Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Analisis Perbandingan Implementasi RPKI di Edge Router dan Route Reflector (BIRD) untuk Mitigasi BGP Hijacking dengan Monitoring Berbasis Grafana

Irfan Kurnia [1]*, Antoni Haikal [2]**
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
irfankurnia03ex@gmail.com [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

BGP Hijack, RPKI, BIRD, MikroTik, Grafana.

ABSTRACT

Border Gateway Protocol (BGP) tidak memiliki mekanisme autentikasi bawaan untuk memverifikasi keaslian pengumuman rute, sehingga rentan terhadap serangan BGP hijacking yang dapat mengakibatkan pengalihan lalu lintas jaringan ke jalur yang tidak semestinya dan berpotensi mengganggu layanan jaringan. Resource Public Key Infrastructure (RPKI) dikembangkan sebagai mekanisme keamanan berbasis kriptografi untuk memitigasi BGP hijacking melalui Route Origin Validation (ROV). Penelitian ini menganalisis perbandingan implementasi RPKI pada Edge Router (MikroTik) dan Route Reflector (BIRD) pada lingkungan simulasi jaringan ISP berbasis virtualisasi menggunakan tiga skenario pengujian dengan variasi 500, 1.000, dan 5.000 prefix. Seluruh data penggunaan sumber daya dan status validasi prefix selama pengujian divisualisasikan menggunakan Grafana berbasis Prometheus. Hasil pengujian menunjukkan bahwa kedua implementasi berhasil memblokir seluruh prefix invalid dan mengarahkan traffic client menuju prefix valid sehingga serangan BGP hijacking berhasil dimitigasi. Terdapat perbedaan pada lokasi filtering, di mana implementasi RPKI di Edge Router memblokir prefix invalid pada titik ingress sebelum masuk ke routing table sehingga prefix invalid tidak pernah diteruskan ke jaringan internal, sedangkan implementasi di route reflector memfilter prefix invalid secara terpusat pada BIRD dengan Edge Router masih menerima prefix invalid sebelum difilter. Dari sisi penggunaan sumber daya, selisih penggunaan CPU Edge Router akibat penerapan RPKI berkisar antara 0,20% hingga 0,80%, lebih kecil dibandingkan BIRD yang berkisar antara 1,00% hingga 3,80%. Selisih penggunaan memori Edge Router berkisar antara 1,00 MB hingga 1,98 MB, lebih besar dibandingkan selisih penggunaan memori BIRD yang berkisar antara 0,02 MB hingga 0,15 MB. Hasil penelitian ini memberikan gambaran empiris bagi administrator jaringan dalam memilih lokasi implementasi RPKI yang sesuai berdasarkan arsitektur dan kebutuhan skalabilitas jaringan.

This is an open access article under the CC–BY-SA license.

I. PENDAHULUAN

Border Gateway Protocol (BGP) merupakan protokol routing inter-domain yang digunakan pada jaringan Internet, bekerja sebagai protokol path vector yang bertanggung jawab dalam mempertukarkan informasi ketercapaian jaringan antar Autonomous System (AS) [1]. Namun, BGP tidak memiliki mekanisme keamanan untuk memvalidasi pembaruan rute, sehingga membuka peluang terjadinya serangan routing termasuk BGP hijacking [2]. BGP hijacking merupakan serangan berupa pengumuman rute yang tidak sah pada protokol BGP yang memungkinkan lalu lintas jaringan dialihkan menuju AS yang tidak berwenang [3], dengan dampak meliputi traffic interception, traffic blackholing, serta terganggunya layanan jaringan [4]. Salah satu insiden yang banyak dijadikan referensi adalah kasus Pakistan Telecom pada tahun 2008, di mana Pakistan

e-ISSN: 2548-6861

Telecom (AS17557) secara keliru mengumumkan prefix 208.65.153.0/24 yang kemudian dipropagasikan ke seluruh Internet dan menyebabkan pengalihan lalu lintas YouTube dalam skala global [5].

Sebagai solusi terhadap kelemahan autentikasi pada BGP, dikembangkan Resource Public Key Infrastructure (RPKI), yaitu sistem keamanan berbasis kriptografi untuk memverifikasi kepemilikan prefix IP dan ASN [6]. Komponen utamanya adalah Route Origin Authorization (ROA), yang menghasilkan Validated ROA Payload (VRP) untuk menentukan status valid, invalid, atau unknown terhadap suatu prefix [7]. Saat ini mayoritas rute IPv4 global telah tercakup ROA dan propagasi rute invalid menurun sekitar 24% sejak awal tahun 2022 [8], namun implementasi ROV masih belum diterapkan secara konsisten pada seluruh jaringan Internet karena masih terdapat AS yang meneruskan trafik menuju origin invalid [9].

Berbagai penelitian sebelumnya menunjukkan bahwa RPKI mampu meningkatkan keamanan routing BGP. Iryani et al. membuktikan bahwa RPKI mampu memfilter rute tidak valid dengan tambahan penggunaan CPU sebesar 3,6% dan memori sebesar 0,75% [10]. Pranaya dan Wellem menunjukkan bahwa implementasi RPKI menggunakan BIRD mampu membatasi propagasi prefix invalid dalam jaringan internal AS [6], sedangkan Rahayu dan Suharjo membuktikan bahwa RPKI pada MikroTik RouterOS v7 mampu menolak prefix invalid dari jaringan eksternal [11]. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada implementasi RPKI pada satu titik arsitektur jaringan secara terpisah, sehingga belum ditemukan penelitian yang membandingkan implementasi RPKI pada Edge Router dan Route Reflector dalam satu lingkungan simulasi dengan parameter pengujian yang identik. Perlu dicatat bahwa yang dimaksud identik pada penelitian ini adalah infrastruktur, topologi, dan parameter pengujian, bukan kesetaraan platform perangkat lunak routing, mengingat kedua lokasi implementasi menggunakan perangkat lunak yang secara arsitektural berbeda (MikroTik RouterOS dan BIRD).

Dalam arsitektur jaringan ISP, Edge Router berfungsi sebagai titik ingress yang menerima route dari jaringan eksternal melalui eBGP, sedangkan Route Reflector mendistribusikan informasi routing kepada router internal melalui iBGP. BIRD merupakan salah satu perangkat lunak routing yang mendukung implementasi BGP dan integrasi dengan validator RPKI [6]. Perbedaan lokasi implementasi RPKI pada kedua titik tersebut berpotensi memengaruhi proses penerimaan, propagasi, dan pemilihan route dalam jaringan. Selain itu, pemantauan kondisi jaringan diperlukan untuk mengamati perubahan status validasi prefix dan kinerja perangkat selama pengujian berlangsung, di mana Prometheus digunakan untuk mengumpulkan metrik penggunaan sumber daya dan Grafana untuk memvisualisasikannya dalam bentuk dashboard monitoring secara real-time [12][13].

Penelitian ini menganalisis perbandingan implementasi RPKI pada Edge Router (MikroTik) dan Route Reflector (BIRD) untuk mitigasi BGP hijacking menggunakan lingkungan simulasi jaringan ISP berbasis virtualisasi dengan tiga skenario pengujian. Selain membandingkan kemampuan kedua implementasi dalam memblokir prefix invalid dan memengaruhi jalur forwarding traffic, penelitian ini juga memanfaatkan Grafana sebagai media visualisasi monitoring untuk menampilkan penggunaan sumber daya perangkat serta perubahan status validasi prefix selama proses pengujian berlangsung. Hasil penelitian ini diharapkan dapat memberikan gambaran empiris mengenai pengaruh lokasi implementasi RPKI terhadap proses validasi prefix, propagasi route, dan jalur forwarding traffic pada arsitektur routing jaringan Internet Service Provider (ISP).

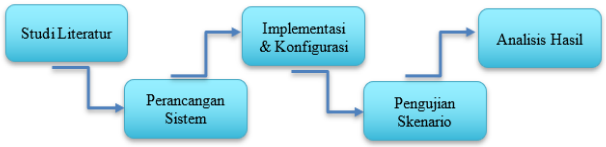
II. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif komparatif untuk membandingkan hasil implementasi RPKI pada Edge Router dan Route Reflector. Evaluasi dilakukan melalui serangkaian pengujian terkontrol dengan pengukuran parameter yang telah ditentukan, kemudian hasil pengujian dianalisis secara kuantitatif untuk mengetahui perbedaan karakteristik dari masing-masing skenario. Metode serupa juga digunakan pada penelitian sistem keamanan berbasis cloud yang melakukan pengujian dan analisis kuantitatif terhadap performa sistem berdasarkan beberapa parameter pengukuran [14]. Metode ini dipilih karena tujuan utama penelitian adalah membuktikan apakah lokasi penerapan RPKI/ROV memengaruhi kemampuan memblokir prefix invalid serta dampaknya terhadap beban sistem.

