ANALISIS PERBANDINGAN PROTOKOL *ROUTING* BGP, EIGRP, DAN OSPF TERHADAP SERANGAN *DDOS* DAN *PACKET SNIFFING*

SKRIPSI

LINGGA FATTAH ADRITAMA 2007421020

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2024

ANALISIS PERBANDINGAN PROTOKOL *ROUTING* BGP, EIGRP, DAN OSPF TERHADAP SERANGAN *DDOS* DAN *PACKET SNIFFING*

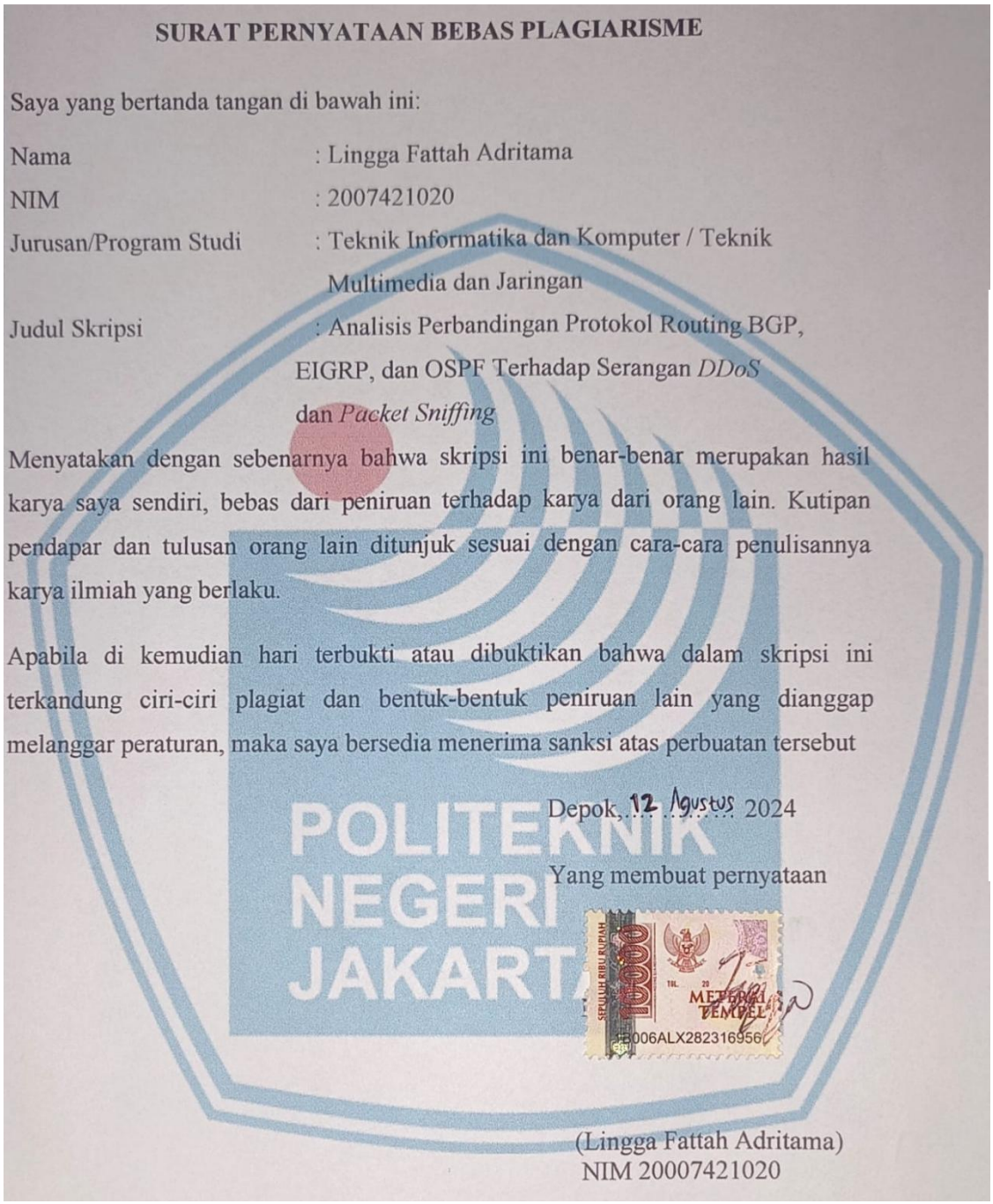
SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

LINGGA FATTAH ADRITAMA 2007421020

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2024

SURAT PERNYATAAN BEBAS PLAGIARISME



SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Lingga Fattah Adritama
NIM : 2007421020
Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Perbandingan Protokol Routing BGP, EIGRP, dan OSPF Terhadap Serangan *DDoS* dan *Packet Sniffing*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapar dan tulusan orang lain ditunjuk sesuai dengan cara-cara penulisannya karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut

Depok, 12 Agustus 2024

Yang membuat pernyataan

10000 METERAI TEMPEL 006ALX282316956

(Lingga Fattah Adritama)
NIM 20007421020

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama	: Lingga Fattah Adritama
NIM	: 2007421020
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul skripsi	: Analisis Perbandingan Protokol *Routing* BGP, EIGRP, Dan OSPF Terhadap Serangan *DDoS* Dan *Packet Sniffing*.

