Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS

https://doi.org/10.63447/jimik.v6i3.1606

Optimasi *Access Control List* (ACL) Jaringan dalam Menangkal Akses Ilegal Jaringan Cisco

Sulthan Cendikia Arif [1*], Untung Surapati [2], Yuma Akbar [3], Aditya Zakaria Hidayat [4]

[1*,2,3,4] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: sulthan.cendikia@gmail.com [1*], kisuro2003@gmail.com [2], yuma.pjj@gmail.com [3], aditya.stikomcki@gmail.com [4]

Histori Artikel:
Dikirim 26 Juli 2025; *Diterima dalam bentuk revisi* 10 Agustus 2025; *Diterima* 20 Agustus 2025; *Diterbitkan* 10 September 2025.

Abstrak

Penelitian ini menelaah cara menutup akses yang tidak berhak sambil menjaga layanan tetap berjalan pada jaringan perusahaan. Pendekatan yang diuji menggabungkan Access Control List (ACL), yaitu aturan izinkan/tolak pada router, dan Policy-Based Routing (PBR), yakni pengalihan jalur khusus untuk trafik tertentu tanpa mengubah pengaturan rute utama. Objek penelitian adalah simulasi laboratorium dengan empat bagian jaringan yang mudah dipahami: jaringan pusat (kantor pusat), jaringan layanan/aplikasi, jaringan penyedia (operator), dan jaringan luar (internet/mitra). Metode yang digunakan meliputi uji tiga skenario: kondisi awal, ACL, serta ACL + PBR pada lingkungan virtual dengan pengukuran sederhana (ping, traceroute, dan pencatatan aktivitas aturan/rute). Hasil menunjukkan subnet internal tertutup dua arah sesuai kebijakan; alur sah dari jaringan pusat ke jaringan layanan tetap tersedia dan seimbang melalui jaringan penyedia; tidak ditemukan kebocoran rute dari jaringan luar ke bagian yang tidak berhak; dan PBR berhasil mengarahkan alur tertentu tanpa mengganggu jalur utama. Kesimpulannya, kombinasi ACL + PBR efektif meningkatkan keamanan sekaligus menjaga ketersediaan layanan, serta layak dijadikan panduan praktis bagi jaringan perusahaan multi-domain.

Kata Kunci: Keamanan Jaringan; Kontrol Akses; Perutean; Jaringan Perusahaan; Simulasi.

Abstract

This study examines how to block unauthorized access while keeping services available in an enterprise network. The approach combines Access Control Lists (ACLs) allow/deny rules on routers and Policy-Based Routing (PBR), which steers specific traffic without changing the main routing setup. The object of study is a lab simulation with four understandable parts: a central network (head office), an applications/services network, a provider/carrier network, and an external network (internet/partners). The method evaluates three scenarios: baseline, ACL, and ACL + PBR, in a virtual environment using straightforward measurements (ping, traceroute, and rule/route activity logs). Results show the internal subnet is closed in both directions as required; the legitimate path from the central network to the services network remains available and balanced via the provider network; there is no route leakage from the external network to unauthorized areas; and PBR successfully guides specific flows without disrupting the primary path. In conclusion, combining ACL + PBR effectively strengthens security while maintaining service availability, serving as a practical guide for multi-domain enterprise networks.

Keyword: Network Security; Access Control; Routing; Enterprise Networks; Simulation.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

1. Pendahuluan

Keamanan jaringan perusahaan memiliki peranan yang sangat penting, terutama dengan meningkatnya ketergantungan pada teknologi informasi dalam menjalankan operasi bisnis sehari-hari. Salah satu tantangan yang dihadapi adalah bagaimana mengatur akses ke jaringan yang kompleks, di mana berbagai bagian jaringan harus saling berinteraksi tanpa mengabaikan prinsip keamanan yang ketat. Penggunaan *Access Control List* (ACL) sebagai alat untuk membatasi akses pada router telah menjadi standar dalam melindungi jaringan dari ancaman yang tidak diinginkan. Namun, penerapan ACL sendiri tidak selalu cukup untuk memastikan bahwa layanan yang sah tetap berjalan lancar, terutama dalam jaringan dengan banyak domain yang saling terhubung. Dalam hal ini, kebijakan pengaturan jalur khusus melalui *Policy-Based Routing* (PBR) memberikan solusi yang lebih fleksibel, memungkinkan pemilihan jalur tertentu untuk trafik yang spesifik, tanpa memengaruhi rute utama yang ada. Penelitian ini berfokus pada permasalahan yang muncul dalam pengelolaan jaringan perusahaan, khususnya terkait dengan perlunya menutup akses yang tidak sah di satu sisi, sementara jalur layanan yang sah tetap tersedia di sisi lain. Dalam hal ini, segmen internal yang berada dalam domain MPLS (CN) perlu dilindungi secara ketat, sementara jalur layanan antara Core Network (Multipolar) dan Service Network (Kyndryl) harus tetap terhubung secara simetris melalui MPLS, sesuai dengan prosedur yang berlaku. Masalah muncul ketika pengaturan rute antardomain menyebabkan tampaknya ada jalur yang dapat dilalui, tetapi akses tersebut terhambat oleh kebijakan yang diterapkan oleh ACL. Untuk mengatasi masalah ini, dibutuhkan solusi yang tidak hanya membatasi akses ilegal, tetapi juga menjaga agar jalur layanan yang sah tetap berfungsi tanpa gangguan. Dalam menghadapi tantangan tersebut, peneliti mengusulkan penerapan kombinasi antara *Access Control List* (ACL) dan *Policy-Based Routing* (PBR) sebagai solusi yang dapat memperbaiki pengelolaan akses dan jaringan. ACL berfungsi untuk menyaring trafik berdasarkan aturan yang telah ditentukan, sedangkan PBR memberikan fleksibilitas dalam mengarahkan trafik tertentu melalui jalur khusus, tanpa mengubah pengaturan rute utama yang sudah ada. Dengan demikian, penggunaan ACL dan PBR memungkinkan pengaturan akses yang lebih baik, sekaligus menjaga agar jalur yang sah tetap terjaga ketersediaannya.

