JURNAL FASILKOM
Volume 14 No. 2 | Bulan Agustus: 293-300

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Implementasi BGP dengan RPKI Pada Jaringan PT. Bintang Mataram Teknologi Menggunakan Mikrotik Router OS

Tri Budi Rahayu[1], Imam Suharjo[2]
[12]Teknologi Informatika, Teknologi Informasi, Universitas Mercubuanan Yogyakarta
[1]201110169@student.mercubuana-yogya.ac.id, [2]imam@mercubuana-yogya.ac.id

Abstract

The Border Gateway Protocol (BGP) protocol serves as the foundation for exchanging routing information among Autonomous Systems (AS) on the Internet. However, BGP security has become a primary concern due to its vulnerability to attacks such as hijacking and spoofing. The Resource Public Key Infrastructure (RPKI) serves as a solution that confirms the origin of BGP routes, thereby reducing the risk of such attacks. The aim of this research is to implement and evaluate BGP security with RPKI on the network of PT. Bintang Mataram Teknologi using MikroTik RouterOS 7. The implementation involves configuring RPKI on MikroTik routers to confirm and authorize the origin of BGP routes. Security evaluation is conducted by analyzing the effectiveness of RPKI in reducing the risk of BGP attacks, including origin hijacking and spoofing. Measurements are made on the reliability of BGP routes, the ability to detect attacks, and the additional overhead generated by RPKI implementation. The research findings indicate that the implementation of RPKI on the network of PT. Bintang Mataram Teknologi using MikroTik RouterOS 7 can enhance BGP security by confirming the origin of received routes. The evaluation demonstrates that RPKI is effective in mitigating BGP attack risks, with acceptable additional overhead in network operations. This research contributes to strengthening network infrastructure security, particularly in the context of implementing MikroTik RouterOS 7 to deploy RPKI in safeguarding services and sensitive data from BGP attacks.

Keywords: routing, border gateway protocol (BGP), resource public key infrastructure (RPKI), mikrotik

Abstrak

Protokol Border Gateway Protocol (BGP) merupakan pondasi dalam pertukaran informasi routing antar Autonomous System (AS) di internet. Namun, keamanan BGP telah menjadi perhatian utama karena rawan terhadap serangan seperti hijacking dan spoofing. Resource Public Key Infrastructure (RPKI) menjadi solusi yang mengonfirmasi asal rute BGP, mengurangi risiko serangan tersebut. Tujuan dari penelitian ini adalah untuk menerapkan dan mengevaluasi keamanan BGP dengan RPKI pada jaringan PT. Bintang Mataram Teknologi yang menggunakan MikroTik RouterOS 7. Implementasi melibatkan konfigurasi RPKI pada router MikroTik untuk mengonfirmasi dan memberikan izin pada asal rute BGP. Simulasi serta implementasi dilakukan menggunakan EVE-NG sebagai simulator dan sebuah Virtual Server yang berperan sebagai RPKI Validator. Pengujian dilakukan menggunakan 3 AS, 6 router, 2 virtual PC, 1 virtual server untuk validator, dan 1 virtual PC sebagai fake server DNS Google. Hasil penelitian menunjukkan bahwa implementasi RPKI pada jaringan PT. Bintang Mataram Teknologi dengan menggunakan MikroTik RouterOS 7 dapat meningkatkan keamanan BGP dengan mengonfirmasi asal rute yang diterima. Evaluasi menunjukkan bahwa RPKI efektif dalam mengurangi risiko serangan BGP, dengan tambahan beban yang masih dapat diterima dalam operasi jaringan. Penelitian ini memberikan sumbangan dalam memperkuat keamanan infrastruktur jaringan, terutama dalam konteks penerapan MikroTik RouterOS 7 untuk mengimplementasikan RPKI dalam melindungi layanan dan data sensitif dari serangan terhadap BGP.

Kata kunci: rute, *border gateway protocol* (BGP), *resource public key infrastructure* (RPKI), mikrotik

1. Pendahuluan

PT. Bintang Mataram Teknologi merupakah sebuah perusahaan yang bergerak di bidang penyedia jasa teknologi informasi *Internet Service Provider* (ISP) memahami betapa pentingnya keamanan jaringan agar terhindar dari ancaman dan kejahatan *cyber*. Karena bergerak di bidang ini, salah satu elemen fundamental yang harus diperhatikan adalah terkait keamanan protokol BGP (*Border Gateway Protocol)*. BGP merupakan protokol penting dalam pertukaran informasi rute antar *domain* di *internet*. Namun, kerentanan *inherent* dalam desentralisasi BGP telah membuatnya rentan terhadap berbagai serangan, termasuk *hijacking* dan *route leaking*, yang dapat mengakibatkan gangguan serius pada layanan internet. Tentu jika serangan ini terjadi sangat beresiko terhadap pelayanan yang diberikan oleh PT. Bintang Mataram Teknologi.

BGP adalah protokol *routing* utama di internet yang digunakan untuk bertukar informasi *routing* antar jaringan. BGP beroperasi dengan memetakan tabel IP *network* yang menunjukkan jaringan-jaringan yang dapat dicapai antar *Autonomous System* (AS)[1]. Selain itu, BGP juga meningkatkan keamanan manajemen jaringan dengan menggunakan fitur RPKI untuk memverifikasi pesan *routing* yang dikirim antar-router. Protokol ini mendukung *Classless Inter-Domain Routing* (CIDR) dan biasanya diterapkan pada *Internet Service Provider* (ISP) atau organisasi lainnya. *Autonomous System* (AS) adalah kumpulan *router* yang berada di bawah administrasi suatu entitas tertentu (misalnya, ISP) dan mengikuti kebijakan *routing*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