Perlu ditegaskan bahwa perbandingan dalam penelitian ini dilakukan pada tingkat lokasi arsitektur implementasi, bukan perbandingan platform routing yang setara secara langsung. Proses validasi pada kedua skenario dieksekusi pada perangkat lunak routing yang berbeda, yaitu MikroTik RouterOS pada Edge Router dan BIRD pada Route Reflector, sehingga perbedaan arsitektur internal dan mekanisme kerja masing-masing platform turut melekat pada hasil setiap skenario. Untuk menjaga validitas perbandingan pada tingkat arsitektur, kedua skenario tetap diuji di atas infrastruktur virtual, topologi, dan spesifikasi perangkat keras yang identik, sehingga variabel di luar perbedaan lokasi implementasi dan platform routing dapat dikendalikan seminimal mungkin.

Pengujian dilakukan sebanyak lima kali pengulangan pada setiap skenario untuk mengurangi pengaruh fluktuasi penggunaan sumber daya pada lingkungan

virtualisasi, dengan nilai yang digunakan merupakan rata-rata dari seluruh percobaan. Pengukuran dilakukan menggunakan parameter uji yang sama pada infrastruktur virtual dan topologi yang identik agar kinerja kedua skenario dapat dibandingkan secara langsung. Urutan kerja penelitian ditunjukkan pada Gambar 1, mulai dari studi literatur, perancangan sistem, implementasi dan konfigurasi, pengujian skenario, hingga analisis hasil.



Gambar 1. Alur Penelitian

A. Studi Literatur

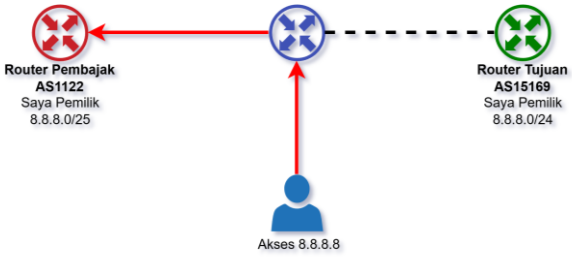
Pada bagian ini akan dijelaskan beberapa konsep dasar yang terkait dengan penelitian ini.

1) BGP

Border Gateway Protocol (BGP) merupakan protokol inter-domain standar Internet yang bertanggung jawab dalam pertukaran informasi ketercapaian jaringan (Network Reachability Information/NRI) antar Autonomous System (AS) [1]. BGP bekerja dengan mempertukarkan informasi ketercapaian jaringan melalui mekanisme route advertisement antar-AS. Sebagai protokol path vector, BGP menyertakan informasi AS-path pada setiap pengumuman rute sehingga dapat digunakan untuk menghindari terjadinya routing loop [15]. Informasi rute tersebut mencakup jumlah AS yang berada dalam jalur penyampaian informasi, sehingga memungkinkan pembentukan grafik koneksi antar-AS untuk menghindari routing loop [15]. Selain itu, BGP mendukung penerapan kebijakan routing (policy routing) yang ditentukan oleh administrator jaringan dalam proses pemilihan jalur antar-AS [15]. Meskipun efektif dalam menjaga konektivitas Internet global, BGP tidak memiliki mekanisme autentikasi bawaan untuk memverifikasi keaslian pengumuman rute [1]. Kondisi ini menyebabkan BGP rentan terhadap kesalahan konfigurasi maupun serangan yang dikenal sebagai BGP hijacking [2].

2) BGP Hijacking

BGP hijacking merupakan kondisi ketika suatu Autonomous System (AS) mengumumkan prefix yang bukan miliknya sehingga lalu lintas jaringan dapat dialihkan ke jalur yang tidak semestinya [16]. Bentuk umum serangan ini terjadi ketika sebuah AS secara salah mengumumkan dirinya sebagai origin bagi suatu prefix, padahal AS tersebut tidak menyediakan konektivitas data yang sebenarnya untuk prefix tersebut [16]. Serangan ini dapat menimbulkan berbagai dampak, seperti traffic blackholing, traffic interception, penyadapan data, maupun gangguan layanan jaringan [4]. Traffic blackholing terjadi ketika lalu lintas jaringan dibuang sehingga tidak pernah mencapai tujuan, sedangkan traffic interception terjadi ketika lalu lintas korban dialihkan oleh AS penyerang sebelum diteruskan kembali ke tujuan yang sebenarnya [4]. Sejumlah insiden nyata telah menunjukkan bahwa BGP hijacking dapat menimbulkan dampak dalam skala global [4]. Kondisi tersebut menunjukkan bahwa tanpa mekanisme validasi, BGP tidak dapat menjamin keaslian pengumuman rute yang diterima [4]. Ilustrasi BGP hijacking ditunjukkan pada Gambar 2, dimana Router Pembajak mengumumkan prefix yang sebenarnya dimiliki oleh Router Tujuan sehingga lalu lintas dari pengguna menuju prefix tersebut dialihkan ke jalur yang salah.



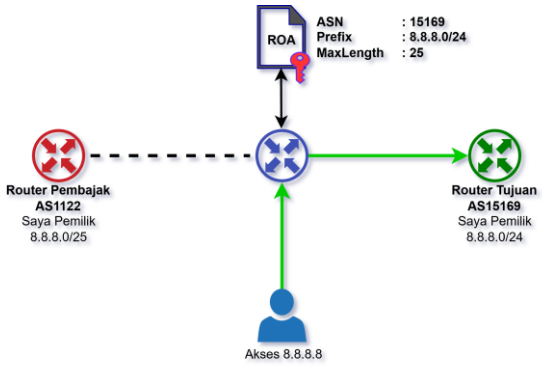
Gambar 2. Ilustrasi BGP Hijack tanpa RPKI

3) Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure (RPKI) merupakan sistem yang digunakan untuk mengamankan infrastruktur routing Internet. Salah satu komponen utama dalam RPKI adalah Route Origin Authorization (ROA), yaitu objek yang menghubungkan blok alamat IP dengan Autonomous System Number (ASN) yang berhak mengumumkan blok alamat tersebut. Dalam implementasinya, validator seperti Routinator melakukan validasi terhadap objek RPKI yang tersedia untuk menghasilkan status validasi berupa valid, invalid, atau unknown/not found. Informasi hasil validasi tersebut selanjutnya dapat digunakan oleh router untuk memverifikasi keabsahan pengumuman rute yang diterima [6].

Penerapan RPKI memungkinkan proses filtering terhadap rute yang tidak valid sehingga routing diarahkan hanya pada rute yang valid [10]. Selain itu, mayoritas rute IPv4 global telah tercakup oleh Route Origin Authorization (ROA), sementara propagasi rute invalid menurun sekitar 24% sejak awal tahun 2022 [8]. Meskipun demikian, penerapan Route Origin Validation (ROV) masih belum dilakukan secara luas pada seluruh Autonomous System (AS), sehingga propagasi prefix invalid masih berpotensi terjadi pada sebagian jaringan Internet [9]. Mekanisme penerapan RPKI dalam proses validasi pengumuman route ditunjukkan pada Gambar 3.

e-ISSN: 2548-6861



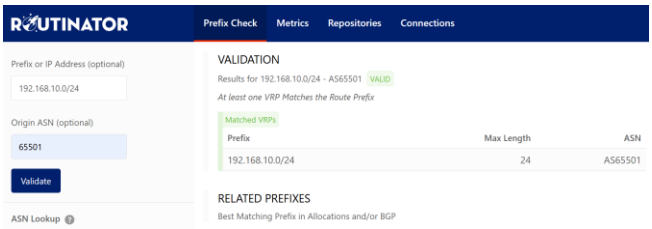
Gambar 3. Ilustrasi BGP Hijack dengan RPKI

4) Route Origin Validation (ROV)

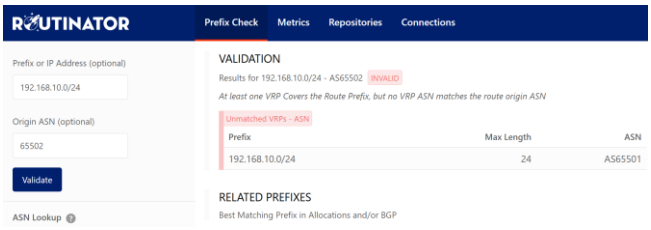
Route Origin Validation (ROV) merupakan proses validasi pengumuman prefix menggunakan data Resource Public Key Infrastructure (RPKI) untuk menentukan keabsahan asal suatu rute. Proses ini dilakukan dengan membandingkan informasi prefix dan Autonomous System (AS) yang mengumumkan route terhadap data Route Origin Authorization (ROA) yang tersedia [6][7].