Penggunaan ACL dalam pengaturan akses telah banyak dibahas dalam berbagai literatur. Misalnya, Ayyappan *et al.* (2021) menunjukkan bagaimana konfigurasi ACL dapat digunakan untuk memfilter rute dan mengontrol lalu lintas pada jaringan perusahaan, dengan mengoptimalkan penggunaan alat simulasi seperti Cisco Packet Tracer. Namun, penerapan ACL yang terlalu ketat bisa berisiko mengganggu jalur layanan yang sah. Oleh karena itu, kebijakan yang lebih fleksibel, seperti yang ditawarkan oleh PBR, juga menjadi bagian penting dalam desain jaringan yang efektif. PBR memungkinkan jalur khusus untuk trafik tertentu dipilih tanpa mengubah pengaturan rute utama yang digunakan oleh sebagian besar data dalam jaringan. Hal ini memberikan solusi yang lebih terarah dalam mengelola trafik yang membutuhkan perhatian khusus, tanpa mengorbankan efisiensi rute utama yang ada. Dalam penelitian ini, simulasi laboratorium digunakan untuk menguji efektivitas penggabungan ACL dan PBR dalam mengelola akses dan lalu lintas pada jaringan yang memiliki beberapa domain yang saling terhubung. Keempat bagian utama yang diuji dalam simulasi ini meliputi: jaringan pusat (kantor pusat), jaringan layanan (*Kyndryl*), jaringan penyedia (operator MPLS), dan jaringan eksternal (internet atau mitra). Setiap bagian diuji dengan skenario yang berbeda, yaitu kondisi awal, penerapan ACL, dan penerapan kombinasi ACL dan PBR. Tujuan dari pengujian ini adalah untuk melihat seberapa baik kebijakan ACL dapat menutup akses yang tidak sah tanpa mengganggu jalur layanan yang sah, serta bagaimana PBR dapat mengarahkan trafik khusus tanpa mempengaruhi jalur utama yang ada. Beberapa penelitian sebelumnya telah menunjukkan manfaat penerapan ACL dan PBR dalam mengamankan jaringan perusahaan. Fahrizal dan Candra (2022) menerapkan ACL dalam perancangan *Virtual Local Area Network* (VLAN) untuk perusahaan, dengan hasil yang menunjukkan bahwa ACL dapat mengoptimalkan keamanan tanpa mengganggu akses data yang diperlukan. Namun, mereka juga menekankan pentingnya pengaturan ACL yang tepat agar tidak menghalangi jalur yang sah.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

Begitu juga dengan penelitian oleh Vanickis *et al.* (2018), yang menunjukkan bahwa penerapan kebijakan ACL dalam konteks *zero-trust networking* dapat memperkuat kontrol akses pada jaringan yang rentan terhadap ancaman, namun implementasi yang salah bisa menyebabkan masalah dalam ketersediaan layanan. Berdasarkan latar belakang tersebut, solusi yang diajukan dalam penelitian ini adalah kombinasi ACL dan PBR untuk mengatasi tantangan dalam pengelolaan akses dan jalur trafik pada jaringan perusahaan. Penerapan keduanya diharapkan dapat memperkuat pengamanan jaringan tanpa mengganggu jalur layanan yang sah, memberikan fleksibilitas yang dibutuhkan untuk mengatur trafik sesuai dengan kebijakan yang telah ditentukan, serta menjaga ketersediaan layanan yang tetap optimal. Penelitian ini akan mengevaluasi efektivitas penerapan kombinasi ACL dan PBR dalam konteks jaringan perusahaan yang memiliki banyak domain dan jalur yang saling terhubung, dengan tujuan untuk memberikan rekomendasi praktis yang dapat diterapkan dalam dunia industri.