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin, Tanggal 29, Bulan Juli, Tahun 2024, dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I	: Asep Kurniawan, S.Pd., M.Kom	( )
Penguji I	: Maria Agustin, S.Kom., M.Kom	( )
Penguji II	: Susana Dwi Yulianti, S.Kom., M.Kom	( )
Penguji III	: Iik Muhammad Malik Matin, S.Kom., M.T	( )

Mengetahui :

Ketua Jurusan Teknik Informatika dan Komputer

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Dengan memanjatkan puji dan syukur atas kehadirat Allah SWT karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan skripsi yang diberi judul "Analisis Perbandingan Protokol *routing* BGP, EIGRP, dan OSPF Terhadap Serangan *DDoS* dan *Packet Sniffing*" dengan tepat waktu dan sesuai ketentuan yang ada. Adapun tujuan penulisan laporan ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik. Dalam prosesnya, penulis menyadari bahwa penyusunan laporan ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

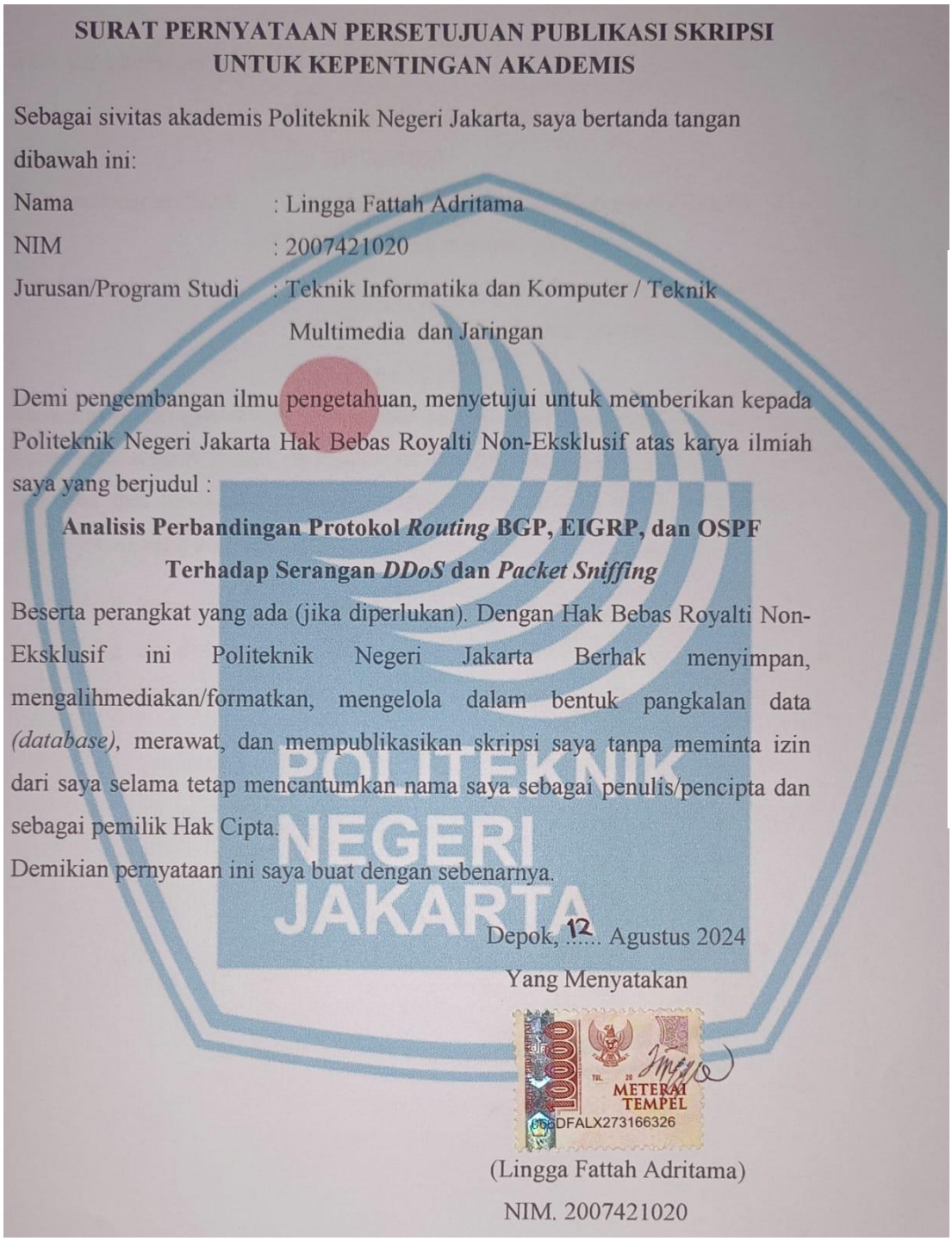
1. Allah SWT yang telah memberikan kemudahan dan kelancaran kepada penulis dalam pengerjaan skripsi dan penulisan laporan.
2. Bapak Asep Kurniawan, S.Pd., M. Kom, selaku dosen pembimbing yang telah meluangkan memberikan dukungan dan bimbingan penyusunan skripsi ini.
3. Orang tua dan keluarga yang selalu memberikan bantuan baik moral maupun material.
4. Teman-teman seperjuangan penulis yang telah memberikan bantuan serta masukan selama penelitian.
5. Seluruh jajaran dosen dan staff Program Studi Teknik Informatika dan Komputer Politeknik Negeri Jakarta

Akhir kata, penulis menyadari bahwa laporan skripsi ini masih memiliki banyak kesalahan dan kekurangan, untuk itu kritik dan saran yang membangun sangat penulis harapkan demi pengembangan diri maupun kesempurnaan laporan ini.

Depok, 15 Agustus 2024

Lingga Fattah Adritama

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS



SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademis Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Lingga Fattah Adritama
NIM : 2007421020
Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis Perbandingan Protokol *Routing* BGP, EIGRP, dan OSPF Terhadap Serangan *DDoS* dan *Packet Sniffing*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 12 Agustus 2024