Hasil validasi ROV terdiri atas tiga status utama, yaitu valid, invalid, dan unknown/not found. Status valid menunjukkan bahwa terdapat data ROA yang sesuai dengan prefix dan AS yang mengumumkan route. Status invalid menunjukkan bahwa terdapat data ROA yang mencakup prefix tersebut, tetapi tidak sesuai dengan informasi yang diumumkan. Sementara itu, status unknown menunjukkan bahwa tidak ditemukan data ROA yang dapat digunakan untuk memvalidasi prefix tersebut [7].

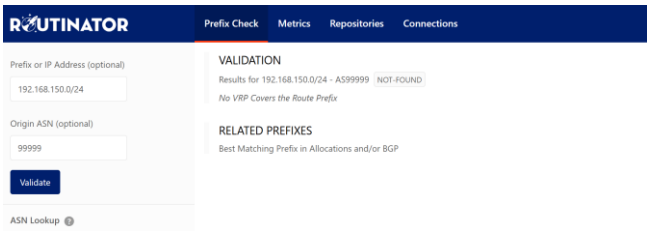
Dalam implementasinya, router memperoleh informasi hasil validasi melalui Validated ROA Payload (VRP) yang dihasilkan oleh validator RPKI, seperti Routinator. Informasi tersebut digunakan untuk menentukan status validasi prefix sebelum route diproses lebih lanjut oleh router [6][7]. Contoh proses validasi prefix menggunakan Routinator ditunjukkan pada Gambar 4, 5, dan 6.



Gambar 4. Tampilan Routinator prefix valid



Gambar 5. Tampilan Routinator prefix invalid



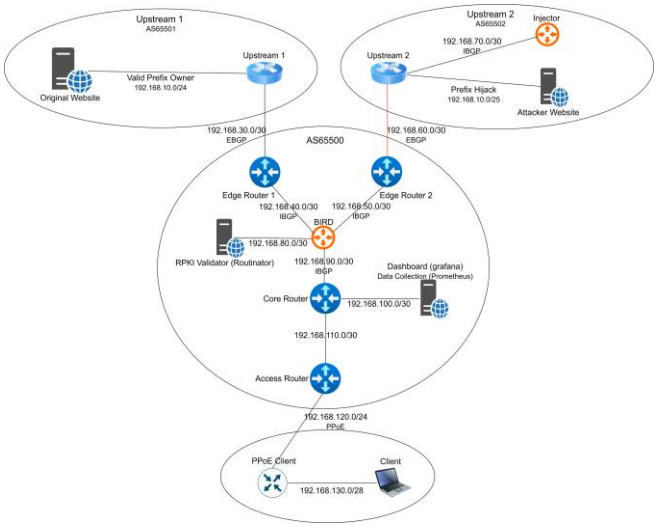
Gambar 6. Tampilan Routinator prefix unknown

B. Perancangan Sistem

Tahap ini merupakan proses perancangan dari keseluruhan lingkungan simulasi yang akan dibangun. Rancangan ini adalah fondasi teknis untuk melakukan eksperimen perbandingan dua model implementasi RPKI.

1) Arsitektur Jaringan

Arsitektur yang digunakan merepresentasikan tiga Autonomous System (AS) yang saling terhubung melalui BGP: dua AS Upstream (Upstream 1 – AS65501 dan Upstream 2 – AS65502), satu AS ISP (AS65500) yang menjalankan domain iBGP (edge–core–access) dengan BIRD sebagai route-reflector, Routinator sebagai validator RPKI (RTR), serta Grafana untuk monitoring. Topologi bisa dilihat pada Gambar 7.



Gambar 7. Topologi Pengujian

Penelitian ini menguji dua model penempatan kebijakan:

- Model 1 – Validasi di Edge Router : MikroTik melakukan validasi menggunakan VRP dari Routinator kemudian memfilter prefix sesuai kebijakan routing, kemudian disebarkan ke router internal.
- Model 2 – Validasi di BIRD : BIRD menerima prefix dari Edge Router, kemudian BIRD melakukan validasi menggunakan VRP dari Routinator sebelum mendistribusikan ke router lain melalui iBGP.

2) Spesifikasi Perangkat Keras dan Lunak

Penelitian dilakukan menggunakan dua perangkat, yaitu satu laptop dan satu PC, dengan spesifikasi perangkat sebagaimana ditunjukkan pada Tabel I, Tabel II, dan Tabel III.

Komponen	Spesifikasi
Perangkat Utama	Laptop Lenovo Model 82TT
Prosesor (CPU)	Intel® Core™ i5-1235U (12th Gen, 12 CPUs)
Memori (RAM)	16 GB DDR4
Penyimpanan	SSD 512 GB
Sistem Operasi Host	Windows 11 Home Single Language

Tabel I. Spesifikasi Laptop

Komponen	Spesifikasi
Perangkat Utama	PC Lenovo Model 12CEA03FID
Prosesor (CPU)	Intel® Core™ i3-1215U (12th Gen, 8 CPUs)
Memori (RAM)	8 GB DDR4
Penyimpanan	SSD 512 GB
Sistem Operasi Host	Windows 11 Home Single Language

Tabel II. Spesifikasi PC

Komponen	Versi
MikroTik CHR	RouterOS v7.22
BIRD	2.14
Routinator	0.15.1
Ubuntu Server	24.04.1 LTS
Prometheus	2.45.3
Grafana	13.0.1
Apache	2.4.58
VMware Workstation	16 Pro

Tabel III. Spesifikasi Perangkat Lunak

C. Implementasi & Konfigurasi

Implementasi sistem dilakukan pada lingkungan virtual menggunakan VMware Workstation yang dijalankan pada satu laptop dan satu PC. Topologi jaringan terdiri dari web server, upstream router, edge router, route reflector berbasis BIRD, validator Routinator, router internal, injector, dan client yang digunakan untuk pengujian propagasi route dan forwarding trafik.

Seluruh router pada topologi penelitian menggunakan MikroTik RouterOS v7, kecuali injector dan route reflector yang menggunakan BIRD Internet Routing Daemon (BIRD). Edge router membangun sesi eBGP dengan upstream router serta sesi iBGP dengan route reflector untuk mendistribusikan route ke jaringan internal.

Pada skenario implementasi RPKI di Edge Router, proses Route Origin Validation (ROV) dilakukan pada Edge Router menggunakan data Validated ROA Payload (VRP) yang diperoleh dari Routinator melalui protokol RTR (RPKI-to-Router). Prefix dengan status invalid difilter sebelum didistribusikan ke router internal.

Pada skenario implementasi RPKI terpusat, Edge Router menerima pengumuman prefix dari Upstream Router melalui sesi eBGP dan meneruskannya ke BIRD melalui sesi iBGP. Selanjutnya, BIRD diimplementasikan sebagai Route Reflector sekaligus melakukan proses ROV menggunakan data VRP dari Routinator sebelum mendistribusikan route hasil validasi ke Router Internal.

Routinator digunakan sebagai validator RPKI untuk memproses data Route Origin Authorization (ROA) dan menghasilkan VRP yang digunakan dalam proses validasi prefix pada router. Selain itu, Prometheus digunakan untuk mengumpulkan data performa perangkat jaringan, sedangkan Grafana digunakan untuk menampilkan visualisasi monitoring selama proses pengujian berlangsung.

Implementasi monitoring dilakukan untuk mengamati penggunaan CPU, memori, stabilitas sesi BGP, serta propagasi prefix selama simulasi BGP hijacking dilakukan.

D. Pengujian Skenario

Pengujian skenario dilakukan untuk membandingkan implementasi Resource Public Key Infrastructure (RPKI) pada Edge Router dan Route Reflector (BIRD) dalam mitigasi BGP hijacking, menggunakan topologi dan parameter yang sama pada setiap skenario. Skenario terdiri dari tiga kondisi utama, yaitu tanpa implementasi RPKI, implementasi RPKI pada Route

e-ISSN: 2548-6861

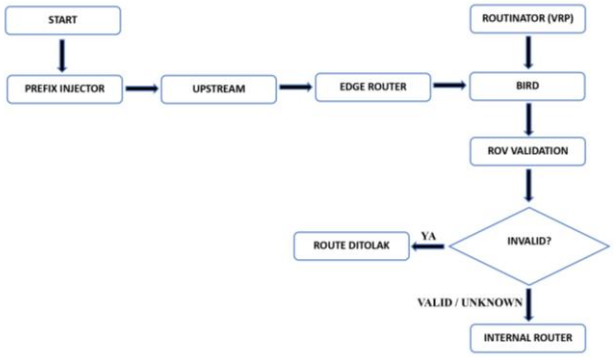
Reflector (BIRD), dan implementasi RPKI pada Edge Router, yang masing-masing diawali dengan kondisi normal sebagai acuan sebelum prefix invalid diinjeksikan ke jaringan. Skenario tanpa RPKI digunakan sebagai pembanding, di mana seluruh prefix dari upstream router diteruskan tanpa validasi sehingga dapat dipropagasikan ke router internal.