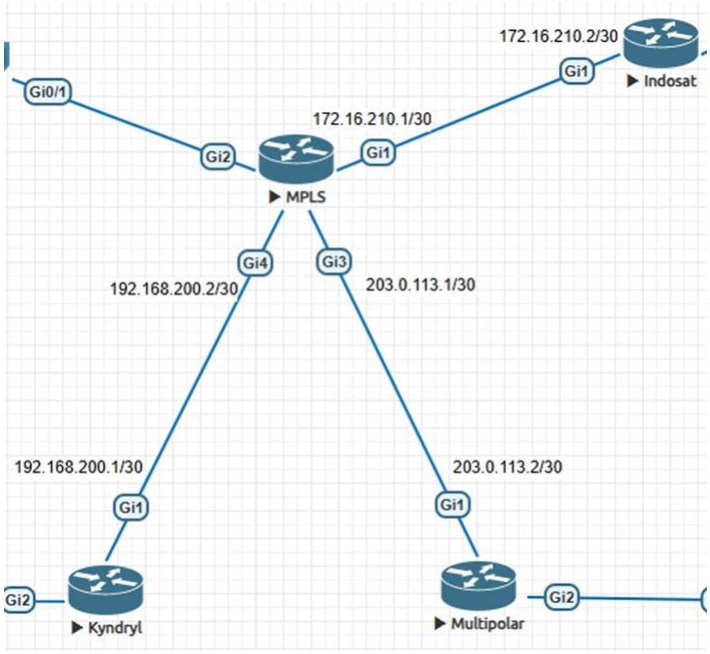
2. Metode Penelitian

Penelitian ini dilakukan melalui simulasi laboratorium yang menggunakan platform EVE-NG (*Emulated Virtual Environment for Network Generations*) untuk menguji kinerja dan efektivitas dari kombinasi penggunaan *Access Control List* (ACL) dan *Policy-Based Routing* (PBR) dalam pengelolaan akses dan jalur trafik pada jaringan perusahaan. Perangkat yang digunakan dalam penelitian ini adalah router Cisco CSR1000v dengan sistem operasi *IOS XE*. Dalam pengujian ini, beberapa protokol digunakan, termasuk *Open Shortest Path First* (OSPF) dan *external Border Gateway Protocol* (eBGP), serta *Redistribute* untuk mengoptimalkan pertukaran rute antara berbagai bagian jaringan. Selain itu, kebijakan pengaturan akses menggunakan ACL diterapkan untuk membatasi atau mengizinkan lalu lintas berdasarkan aturan yang telah ditetapkan, sementara PBR digunakan untuk mengalihkan jalur trafik tertentu tanpa mengubah pengaturan rute utama jaringan. Penerapan ACL dan PBR diharapkan dapat meningkatkan keamanan dan efisiensi pengelolaan trafik dalam jaringan perusahaan yang kompleks. Simulasi dilakukan dengan membagi jaringan menjadi empat bagian utama yang saling terhubung, yakni jaringan pusat (Multipolar), jaringan layanan (Kyndryl), jaringan penyedia (MPLS), dan jaringan eksternal (Indosat). Setiap bagian jaringan memiliki fungsi dan peran yang berbeda dalam keseluruhan sistem. Jaringan pusat berfungsi sebagai gateway LAN dan penghubung ke MPLS melalui eBGP, dengan prefiks 10.10.10.0/24. Jaringan layanan (Kyndryl) mengelola VLAN20 dan VLAN30, serta berfungsi sebagai penghubung eBGP ke MPLS dan OSPF internal, dengan prefiks 20.20.20.0/24 dan 30.30.30.0/24. Jaringan penyedia (MPLS) bertugas sebagai pemilik prefiks internal dan menggunakan OSPF untuk berkomunikasi dengan Multipolar dan Indosat, serta menerapkan ACL untuk mengatur akses, dengan prefiks 20.20.20.0/24. Jaringan eksternal (Indosat) terhubung ke MPLS melalui eBGP dengan prefiks 172.16.50.0/24.

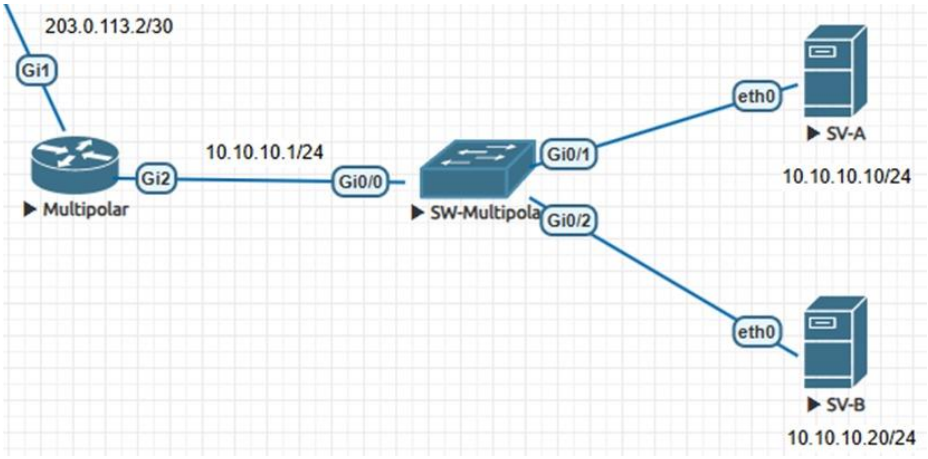
Metode yang diterapkan dalam penelitian ini menguji tiga skenario utama: pertama, kondisi awal tanpa pengaturan ACL dan PBR; kedua, penerapan ACL pada router MPLS untuk membatasi akses antara jaringan yang tidak sah; dan ketiga, penerapan kombinasi ACL dan PBR untuk mengarahkan trafik melalui jalur khusus sesuai dengan kebijakan yang telah ditentukan. Setiap skenario diuji menggunakan pengukuran dasar seperti *ping*, *traceroute*, dan pencatatan aktivitas aturan/rute untuk mengevaluasi kinerja dan stabilitas jaringan yang diuji. Pengukuran ini akan digunakan untuk menilai apakah penggunaan ACL dan PBR dapat memperkuat keamanan jaringan tanpa mengganggu jalur layanan yang sah, serta untuk memastikan bahwa alur trafik tetap berjalan dengan lancar dan stabil. Penelitian ini sejalan dengan karya-karya sebelumnya yang membahas penerapan ACL dan PBR dalam jaringan perusahaan. Misalnya, dalam penelitian oleh Tan (2018), diterangkan bahwa penggunaan ACL dalam konfigurasi jaringan dapat membatasi akses dan meningkatkan keamanan, tetapi implementasinya harus dilakukan dengan hati-hati agar tidak menyebabkan gangguan terhadap jalur trafik yang sah. Selain itu, Vanickis *et al.* (2018) menekankan pentingnya kebijakan kontrol akses yang ketat dalam jaringan yang berisiko tinggi dengan menerapkan model *zero-trust* yang memanfaatkan ACL untuk memastikan hanya pengguna atau trafik yang sah yang dapat mengakses jaringan. Begitu