Yang Menyatakan

(Lingga Fattah Adritama)
NIM. 2007421020

ANALISIS PERBANDINGAN PROTOKOL *ROUTING* BGP, EIGRP, DAN OSPF TERHADAP SERANGAN *DDOS* DAN *PACKET SNIFFING*

ABSTRAK

Keberadaan internet menjadi faktor utama dalam kemudahan penyebaran informasi, yang dimanfaatkan oleh individu dan berbagai lembaga di berbagai sektor. Hal ini meningkatkan efisiensi & efektivitas dalam aktivitas masyarakat. Namun, jaringan dan protokol *routing* yang menjadi kunci akses internet tidak selalu aman dari serangan luar. Misalnya, serangan DDoS dapat membanjiri sumber daya perangkat, mengakibatkan penurunan kualitas atau bahkan kegagalan jaringan. Serangan *packet sniffing* mengancam *traffic* jaringan dengan potensi pencurian data, penyadapan kredensial, dan ancaman terhadap aspek keamanan lainnya. Penelitian ini bertujuan untuk menganalisis performa protokol BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* berbasis aplikasi GNS3. Diperlukan analisis untuk memahami kinerja protokol BGP, EIGRP, dan OSPF dalam menghadapi serangan DDoS dan *packet sniffing* berdasarkan parameter *latency, jitter, throughput,* dan *packet loss*. Pengamanan terhadap serangan DDoS dilakukan menggunakan metode *traffic shaping.* IPSec/IKEv2 digunakan untuk mengamankan serangan *packet sniffing*. Hasil pengujian menunjukkan performa OSPF yang lebih baik dalam hal *latency, packet loss*, dan *throughput*. Dalam skenario pengamanan, protokol BGP menunjukkan nilai *jitter* lebih rendah, yaitu 8,83 ms, dibandingkan dengan EIGRP sebesar 8,68 ms, dan OSPF sebesar 12 ms. Hasil penelitian menunjukkan bahwa protokol BGP dan EIGRP lebih unggul dalam beberapa kondisi uji, tetapi protokol OSPF lebih baik dalam hal nilai indeks QoS secara keseluruhan.

Kata kunci: BGP, EIGRP, OSPF, DDoS, *packet sniffing*, *traffic shaping*, IPSec/IKEv2

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat pesat serta didukung dengan keberadaan internet menjadi faktor utama dalam kemudahan proses penyebaran informasi secara cepat dan efisien. Saat ini, internet tidak hanya dimanfaatkan oleh individu tetapi juga oleh berbagai lembaga seperti instansi, organisasi, perguruan tinggi, serta lembaga pemerintah atau swasta. Dengan permintaan akan akses jaringan komputer yang semakin meningkat, perlindungan keamanan jaringan yang efektif sangatlah penting (Permana, 2019). Proses keamanan jaringan komputer bertujuan untuk menghalangi dan mendeteksi penggunaan jaringan komputer yang tidak sah. Sasaran utamanya adalah untuk mengantisipasi risiko-risiko yang mungkin timbul dari ancaman fisik atau logis terhadap jaringan komputer, yang bisa mengganggu aktivitas yang sedang berlangsung di dalamnya, baik secara langsung maupun tidak langsung. Selain itu, tujuan lainnya adalah untuk menjaga keamanan data pada sistem komputer dari berbagai macam ancaman (Permana, 2019) . Banyak sistem jaringan memiliki celah dari berbagai aspek. Kerentanan ini mungkin berasal dari sistem itu sendiri. Selain itu, ada kemungkinan bahwa suatu kerentanan terbentuk akibat kelalaian manajemen. Celah tersebut dapat dimanfaatkan oleh para peretas untuk melakukan berbagai serangan, termasuk kebocoran kata sandi (He, 2021).

Berdasarkan laporan Cloudflare “DDoS *threat report for* 2023 Q2” (Yoachimik & Pacheco, 2023) bahwa terdapat peningkatan masif sebesar 600% dalam insiden keamanan siber pada kuartal kedua tahun 2023 yang menargetkan perusahaan-perusahaan *cryptocurrency*, disertai dengan kenaikan signifikan sebesar 15% untuk serangan HTTP DDoS. Serangan *Distributed Denial of Service* (DDoS) saat ini menjadi salah satu jenis serangan yang paling umum. DDoS bertujuan menyebabkan kegagalan sistem server dengan membanjiri jaringan dengan paket atau permintaan. Oleh karena itu, dibutuhkan sistem yang mampu mengklasifikasikan serangan DDoS untuk mengidentifikasinya (Zidane, 2022).

Terdapat juga serangan *sniffing*, yaitu pada tahun 2023, peneliti keamanan menemukan kerentanan baru dalam protokol OSPF yang memungkinkan penyerang untuk mencegat dan membaca data yang ditransmisikan di jaringan *Packet sniffing* merupakan aktivitas menganalisis paket jaringan untuk memantau lalu lintas, *troubleshoot*, dan mengumpulkan bukti untuk tujuan forensik jaringan. Wireshark merupakan salah satu *tools* analisis yang paling populer untuk melakukan *packet sniffing* (Syaffiq et al., 2021) . Namun di sisi lain, *packet sniffing* juga dapat dilakukan oleh seorang peretas yang terhubung ke jaringan target untuk melakukan penyerangan seperti *session hijacking*, *denial of service*, atau serangan *man-in-the-middle* seperti menyadap paket-paket dalam jaringan dan serangan lanjutan lainnya (Tuli, 2020).

OSPF adalah standard protokol *routing* terbuka yang memiliki kemampuan untuk mengontrol jaringan yang besar (Anusuya & Baulkani, 2022) . Penelitian sebelumnya, membahas perbandingan performa *routing* telah dilakukan, dengan skenario simulasi berdurasi 4 menit untuk transmisi data suara, HTTP, dan video dalam topologi *full mesh* dan *half mesh* untuk RIP, OSPF, dan EIGRP. Terlihat bahwa OSPF memberikan performa yang lebih baik dalam transfer video, merespons perubahan jaringan dengan lebih cepat, dan lebih baik dalam memanfaatkan *bandwidth*, serta menghasilkan *delay* paling sedikit dalam jaringan. OSPF juga menghasilkan *throughput* yang lebih baik daripada protokol lain yang dievaluasi (Kabir et al., 2021). *routing* BGP telah berperan penting selama lebih dari 25 tahun dalam mendukung pertumbuhan internet. Keunggulan utama BGP terletak pada kemampuannya menangani jaringan berskala besar dengan jumlah koneksi yang sangat banyak. Selain itu, BGP menawarkan fleksibilitas tinggi dalam mengatur aliran data, sehingga menjadi pilihan ideal untuk menerapkan kebijakan perutean yang kompleks dan dinamis (Abhashkumar et al., 2021).