Setiap skenario dijalankan sebanyak lima kali dengan durasi lima menit per percobaan untuk mengurangi pengaruh fluktuasi sumber daya. Pada setiap percobaan, nilai CPU dan memori dicatat pada dua kondisi, yaitu baseline saat perangkat idle dan puncak saat prefix aktif diiklankan serta validasi RPKI berlangsung. Nilai puncak dari kelima percobaan kemudian dirata-ratakan untuk memperoleh nilai akhir yang digunakan dalam analisis penggunaan sumber daya.

Simulasi dilakukan menggunakan injector berbasis BIRD yang mengiklankan prefix berstatus valid, invalid, dan unknown melalui upstream router. Prefix invalid menggunakan ASN yang tidak sesuai data ROA untuk mensimulasikan BGP hijacking, sedangkan prefix unknown mensimulasikan prefix yang tidak memiliki data ROA pada validator. Prefix pengujian disiapkan dalam tiga variasi jumlah dengan proporsi tetap: 500 prefix (350 valid, 50 invalid, 100 unknown), 1.000 prefix (700 valid, 100 invalid, 200 unknown), dan 5.000 prefix (3.500 valid, 500 invalid, 1.000 unknown), untuk mengamati pengaruh peningkatan jumlah route terhadap validasi dan penggunaan sumber daya. Pembaruan data ROA lokal dilakukan menggunakan mekanisme SLURM pada Routinator untuk menghasilkan status validasi prefix yang berbeda selama pengujian.

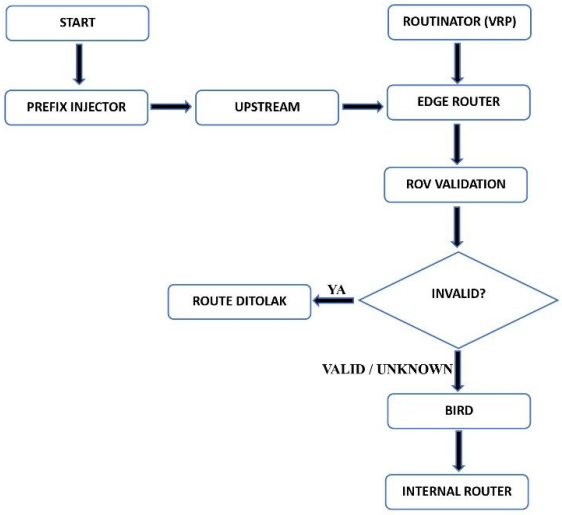
Prefix berstatus unknown pada penelitian ini secara sengaja tetap diteruskan (default-allow) dan tidak diblokir oleh kedua implementasi RPKI, mengikuti praktik umum penerapan ROV di dunia nyata di mana status unknown tidak serta-merta dianggap sebagai ancaman, mengingat belum seluruh prefix IPv4 global tercakup data ROA [8], dan penerapan ROV itu sendiri belum dilakukan secara konsisten oleh seluruh Autonomous System [9]. Kebijakan ini bukan merupakan keterbatasan teknis RPKI/ROV, melainkan kebijakan default yang lazim diterapkan agar prefix sah yang belum terdaftar ROA-nya tidak ikut terblokir (menghindari false positive). Dengan demikian, ruang lingkup pengujian difokuskan pada kemampuan sistem memitigasi prefix invalid, sedangkan penanganan unknown tidak diuji secara mendalam pada skenario BGP hijacking.

Pada skenario implementasi RPKI terpusat di route reflector (BIRD), Edge Router menerima seluruh route dari upstream router dan meneruskannya ke BIRD melalui sesi iBGP tanpa proses validasi. Selanjutnya, BIRD melakukan proses ROV menggunakan data VRP dari Routinator sebelum mendistribusikan route ke Router Internal, dengan prefix invalid difilter pada BIRD sedangkan prefix valid dan unknown tetap dipropagasikan. Alur validasi dan filtering prefix pada skenario ini ditunjukkan pada Gambar 8.



Gambar 8. Diagram alur RPKI di BIRD

Pada skenario implementasi RPKI di Edge Router, Edge Router menerima route dari Upstream Router melalui sesi eBGP kemudian melakukan proses Route Origin Validation (ROV) menggunakan data Validated ROA Payload (VRP) dari Routinator. Prefix dengan status invalid difilter pada Edge Router sehingga tidak diteruskan ke Route Reflector maupun router internal. Sementara itu, prefix dengan status valid dan unknown tetap diteruskan ke BIRD melalui sesi iBGP untuk didistribusikan ke router internal. Alur validasi dan filtering prefix pada skenario implementasi RPKI di Edge Router ditunjukkan pada Gambar 9.



Gambar 9. Diagram alur RPKI di Edge Router

Parameter performa yang diamati pada penelitian ini meliputi penggunaan CPU, memori, status validasi prefix, propagasi route, dan forwarding trafik selama proses pengujian berlangsung. Penggunaan CPU dan memori dikumpulkan menggunakan Prometheus dan divisualisasikan melalui Grafana, sedangkan status sesi BGP dan status

validasi prefix pada setiap perangkat juga ditampilkan melalui dashboard Grafana untuk memudahkan pengamatan selama eksperimen berlangsung. Data prefix valid, invalid, dan unknown diamati melalui routing table pada Edge Router, Route Reflector (BIRD), dan router internal untuk melihat perubahan propagasi route setelah proses validasi dilakukan.

Pengamatan forwarding trafik dilakukan menggunakan traceroute dan pengujian akses client terhadap prefix tujuan untuk mengetahui jalur routing yang digunakan selama simulasi BGP hijacking berlangsung. Implementasi RPKI dianalisis berdasarkan kemampuan sistem dalam memblokir prefix invalid dan pengaruhnya terhadap jalur forwarding trafik, sedangkan penggunaan CPU dan memori dianalisis untuk mengetahui dampak proses validasi RPKI terhadap penggunaan sumber daya perangkat jaringan selama proses pengujian berlangsung.

E. Analisis Hasil

Analisis hasil dilakukan dengan membandingkan data pengujian pada setiap skenario implementasi RPKI, yaitu tanpa implementasi RPKI, implementasi RPKI pada Route Reflector (BIRD), dan implementasi RPKI pada Edge Router. Perbandingan dilakukan terhadap status validasi prefix, forwarding trafik, penggunaan CPU, dan memori untuk mengetahui pengaruh lokasi implementasi RPKI terhadap mitigasi BGP hijacking dan penggunaan sumber daya perangkat jaringan.

Analisis dilakukan pada control plane dan forwarding plane jaringan untuk melihat pengaruh lokasi implementasi RPKI terhadap propagasi route dan jalur forwarding trafik selama simulasi BGP hijacking berlangsung.

Analisis validasi prefix dilakukan berdasarkan kemampuan sistem dalam menerima, memvalidasi, dan membatasi propagasi prefix dengan status invalid pada jaringan internal. Selain itu, pengamatan juga dilakukan terhadap propagasi prefix valid, invalid, dan unknown pada Edge Router, Route Reflector (BIRD), dan router internal untuk melihat perubahan propagasi route setelah proses validasi dilakukan.

Analisis forwarding trafik dilakukan menggunakan traceroute dan pengujian akses client terhadap prefix tujuan untuk mengamati jalur routing yang digunakan selama simulasi BGP hijacking berlangsung. Hasil pengujian digunakan untuk melihat pengaruh lokasi implementasi RPKI terhadap jalur forwarding trafik setelah proses validasi route dilakukan.

Analisis penggunaan CPU dan memori dilakukan menggunakan nilai rata-rata (mean) dari lima kali pengujian pada setiap skenario untuk memperoleh hasil pengukuran yang lebih konsisten. Perbandingan dilakukan berdasarkan perubahan penggunaan sumber daya antara kondisi tanpa implementasi RPKI dan kondisi setelah proses validasi RPKI diterapkan. Hasil tersebut digunakan untuk mengamati dampak proses Route Origin Validation (ROV) terhadap penggunaan sumber daya perangkat jaringan.