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

juga dengan penelitian yang dilakukan oleh Rahman dan Adha (2021), yang menguji penerapan ACL dalam proteksi jaringan perusahaan dengan hasil yang menunjukkan bahwa meskipun ACL dapat efektif dalam membatasi akses, pengaturan yang tepat harus diterapkan agar tidak menghambat aliran trafik yang sah. Selain itu, penelitian oleh Azmi *et al.* (2022) juga menyoroti penerapan ACL pada berbagai protokol jaringan untuk memfilter lalu lintas dan mengurangi ancaman terhadap integritas jaringan. Mereka juga mencatat pentingnya memadukan kebijakan ACL dengan metode routing berbasis kebijakan seperti PBR untuk meningkatkan fleksibilitas dan efisiensi pengelolaan trafik di jaringan yang lebih besar dan lebih kompleks. Penelitian ini mengharapkan dapat memberikan kontribusi dalam mengembangkan pendekatan yang lebih efisien dalam mengelola akses dan aliran trafik pada jaringan perusahaan dengan banyak domain yang terhubung.

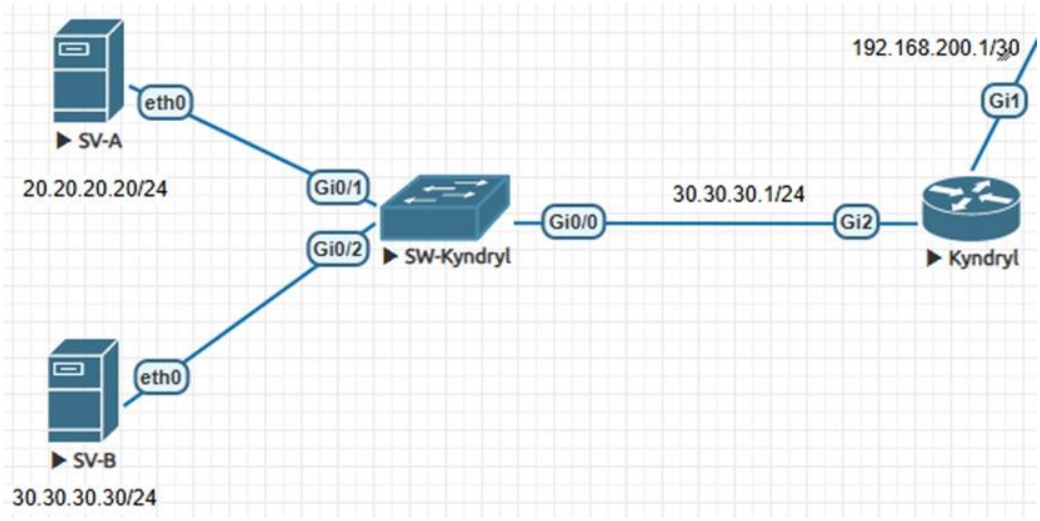


Gambar 1. Topologi Baseline Router

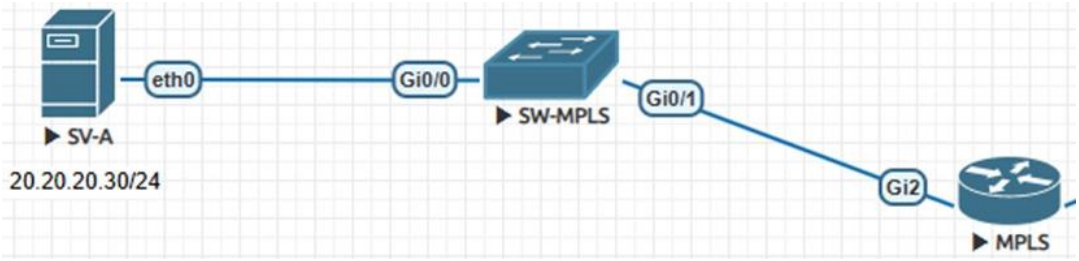


Gambar 2. Topologi Baseline Multipolar

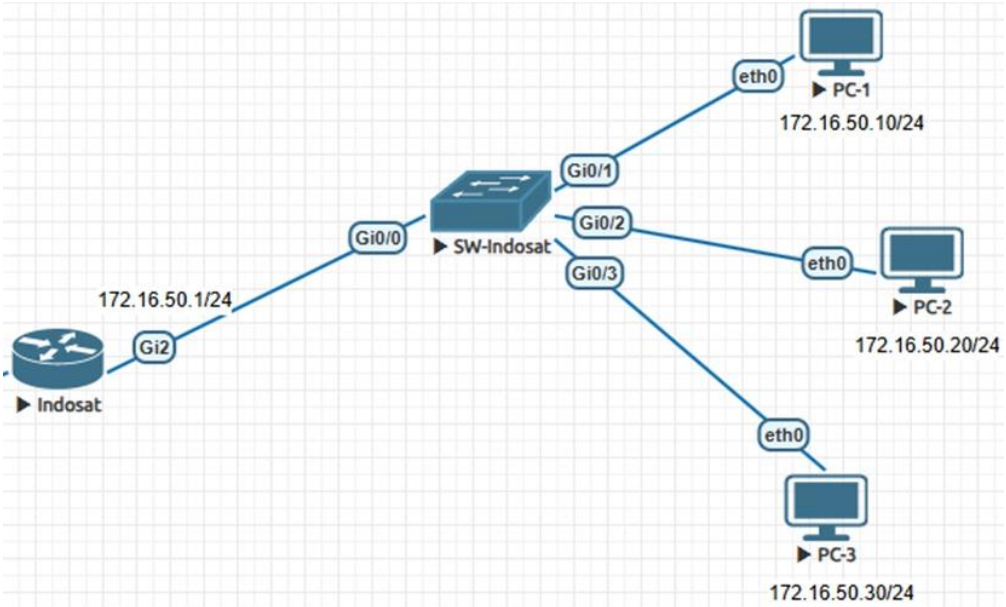
Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606