Keamanan protokol *routing* memainkan peran penting dalam menjaga stabilitas dan keandalan jaringan. Protokol *routing* yang aman membantu memastikan bahwa data dirutekan dengan benar dan efisien, dan bahwa jaringan terlindungi dari serangan berbahaya. Kerentanan dalam protokol *routing* memungkinkan

penyerang untuk menerapkan serangan DDoS dengan mengarahkan lalu lintas palsu ke perangkat jaringan tertentu (Bovet & Pierce, 2021). Selain itu, serangan *sniffing* memungkinkan penyerang untuk mencegat dan membaca data yang ditransmisikan di jaringan. Kerentanan dalam protokol *routing* dapat memungkinkan penyerang untuk mendapatkan akses ke informasi sensitif, seperti alamat IP dan *password* (Zeadally et al., 2020).

Berdasarkan penelitian (Suteja & Ratama, 2023) membahas metode *traffic shaping* yang dalam penerapannya dapat mengoptimalkan *bandwidth* . Penelitian tersebut melakukan uji coba dengan 6 skenario *speed test*, yaitu 25 Mbps, 50 Mbps, 75 Mbps, 100 Mbps, 150 Mbps, dan 200Mbps. Hasilnya menunjukkan nilai rata-rata *latency* sangat bagus berdasarkan standard TIPHON yaitu 6.67 ms dan *jitter* 3 ms. Metode *traffic shaping* ini juga dapat melindungi jaringan dan aplikasi dari lonjakan lalu lintas, karena dapat mengontrol jumlah data yang masuk dan keluar dari jaringan, mengelola pengguna jaringan yang mencurigakan, serta mencegah serangan seperti DDoS yang dapat menghabiskan *bansdwidth* jaringan (F5, n.d.).

Penelitian (Hudaya dan Primananda, 2023) membahas kinerja dua protokol *routing* yaitu OSPF dan IS-IS terhadap serangan DDoS (*Distributed Denial of Service*). Penelitian ini melakukan pengujian performa OSPF dan IS-IS setelah dan sebelum dilakukan serangan DDoS. Berdasarkan penelitian dapat ditarik kesimpulan bahwa serangan DDoS berhasil menyebabkan penurunan *success rate*, peningkatan *packet loss*, peningkatan waktu konvergensi, dan peningkatan *round-trip time* rata-rata pada kedua protokol. Sehingga perlu diterapkannya penerapan metode pengamanan.

Penelitian (Tama dkk., 2023) bertujuan untuk menganalisis hasil performa protokol *routing* OSPF terhadap serangan *route injection* dengan menggunakan *tools* Loki dan Wireshark. Pada penelitian tersebut penulis menyadari bahwa protokol *routing* OSPF tidak memiliki metode keamanan secara *default*, sehingga hasil pengujian serangan berdampak pada isi paket, yaitu paket-paket dapat

diketahui oleh penyusup/penyerang sehingga penulis menerapkan *passive interface* pada protokol *routing* sebagai metode keamanan.

Penelitian mengenai protokol keamanan IPSec pernah dibuat sebelumnya, yaitu (Santoso dkk., 2021). Penelitian tersebut merancang sebuah infrastruktur jaringan berbasis L2TP dan IPSec pada *router* MikroTik. Untuk pengujian keamanan penulis melakukan *sniffing* dengan *tools* Wireshark. Hasil penelitian, menunjukkan bahwa paket berhasil terenkripsi sehingga integritas dan keamanan tranmisi data dalam jaringan dapat terjaga. Penulis kemudian mengusulkan untuk menerapkan protokol IPSec pada *router* selain MikroTik serta menggunakan metode enkripsi yang berbeda. Selain itu, tingkat keamanan IPSec lebih tinggi jika dibandingkan dengan metode VPN *Tunnel*, yang mana jalur komunikasinya dilengkapi dengan kriptografi (Ariyadi dan Agung Prabowo, 2021).

Penelitian ini merupakan pengembangan dari penelitian-penelitian yang telah dilakukan sebelumnya. Pada penelitian ini, penulis akan membahas mengenai performa protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan menggunakan aplikasi GNS3. Untuk mengukur performa kedua protokol, penulis akan menggunakan beberapa parameter, mencakup *latency*, *throughput*, *jitter*, dan *packet loss*. Metode serangan yang akan disimulasikan pada penelitian ini adalah *packet sniffing* dan DDoS (*Distributed Denial of Service*). Adapun untuk metode keamanan yang akan digunakan adalah IPSec dengan enkripsi IKEv2 serta penerapan *traffic shaping* pada dua protokol yaitu BGP dan OSPF. Pada tahap akhir, penulis akan menganalisis hasil penerapan metode tersebut serta kinerja tiga protokol *routing* yaitu BGP, EIGRP, dan OSPF terhadap pengujian serangan DDoS dan *packet sniffing*.

1.2 Perumusan Masalah

Rumusan masalah yang menjadi dasar penelitian ini adalah sebagai berikut:

1. Bagaimana mensimulasikan protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* dengan metode pengamanan *traffic shaping* dan IPSec berbasis GNS3?

2. Bagaimana menganalisis perbandingan protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* dengan metode pengamanan *traffic shaping* dan IPSec berbasis GNS3?

1.3 Batasan Masalah

Berikut adalah batasan masalah yang hanya membatasi pada ruang lingkup penelitian dalam pengujian performa protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* dengan pengamanan IPSec dan *traffic shaping*, yaitu sebagai berikut:

1. Penelitian ini membatasi fokus pengujian menggunakan aplikasi GNS3 untuk simulasi jaringan.
2. Pengujian yang dilakukan terbatas pada 3 protokol *routing*, yaitu BGP, EIGRP, dan OSPF.
3. Penelitian terbatas menggunakan *tools* Wireshark untuk serangan *packet sniffing*, dan Hping3 untuk simulasi DDoS (*Distributed Denial of Service*).
4. Metode pengamanan yang diterapkan diantaranya; penerapan *traffic shaping* dan IPSec dengan metode enkripsi IKEv2.
5. Untuk mengukur performa protokol *routing*, parameter QoS (*Quality of Service*) digunakan dalam penelitian ini, mencakup *latency*, *throughput*, *jitter*, *packet loss*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

1. Untuk melakukan simulasi protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* dengan metode pengamanan *traffic shaping* dan IPSec berbasis GNS3.
2. Untuk melakukan analisis perbandingan protokol *routing* BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* dengan metode pengamanan *traffic shaping* dan IPSec berbasis GNS3.