tertentu. Setiap AS diberi nomor identitas yang disebut *Autonomous System Number* (ASN), yang merupakan angka 32-bit. Pemberian ASN ini diatur oleh *Regional Internet Registry* (RIR). Saat ini, ada lima RIR: APNIC, ARIN, RIPE NCC, LACNIC, dan AFRINIC. *Router* dalam AS yang sama menggunakan *Interior Gateway Protocol* (IGP) untuk *routing* paket IP di dalam AS tersebut, sementara *Border Gateway Protocol* (BGP) digunakan untuk *routing* ke AS lain. Secara umum, *router* dalam suatu AS yang menjalankan BGP adalah *router* yang menghubungkan AS tersebut dengan AS lain [2]. Router dalam suatu AS dapat melakukan pertukaran rute dari dan ke luar AS tersebut serta mempublikasikan atau mengumumkan rute (BGP *announcement* atau *route advertisement*) ke berbagai tujuan (jaringan) di Internet. Jaringan-jaringan di Internet menggunakan IP prefix tertentu sebagai alamatnya sesuai aturan pengalamatan pada *Internet Protocol* (IP). Suatu prefix jaringan biasanya dituliskan dalam notasi CIDR, misalnya, 195.55.100.0/24, yang berarti 24-bit dari alamat tersebut dialokasikan untuk network prefix dan 8-bit sisanya digunakan untuk alamat host yang berada pada jaringan tersebut. Host dengan alamat 195.55.100.1 hingga 195.55.100.254 berada pada jaringan ini [2]. Salah satu kelemahan dari protokol BGP adalah kemampuannya untuk diserang melalui metode yang dikenal sebagai BGP *hijacking* atau prefix *hijacking* [3][[4].

BGP *Route Hijacking*, juga dikenal sebagai *Prefix Hijacking*, *Route Hijacking*, atau *IP Hijacking*, adalah pengambilalihan blok alamat IP secara tidak sah dengan merusak tabel *routing Internet* yang menggunakan *Border Gateway Protocol* (BGP). Sebuah alamat IP Prefix diiklankan di internet menggunakan protokol BGP dengan blok alamat IPv4 atau IPv6, serta jalur *Autonomous System Number* (AS *Number*) yang menunjukkan *Next-Hop* ASN yang harus dilalui untuk mencapai blok alamat tersebut. Dalam insiden BGP *Hijacking*, penyerang dapat memanipulasi IP Prefix dengan mengalihkan rute lalu lintas untuk mencegat atau memodifikasi trafik. Dampak insiden BGP *Hijacking* yang sering terjadi adalah perlambatan koneksi pengguna ke jaringan. Lebih buruk lagi, penyerang dapat menciptakan "*black hole*" di seluruh jaringan, termasuk layanan internal organisasi, sehingga mengakibatkan "*down*". Insiden ini menyerupai serangan DDoS [5].

Salah satu cara untuk mencegah *IP Hijacking* adalah dengan menerapkan RPKI (*Resource Public Key Infrastructure*) merupakan metode kriptografi yang mengasosiasikan *routing table* BGP dengan origin AS yang benar [6]. RPKI memiliki konsep Setiap alamat IP akan disertifikasi oleh root CA yang memastikan bahwa hanya pemilik sah dari alamat IP tersebut yang dapat menggunakannya di internet. RPKI bekerja dengan memfilter alamat IP sesuai dengan pemiliknya. Router-router yang terhubung ke internet diatur agar terhubung ke Validator RPKI untuk melakukan validasi ASN dan alamat IP. Dengan demikian, router dapat membedakan mana alamat IP yang valid dan mana yang tidak. Dengan metode RPKI, alamat jaringan dalam internet (dikenal sebagai prefix) difilter sesuai dengan kepemilikan mereka, memverifikasi apakah rute jaringan yang ditambahkan ke BGP berasal dari AS yang diizinkan atau tidak [7].

Kajian penelitian terdahulu dilakukan oleh Ernawati dan Endrawan [8] mengenai kinerja jaringan komputer dengan memanfaatkan *Border Gateway Protocol* (BGP) dan *Dynamic Routing*. Hasil pengujian menunjukkan bahwa sistem jaringan komputer yang menggunakan BGP memiliki efisiensi yang tinggi, dengan rata-rata *latency* sebesar 0 ms (dibandingkan dengan 82 ms tanpa BGP) dan *traceroute* (konten lokal) sebanyak 4 hop (dibandingkan dengan 8 hop tanpa BGP). Namun, *traceroute* untuk konten non-lokal menunjukkan persentase yang sama, hal ini disebabkan karena seluruh *prefix* non-lokal harus diperoleh dari *port backbone* yang merupakan port lama tanpa BGP. Testart, dkk [9]. melakukan penelitian untuk mengevaluasi dampak penerapan dan registrasi *Resource Public Key Infrastructure* (RPKI). Hasil studi menunjukkan bahwa registrasi *Autonomous System* (AS) dan *prefix* ke dalam *Regional Internet Registry* (RIR) efektif dalam mencegah serangan *hijacking*. Semakin banyak AS dan prefix yang didaftarkan, semakin kecil peluang untuk dilakukan *hijacking*. Pranaya dan Weelem [2] melakukan penelitian mengenai implementasi BGP dan RPKI menggunakan *Bird Internet Routing Daemon* (BIRD). Hasil penelitian menunjukkan bahwa router pada AS berhasil melakukan validasi terhadap *routing advertisement* yang diterima dari BGP peer-nya. Semua subnet yang *invalid* dan *unknown* tidak diteruskan ke router lain dalam AS di mana router tersebut berada, sehingga kekacauan *routing* dapat dicegah. Penelitian lain oleh Iryani, dkk [10] melakukan penelitian untuk mengukur kinerja *Border Gateway Protocol Resource Public Key Infrastructure* (BGP RPKI) di PT Time Excelindo. Hasil implementasi BGP RPKI dalam jaringan menunjukkan bahwa penggunaan *filtering* dapat meningkatkan penggunaan sumber daya CPU dan memori, sambil mengurangi kemampuan router dalam menerima informasi *prefix*, meskipun dampaknya sedikit atau tidak signifikan. Dalam hal kinerja jaringan yang berjalan, studi ini menunjukkan bahwa jaringan sebelum menerapkan RPKI memiliki kualitas yang lebih optimal, dengan selisih kecepatan sebesar 0,11 Mbps, 0,01 Mbps untuk nilai upload, dan nilai latensi sebesar 0,13 ms.