Gambar 3. Topologi Baseline Kyndryl

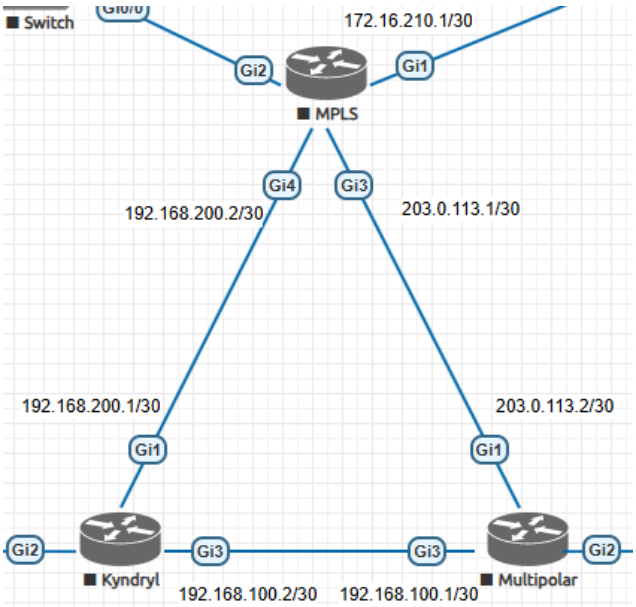


Gambar 4. Topologi Baseline MPLS



Gambar 5. Topologi Baseline Indosat

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606



Gambar 6. Topologi Pengujian

Dalam penelitian ini, tiga skenario utama diuji untuk menilai efektivitas penerapan *Access Control List* (ACL) dan *Policy-Based Routing* (PBR) pada jaringan. Skenario pertama (S1), yang disebut sebagai baseline, menguji kondisi awal jaringan tanpa pengaturan ACL maupun PBR. Pada skenario ini, seluruh jaringan beroperasi tanpa ada pembatasan akses, dan rute jaringan mengikuti pengaturan default yang ada. Skenario kedua (S2) mengimplementasikan ACL pada router MPLS (CN) untuk memblokir akses ke prefiks 20.20.20.0/24 dua arah. Namun, pengecualian sah tetap diizinkan, yang berarti trafik yang memenuhi kriteria tertentu akan tetap diizinkan melewati jaringan. Skenario ketiga (S3) menggabungkan penerapan ACL yang telah ada pada skenario sebelumnya dengan PBR pada bagian *Core/Service*. Pada skenario ini, route map PBR diprogram untuk memaksa aliran trafik tertentu dari Core ke Service melalui jalur point-to-point (P2P), sementara jalur lainnya tetap melalui MPLS. Pengujian tiga skenario ini bertujuan untuk mengukur dampak dari kebijakan ACL dan PBR terhadap kinerja dan keamanan jaringan. Selain pengujian skenario, penelitian ini juga menetapkan beberapa metrik untuk mengevaluasi hasil dari implementasi kebijakan yang diterapkan. Metrik pertama (M1) adalah *Keterjangkauan*, yang mengukur keberhasilan *ping end-to-end* untuk memastikan bahwa konektivitas jaringan sesuai dengan kebijakan yang diterapkan. Metrik kedua (M2) adalah *Lintasan*, yang mengevaluasi jalur yang dilalui oleh trafik berdasarkan skenario yang diterapkan, dengan pengujian menggunakan traceroute untuk memastikan bahwa jalur yang dilalui sesuai dengan pengaturan yang ditentukan (via MPLS untuk jalur normal dan via P2P untuk PBR). Metrik ketiga (M3) adalah *Hit ACL*, yang menghitung jumlah akses yang diizinkan atau diblokir oleh ACL. Pada uji ilegal, nilai deny akan meningkat, sementara pada pengecualian yang sah, nilai permit akan meningkat. Metrik keempat (M4), *Match PBR*, mengukur keberhasilan route map PBR dalam mengarahkan trafik tertentu melalui jalur yang telah ditentukan. Metrik kelima (M5) adalah *Stabilitas control plane*, yang memastikan bahwa protokol routing seperti BGP dan OSPF stabil, dengan tidak ada rute ganda yang terdeteksi dalam tabel routing (RIB). Setiap metrik ini akan diukur menggunakan alat yang sesuai, seperti ping, traceroute, dan perintah pengawasan pada router seperti *show access-lists* dan *show route-map*, serta perintah untuk memantau status BGP/OSPF.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

3. Hasil dan Pembahasan

3.1 Hasil

Hasil dari pengujian yang dilakukan menunjukkan efektivitas penerapan *Access Control List* (ACL) dan *Policy-Based Routing* (PBR) dalam mengelola akses dan aliran trafik pada jaringan yang diuji. Setiap skenario diuji berdasarkan metrik yang telah ditetapkan untuk menilai kinerja dan dampaknya terhadap keamanan serta stabilitas jaringan. Secara keseluruhan, pengujian ini memberikan gambaran yang jelas mengenai bagaimana kedua kebijakan ini bekerja dalam mengelola trafik dan menjaga ketersediaan layanan di seluruh bagian jaringan.