1.4.2 Manfaat

1. Menemukan performa protokol *routing* yang lebih baik antara BGP, EIGRP, dan OSPF terhadap serangan DDoS dan *packet sniffing* berdasarkan parameter pengujian.
2. Mendapatkan hasil efektivitas metode pengamanan *traffic shaping* dan IPSEC/IKEv2 terhadap protokol *routing* BGP, EIGRP, dan OSPF.
3. Merekomendasikan protokol *routing* dengan hasil terbaik berdasarkan pengujian di antara ketiga protokol yaitu BGP, EIGRP, dan OSPF.

1.5 Sistematika Penulisan

Berikut merupakan sistematika penulisan yang digunakan pada penelitian ini, yaitu sebagai berikut:

1. BAB I PENDAHULUAN

Bab Pendahuluan berisi beberapa sub-bab, diantaranya; latar belakang dari penelitian, perumusan masalah yang menjadi fokus dalam penelitian, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan laporan.

2. BAB II TINJAUAN PUSTAKA

Bab Tinjauan Pustaka berisi tentang penjelasan terkait penelitian sejenis yang pernah dilakukan sebelumnya. Penelitian-penelitian tersebut dijadikan sebagai referensi dan landasan teori pendukung dan dianalisis guna mengetahui perbedaan dan keterbaharuan yang dilakukan.

3. BAB III METODE PENELITIAN

Bab Metode penelitian ini berisi penjelasan mengenai metode penelitian yang akan digunakan, mencakup perancangan penelitian, tahapan-tahapan yang akan dilakukan dalam penelitian, serta objek dari penelitian.

4. BAB IV HASIL DAN PEMBAHASAN

Bab Hasil dan Pembahasan berisi tentang analisis kebutuhan, perancangan sistem, simulasi sistem yang telah dirancang, pengujian serta analisis data hasil pengujian.

5. BAB V PENUTUP

Bab Penutup berisi rangkuman hasil pengujian dari bab sebelumnya, serta menyajikkan masukkan untuk penelitian masa depan berdasarkan temuan yang diperoleh.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat diketahui protokol OSPF memiliki keunggulan dalam aspek *latency, packet loss,* dan *throughput* yang lebih rendah dibandingkan dengan protokol BGP dan EIGRP, khususnya setelah diterapkannya metode keamanan *traffic shaping*. Hasil perolehan nilai rata-rata keseluruhan pengujian QoS dengan standarisasi TIPHON, protokol OSPF memiliki nilai rata-rata 3 dan masuk kategori "Bagus". Sementara untuk protokol BGP dan EIGRP termasuk ke dalam kategori "Sedang" dengan nilai rata-rata 2,92. Dengan begitu, dapat ditarik kesimpulan bahwa protokol *routing* OSPF memiliki keunggulan daripada dua protokol *routing* yang diuji dengan serangan DDoS.

Untuk skenario pengujian serangan *packet sniffing*, ketiga protokol terbukti dapat memitigasi serangan *packet sniffing* dengan penerapan keamanan IPSec/IKEv2 pada *Router* 1 dan *Router* 3. Metode tersebut dapat menjaga kerahasiaan lalu lintas jaringan yang mencakup informasi paket, alamat IP, protokol ataupun data jaringan lainnya yang terdeteksi oleh *packet capture* pada skenario tanpa pengamanan.

5.2 Saran

Untuk penelitian selanjutnya, disarankan untuk mengambil langkah-langkah lanjutan dalam menguji dan menganalisis keamanan jaringan. Termasuk melakukan pengujian serangan yang lebih kompleks dengan menggunakan pendekatan dan *tools* yang berbeda. Selain itu, dapat mengeksplorasi lebih dalam mengenai faktor-faktor jaringan seperti keamanan, skalabilitas, dan kinerja. Dengan melakukan hal ini, akan memungkinkan untuk meningkatkan tingkat keamanan jaringan serta memperbaiki infrastruktur jaringan secara keseluruhan. Selanjutnya, pengembangan teknologi dan metode baru dalam bidang keamanan jaringan juga dapat dijelajahi untuk mengatasi tantangan yang mungkin muncul di masa depan.

DAFTAR PUSTAKA

Abhashkumar, A., Subramanian, K., Andreyev, A., Kim, H., Kishore Salem, N., Yang, J., Lapukhov, P., Akella, A., & Zeng, H. (2021). *Running BGP in Data Centers at Scale Running BGP in Data Centers at Scale*. https://www.usenix.org/conference/nsdi21/presentation/abhashkumar

AlliedTelesis. (n.d.). *Traffic Shaping Feature Overview and Configuration Guide*.

Alvionita, S., & Nurwasito, H. (2019a). *Analisis Kinerja Protokol Routing OSPF, RIP dan EIGRP Pada Topologi Jaringan Mesh* (Vol. 3, Issue 8). http://j-ptiik.ub.ac.id

Alvionita, S., & Nurwasito, H. (2019b). *Analisis Kinerja Protokol Routing OSPF, RIP dan EIGRP Pada Topologi Jaringan Mesh* (Vol. 3, Issue 8). http://j-ptiik.ub.ac.id

Anusuya, S., & Baulkani, S. (2022). Performance Analysis of Routing Protocols RIP, OSPF and EIGRP. *International Research Journal of Engineering and Technology*. www.irjet.net

Ariyadi, T., & Agung Prabowo, M. (2021). *Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security*. *6*(1).