Berdasarkan pemaparan permasalahan dan kajian penelitian terdahulu, peneliti melakukan penelitian pada PT. Bintang Mataram Teknologi bertujuan untuk mengevaluasi keamanan protokol BGP dalam suatu AS untuk mengamankan AS tersebut dari serangan *BGP hijacking* dengan mengatasinya menggunakan RPKI. Penelitian ini menggunakan arsitektur jaringan atau skenario sebenarnya pada PT. Bintang Mataram

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Teknologi dengan memanfaatkan penggunaan simulator EVE-NG dan Virtual server sebagai RPKI validator dan protokol BGP dikonfigurasi dengan menggunakan Mikrotik RouterOS versi 7. MikroTik RouterOS versi 7 memungkinkan pengguna untuk mengatur dan mengelola protokol BGP serta menerapkan fitur-fitur keamanan seperti RPKI untuk memverifikasi keaslian informasi *routing*. Pengujian dilakukan dengan menggunakan 3 AS, 6 router, 2 virtual PC, 1 virtual server untuk validator, dan 1 virtual PC sebagai fake server DNS Google.

2. Metode Penelitian

2.1 Alur Peneltian

Tahapan dalam penelitian ini terdiri dari beberapa langkah yakni seperti Gambar 1 berikut ini:

Gambar 1. Alur Penelitian

Langkah yang pertama dimulai dengan melakukan identifikasi masalah yaitu bagaimana mengimplementasikan keamanan BGP dan RPKI menggunakan MikroTik RouterOS versi 7 ke dalam suatu AS. Langkah yang kedua adalah menganalisis topologi dan kebutuhan sistem serta perangkat yang digunakan untuk diimplementasikan di simulasi. Langkah yang ketiga, membuat perancangan topologi jaringan dan mengimplementasikan protokol BGP dan RPKI menggunakan MikroTik RouterOS versi 7 ke dalam simulasi menggunakan EVE-NG sebagai simulator dan sebuah Virtual Server yang berperan sebagai RPKI Validator. Langkah berikutnya melakukan proses pengujian dilakukan menggunakan 3 AS, 6 router, 2 virtual PC, 1 virtual server untuk validator, dan 1 virtual PC sebagai fake server DNS Google. Setelah langkah tersebut, dilakukan pengujian untuk filtering prefix. Tahap terakhir adalah membuat kesimpulan berdasarkan hasil implementasi dan evaluasi.

2.2 BGP (*Border Gateway Protokol*)

BGP adalah salah satu komponen utama *routing* yang digunakan di internet untuk pertukaran tabel routing antar *autonomous system*. Salah satu keunggulan dari protokol routing BGP adalah atribut-atribut pendukungnya, yang digunakan sebagai parameter untuk menentukan jalur terbaik ke suatu situs, serta mengatur masuk dan keluarnya pembaruan routing dari *router-router* tetangga BGP [11].

2.3 RPKI (*Resource Publik Key Infrastruktur*)

RPKI adalah metode kriptografi yang memastikan rute jaringan (*prefix*) dan mengelompokkan informasi tabel routing dalam BGP dengan origin AS yang sah. RPKI dirancang untuk mencegah pembajakan rute antar AS. Pembajakan rute ini sangat mungkin terjadi karena infrastruktur internet saat ini terdiri dari 700.000 *prefix* yang dikelola oleh 5 registri internet regional. Banyaknya *prefix* tersebut membuat sulit untuk mengetahui pemilik IP *address*, yang kemudian dimanfaatkan oleh cracker untuk membajak IP *address* dalam protokol BGP [2].

2.4 Routinator

Routinator 3000, atau biasa disebut *routinator*, adalah perangkat lunak RPKI *relying party* berbasis *open source* yang dikembangkan oleh NLnet Labs menggunakan bahasa pemrograman Rust. *Routinator* dirancang untuk dapat digunakan dengan aman dan berjalan secara minimalis tanpa memerlukan perangkat keras dengan spesifikasi tinggi di hampir semua sistem operasi. *Routinator* terhubung ke *Trust Anchors* dari lima *Regional Internet Registries* (RIR) — APNIC, AFRINIC, ARIN, LACNIC, dan RIPE NCC. *Routinator* mengunduh semua sertifikat dan ROA dari berbagai repositori, memverifikasi tanda tangan, dan menyediakan hasilnya agar dapat digunakan dalam *router* yang akan menerapkan RPKI [7].