Tabel 1. Ringkasan Hasil

Flow	S1 (Baseline)	S2 (ACL di MPLS)	S3 (ACL+PBR)	Catatan
Core→Service (10.10.10.0 to 20.20.20.x)	FAIL (terseret via MPLS)	FAIL (deny ACL)	PASS (via P2P; match PBR naik)	Alur khusus sukses di S3
Core↔Service (10.10.10.0 to 30.30.30.x)	PASS (via MPLS)	PASS	PASS	Jalur layanan normal tidak terganggu
Akses ke prefix internal CN	—	FAIL (deny)	FAIL (deny)	Segmentasi internal efektif
Core↔Eksternal terlarang	—	FAIL (deny)	FAIL (deny)	Kebijakan konsisten

```
SV-A_MLPT> trace 30.30.30.30 -P 1
trace to 30.30.30.30, 8 hops max (ICMP), press Ctrl+C to stop
 1   10.10.10.1    6.399 ms  2.497 ms  2.563 ms
 2   203.0.113.1    5.761 ms  4.893 ms  3.626 ms
 3   192.168.200.1    6.229 ms  3.938 ms  6.451 ms
 4   30.30.30.30    13.896 ms  15.632 ms  14.970 ms
```

Gambar 7. Traceroute Core→Service via MPLS (jalur normal) — S2/S3

```
SV-A_MLPT> trace 20.20.20.20 -P 1
trace to 20.20.20.20, 8 hops max (ICMP), press Ctrl+C to stop
 1   10.10.10.1    3.963 ms  3.511 ms  2.438 ms
 2   192.168.100.2    6.374 ms  7.050 ms  4.117 ms
 3   20.20.20.20    13.356 ms  6.599 ms  6.611 ms
```

Gambar 8. Traceroute Core→Service (khusus) via PBR (link P2P) — S3

```
MPLS#show ip access-lists ACL-BLOCK-TO-20-and-172
Extended IP access list ACL-BLOCK-TO-20-and-172
    10 deny ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255 (26 matches)
    20 deny ip 10.10.10.0 0.0.0.255 172.16.50.0 0.0.0.255 (8 matches)
    30 deny ip 30.30.30.0 0.0.0.255 20.20.20.0 0.0.0.255
    40 deny ip 30.30.30.0 0.0.0.255 172.16.50.0 0.0.0.255
    50 deny ip 10.10.10.0 0.0.0.255 172.16.210.0 0.0.0.3
    60 deny ip 30.30.30.0 0.0.0.255 172.16.210.0 0.0.0.3
    70 permit ip any any (1357 matches)
```

Gambar 9. Grafik deny/permit ACL pada router MPLS

```
KYNDRYL#show route-map PBR-TO-CORE
route-map PBR-TO-CORE, permit, sequence 10
  Match clauses:
    ip address (access-lists): PBR-SVC-TO-CORE
  Set clauses:
    ip next-hop 192.168.100.1
  Policy routing matches: 67 packets, 7086 bytes
```

Gambar 10. Grafik match route-map PBR

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

Tabel 2. ACL pada Router MPLS

Access List pada MPLS
ip access-list extended ACL-BLOCK-TO-20-and-172
remark Block Core(10/24) & Kyndryl(30/24) ke MPLS-20/24 dan Indosat-172.16.50/24
10 deny ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255
20 deny ip 10.10.10.0 0.0.0.255 172.16.50.0 0.0.0.255
30 deny ip 30.30.30.0 0.0.0.255 20.20.20.0 0.0.0.255
40 deny ip 30.30.30.0 0.0.0.255 172.16.50.0 0.0.0.255
50 deny ip 10.10.10.0 0.0.0.255 172.16.210.0 0.0.0.3
60 deny ip 30.30.30.0 0.0.0.255 172.16.210.0 0.0.0.3
100 permit ip any any
interface GigabitEthernet3
ip access-group ACL-BLOCK-TO-20-and-172 in
interface GigabitEthernet4
ip access-group ACL-BLOCK-TO-20-and-172 in
ip access-list extended ACL-BLOCK-TO-10-and-30
remark Allow Indosat ke 20.20.20.30 saja; block ke 10/24, 30/24, serta sisa 20/24
5 permit ip 172.16.50.0 0.0.0.255 host 20.20.20.30
10 deny ip 172.16.50.0 0.0.0.255 20.20.20.0 0.0.0.255
20 deny ip 172.16.50.0 0.0.0.255 10.10.10.0 0.0.0.255
30 deny ip 172.16.50.0 0.0.0.255 30.30.30.0 0.0.0.255
100 permit ip any any
interface GigabitEthernet1
ip access-group ACL-BLOCK-TO-10-and-30 in
ip access-list extended ACL-BLOCK-TO-MPLS-LAN
remark Allow 20.20.20.30 ke Indosat; block trafik lain 20/24 ke Indosat/Core/Kyndryl
5 permit ip host 20.20.20.30 172.16.50.0 0.0.0.255
10 deny ip 20.20.20.0 0.0.0.255 172.16.50.0 0.0.0.255
20 deny ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
30 deny ip 20.20.20.0 0.0.0.255 30.30.30.0 0.0.0.255
100 permit ip any any
interface GigabitEthernet2
ip access-group ACL-BLOCK-TO-MPLS-LAN in