Data hasil pengujian divisualisasikan menggunakan Grafana berdasarkan data monitoring dari Prometheus untuk mempermudah proses pengamatan perubahan penggunaan sumber daya perangkat selama proses eksperimen berlangsung.

III. HASIL DAN PEMBAHASAN

Bab ini membahas hasil pengujian implementasi Resource Public Key Infrastructure (RPKI) pada Edge Router dan Route Reflector (BIRD) berdasarkan parameter penggunaan CPU, memori, status validasi prefix, propagasi route, dan forwarding trafik. Pengujian dilakukan untuk mengetahui pengaruh lokasi implementasi RPKI terhadap mitigasi BGP hijacking serta dampaknya terhadap penggunaan sumber daya perangkat jaringan.

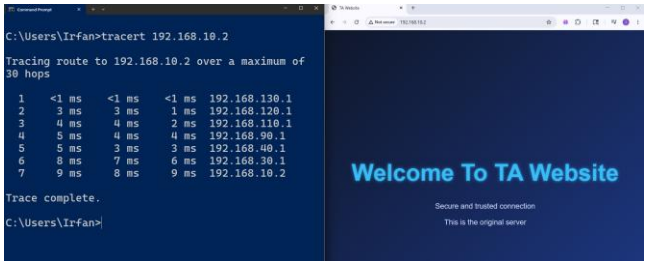
A. Hasil Pengujian Validasi Prefix

1) Pengujian Tanpa RPKI

Pengujian tanpa implementasi RPKI dilakukan untuk mengamati perubahan forwarding traffic sebelum dan setelah simulasi BGP hijacking dilakukan. Pengujian diawali dengan kondisi normal untuk memastikan bahwa jalur routing berjalan sesuai konfigurasi jaringan sebelum prefix dengan status invalid diinjeksikan ke dalam jaringan.

Hasil traceroute pada kondisi normal menunjukkan bahwa forwarding traffic berjalan melalui jalur routing yang sesuai tanpa adanya pengalihan route yang tidak sah. Jalur routing yang digunakan client masih mengarah ke prefix tujuan yang benar sesuai konfigurasi jaringan yang telah ditetapkan.

Gambar 10 menunjukkan hasil traceroute dan akses web server pada kondisi normal jaringan.



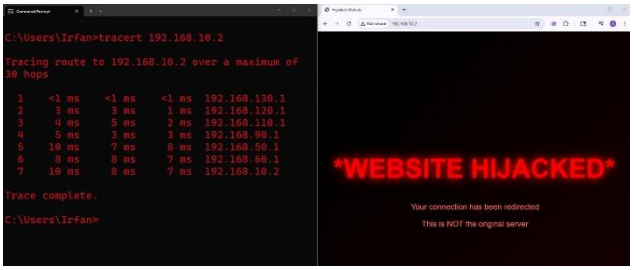
Gambar 10. Traceroute dan akses web tanpa RPKI.

e-ISSN: 2548-6861

Setelah simulasi BGP hijacking dilakukan, upstream 2 mengiklankan prefix invalid 192.168.10.0/25 menuju Edge Router 2. Karena tidak terdapat proses validasi RPKI, Edge Router 2 menerima seluruh route yang berasal dari Upstream 2 termasuk prefix dengan status invalid. Route tersebut kemudian digunakan sebagai jalur routing aktif dan dipropagasikan ke jaringan internal.

Hasil pengujian menunjukkan bahwa forwarding traffic diarahkan menuju jalur hasil hijacking karena prefix invalid dipilih sebagai route aktif pada Edge Router. Kondisi tersebut menyebabkan client diarahkan menuju web server hasil hijacking.

Gambar 11 menunjukkan hasil traceroute dan akses web pada skenario tanpa implementasi RPKI setelah simulasi BGP hijacking dilakukan.



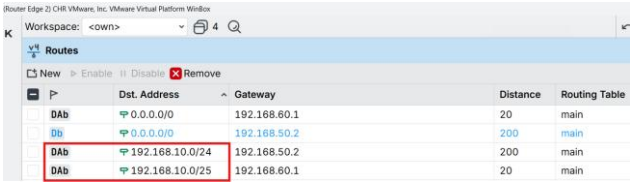
Gambar 11. Traceroute dan akses web tanpa RPKI ketika di hijack.

2) Pengujian Implementasi RPKI di Route Reflector (BIRD)

Pada skenario implementasi RPKI terpusat di route reflector (BIRD), Edge Router 2 menerima seluruh prefix dari Upstream2 kemudian meneruskannya ke BIRD melalui sesi iBGP tanpa proses validasi. Selanjutnya, BIRD melakukan proses Route Origin Validation (ROV) menggunakan data Validated ROA Payload (VRP) dari Routinator sebelum mendistribusikan route ke Router Internal.

Hasil pengujian menunjukkan bahwa prefix invalid 192.168.10.0/25 masih diterima oleh Edge Router 2 dari Upstream 2 karena proses validasi belum dilakukan pada perangkat tersebut. Prefix tersebut digunakan sebagai jalur routing aktif pada Edge Router 2 berdasarkan prinsip Longest Prefix Match (LPM) terhadap prefix valid 192.168.10.0/24. Berdasarkan routing table pada Edge Router 2, prefix tersebut ditandai dengan flag DAb yang menunjukkan bahwa route diterima secara dinamis melalui protokol BGP dan digunakan sebagai jalur routing aktif pada perangkat.

Gambar 12 menunjukkan bahwa prefix invalid masih diterima pada routing table Edge Router 2 pada implementasi RPKI di Route Reflector (BIRD).



Gambar 12. Routing Table di Edge 2 saat RPKI di BIRD

Setelah prefix diterima dari Edge Router 2, BIRD melakukan proses validasi menggunakan data ROA yang diperoleh dari Routinator melalui protokol RTR. Hasil pengujian menunjukkan bahwa prefix 192.168.10.0/25 teridentifikasi sebagai prefix invalid karena ASN pengiklan tidak sesuai dengan data ROA yang terdaftar. Berdasarkan hasil validasi tersebut, BIRD menolak prefix invalid sehingga route hasil hijacking tidak dipropagasikan ke router internal maupun ke Edge Router 1 melalui proses Route Reflection.

Gambar 13 menunjukkan proses filtering prefix invalid pada route reflector (BIRD).

Gambar 13. Filtering prefix invalid pada route reflector (BIRD).

Hasil pengamatan pada Router Internal menunjukkan bahwa prefix invalid tidak lagi diterima setelah proses filtering dilakukan pada BIRD. Kondisi tersebut menunjukkan bahwa implementasi RPKI pada Route Reflector mampu membatasi propagasi route hasil hijacking pada jaringan internal.

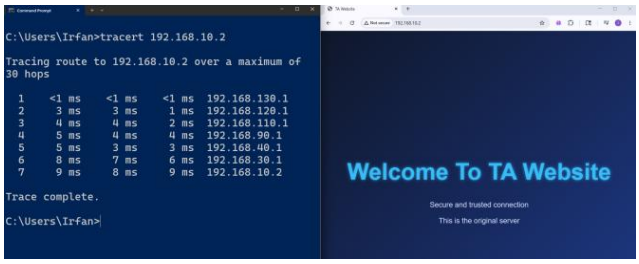
Gambar 14 menunjukkan bahwa prefix invalid tidak dipropagasikan ke router internal pada implementasi RPKI di Route Reflector (BIRD).

Gambar 14. Routing table router internal pada implementasi RPKI di BIRD.

Pengamatan forwarding traffic menggunakan traceroute menunjukkan bahwa jalur routing kembali diarahkan menuju prefix asli setelah proses filtering dilakukan pada BIRD. Kondisi tersebut menunjukkan bahwa

implementasi RPKI pada Route Reflector berhasil mencegah propagasi prefix invalid ke jaringan internal sehingga forwarding traffic tidak lagi diarahkan menuju jalur hasil hijacking.

Gambar 15 menunjukkan hasil traceroute dan akses web server pada implementasi RPKI di Route Reflector (BIRD).



Gambar 15. Traceroute dan Akses Web Server pada RPKI BIRD.

Berdasarkan hasil pengujian tersebut, implementasi RPKI pada Route Reflector (BIRD) mampu memitigasi propagasi prefix invalid pada jaringan internal melalui proses validasi terpusat menggunakan mekanisme Route Origin Validation (ROV). Prefix hasil hijacking berhasil difilter sebelum dipropagasikan ke Router Internal sehingga forwarding traffic kembali menggunakan jalur routing menuju prefix valid.