Aryanti, S., Aspriyono, H., & Khairil. (2023). PENGEMBANGAN SISTEM KEAMANAN JARINGAN WIFI BERBASIS MIKROTIK MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC). *Desember Jurnal TEKNOSIA*, *17*(2), 88–95. https://ejournal.unib.ac.id/index.php/teknosia

Cisco. (n.d.). *OSPF Support for Fast Hello Packets*.

F5. (n.d.). *GLOSSARY: CYBERSECURITY TERMS & DEFINITIONS | What is Traffic Shaping?*

Hanipah, R., & Dhika, H. (2020). ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN DENGAN WIRESHARK. *Journal of Computer and Information Technology*, *4*(1). http://e-journal.unipma.ac.id/index.php/doubleclickTelepon:

He, X. (2021). Research on Computer Network Security Problems and Countermeasures. *Journal of Physics: Conference Series*, *1992*(3). https://doi.org/10.1088/1742-6596/1992/3/032069

Hudaya, A., & Primananda, R. (2023). *Analisis Perbandingan Dampak Serangan Distributed Denial of Service pada Protokol Routing OSPF dan IS-IS* (Vol. 7, Issue 4). http://j-ptiik.ub.ac.id

Isro, A. B., Zy, A. T., & Andika, S. (2024). Optimalisasi Load Balancing Menggunakan Metode NDLC untuk Meningkatkan Kualitas Layanan Jaringan Internet. *Journal of Information System Research (JOSH)*, *5*(4), 988–997. https://doi.org/10.47065/josh.v5i4.5484

Kabir, M. H., Kabir, M. A., Islam, M. S., Mortuza, M. G., & Mohiuddin, M. (2021). Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols †. *Engineering Proceedings*, *10*(1). https://doi.org/10.3390/ecsa-8-11285

Oracle. (2021, June). *Oracle VM VirtualBox Overview*. https://www.oracle.com/assets/oracle-vm-virtualbox-overview-2981353.pdf

Permana, R. (2019). Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak. *International Journal of Natural Sciences and Engineering*, *3*(1).

Pranaya, V. B., & Wellem, T. (2021). Implementasi BGP dan Resource Public Key Infrastructure menggunakan BIRD untuk Keamanan Routing. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(6), 1161–1170. https://doi.org/10.29207/resti.v5i6.3631

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN SITE TO SITE IMPLEMENTATION USING PROTOCOL L2TP AND IPSEC. *TEKNOKOM*, *4*(1), 30–36. https://doi.org/10.31943/teknokom.v4i1.59

Sudarianto, T., & Mukti, A. R. (2023). *Perancangan Jaringan Komputer Menggunakan Metode Top Down Studi Kasus STKIP Nurul Huda*.

Suteja, B., & Ratama, N. (2023). ANALISIS QOS (QUALITY OF SERVICE) DENGAN METODE TRAFICK SHAPING PADA JARINGAN INTERNET (STUDY KHASUS : PT. NETCITI PERSADA ALAM

SUTERA TANGERANG). *JORAPI : Journal of Research and Publication Innovation*, *1*(2).

Syaffiq, M., Malek, A., & Amran, A. R. (2021). A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity. In *Journal of Engineering Technology* (Vol. 9, Issue 1).

Tama, S. A., Data, M., & Bakhtiar, F. A. (2023). *Analisis Ketahanan Routing Protocol Open Shortest Path First (OSPF) terhadap Serangan Route Injection* (Vol. 7, Issue 7). http://j-ptiik.ub.ac.id

Tuli, R. (2020). Packet Sniffing and Sniffing Detection. *International Journal of Innovations in Engineering and Technology*, *16*(1). https://doi.org/10.21172/ijiet.161.04

Utami, P. R. (2020). ANALISIS PERBANDINGAN QUALITY OF SERVICE JARINGAN INTERNET BERBASIS WIRELESS PADA LAYANAN INTERNET SERVICE PROVIDER (ISP) INDIHOME DAN FIRST MEDIA. *Jurnal Ilmiah Teknologi Dan Rekayasa*, *25*(2), 125–137. https://doi.org/10.35760/tr.2020.v25i2.2723

Wangsa, E., & Zain, A. R. (2023). *Analisis Kinerja Routing Protocol BGP Dan EIGRP Terhadap Serangan Packet Sniffing Dan Spoofing Berbasis GNS 3*.

Yoachimik, O., & Pacheco, J. (2023). *DDoS threat report for 2023 Q2*. Https://Blog.Cloudflare.Com/Ddos-Threat-Report-2023-Q2/.

Zidane, M. (2022). Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *6*(1), 172–180. http://j-ptiik.ub.ac.id

DAFTAR RIWAYAT HIDUP

Lingga Fattah Adritama.

Lahir di Jakarta Agustus 2002.

Menyelesaikan pendidikan dasar di SD Negeri Palsigunung dan lulus pada tahun 2014. Kemudian melanjutkan pendidikan tingkat menengah pertama di SMP Mutiara Bangsa dan lulus pada tahun 2017. Kemudian melanjutkan pendidikan menengah kejuruan di SMK Negeri 3 Depok dan lulus pada tahun 2020. Pada tahun 2020 penulis melanjutkan pendidikan sebagai mahasiswa Diploma Empat (D4) di Politeknik Negeri Jakarta jurusan Teknik Informatika dan Komputer dengan Program Studi Teknik Multimedia dan Jaringan.