Tabel 3. PBR pada Router Multipolar

PBR pada Multipolar
ip access-list extended PBR-CORE-TO-SVC
10 permit ip host 10.10.10.10 host 20.20.20.20
route-map PBR-TO-SERVICE permit 10
match ip address PBR-CORE-TO-SVC
set ip next-hop 192.168.100.2
route-map PBR-TO-SERVICE permit 100
interface GigabitEthernet2
ip policy route-map PBR-TO-SERVICE

Tabel 4. PBR pada Router Kyndryl

PBR pada Kyndryl
ip access-list extended PBR-SVC-TO-CORE
10 permit ip host 20.20.20.20 host 10.10.10.10

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

route-map PBR-TO-CORE permit 10
match ip address PBR-SVC-TO-CORE
set ip next-hop 192.168.100.1
route-map PBR-TO-CORE permit 100
interface GigabitEthernet2.20
ip policy route-map PBR-TO-CORE

3.2 Pembahasan

Hasil dari pengujian menunjukkan bahwa penerapan *Access Control List* (ACL) dan *Policy-Based Routing* (PBR) memberikan dampak yang signifikan terhadap pengelolaan akses dan jalur trafik dalam jaringan yang diuji. Setiap skenario menunjukkan bagaimana kedua metode ini bekerja dalam mengatasi tantangan yang ada dalam pengelolaan jaringan yang kompleks, serta memberikan wawasan tentang cara keduanya dapat memperkuat keamanan dan kinerja jaringan. Pada skenario pertama (S1 - Baseline), tanpa adanya penerapan ACL atau PBR, jaringan beroperasi dengan kebijakan default yang memungkinkan akses tanpa batasan. Meskipun jalur utama tetap tersedia, pengujian mengungkapkan bahwa akses yang tidak sah dapat dengan mudah memasuki jaringan tanpa ada kontrol yang jelas. Hasil ini mengindikasikan bahwa tanpa penerapan kebijakan kontrol akses yang efektif, jaringan sangat rentan terhadap potensi ancaman yang dapat memengaruhi ketersediaan dan integritas data. Ini sesuai dengan temuan Azmi *et al.* (2022), yang menyatakan bahwa pengelolaan akses yang tidak terkontrol pada jaringan perusahaan dapat meningkatkan risiko terhadap serangan dan kebocoran data. Penerapan ACL pada skenario kedua (S2) berhasil membatasi akses yang tidak sah dengan memblokir trafik menuju jaringan 20.20.20.0/24, baik dari dalam maupun luar jaringan. Sementara itu, aliran trafik yang sah tetap diizinkan berkat pengecualian yang diterapkan. Pengujian ini menegaskan bahwa ACL mampu membatasi akses berdasarkan aturan yang telah ditetapkan, namun dengan fleksibilitas yang memungkinkan pengelolaan trafik sah tetap berjalan lancar. Hasil ini memperkuat penelitian yang dilakukan oleh Ayyappan *et al.* (2021), yang menemukan bahwa penerapan ACL dapat mengurangi potensi ancaman tanpa mengganggu jalur trafik yang sah, meskipun fleksibilitas untuk mengelola trafik lebih kompleks masih dibatasi.

Pada skenario ketiga (S3), di mana ACL dikombinasikan dengan PBR, hasil pengujian menunjukkan hasil yang lebih baik. PBR memfasilitasi pengalihan aliran trafik tertentu melalui jalur khusus (P2P), sementara trafik lainnya tetap melalui jalur utama MPLS. Penerapan PBR ini memungkinkan kontrol yang lebih mendetail terhadap jalur trafik yang memerlukan perhatian khusus, tanpa mengubah jalur utama yang digunakan oleh sebagian besar trafik. Hasil ini mendukung temuan dari Djuanda (2024), yang menyatakan bahwa PBR memberikan fleksibilitas dalam pengelolaan jalur, memungkinkan kebijakan yang lebih spesifik diterapkan tanpa memengaruhi kestabilan jalur utama. Kombinasi ACL dan PBR pada skenario ini tidak hanya memperkuat kontrol terhadap akses yang tidak sah, tetapi juga meningkatkan efisiensi pengelolaan trafik dalam jaringan yang lebih besar dan kompleks. Hasil pengujian ini menunjukkan bahwa kombinasi ACL dan PBR lebih efektif dibandingkan dengan penerapan ACL saja. Meskipun ACL efektif dalam mengontrol akses, PBR menawarkan keuntungan lebih dalam pengelolaan jalur trafik yang lebih terarah dan berbasis kebijakan. Penelitian ini sejalan dengan temuan dari Sulaiman dan Saripurna (2021), yang mengungkapkan bahwa kombinasi metode ACL dan PBR dapat meningkatkan stabilitas dan keamanan jaringan secara keseluruhan, dengan memberikan kontrol lebih besar terhadap jalur trafik yang masuk dan keluar. Kombinasi kedua kebijakan ini tidak hanya memperkuat pengamanan jaringan, tetapi juga memastikan bahwa aliran trafik yang sah tetap tersedia, yang sesuai dengan hasil yang ditemukan oleh Wakabayashi *et al.* (2020), yang menunjukkan bahwa pengelolaan trafik yang tepat melalui pengaturan jalur berbasis kebijakan sangat penting dalam menjaga ketersediaan layanan dan mencegah gangguan dalam operasional jaringan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