3) Pengujian Implementasi RPKI pada Edge Router

Pada skenario implementasi RPKI pada Edge Router, proses Route Origin Validation (ROV) dilakukan secara langsung pada Edge Router 2 sebelum prefix dipropagasikan ke jaringan internal. Edge Router 2 menerima prefix dari Upstream 2 kemudian melakukan validasi menggunakan data Validated ROA Payload (VRP) yang diperoleh dari Routinator melalui protokol RTR.

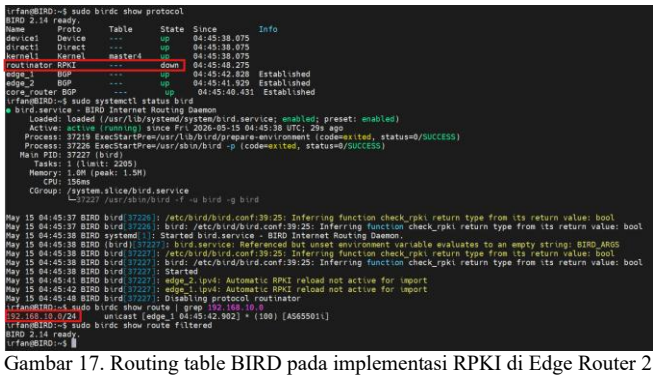
Hasil pengujian menunjukkan bahwa prefix invalid 192.168.10.0/25 berhasil terdeteksi sebagai route yang tidak sesuai dengan data ROA sehingga prefix tersebut ditolak sebelum masuk ke routing table Edge Router 2. Berdasarkan routing table pada perangkat, prefix invalid ditandai dengan status inactive (DFbI) yang menunjukkan bahwa route tidak digunakan sebagai jalur routing aktif setelah proses validasi RPKI dilakukan. Dengan demikian, prefix hasil hijacking tidak dipropagasikan ke BIRD maupun ke Router Internal.

Gambar 16 menunjukkan routing table pada Edge Router 2 setelah proses validasi RPKI dilakukan, di mana prefix invalid 192.168.10.0/25 ditandai dengan status inactive (DFbI) yang menunjukkan bahwa prefix tersebut tidak digunakan sebagai jalur routing aktif.

Gambar 16. Filtering prefix invalid pada Edge Router 2

Hasil pengamatan pada routing table BIRD menunjukkan bahwa hanya prefix valid 192.168.10.0/24 yang diterima setelah proses validasi dilakukan. Prefix invalid tidak diteruskan ke Route Reflector karena telah difilter sebelumnya pada edge router sehingga route hasil hijacking tidak dipropagasikan ke jaringan internal.

Gambar 17 menunjukkan routing table pada BIRD setelah proses filtering dilakukan pada Edge Router.



Gambar 17. Routing table BIRD pada implementasi RPKI di Edge Router 2

Hasil pengamatan pada router internal menunjukkan bahwa prefix invalid tidak diterima pada jaringan internal karena proses filtering telah dilakukan sebelum route dipropagasikan ke Route Reflector. Kondisi tersebut menyebabkan hanya prefix valid yang digunakan sebagai jalur routing aktif pada jaringan internal.

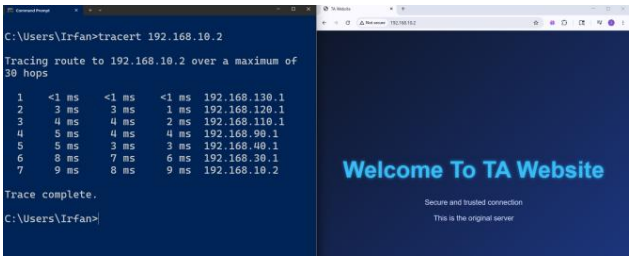
Gambar 18 menunjukkan routing table Router Internal pada implementasi RPKI di Edge Router.

Gambar 18. Routing Table Internal pada Edge Router RPKI

Pengamatan forwarding traffic menggunakan traceroute menunjukkan bahwa jalur routing tetap diarahkan menuju prefix asli setelah simulasi BGP hijacking dilakukan. Selain itu, hasil pengujian akses web server menunjukkan bahwa client tetap terhubung ke server asli karena prefix invalid tidak digunakan sebagai jalur routing aktif pada Edge Router setelah proses validasi RPKI dilakukan.

e-ISSN: 2548-6861

Gambar 19 menunjukkan hasil traceroute dan akses web server pada implementasi RPKI di Edge Router.



Gambar 19. Traceroute dan Akses Web Server pada RPKI Edge Router.

Berdasarkan hasil pengujian tersebut, implementasi RPKI pada Edge Router mampu memitigasi propagasi prefix invalid sebelum route masuk ke jaringan internal. Proses validasi yang dilakukan langsung pada Edge Router menyebabkan prefix hasil hijacking tidak masuk ke routing table aktif perangkat sehingga forwarding traffic tetap menggunakan jalur routing menuju prefix valid. Selain itu, implementasi RPKI pada Edge Router juga mampu mencegah propagasi route invalid ke Route Reflector maupun Router Internal secara lebih awal dibandingkan implementasi RPKI terpusat pada Route Reflector (BIRD).

4) Perbandingan Propagasi Prefix pada Setiap Skenario

Pengujian dilakukan pada tiga skenario dengan variasi 500, 1.000, dan 5.000 prefix. Hasil pengamatan menunjukkan pola propagasi prefix yang konsisten pada seluruh variasi jumlah prefix yang diuji, sehingga hasil perbandingan propagasi prefix disajikan secara ringkas pada Tabel IV.

Skenario	Node	Valid	Invalid	Unknown
Tanpa RPKI	Edge Router	✓	✓	✓
	BIRD	✓	✓	✓
	Router Internal	✓	✓	✓
RPKI di BIRD	Edge Router	✓	✓	✓
	BIRD	✓	✖	✓
	Router Internal	✓	✖	✓
RPKI di Edge	Edge Router	✓	✖	✓
	BIRD	✓	✖	✓
	Router Internal	✓	✖	✓

Tabel IV. Propagasi Prefix

Berdasarkan Tabel IV, terdapat perbedaan propagasi prefix yang signifikan antara ketiga skenario pengujian. Pada skenario tanpa implementasi RPKI, seluruh prefix termasuk prefix invalid diterima dan dipropagasikan ke seluruh titik jaringan tanpa proses validasi sehingga prefix hasil hijacking tersebar hingga ke Router Internal.

Pada skenario implementasi RPKI di Route Reflector (BIRD), Edge Router masih menerima prefix invalid dari Upstream karena proses validasi belum dilakukan pada perangkat tersebut. Prefix invalid baru difilter pada BIRD menggunakan data VRP dari Routinator sebelum dipropagasikan ke Router Internal sehingga prefix hasil hijacking tidak diteruskan ke jaringan internal. Meskipun demikian, Edge Router tetap memiliki prefix invalid di routing table-nya sehingga keputusan routing lokal pada Edge Router masih dipengaruhi oleh keberadaan prefix invalid berdasarkan prinsip Longest Prefix Match (LPM).

Pada implementasi RPKI di Edge Router, prefix invalid langsung diblokir sebelum masuk ke routing table menggunakan data VRP dari Routinator melalui protokol RTR sehingga tidak diteruskan ke BIRD maupun Router Internal. Prefix unknown tetap diteruskan karena tidak memiliki data ROA pada validator sehingga tidak dikategorikan sebagai invalid. Pola propagasi prefix yang sama pada seluruh variasi jumlah prefix menunjukkan bahwa mekanisme filtering pada kedua implementasi RPKI bekerja secara konsisten dan tidak dipengaruhi oleh jumlah prefix yang diuji.

B. Hasil Pengujian Penggunaan Sumber Daya

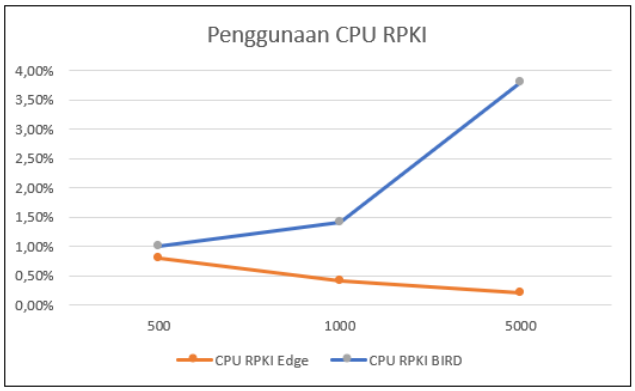
Analisis penggunaan sumber daya perangkat dilakukan dengan membandingkan penggunaan CPU dan memori pada kondisi tanpa RPKI dan dengan RPKI di Edge Router (MikroTik) dan Route Reflector (BIRD). Sebagaimana dijelaskan pada bagian Pengujian Skenario, nilai yang dianalisis pada bagian ini merupakan rata-rata dari nilai puncak kelima percobaan pada setiap skenario. Data CPU dan memori dikumpulkan menggunakan Prometheus dan divisualisasikan melalui Grafana. Tabel V menunjukkan rata-rata penggunaan CPU dan memori tanpa RPKI, sedangkan Tabel VI menunjukkan kondisi dengan RPKI. Selanjutnya, hasil perbandingan kedua skenario dianalisis berdasarkan selisih peningkatan penggunaan sumber daya. Visualisasi selisih peningkatan penggunaan CPU ditampilkan pada Gambar 20, sedangkan visualisasi selisih peningkatan penggunaan memori ditampilkan pada Gambar 21.