LAMPIRAN

Lampiran Konfigurasi *Router* 1 Protokol BGP

```
R1> enable
R1# configure terminal
R1(config)# ip route 20.20.20.0 255.255.255.252 10.10.10.2
R1(config)# interface Serial1/1
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# exit
R1(config)# router bgp 100
R1(config-router)# bgp log-neighbor-changes
R1(config-router)# neighbor 172.16.1.2 remote-as 300
R1(config-router)# neighbor 172.16.1.2 update-source Tunnel0
R1(config-router)# address-family ipv4
R1(config-router-af)# network 192.168.10.0
R1(config-router-af)# neighbor 172.16.1.2 activate
R1(config-router-af)# exit-address-family
R1(config-router)# exit
R1(config)# policy-map child-policy
R1(config-pmap)# class class-default
R1(config-pmap-c)# police 500000 250000 250000 conform-action transmit exceed-action
drop violate-action drop
R1(config-pmap-c)# fair-queue
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# policy-map SHAPE-TRAFFIC
R1(config-pmap)# class class-default
R1(config-pmap-c)# shape average 100000 10000 10000
R1(config-pmap-c)# service-policy child-policy
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R1(config-ikev2-proposal)# encryption aes-cbc-256
R1(config-ikev2-proposal)# integrity sha256
R1(config-ikev2-proposal)# group 14
R1(config-ikev2-proposal)# exit
R1(config)# crypto ikev2 policy IKEv2-POLICY
R1(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R1(config-ikev2-policy)# exit
R1(config)# crypto ikev2 keyring IKEv2-KEYRING
R1(config-ikev2-keyring)# peer R3
R1(config-ikev2-keyring-peer)# address 20.20.20.2
R1(config-ikev2-keyring-peer)# pre-shared-key local cisco111
R1 (config-ikev2-keyring-peer)# pre-shared-key remote cisco333
R1 (config-ikev2-keyring-peer)# exit
R1 (config-ikev2-keyring)# exit
R1 (config)# crypto ikev2 profile IKEv2-PROFILE
```

```
R1 (config-ikev2-profile)# match identity remote address 20.20.20.2 255.255.255.255
R1 (config-ikev2-profile)# authentication remote pre-share
R1 (config-ikev2-profile)# authentication local pre-share
R1 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R1 (config-ikev2-profile)# exit
R1 (config)# interface Tunnel0
R1 (config-if)# ip address 172.16.1.1 255.255.255.252
R1 (config-if)# tunnel source 10.10.10.1
R1 (config-if)# tunnel destination 20.20.20.2
R1 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R1(config-if)# exit
R1(config)# end
R1# write memory
```

Lampiran Konfigurasi *Router* 2 Protokol BGP

```
R2> enable
R2# configure terminal
R2(config)# router bgp 200
R2(config-router)# bgp log-neighbor-changes
R2(config-router)# network 20.20.20.0 mask 255.255.255.252
R2(config-router)# neighbor 10.10.10.1 remote-as 100
R2(config-router)# neighbor 20.20.20.2 remote-as 300
R2(config-router)# exit
R2(config)# interface Serial1/1
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface Serial1/2
R2(config-if)# ip address 20.20.20.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
```

Lampiran Konfigurasi *Router* 3 Protokol BGP

```
R3> enable
R3# configure terminal
R3(config)# ip route 10.10.10.0 255.255.255.252 20.20.20.1
R3(config)# interface Serial1/1
R3(config-if)# ip address 20.20.20.2 255.255.255.252
R3(config)# interface FastEthernet0/0
R3(config-if)# ip address 192.168.50.1 255.255.255.0
R3(config-if)# exit
R3(config)# router bgp 300
R3(config-router)# bgp log-neighbor-changes
R3(config-router)# neighbor 172.16.1.1 remote-as 100
R3(config-router)# neighbor 172.16.1.1 update-source Tunnel0
R3(config-router)# address-family ipv4
R3(config-router-af)# network 192.168.50.0
R3(config-router-af)# neighbor 172.16.1.1 activate
R3(config-router-af)# exit-address-family
R3(config-router)# exit
R3(config)# policy-map child-policy
R3(config-pmap)# class class-default
R3(config-pmap-c)# police 500000 250000 250000 conform-action transmit exceed-
action drop violate-action drop
R3(config-pmap-c)# fair-queue
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# policy-map SHAPE-TRAFFIC
R3(config-pmap)# class class-default
R3(config-pmap-c)# shape average 100000 10000 10000
R3(config-pmap-c)# service-policy child-policy
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R3(config-ikev2-proposal)# encryption aes-cbc-256
R3(config-ikev2-proposal)# integrity sha256
R3(config-ikev2-proposal)# group 14
R3(config-ikev2-proposal)# exit
R3(config)# crypto ikev2 policy IKEv2-POLICY
R3(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R3(config-ikev2-policy)# exit
R3(config)# crypto ikev2 keyring IKEv2-KEYRING
R3(config-ikev2-keyring)# peer R1
R3(config-ikev2-keyring-peer)# address 10.10.10.1
R3(config-ikev2-keyring-peer)# pre-shared-key local cisco333
R3 (config-ikev2-keyring-peer)# pre-shared-key remote cisco111
R3 (config-ikev2-keyring-peer)# exit
R3 (config-ikev2-keyring)# exit
R3 (config)# crypto ikev2 profile IKEv2-PROFILE
R3 (config-ikev2-profile)# match identity remote address 10.10.10.1 255.255.255.255
R3 (config-ikev2-profile)# authentication remote pre-share
```

```
R3 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R3 (config-ikev2-profile)# exit
R3 (config)# interface Tunnel0
R3 (config-if)# ip address 172.16.1.2 255.255.255.252
R3 (config-if)# tunnel source 20.20.20.2
R3 (config-if)# tunnel destination 10.10.10.1
R3 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R3(config-if)# exit
R3(config)# end
R3# write memory
```