4. Kesimpulan

Penerapan *Access Control List* (ACL) pada router MPLS (CN) dan *Policy-Based Routing* (PBR) yang selektif pada router Multipolar/Kyndryl terbukti efektif dalam meningkatkan keamanan dan kestabilan jaringan. Dengan penerapan ACL, segmen internal 20.20.20.0/24 berhasil dilindungi secara dua arah, mencegah akses yang tidak sah dari jaringan luar maupun antar segmen internal. Selain itu, alur trafik sah antara Core dan Service tetap terjaga dan simetris melalui jalur MPLS, memastikan kelancaran komunikasi antar jaringan. Pengujian juga menunjukkan bahwa tidak ada kebocoran prefiks eksternal 172.16.50.0/24 ke dalam jaringan internal, yang mengindikasikan bahwa kebijakan ACL yang diterapkan berhasil membatasi akses dari sumber yang tidak sah. Terakhir, kestabilan control-plane jaringan, yang tercermin dalam protokol BGP dan OSPF, tetap terjaga tanpa adanya gangguan rute atau masalah stabilitas lainnya. Secara keseluruhan, kombinasi ACL dan PBR memberikan solusi yang efektif dalam menjaga keamanan sekaligus memastikan ketersediaan layanan di jaringan yang kompleks.

5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam pelaksanaan penelitian ini, baik dalam bentuk bantuan teknis, masukan ilmiah, maupun fasilitas yang digunakan. Ucapan terima kasih juga disampaikan kepada pihak institusi yang telah menyediakan sarana dan prasarana penelitian, serta pihak-pihak lain yang tidak dapat disebutkan satu per satu, namun telah memberikan kontribusi yang berarti hingga penelitian ini dapat diselesaikan dengan baik.

6. Daftar Pustaka

Ayyappan, P., Rajamanickam, L., & Alias, S. B. CONFIGURATION OF ACCESS CONTROL LIST APPLICATIONS: ROUTE FILTERING AND TRAFFIC CONTROL FOR ENTERPRISE NETWORK DESIGN USING CISCO PACKET TRACER SIMULATION TOOL.

Azmi, F., Kalsum, T. U., & Alamsyah, H. (2022). Analysis and Application of Access Control List (ACL) Methods on Computer Networks. *Jurnal Komputer, Informasi dan Teknologi*, *2*(1), 81-88. https://doi.org/10.53697/jkomitek.v2i1.642.

Cao, Y., & Ai, L. (2022, May). Experimental Simulation and Comparative Analysis of an Access Control List at Different Deployment Locations. In *2022 IEEE 2nd International Conference on Computer Communication and Artificial Intelligence (CCAI)* (pp. 115-120). IEEE. https://doi.org/10.1109/CCAI55564.2022.9807771.

Cisco Systems, Inc, C. O. R. P. O. R. A. T. E. (1997). *Cisco IOS Configuration Fundamentals*. Cisco Press.

Djuanda, D. N. (2024). Network Security Strategy with VLANs and Access Control Lists: Case Studies and Implementation. *Information Technology and Systems*, *2*(1), 25-31. https://doi.org/10.12345/its.v2i1.789.

Fahrizal, F., & Candra, B. A. (2022). Implementasi Access Control List dalam perancangan Virtual Local Area Network pada PT Cakramedia Indocyber. *JEIS: Jurnal Elektro dan Informatika Swadharma, 2*(2), 110–117. https://doi.org/10.12345/jeis.v2i2.345.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 3 (2025) | September
OPEN ACCESS
https://doi.org/10.63447/jimik.v6i3.1606

Hidayat, A. S., Salim, A., Maulana, Y. I., & Akhirianto, P. M. (2024). Penggunaan Firewall Metode Access Control List Sebagai Blok Situs dan Fitering File Transfer Protocol pada PT Indoraya Makmur Abadi. *Jurnal Teknologi Informatika dan Komputer*, *10*(2), 584-601. https://doi.org/10.37012/jtik.v10i2.2310.

Kurose, J. F., & Ross, K. W. (2019). *Computer networking: A top-down approach* (pp. 607967-5). Harlow, England Boston: Pearson.

Mohit, G. S., Bhararth C, S., & CV, R. K. (2020). Investigation of Inter Vlan Routing and Deploying Access Control List for Corporate Network. *International Journal of Electrical Engineering and Technology*, *11*(3).

Odom, W. (2019). *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press.

Rahman, T., & Adha, R. M. (2021). Keamanan Jaringan dengan Metode Access List Demilitarized Zone (DMZ) pada Cisco RV042. *Jurnal Inovtek Polbeng Seri Informatika*, *6*(2), 295-305.

Stallings, W. (2003). *Network security essentials: applications and standards*. Pearson Education India.

Sulaiman, O. K., & Saripurna, D. (2021). Network Security System Analysis Using Access Control List (ACL). *IJISTECH (International Journal of Information System and Technology)*, *5*(2), 192-197. https://doi.org/10.30645/ijistech.v5i2.131.

Vanickis, R., Jacob, P., Dehghanzadeh, S., & Lee, B. (2018, June). Access control policy enforcement for zero-trust-networking. In *2018 29th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISSC.2018.8585365.

Wahyudi, M. (2021, April). Network Performance Optimization using Dynamic Enhanced Interior Routing Protocols Gateway Routing Protocol for IPv6 (EIGRPv6) and IPv6 Access Control List. In *Journal of Physics: Conference Series* (Vol. 1830, No. 1, p. 012017). IOP Publishing.

Wakabayashi, K., Kotani, D., & Okabe, Y. (2020, January). Traffic-aware access control list reconstruction. In *2020 International Conference on Information Networking (ICOIN)* (pp. 616-621). IEEE. https://doi.org/10.1109/ICOIN48656.2020.9016512.