2.5 Simulator EVE-NG

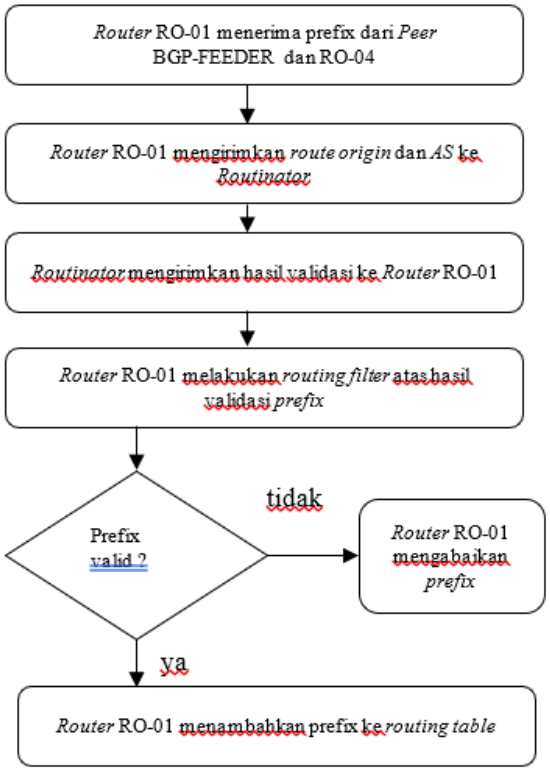
EVE-NG adalah alat yang memungkinkan admin jaringan untuk mensimulasikan router, sakelar, firewall, dan banyak perangkat virtual lainnya. Di lab jaringan, perangkat dari berbagai vendor dapat dibuat. Jika vendor jaringan memiliki alat virtual, kemungkinan besar dapat berjalan di EVE-NG. EVE-NG juga mendukung penambahan gambar server Linux dan Windows. Untuk migrasi atau peningkatan jaringan/keamanan/sistem yang besar, namun tidak memiliki lab untuk menguji semua skenario secara lengkap, EVE-NG bisa menjadi solusi. Versi komunitasnya sepenuhnya gratis dan open source [12].

3. Hasil dan Pembahasan

Pada penelitian ini *routing* filter diterapkan pada MikroTik RouterOS versi 7 dengan menerapkan protokol BGP dan RPKI untuk melakukan validasi prefix dan AS.

Pada Gambar 2 menunjukkan proses penerapan tersebut :

P-ISSN : 2089-3353
E-ISSN : 2808-9162



Gambar 2. Skenario Validasi Prefix dan AS

Berikut ini adalah penjelasan dari proses validasi prefix dan AS :

Router RO-01 menerima prefix dari dua BGP *Peer* menggunakan protokol BGP. Router RO-01 kemudian mengirimkan route origin yang diterima ke Routinator yang betindak sebagai RPKI Validator. *Routinator* melakukan validasi data dengan mencocokan *route* origin dan AS dengan ROA yang ada di RIR. Setelah dilakukan validasi di *Routinator* kemudian data dikirim kembali ke *Router* RO-01. Proses selanjutnya, *Router* RO-01 melakukan *routing* filter sesuai hasil validasi, apabila hasil validasi invalid maka prefix akan diabaikan, sebaliknya apabila hasilnya valid maka prefix akan diinstall ke *routing table*.

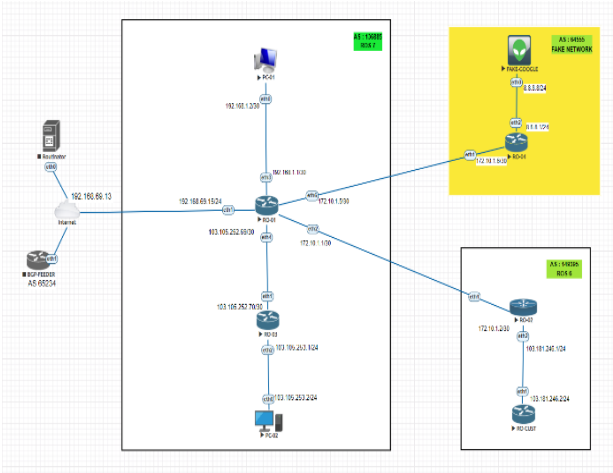
3.1 Spesifikasi Perangkat, Topologi dan Simulasi Jaringan

Sebelum memulai proses simulasi, perlu dipetakan spesifikasi perangkat yang digunakan pada penelitian ini :

Tabel 1. Spesifikasi Perangkat dan Alokasi IP Address

Perangkat Jaringan	Spesifikasi	*Interface*	IP Address	AS Number
Router BGP-FEEDER	Routerboard CCR2116-12G-4S+	SSTP-1	10.10.12.153	136885
Routinator	*Virtual Machine*	Eth0	192.168.69.13	
Router (RO-01)	Mikrotik CHR RouterOS v7.11.2	Ether1 Ether2	192.168.69.15 172.10.1.1	136885 65432
		Ether3 Ether4 Ether6 SSTP	192.168.1.1 103.105.252.1 172.10.1.5 10.10.12.154	
Router (RO-02)	Mikrotik CHR RouterOS v6.49.13	Ether1 Ether2	172.10.1.2 103.181.246.1	149395
Router (RO-03)	Mikrotik CHR RouterOS v7.11.2	Ether1 Ether2	103.105.252.2 103.105.253.1	136885
Router (RO-04)	Mikrotik CHR RouterOS v7.11.2	Ether1 Ether2	172.10.1.6 8.8.8.1	64555
Router (RO-CUST)	Mikrotik CHR RouterOS v6.49.13	Ether1	103.181.246.2	
User (PC-01)	Virtual PC	Eth0	192.168.1.2	
User (PC-02)	Virtual PC	Eth0	103.105.253.2	
FAKE-GOOGLE	Virtual PC	Eth0	8.8.8.8	

Berdasarkan pemetaan spesifikasi perangkat jaringan tersebut, menghasilkan topologi jaringan seperti terlihat pada Gambar 3 dibawah ini :



Gambar 3. Topologi Jaringan Menggunakan Simulator EVE-NG

Proses simulasi dilakukan dengan menggunakan aplikasi virtualisasi VMware yang memungkinkan beberapa *virtual machine* (VM) dijalan bersamaan. *Virtual Machine* (VM) pertama digunakan untuk menginstall simulator jaringan EVE-NG yang akan digunakan untuk implementasi fungsi Router MikroTik. *Virtual Machine* (VM) kedua diinstall *Operating System* (OS) Linux Ubuntu versi 20.04.0 LTS yang berfungsi untuk menjalankan aplikasi Routinator sebagai RPKI Validator.