Prefix	CPU Edge	Memory Edge	CPU BIRD	Memory BIRD
500	9.20 %	0.70 MB	6.40 %	0.31 MB
1000	14.40 %	2.20 MB	8.40 %	0.56 MB
5000	50.80 %	8.16 MB	20.20 %	1.04 MB

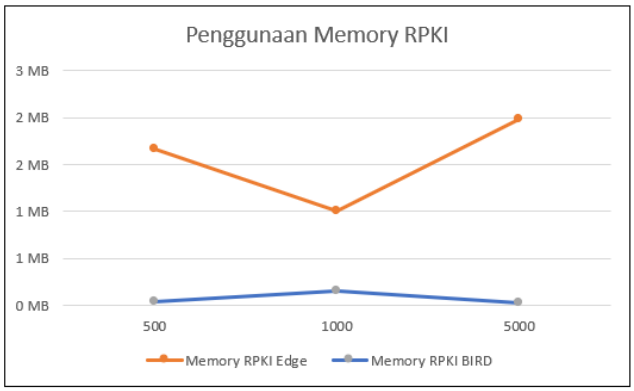
Tabel V. Rata-rata Penggunaan CPU dan Memori Tanpa RPKI.

Prefix	CPU Edge	Memory Edge	CPU BIRD	Memory BIRD
500	10.00 %	2.36 MB	7.40 %	0.35 MB
1000	14.80 %	3.20 MB	9.80 %	0.71 MB
5000	51.00 %	10.14 MB	24.00 %	1.06 MB

Tabel VI. Rata-rata Penggunaan CPU dan Memori Dengan RPKI.



Gambar 20 Penggunaan CPU RPKI



Gambar 21 Penggunaan Memory RPKI

Berdasarkan Tabel V dan Tabel VI, penggunaan CPU pada Edge Router menunjukkan peningkatan nilai seiring bertambahnya jumlah prefix pada kedua kondisi pengujian, baik dengan maupun tanpa RPKI. Pada setiap variasi prefix, penggunaan CPU Edge Router dengan RPKI selalu lebih tinggi dibandingkan tanpa RPKI, yaitu dari 9,20% menjadi 10,00% pada 500 prefix, dari 14,40% menjadi 14,80% pada 1.000 prefix, dan dari 50,80% menjadi 51,00% pada 5.000 prefix. Namun, selisih penggunaan CPU akibat penerapan RPKI pada Edge Router justru menyempit seiring bertambahnya jumlah prefix, yaitu 0,80% pada 500 prefix, 0,40% pada 1.000 prefix, dan 0,20% pada 5.000 prefix.

Pola yang berbeda ditunjukkan oleh BIRD. Penggunaan CPU BIRD dengan RPKI juga selalu lebih tinggi dibandingkan tanpa RPKI pada setiap variasi prefix, yaitu dari 6,40% menjadi 7,40% pada 500 prefix, dari 8,40% menjadi 9,80% pada 1.000 prefix, dan dari 20,20% menjadi 24,00% pada 5.000 prefix. Berbeda dengan Edge Router, selisih penggunaan CPU akibat penerapan RPKI pada BIRD justru melebar seiring bertambahnya jumlah prefix, yaitu 1,00% pada 500 prefix, 1,40% pada 1.000 prefix, dan 3,80% pada 5.000 prefix. Dengan demikian, arah perubahan selisih pada kedua perangkat berlawanan: Edge Router mengalami penyempitan selisih, sedangkan BIRD mengalami pelebaran selisih seiring bertambahnya jumlah prefix.

Pada parameter memori, penggunaan memori Edge Router dengan RPKI selalu lebih tinggi dibandingkan tanpa RPKI pada setiap variasi prefix, yaitu dari 0,70 MB menjadi 2,36 MB pada 500 prefix, dari 2,20 MB menjadi 3,20 MB pada 1.000 prefix, dan dari 8,16 MB menjadi 10,14 MB pada 5.000 prefix, dengan selisih berturut-turut sebesar 1,66 MB, 1,00 MB, dan 1,98 MB. Pola selisih ini tidak berubah secara searah, berbeda dengan pola CPU yang selisihnya menyempit secara konsisten. Sementara itu, penggunaan memori BIRD dengan RPKI meningkat dalam rentang yang jauh lebih kecil dibandingkan Edge Router, yaitu dari 0,31 MB menjadi 0,35 MB pada 500 prefix, dari 0,56 MB menjadi 0,71 MB pada 1.000 prefix, dan dari 1,04 MB menjadi 1,06 MB pada 5.000 prefix, dengan selisih berturut-turut sebesar 0,04 MB, 0,15 MB, dan 0,02 MB.

Perbedaan selisih penggunaan CPU dan memori antara Edge Router dan BIRD tidak dapat diatribusikan semata-mata pada lokasi implementasi RPKI. Kedua perangkat berjalan pada platform yang berbeda, yaitu MikroTik RouterOS (CHR) pada Edge Router dan BIRD sebagai daemon routing di atas Ubuntu Server, sehingga arsitektur proses dan cara masing-masing menangani ROV secara internal turut menjadi faktor perancu (confounding factor). Selain itu, BIRD sebagai route reflector secara inheren menangani volume prefix yang lebih besar karena mendistribusikan route ke seluruh router internal melalui iBGP, sehingga beban validasi RPKI berpotensi lebih terasa dibandingkan pada Edge Router. Dengan demikian, selisih penggunaan sumber daya ini lebih tepat dimaknai sebagai dampak RPKI pada masing-masing platform sesuai perannya, bukan perbandingan efisiensi yang setara (apple-to-apple).

C. Monitoring Berbasis Grafana

Monitoring penggunaan sumber daya perangkat dan status validasi prefix selama proses pengujian dilakukan menggunakan Grafana dengan data yang dikumpulkan oleh Prometheus. Dashboard Grafana menampilkan informasi penggunaan CPU, penggunaan memori, status sesi BGP, serta status validasi prefix secara visual selama simulasi BGP hijacking berlangsung.

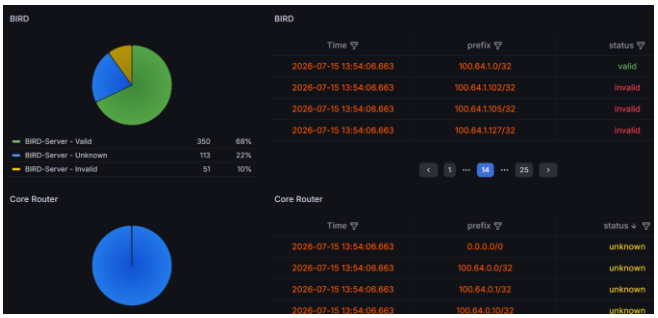
Gambar 22 menunjukkan tampilan dashboard Grafana yang memvisualisasikan penggunaan CPU dan memori pada edge router dan BIRD, serta status sesi BGP selama proses pengujian berlangsung.

e-ISSN: 2548-6861

Gambar 22. Dashboard Grafana Monitoring CPU, Memori, dan BGP Status

Berdasarkan Gambar 22, dashboard Grafana menampilkan penggunaan CPU dalam bentuk grafik waktu untuk Router Edge 1, Router Edge 2, dan BIRD secara bersamaan, sehingga perubahan penggunaan CPU pada setiap perangkat dapat diamati selama proses injeksi prefix berlangsung. Selain itu, penggunaan memori ditampilkan dalam satuan MiB untuk masing-masing perangkat, serta status sesi BGP yang menunjukkan kondisi koneksi antar perangkat dalam jaringan.

Gambar 23 menunjukkan tampilan dashboard Grafana yang memvisualisasikan status validasi prefix pada Edge Router selama proses pengujian berlangsung.



