpengaruh terhadap pengendalian akses manajemen dan perlindungan terhadap serangan lokal seperti spoofing, loop, atau flooding.

Pada MikroTik, kontrol yang dominan Fail berkaitan dengan ARP protection, bridge loop protection, disable MAC server, baseline firewall input, SNMPv3 only, dan stateful firewall. Temuan ini menunjukkan bahwa penguatan perangkat MikroTik tidak hanya perlu difokuskan pada akses manajemen, tetapi juga pada pembatasan layanan bawaan dan pengaturan firewall dasar. MikroTik memiliki beberapa layanan manajemen yang dapat memudahkan administrasi, tetapi dalam perspektif hardening layanan tersebut perlu dibatasi sesuai zona jaringan dan kebutuhan operasional.

Pada Ruijie, kontrol yang dominan Fail berkaitan dengan AAA framework, BPDU Guard, DAI, DHCP Snooping, port security/flood control, storm control, dan VTY ACL. Pola ini mirip dengan Cisco pada aspek proteksi Layer 2 dan akses manajemen. Namun, jumlah Fail pada beberapa kontrol lain seperti HTTP/HTTPS management dan SSH version 2 menunjukkan bahwa hardening layanan manajemen juga perlu diperhatikan. Hal ini memperkuat argumen bahwa baseline multi-vendor perlu adaptif terhadap sintaks dan fitur vendor, tetapi tetap mengarah pada tujuan keamanan yang sama — sejalan dengan temuan

Imoukhuede et al. (2025) mengenai perlunya strategi hardening yang disesuaikan dengan karakteristik masing-masing vendor pada lingkungan multivendor.

Makna Dominasi Integrity pada CIA Impact

Dominasi Integrity pada kontrol Fail menunjukkan bahwa sebagian besar ketidaksesuaian baseline berkaitan dengan keutuhan konfigurasi, validitas mekanisme keamanan, dan pencegahan perubahan atau manipulasi yang tidak sah. Dalam konteks perangkat jaringan, Integrity tidak hanya berarti integritas data, tetapi juga mencakup integritas konfigurasi perangkat, integritas proses autentikasi, integritas jalur manajemen, dan integritas mekanisme kontrol trafik. Kontrol seperti AAA, local privilege, DHCP Snooping, DAI, port security, SNMPv3, logging, dan VTY ACL berperan dalam memastikan bahwa konfigurasi dan aktivitas jaringan tidak mudah dimanipulasi oleh pihak yang tidak berwenang. Pola ini sejalan dengan kerangka kontrol keamanan informasi pada NIST SP 800-53 Revisi 5 (National Institute of Standards and Technology, 2020), yang menempatkan integritas konfigurasi sebagai salah satu kontrol inti dalam manajemen keamanan sistem.

Meskipun Integrity menjadi aspek dominan, Confidentiality dan Availability tetap signifikan. Confidentiality muncul pada kontrol yang berkaitan dengan pembatasan akses manajemen, penggunaan protokol aman, dan pengamanan monitoring. Availability muncul pada kontrol Layer 2 dan proteksi gangguan jaringan, seperti BPDU Guard, storm control, loop guard, DHCP Snooping, dan firewall baseline. Dengan demikian, hasil CIA Impact memberikan gambaran bahwa hardening konfigurasi tidak dapat difokuskan pada satu aspek saja. Administrator perlu menyeimbangkan perlindungan akses, keutuhan konfigurasi, dan ketersediaan layanan, sebagaimana ditekankan pula dalam pedoman manajemen konfigurasi berbasis keamanan NIST SP 800-128 (Johnson et al., 2011).

Implikasi Praktis bagi Audit Hardening Jaringan

Framework yang diusulkan dapat digunakan sebagai alat bantu audit berkala pada jaringan multi-vendor. Administrator dapat menjalankan audit dalam satu sesi, memperoleh ringkasan per vendor dan per perangkat, lalu memprioritaskan kontrol yang paling sering gagal. Daftar kontrol dominan yang Fail dapat digunakan sebagai dasar penyusunan roadmap hardening. Misalnya, jika AAA, SNMPv3, dan VTY ACL gagal pada banyak perangkat, maka organisasi dapat memprioritaskan perbaikan akses manajemen; jika DHCP

Snooping, DAI, BPDU Guard, dan storm control gagal pada banyak perangkat, maka prioritas dapat diarahkan pada penguatan Layer 2.