Router BGP-FEEDER adalah *routing server* yang menyediakan *prefix list* origin yang terdistribusi secara

realtime di jaringan internet global. Komunikasi dari router BGP-FEEDER dengan *router* RO-01 memanfaatkan jalur *tunneling* dengan *Virtual Private Network* (VPN) *Point-to-Point Tunneling Protocol* (PPTP).

Server Routinator berfungsi sebagai RPKI Validator terhubung secara langsung dengan Router RO-01 di *interface* ether1. Virtual PC PC-01 terhubung langsung dengan router RO-01 pada *interface* ether3. Router RO-02 menggunakan MikroTik versi 6.49.13 terhubung dengan RO-01 di interface ehter2, yang berfungsi untuk melakukan evaluasi BGP as-path. Router RO-03 menggunakan MikroTik versi 7.11.2 terhubung dengan router RO-01 di interface ether4, berfungsi untuk melakukan evaluasi BGP as-path. Virtual PC PC-02 terhubung dengan router RO-03 di interface ether2, yang berfungsi untuk melakukan pengecekan jalur *routing* ke arah Server DNS Google 8.8.8.8. Router RO-04 difungsikan sebagai traffic generator yang melakukan BGP hijacking dari prefix ip DNS Google 8.8.8.0/24.

Virtual PC FAKE-GOOGLE dikonfigurasi menggunakan IP 8.8.8.8 terhubung dengan router RO-04 yang berfungsi sebagai *dummy* server DNS Google. Konfigurasi BGP di *router* RO-01 dan *router* RO-03 menggunakan *AS Number* 136885, *router* RO-01 dan RO-03 akan melakukan *advertise prefix* 103.105.252.0/23. *Router* RO-01 akan menerima seluruh *prefix* yang ada di internet dari *router* BGP-FEEDER dan menerima *prefix* 8.8.8.0/24 dari *router* RO-04.

Tabel 2. Distribusi Prefix IP

Router	IP	ASN	Prefix diadvertise
BGP-FEEDER	10.11.12.13	65234	Semua prefix (*full route*)
RO-01	192.168.69.15	136885	Full route + 103.105.252.0/24
RO-02	172.10.1.2	149395	103.181.246.0/24
RO-03	103.105.252.70	136885	103.105.253.0/24
RO-04	172.10.1.6	64555	8.8.8.0/24

3.2 Konfigurasi dan Implementasi BGP dan RPKI Pada Perangkat Jaringan

Pada simulasi ini, perangkat Routinator sudah berjalan normal menggunakan IP 192.168.69.13, langkah selanjutnya adalah melakukan konfigurasi pada perangkat lain, dimulai dengan :

Konfigurasi Router RO-01 :

/ip firewall address-list
add address=192.168.1.0/24 list=NETEXPORT
add address=192.168.69.0/24 list=NETEXPORT
add address=103.105.252.0/24 list=NETEXPORT

/routing bgp template
set default as=136885 disabled=no output.network=NETEXPORT routing-table=main

/routing filter rule
add chain=EXPORT_RO02 disabled=yes rule=
"if (afi ipv4 && dst in NETEXPORT) { accept}"
add chain=EXPORT_RO02 disabled=no rule=accept
add chain=IMPORT_RO02 disabled=no rule="rpki-verify RPKI136885"
add chain=IMPORT_RO02 disabled=no rule=
"if (rpki invalid) {reject} else {accept}"
add chain=EXPORT_RO03 disabled=no rule=accept
add chain=IMPORT_RO03 disabled=no rule=accept
add chain=EXPORT_RO04 disabled=no rule=accept
add chain=IMPORT_RO04 disabled=no rule="rpki-verify RPKI136885"
add chain=IMPORT_RO04 disabled=no rule=
"if (rpki invalid) {reject} else {accept}"
add chain=DENY_ALL disabled=no rule="reject;"
add chain=ACCEPT_IN disabled=no rule="if (dst-len in 8-24 && bgp-as-path-slow-
legacy 15169) { set gw 192.168.69.1; accept; }"

/routing rpki
*add address=192.168.69.13 disabled=no expire-interval=7200 group=RPKI136885 *
port=3323 preference=1 refresh-interval=60 retry-interval=600 vrf=main

/routing bgp connection
add address-families=ip as=136885 connect=yes disabled=no input.filter=
*IMPORT_RO02 listen=yes local.address=172.10.1.1 .role=ebgp name=RO-02 *
output.default-originate=if-installed .filter-chain=EXPORT_RO02 .network=
*NETEXPORT remote.address=172.10.1.2/32 .as=149395 routing-table=main *
templates=default
*add address-families=ip as=136885 connect=yes disabled=no hold-time=10s *
*input.filter=IMPORT_RO03 listen=yes local.role=ibgp-rr name=RO-03 *
*nexthop-choice=force-self output.default-originate=if-installed *
.filter-chain=EXPORT_RO03 .network=NETEXPORT remote.address=
103.105.252.2/32 .as=136885 routing-table=main templates=default
Add address-families=ip as=136885 connect=yes disabled=no input.filter=
IMPORT_RO04 listen=yes local.role=ebgp name=RO-04 nexthop-choice=
force-self output.default-originate=if-installed .filter-chain=
*EXPORT_RO04 .network=NETEXPORT remote.address=172.10.1.6/32 .as=64555 *
routing-table=main templates=default
*add address-families=ip as=65432 disabled=no input.filter=ACCEPT_IN *
local.role=ebgp name=peer-feeder output.filter-chain=DENY_ALL
remote.address=10.11.12.13/32 .as=65234 routing-table=main templates=\ AS65432