Gambar 23. Dashboard Grafana Status Validasi Prefix

Berdasarkan Gambar 23, dashboard Grafana menampilkan distribusi status validasi prefix pada Edge Router dalam bentuk diagram lingkaran dan tabel detail yang mencakup informasi waktu, prefix, router, dan status validasi. Status validasi prefix dikategorikan menjadi valid, invalid, dan unknown sesuai dengan hasil Route Origin Validation (ROV) yang dilakukan selama proses pengujian. Visualisasi ini memungkinkan pengamatan perubahan status validasi prefix secara langsung selama simulasi BGP hijacking berlangsung, sehingga perubahan propagasi prefix pada setiap skenario dapat diamati secara visual melalui dashboard Grafana.

IV. KESIMPULAN

Penelitian ini menganalisis perbandingan implementasi RPKI pada Edge Router (MikroTik) dan Route Reflector (BIRD) untuk mitigasi BGP hijacking pada lingkungan simulasi jaringan ISP berbasis virtualisasi. Hasil pengujian menunjukkan bahwa kedua implementasi berhasil memblokir seluruh prefix invalid dan mengarahkan forwarding traffic client menuju prefix valid 192.168.10.0/24 sehingga serangan BGP hijacking berhasil dimitigasi. Prefix berstatus unknown tetap diteruskan ke jaringan internal pada kedua skenario sebagai kebijakan default, karena tidak memiliki data ROA pada validator.

Terdapat perbedaan lokasi filtering antara kedua implementasi. Pada implementasi RPKI di Route Reflector (BIRD), Edge Router masih menerima prefix invalid dari Upstream sehingga routing table-nya tetap memuat prefix invalid yang berpotensi memengaruhi keputusan routing lokal berdasarkan prinsip Longest Prefix Match. Sebaliknya, pada implementasi RPKI di Edge Router, prefix invalid langsung diblokir sebelum masuk ke routing table sehingga tidak pernah diteruskan ke BIRD maupun Router Internal.

Dari sisi penggunaan sumber daya, selisih penggunaan CPU akibat penerapan RPKI pada Edge Router berkisar antara 0,20% hingga 0,80% dan menyempit seiring bertambahnya jumlah prefix, sedangkan pada BIRD selisihnya berkisar antara 1,00% hingga 3,80% dan justru melebar seiring bertambahnya jumlah prefix. Selisih penggunaan memori Edge Router berkisar antara 1,00 MB hingga 1,98 MB, lebih besar dibandingkan selisih memori BIRD yang berkisar antara 0,02 MB hingga 0,15 MB. Seluruh data tersebut divisualisasikan melalui dashboard Grafana berbasis Prometheus yang juga menampilkan status validasi prefix dan kondisi sesi BGP selama pengujian berlangsung.

Penelitian ini memiliki sejumlah keterbatasan yang perlu diperhatikan dalam menginterpretasikan hasil. Pertama, pengujian dilakukan pada lingkungan simulasi berskala kecil sehingga belum sepenuhnya merepresentasikan jaringan ISP produksi. Kedua, variasi jumlah prefix terbatas pada tiga skenario (500, 1.000, dan 5.000), jauh lebih kecil dibandingkan skala tabel routing global saat ini. Ketiga, setiap skenario hanya diuji lima kali pengulangan dan dianalisis menggunakan nilai rata-rata tanpa uji signifikansi statistik (misalnya uji-t atau ANOVA), sehingga belum dapat dipastikan bahwa perbedaan yang diamati signifikan secara statistik dan bukan akibat variasi acak pada lingkungan virtualisasi. Keempat, sebagaimana dijelaskan pada bagian Metode Penelitian, perbandingan dilakukan antara dua platform routing yang berbeda (MikroTik dan BIRD), sehingga sebagian hasil turut dipengaruhi oleh karakteristik masing-masing platform, bukan semata-mata oleh lokasi implementasi RPKI.

Penelitian selanjutnya dapat mempertimbangkan pengujian pada skala prefix yang lebih besar mendekati kondisi jaringan internet global, serta menganalisis pengaruh implementasi RPKI terhadap waktu konvergensi BGP dan stabilitas sesi routing.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Allah SWT atas segala rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Penulis mengucapkan terima kasih kepada keluarga atas dukungan dan doa yang senantiasa diberikan, kepada Bapak Antoni Haikal selaku dosen pembimbing atas bimbingan dan arahan yang diberikan, serta kepada teman-teman seperjuangan atas dukungan dan diskusi selama proses penelitian berlangsung.

DAFTAR PUSTAKA

[1] B. Al-Musawi, P. Branch, and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 377–396, 2017, doi: 10.1109/COMST.2016.2622240.

[2] J. Schlamp, R. Holz, Q. Jacquemart, G. Carle, and E. W. Biersack, "HEAP: Reliable Assessment of BGP Hijacking Attacks," 2016.

[3] N. Sekiguchi and H. Tanaka, "BGP hijack attack policy against AS topology map," *Internet of Things (Netherlands)*, vol. 25, p. 101059, 2024, doi: 10.1016/j.iot.2024.101059.

[4] P. Moriano, R. Hill, and L. J. Camp, "Using bursty announcements for detecting BGP routing anomalies," *Comput. Networks*, vol. 188, no. January, p. 107835, 2021, doi: 10.1016/j.comnet.2021.107835.

[5] RIPE NCC, "YouTube Hijacking: A RIPE NCC RIS Case Study," RIPE NCC. Accessed: Jun. 05, 2026. [Online]. Available: https://www.ripe.net/about-us/news/youtube-hijacking-a-ripe-ncc-ris-case-study/

[6] V. B. Pranaya and T. Wellem, "Implementasi BGP dan Resource Public Key Infrastructure menggunakan BIRD untuk Keamanan Routing," vol. 5, no. 158, pp. 1161–1170, 2021.

[7] R. de Boer and J. de Koning, "BGP Origin Validation (RPKI)," 2013.

[8] D. Madory and J. Snijders, "RPKI ROV Deployment Reaches Major Milestone," APNIC Blog. Accessed: Jun. 05, 2026. [Online]. Available: https://blog.apnic.net/2024/05/08/rpki-rov-deployment-reaches-major-milestone/

[9] R. Tian, Y. Li, X. Yin, H. Zhang, X. Shi, and Z. Wang, "TORCH: Characterizing Invalid Route Filtering via Tunnelled Observation," 2026. doi: 10.48550/arXiv.2603.29207.

[10] N. Iryani, J. G. A. Ginting, and D. D. Andika, "Analisis Performansi BGP Resource Public Key Infrastructure Studi Kasus PT. Time Excelindo," *JTERA (Jurnal Teknol. Rekayasa)*, vol. 7, no. 1, p. 135, 2022, doi: 10.31544/jtera.v7.i1.2022.135-142.

[11] T. B. Rahayu and I. Suharjo, "Implementasi BGP dengan RPKI Pada Jaringan PT. Bintang Mataram Teknologi Menggunakan Mikrotik Router OS," *J. Fasilkom*, vol. 14, no. 2, pp. 293–300, 2024, doi: 10.37859/jf.v14i2.6968.

[12] B. B. Fauzi, I. Muhammad, and R. Hendar, "Pengembangan System Monitoring dan Visualisasi Data Penggunaan Sumber Daya Pada Server Menggunakan Prometheus Dan Grafana Pada Database Terintegrasi di PT . Dirgantara," *e-Proceeding Appl. Sci.*, vol. 11, no. 4, pp. 1004–1010, 2025.

[13] B. Rasyidi and F. Pratama, "Server Monitoring System at PT . XYZ Media Indonesia Based on Grafana and Prometheus Sistem Monitoring Server di PT . XYZ Media Indonesia Berbasis Grafana dan Prometheus," vol. 4, no. October, pp. 1456–1465, 2024.

[14] F. P. E. Putra, F. Khusaini, Amsori, and K. Anam, "Pengembangan Sistem Keamanan berbasis Cloud dengan An- alisis Efek Avalanche pada Jaringan Perusahaan yang Menga- dopsi Infrastruktur Cloud," *J. Inform. dan Teknol. Komput.*, vol. 5, no. 2, pp. 111–118, 2025, doi: 10.55606/jitek.v5i2.6913.

[15] T. Ernawati and J. Endrawan, "Peningkatan Kinerja Jaringan Komputer dengan Border Gateway Protocol (BGP) dan Dynamic Routing (Studi Kasus PT Estiko Ramanda)," *Khazanah Inform. J. Ilmu Komput. dan Inform.*, vol. 4, no. 1, pp. 35–41, 2018, doi: 10.23917/khif.v4i1.5656.

[16] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A prefix hijack alert system," *15th USENIX Secur. Symp.*, pp. 153–166, 2006.