Artifact audit dalam bentuk CSV, grafik, HTML, PDF, dan audit log juga memiliki nilai dokumentasi. CSV memungkinkan analisis lanjutan, grafik memudahkan komunikasi kepada pengambil keputusan, sedangkan audit log membantu penelusuran waktu eksekusi dan status workflow. Penggunaan alias perangkat dan agregasi hasil membuat laporan dapat dibagikan tanpa membuka alamat IP, username, password, secret, SNMP community, atau konfigurasi sensitif. Praktik ini penting karena laporan audit keamanan sering kali memuat informasi yang dapat disalahgunakan apabila dipublikasikan tanpa anonimisasi, sejalan dengan prinsip kehati-hatian yang ditekankan Sasidharan (2022) dalam penerapan audit hardening berbasis CIS Controls pada lingkungan sistem operasi.

Secara ilmiah, hasil penelitian ini memperkuat posisi bahwa audit hardening multi-vendor dapat didekati melalui representasi baseline deklaratif yang dapat dieksekusi ulang, bukan hanya melalui daftar periksa manual. Pendekatan ini membuka peluang integrasi lebih lanjut dengan kerangka policy-as-code sebagaimana diulas Martino et al. (2025), khususnya untuk memperluas cakupan audit ke lingkungan edge dan cloud yang semakin terhubung dengan infrastruktur jaringan konvensional.

Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian ini tidak melakukan audit manual independen sebagai ground truth. Oleh karena itu, penelitian tidak menghitung accuracy, precision, recall, false positive, atau false negative. Hasil Pass dan Fail harus dipahami sebagai keluaran baseline-driven compliance assessment, bukan hasil sertifikasi kepatuhan eksternal.

Kedua, pengujian dilakukan pada satu lingkungan jaringan produksi dengan tiga vend or, sehingga generalisasi ke organisasi lain perlu diuji lebih lanjut. Perangkat, versi sistem operasi, role perangkat, dan kebijakan jaringan dapat memengaruhi hasil audit.

Ketiga, baseline MikroTik dan Ruijie disusun berdasarkan standar keamanan vendor dan adaptasi kontrol umum karena tidak seluruh vendor memiliki CIS Benchmark resmi yang setara dengan Cisco IOS. Hal ini membuat justifikasi rule dan pemetaan CIA Impact perlu terus diperbarui mengikuti perubahan dokumentasi vendor.

Keempat, penelitian ini tidak mencakup vulnerability scanning, penetration testing, traffic analysis, atau remediation automation. Framework menilai kesesuaian konfigurasi terhadap baseline, bukan membuktikan bahwa jaringan telah bebas dari semua kerentanan keamanan.

KESIMPULAN DAN REKOMENDASI

Penelitian ini berhasil merancang, mengimplementasikan, dan mengevaluasi framework otomatisasi audit hardening infrastruktur jaringan berbasis CIS Benchmarks dan standar keamanan vendor. Framework yang dikembangkan terdiri atas modul Collector, Evaluator, dan Report. Collector mengambil konfigurasi aktual melalui SSH, Evaluator membandingkan output perangkat dengan baseline YAML spesifik vendor, sedangkan Report menghasilkan laporan audit dalam bentuk HTML, PDF, CSV, grafik, dan audit log. Prinsip audit-only membuat framework dapat digunakan pada lingkungan produksi tanpa melakukan perubahan konfigurasi otomatis pada perangkat.

Pengujian pada 50 perangkat produksi yang terdiri atas 25 Cisco, 10 MikroTik, dan 15 Ruijie menghasilkan 1.135 kontrol evaluasi. Hasil audit menunjukkan 626 kontrol Pass atau 55,15% dan 509 kontrol Fail atau 44,85%. Satu sesi audit selesai dalam 206 detik dengan seluruh perangkat berhasil diproses pada level perangkat. Analisis CIA Impact menunjukkan bahwa Integrity merupakan aspek paling dominan pada kontrol yang belum memenuhi baseline, diikuti Availability dan Confidentiality. Temuan ini menunjukkan bahwa area autentikasi, otorisasi, validitas konfigurasi, logging, dan proteksi manipulasi trafik perlu menjadi perhatian utama dalam roadmap hardening.

Kontribusi utama penelitian ini adalah penyediaan pendekatan audit hardening konfigurasi multi-vendor yang terstruktur, terdokumentasi, dan adaptif terhadap perbedaan vendor, sekaligus model penerjemahan acuan keamanan multi-sumber ke dalam baseline yang dapat dieksekusi dan dipetakan terhadap dimensi CIA. Pengembangan selanjutnya dapat diarahkan pada validasi manual sebagian hasil audit untuk mengukur akurasi evaluator, penambahan severity scoring, perluasan baseline ke vendor lain, integrasi dengan sistem monitoring keamanan, serta pengembangan remediasi semi-otomatis berbasis persetujuan administrator.