Aturan *routing* filter ke 8 dan 9 adalah proses validasi prefix menggunakan RPKI, apabila prefix dinyatakan invalid maka prefix tersebut akan ditolak dan tidak didistribusikan ke *router* yang lain :

Konfigurasi Router RO-02 :

/routing bgp instance
set default as=149395

/ip address
add address=172.10.1.2/30 interface=ether1 network=172.10.1.0
add address=103.181.246.1/24 interface=ether2 network=103.181.246.0

/ip dhcp-client
add disabled=no interface=ether1

P-ISSN : 2089-3353
E-ISSN : 2808-9162

/routing bgp network
add network=103.181.246.0/24 synchronize=no

/routing bgp peer
*add in-filter=IMPORT_AS136885 name=RO.01-AS136885 out-filter=EXPORT_AS136885 *
remote-address=172.10.1.1 remote-as=136885 update-source=ether1
/routing filter
add action=accept chain=IMPORT_AS136885
add action=accept chain=EXPORT_AS136885
*prefix=103.181.246.0/24 *
prefix-length=24

Konfigurasi Routing RO-03

/routing bgp template
set default as=136885 disabled=no routing-table=main

/ip address
add address=103.105.252.2/30 interface=ether1
network=103.105.252.0
add address=103.105.253.1/24 interface=ether2
network=103.105.253.0

/ip dhcp-client
add interface=ether1

/ip firewall address-list
add address=103.105.253.0/24 list=mynetworks

/routing bgp connection
add as=136885 disabled=no hold-time=10s
input.filter=IMPORT_RO01 local.role=
ibgp-rr name=RO-01 output.filter-chain=EXPORT_RO01
*.network=mynetworks *
remote.address=103.105.252.1/32 .as=136885 routing-table=main templates=default

/routing filter rule
add chain=EXPORT_RO01 disabled=no
rule="if(dst==103.105.253.0/24){accept}"
add chain=IMPORT_RO01 disabled=no rule=accept
/system identity
set name=RO-03

Konfigurasi Router R0-04

/routing bgp template
set default as=64555 disabled=no routing-table=main

/ip address
add address=172.10.1.6/30 interface=ether1 network=172.10.1.4
add address=8.8.8.1/24 interface=ether2 network=8.8.8.0

/ip dhcp-client
add interface=ether1

/ip firewall address-list
add address=8.8.8.0/24 list=MYNETWORKS

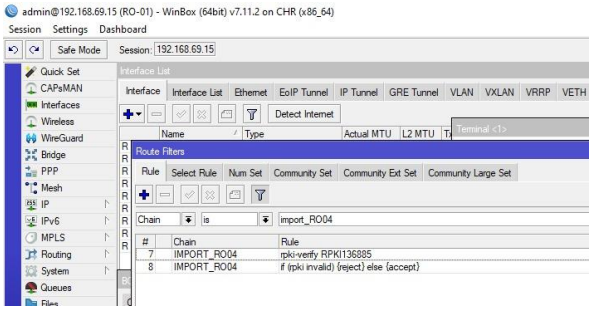
/routing bgp connection
add as=64555 disabled=no input.filter=IMPORT local.role=ebgp
*name=RO-01 *
output.filter-chain=EXPORT .network=MYNETWORKS
remote.address=
172.10.1.5/32 .as=136885 routing-table=main templates=default

/routing filter rule
add chain=IMPORT disabled=no rule=accept
add chain=EXPORT disabled=no rule=accept

/system identity
set name=RO-04

3.3 Hasil Pengujian

Skenario pengujian, dilakukan dengan mengimplementasikan BGP menggunakan *filtering* RPKI/status RPKI aktif. Sebelum melakukan proses simulasi, router RO-01 akan dikonfigurasi terlebih dahulu dengan mengaktifkan status RPKI-nya, berikut hasilnya :



Gambar 4. Status RPKI Aktif

Pertama, Router BGP-FEEDER akan *advertise* prefix 8.8.8.0/24 kepada Router RO-01 menggunakan sintaks dibawah ini :

***Advertise* prefix 8.8.8.0/24 ke RO-01**

[user@CR-JOG.CCR1036-NCDC] > routing bgp advertisements print where prefix=8.8.8.0/24 peer="RO-01"

Prefix 8.8.8.0/24 yang dikirmkan merupakan blok IP milik Google dengan origin ASN yang valid dengan angka 15169.

Tabel 3. Daftar BGP AS Path Yang Valid

IPv4 Prefix	BGP AS Path
8.8.8.8/24	136885,55666,58552,15169
8.8.8.0/24	136885,55666,58552,15169
103.181.246.0/24	136885,149395,149395,149395,149395,149395
103.181.247.0/24	136885,149395,149395,149395,149395,149395
103.58.111.0/24	136885,55666,133832
178.128.80.0/20	136885,58552,14061

Kedua, Router RO-04 akan melakukan hal yang sama dengan BGP-FEEDER yaitu *advertise* prefix 8.8.8.0/24 ke Router RO-01. Berikut sintaks yang digunakan:

***Advertise* prefix 8.8.8.0/24 ke RO-01**

[admin@RO-04] > /routing/bgp/advertisements/print where dst=8.8.8.0/24 peer=RO-01-1 afi=ip nexthop=172.10.1.6 origin=0 as-path=sequence 64555

Pada simulasi ini, Router RO-04 digunakan sebagai pembajak/hijacker IP google dengan prefix 8.8.8.0/24 dan terkoneksi dengan sebuah server palsu dengan IP 8.8.8.8/24. Berikut ini adalah daftar lengkap prefix valid yang digunakan pada topologi jaringan di Gambar 3:

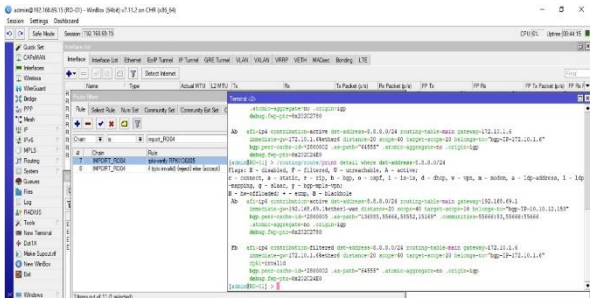
Tabel 4. Data Prefix IPV4 dan AS Origin

IPV4 Prefix	AS Origin	Deskripsi
8.8.8.0/24	**15169**	**Google LLC**
8.8.4.0/24	15169	Google LLC

P-ISSN : 2089-3353
E-ISSN : 2808-9162

103.181.246.0/24	149395	RSUD Tidar Magelang
103.181.247.0/24	149395	RSUD Tidar Magelang
103.58.111.0/24	133832	Universitas Mercu Buana Yogyakarta
178.128.80.0/20	14061	DigitalOcean LLC

Setelah RPKI aktif, prefix 8.8.8.0/24 akan di *advertise* oleh kedua router.



Gambar 5. Hasil *filtering* Menggunakan RPKI

Pada gambar 5 terlihat bahwa router RO-01 menerima prefix 8.8.8.0/24 dari router BGP-FEEDER dan RO-04. Setelah itu router RO-01 akan melakukan *filtering* dari kedua prefix tersebut dengan cara mengirmkan prefik tersebut kepada routinator untuk mengetahui prefix valid yang dikirimkan oleh kedua router tersebut. Routinantor akan memberikan informasi prefix yang valid kepada RO-01. Hasil filtering prefix tersebut tidak akan diproses maupun didistribusikan ke router RO-02, RO-03.

Sebaliknya, skenario yang kedua diimplementasikan jika filtering RPKI statusnya TIDAK AKTIF. Berikut hasilnya :

```
[admin@RO-01] > /routing/route/print detail where dst-address=8.8.8.0/24
Flags: X - disabled, F - filtered, U - unreachable, A - active;
c - connect, s - static, r - rip, b - bgp, o - ospf, i - is-is, d - dhcp, v - vpn, m - modem, a - ldp-addr
ess, l - ldp-mapping, g - slaac, y - bgp-mpls-vpn;
H - hw-offloaded; + - ecmp, B - blackhole
 b   afi-ip4 contribution=candidate dst-address=8.8.8.0/24 routing-table=main gateway=192.168.69.1
       immediate-gw=192.168.69.1%ether1-wan distance=20 scope=40 target-scope=10
       belongs-to="bgp-IP-10.10.12.153"
       bgp.peer-cache-id=*2800004 .as-path="136885,55666,58552,15169" .communities=55666:53,55666:55666
       .atomic-aggregate=no .origin=igp
       debug.fwp-ptr=0x202C2780

 Ab  afi-ip4 contribution=active dst-address=8.8.8.0/24 routing-table=main gateway=172.10.1.6
       immediate-gw=172.10.1.6%ether6 distance=20 scope=40 target-scope=10
       belongs-to="bgp-IP-172.10.1.6"
       bgp.peer-cache-id=*2800003 .as-path="64555" .atomic-aggregate=no .origin=igp
       debug.fwp-ptr=0x202C25A0
[admin@RO-01] >
```

Gambar 6. Hasil Advertise Prefix Pada Router RO-01

Jika *routing* filter dinonaktifkan maka prefix 8.8.8.0/24 yang diterima dari RO-04 akan diproses dan didistribusikan ke RO-02, RO-03, sedangkan prefix origin 8.8.8.0/24 valid yang diterima dari router BGP-FEEDER akan diabaikan dikarenakan jalur *best-path* nya adalah melalui router RO-04, sehingga hal ini akan menyebabkan BGP *hijacking* ke arah server DNS Google. Untuk membuktikan terjadi BGP *hijacking*, dilakukan proses traceroute ke IP DNS Google 8.8.8.8 dari PC-*client*, berikut hasilnya :

```
PC-01> trace 8.8.8.8 -P 1 -m 16
trace to 8.8.8.8, 16 hops max (ICMP), press Ctrl+C to stop
 1   192.168.1.1   3.620 ms  2.211 ms  1.056 ms
 2   172.10.1.6    6.045 ms  2.984 ms  8.683 ms
 3   8.8.8.8       8.276 ms  28.957 ms  8.772 ms
```

Gambar 7. Hasil BGP *Hijacking Traceroute* ke IP 8.8.8.8

Terlihat pada gambar terjadi BGP *hijacking*. Itu dibuktikan dengan jumlah hop ke DNS Google menjadi lebih pendek yaitu 3 hop.