REFERENSI

1. Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), Article 1333. https://doi.org/10.3390/electronics12061333
2. Athauda, I. (2023). Analysis of networking device vulnerabilities and mitigation strategies. ResearchGate. https://doi.org/10.13140/RG.2.2.23992.76800
3. Babaei, A., Kebria, P. M., & Nahavandi, S. (2022). A survey on automation technologies used in network control and management. In 2022 IEEE International Conference on Human-System Interaction (HSI) (pp. 1–6). IEEE. https://doi.org/10.1109/HSI55341.2022.9869444
4. Banerjee, A., Mwanje, S. S., & Carle, G. (2023). Trust and performance in future AI-enabled, open, multi-vendor network management automation. IEEE Transactions on Network and Service Management, 20(2), 995–1007. https://doi.org/10.1109/TNSM.2022.3214296
5. Bringhenti, D., Marchetto, G., Sisto, R., & Valenza, F. (2024). Automation for network security configuration: State of the art and research trends. ACM Computing Surveys, 56(3), 1–37. https://doi.org/10.1145/3616401
6. Center for Internet Security. (2021). CIS benchmarks: Cisco IOS benchmark. Center for Internet Security. https://www.cisecurity.org/cis-benchmarks
7. Cisco Systems. (2023). Cisco IOS security configuration guide. Cisco Systems.
8. Govindappa Venkatesha, G., & Singh, A. (2024). CIS Benchmarks: Enhancing security configurations in multi-cloud infrastructures. IRE Journals, 8(5). https://www.irejournals.com/formatedpaper/1706503.pdf
9. Imoukhuede, A. B., Sheltami, T. R., Mahmoud, A. H., & Barnawi, A. Y. (2025). Optimization of network device hardening in a multivendor environment. Scientific Reports, 15, Article 15042. https://doi.org/10.1038/s41598-025-97894-4
10. Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). Guide for security-focused configuration management of information systems (NIST Special Publication

800-128). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-128

11. Martino, B. D., D'Angelo, S., Pezzullo, G. J., Branco, D., Pelosi, G., Barenghi, A., & Orlando, S. (2025). Review of policy-as-code approaches to manage security and privacy conditions in edge and cloud computing ecosystems. In L. Barolli (Ed.), Advanced Information Networking and Applications (AINA 2025) (Lecture Notes on Data Engineering and Communications Technologies, Vol. 250). Springer. https://doi.org/10.1007/978-3-031-87778-0_32
12. MikroTik. (2024). Securing your router. MikroTik Documentation. https://help.mikrotik.com/docs/display/ROS/Securing+your+router
13. Muhammad, T., & Munir, M. T. (2023). Network automation: A deep dive into modern network automation by using REST APIs. European Journal of Technology, 7(3), 23–42. https://doi.org/10.47672/ejt.1547
14. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
15. Ortiz-Garcés, I., Echeverría, A., & Andrade, R. O. (2021). Automation tasks model for improving hardening levels on campus networks. In 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) (pp. 30–35). IEEE. https://doi.org/10.1109/WorldS451998.2021.9514030
16. Perera, H. M. D. G. V., Samarasekara, K. M., Hewamanna, I. U. K., Kasthuriarachchi, D. N. W., Abeywardena, K. Y., & Yapa, K. (2021). NetBot: An automated router hardening solution for small to medium enterprises. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 15–21). IEEE. https://doi.org/10.1109/IEMCON53756.2021.9623186
17. Ruijie Networks. (2023). Ruijie hardening best practices guide. Ruijie Networks.
18. Santyadiputra, G. S., Listartha, I. M. E., & Saskara, G. A. J. (2021). The effectiveness of Automatic Network Administration (ANA) in network automation simulation at Universitas Pendidikan Ganesha. Journal of Physics: Conference Series, 1810, Article 012028. https://doi.org/10.1088/1742-6596/1810/1/012028

19. Sasidharan, R. (2022). A case study to implement Windows system hardening using CIS Controls. International Journal of Computer Trends and Technology, 70(7), 1–7. https://doi.org/10.14445/22312803/IJCTT-V70I7P101

20. Thati, S. R. (2025). Configuration and compliance automation in modern networks: A framework for enhanced security and operational efficiency. World Journal of Advanced Engineering Technology and Sciences, 15(2), 2513–2519. https://doi.org/10.30574/wjaets.2025.15.2.0613

Proposed Framework for Automating Network Infrastructure Hardening Audits Based on CIS Benchmarks and Vendor Security Standards

ORIGINALITY REPORT

20%	14%	6%	15%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Pamulang Student Paper	6%
2	Submitted to Forum Perpustakaan Perguruan Tinggi Indonesia Jawa Tengah Student Paper	6%
3	journal.thamrin.ac.id Internet Source	4%
4	journalthamrin.com Internet Source	3%

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		