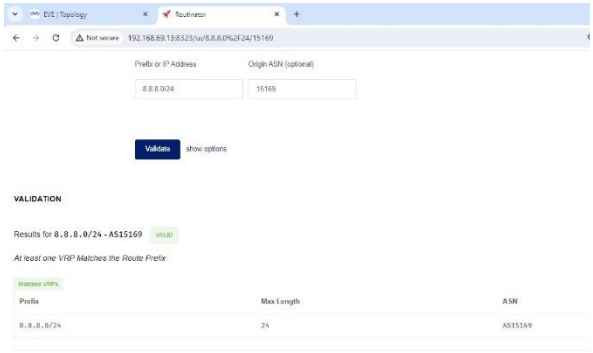
Jika tidak terjadi BGP Hijacking, Ketika dilakukan proses traceroute ke IP DNS Google menjadi lebih Panjang, minimal 4 hop jika melewati jaringan PT. Bintang Mataram Teknologi, berikut hasilnya:

```
PC-02> trace 8.8.4.4 -P 1 -m 16
trace to 8.8.4.4, 16 hops max (ICMP), press Ctrl+C to stop
 1   103.105.253.1   4.747 ms  1.553 ms  2.408 ms
 2   103.105.252.1   8.330 ms  20.667 ms  14.946 ms
 3   192.168.69.1   40.983 ms  12.209 ms  25.681 ms
 4   103.105.252.69   21.084 ms  20.400 ms  26.345 ms
 5   10.10.67.1   22.824 ms  19.136 ms  20.545 ms
 6   10.10.6.29   21.086 ms  20.978 ms  32.647 ms
 7   10.10.6.25   19.472 ms  32.004 ms  22.133 ms
 8   103.105.252.234   26.894 ms  28.166 ms  24.337 ms
 9   119.2.55.82   48.516 ms  28.285 ms  36.058 ms
10   49.128.183.225   25.488 ms  47.683 ms  30.060 ms
11   202.72.203.109   51.362 ms  38.730 ms  41.102 ms
12   202.72.203.1   32.182 ms  33.233 ms  42.833 ms
13   72.14.221.202   51.004 ms  43.004 ms  54.788 ms
14   192.178.109.185   43.671 ms  43.952 ms  41.465 ms
15   142.251.241.3   42.584 ms  44.423 ms  44.432 ms
16   8.8.4.4   37.855 ms  48.055 ms  42.827 ms
```

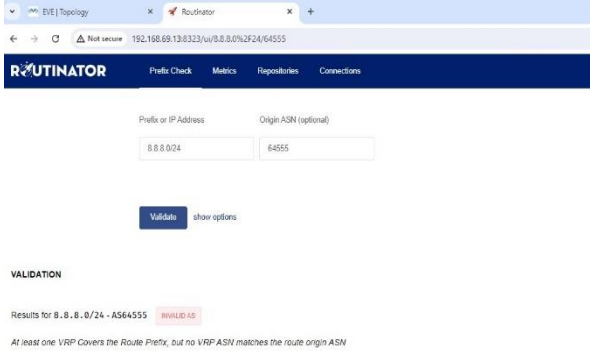
Gambar 8. Hasil Normal *Traceroute* ke IP 8.8.8.8

Proses evaluasi keamanan dilakukan dengan mengaktifkan dan menonaktifkan *routing* filter.

Cara lain untuk mevalidasi prefix dan AS dengan menggunakan fitur bawaan dari Routinator, yang dapat diakses melalui http://192.168.69.13:8323/ui, IP yang digunakan ini merupakan IP dari Routinator



Gambar 9. Hasil Validasi Prefix : Valid



Gambar 10. Hasil Validasi Prefix : Invalid

4. Kesimpulan

Pada penelitian ini dilakukan pembahasan dan implementasi pengamanan jaringan internet yang menggunakan routing protokol BGP dan RPKI yang

dikonfigurasi pada router MikroTik RouterOS versi 7. Prefix IP 8.8.8.0/24 yang diterima dari masing-masing peer kemudian diteruskan ke Routinator sebagai RPKI Validator, masuk pada tahapan tersebut prefix IP 8.8.8.0/24 akan di-validasi antara prefix dan AS. Selanjutnya router akan memilih prefix IP yang statusnya valid yaitu prefix IP 8.8.8.0/24 yang route origin-nya dari AS 15169 untuk diproses masuk ke dalam routing tabel menggunakan routing filter yang telah dikonfigurasi menggunakan RPKI. Pengujian tersebut berhasil mengamankan jaringan di PT. Bintang Mataram Teknologi dari gangguan yang disebabkan BGP hijacking menuju ke arah jaringan server DNS Google.

Daftar Rujukan

[1] A. F. Rochim and Y. Christiyono, "Desain dan Simulasi Internal Border Gateway Protocol (IBGP) Menggunakan Graphical Network Simulator (Studi Kasus pada Jaringan Universitas Diponegoro)," *Transm. J. Ilm. Tek. Elektro*, vol. 16, no. 1, pp. 20–25, 2014, [Online]. Available: https://ejournal.undip.ac.id/index.php/transmisi/article/view/6215/5241.

[2] V. B. Pranaya and T. Wellem, "Implementasi BGP dan Resource Public Key Infrastructure menggunakan BIRD untuk Keamanan Routing," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 6, pp. 1161–1170, 2021, doi: 10.29207/resti.v5i6.3631.

[3] T. E. 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.

[4] U. Faridah, *"Implementasi Border Gateway Protocol (BGP) pada Test Bed IDREN (Indonesian Research Education Network)*. Surabaya: Institut Teknologi Sepuluh November, 2018.

[5] B. H. dan H. M.-B. Bagian Komunikasi Publik, *Ancaman Siber BGP Hijacking*. Badan Siber dan Sandi Negara.

[6] M. Wählisch, O. Maennel, and T. C. Schmidt, "Towards detecting BGP route hijacking using the RPKI," *Comput. Commun. Rev.*, vol. 42, no. 4, pp. 103–104, 2012, doi: 10.1145/2377677.2377702.

[7] 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.

[8] 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.

[9] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark, "To Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 12048 LNCS, pp. 71–87, doi: 10.1007/978-3-030-44081-7_5.

[10] K. Saputro, T. Daniel, *Membangun Server Internet dengan Mikrotik OS.* Yogyakarta: Gava Media, 2008.

[11] R. Jannah, A. N. Laili, W. Pratiwi, A. D. Perkasa, "Automasi Konfigurasi Routing pada Router BGP menggunakan Netmiko," vol. 3, no. 1, pp. 9–14, 2023.

[12] F. Rozi, S. Z. Fajriyah, R. Maulida, "DNS Server Berbasis Ubuntu-22.04.1-Eve- NG-5.0.3.105," *J. Informatics Commun. Technol.*, vol. 4, no. 2, pp. 1–8, 2022.