Lampiran Konfigurasi *Router* 1 Protokol EIGRP

```
R1> enable
R1# configure terminal
R1(config)# ip route 20.20.20.0 255.255.255.252 10.10.10.2
R1(config)# interface Serial1/1
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# exit
R1(config)# router eigrp 123
R1(config-router)# network 10.10.10.0 0.0.0.3
R1(config-router)# network 172.16.1.0 0.0.0.3
R1(config-router)# network 192.168.1  0.0 0.0.0.3
R1(config-router)# exit
R1(config)# policy-map child-policy
R1(config-pmap)# class class-default
R1(config-pmap-c)# police 500000 250000 250000 conform-action transmit exceed-
action drop violate-action drop
R1(config-pmap-c)# fair-queue
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# policy-map SHAPE-TRAFFIC
R1(config-pmap)# class class-default
R1(config-pmap-c)# shape average 100000 10000 10000
R1(config-pmap-c)# service-policy child-policy
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R1(config-ikev2-proposal)# encryption aes-cbc-256
R1(config-ikev2-proposal)# integrity sha256
R1(config-ikev2-proposal)# group 14
R1(config-ikev2-proposal)# exit
R1(config)# crypto ikev2 policy IKEv2-POLICY
R1(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R1(config-ikev2-policy)# exit
R1(config)# crypto ikev2 keyring IKEv2-KEYRING
R1(config-ikev2-keyring)# peer R3
R1(config-ikev2-keyring-peer)# address 20.20.20.2
R1(config-ikev2-keyring-peer)# pre-shared-key local cisco333
```

```
R1 (config-ikev2-keyring-peer)# pre-shared-key remote cisco111
R1 (config-ikev2-keyring-peer)# exit
R1 (config-ikev2-keyring)# exit
R1 (config)# crypto ikev2 profile IKEv2-PROFILE
R1 (config-ikev2-profile)# match identity remote address 20.20.20.2 255.255.255.255
R1 (config-ikev2-profile)# authentication remote pre-share
R1 (config-ikev2-profile)# authentication local pre-share
R1 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R1 (config-ikev2-profile)# exit
R1 (config)# interface Tunnel0
R1 (config-if)# ip address 172.16.1.1 255.255.255.252
R1 (config-if)# tunnel source 10.10.10.1
R1 (config-if)# tunnel destination 20.20.20.2
R1 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R1(config-if)# exit
R1(config)# end
R1# write memory
```

Lampiran Konfigurasi *Router* 2 Protokol EIGRP

```
R2# configure terminal
R2 (config)# interface Serial1/1
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface Serial1/2
R2(config-if)# ip address 20.20.20.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# end
R2# write memory
```

Lampiran Konfigurasi *Router* 3 Protokol EIGRP

```
R3> enable
R3# configure terminal
R3(config)# ip route 10.10.10.0 255.255.255.252 20.20.20.1
R3(config)# interface Serial1/1
R3(config-if)# ip address 20.20.20.2 255.255.255.252
R3(config)# interface FastEthernet0/0
R3(config-if)# ip address 192.168.50.1 255.255.255.0
R3(config-if)# exit
R3(config)# router eigrp 123
R3(config-router)# network 20.20.20.0 0.0.0.3
R3(config-router)# network 172.16.1.0 0.0.0.3
R3(config-router)# network 192.168.50.0 0.0.0.3
R3(config-router)# exit
R3(config)# policy-map child-policy
R3(config-pmap)# class class-default
R3(config-pmap-c)# police 500000 250000 250000 conform-action transmit exceed-
action drop violate-action drop
R3(config-pmap-c)# fair-queue
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# policy-map SHAPE-TRAFFIC
R3(config-pmap)# class class-default
R3(config-pmap-c)# shape average 100000 10000 10000
R3(config-pmap-c)# service-policy child-policy
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R3(config-ikev2-proposal)# encryption aes-cbc-256
R3(config-ikev2-proposal)# integrity sha256
R3(config-ikev2-proposal)# group 14
R3(config-ikev2-proposal)# exit
R3(config)# crypto ikev2 policy IKEv2-POLICY
R3(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R3(config-ikev2-policy)# exit
R3(config)# crypto ikev2 keyring IKEv2-KEYRING
R3(config-ikev2-keyring)# peer R1
R3(config-ikev2-keyring-peer)# address 10.10.10.1
R3(config-ikev2-keyring-peer)# pre-shared-key local cisco333
R3 (config-ikev2-keyring-peer)# pre-shared-key remote cisco111
R3 (config-ikev2-keyring-peer)# exit
R3 (config-ikev2-keyring)# exit
R3 (config)# crypto ikev2 profile IKEv2-PROFILE
R3 (config-ikev2-profile)# match identity remote address 10.10.10.1 255.255.255.255
R3 (config-ikev2-profile)# authentication remote pre-share
R3 (config-ikev2-profile)# authentication local pre-share
R3 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R3 (config-ikev2-profile)# exit
R3 (config)# interface Tunnel0
R3 (config-if)# ip address 172.16.1.2 255.255.255.252
```

```
R3 (config-if)# tunnel source 20.20.20.2
R3 (config-if)# tunnel destination 10.10.10.1
R3 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R3(config-if)# exit
R3(config)# end
R3# write memory
```

Lampiran Konfigurasi *Router* 1 Protokol OSPF

```
R1> enable
R1# configure terminal
R1(config)# ip route 20.20.20.0 255.255.255.252 10.10.10.2
R1(config)# interface Serial1/1
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 172.16.1.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# exit
R1(config)# policy-map child-policy
R1(config-pmap)# class class-default
R1(config-pmap-c)# police 500000 250000 250000 conform-action transmit exceed-
action drop violate-action drop
R1(config-pmap-c)# fair-queue
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# policy-map SHAPE-TRAFFIC
R1(config-pmap)# class class-default
R1(config-pmap-c)# shape average 100000 10000 10000
R1(config-pmap-c)# service-policy child-policy
R1(config-pmap-c)# exit
R1(config-pmap)# exit
R1(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R1(config-ikev2-proposal)# encryption aes-cbc-256
R1(config-ikev2-proposal)# integrity sha256
R1(config-ikev2-proposal)# group 14
R1(config-ikev2-proposal)# exit
R1(config)# crypto ikev2 policy IKEv2-POLICY
R1(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R1(config-ikev2-policy)# exit
R1(config)# crypto ikev2 keyring IKEv2-KEYRING
R1(config-ikev2-keyring)# peer R3
R1(config-ikev2-keyring-peer)# address 20.20.20.2
R1(config-ikev2-keyring-peer)# pre-shared-key local cisco111
R1 (config-ikev2-keyring-peer)# pre-shared-key remote cisco333
R1 (config-ikev2-keyring-peer)# exit
R1 (config-ikev2-keyring)# exit
R1 (config)# crypto ikev2 profile IKEv2-PROFILE
```

```
R1 (config)# crypto ikev2 profile IKEv2-PROFILE
R1 (config-ikev2-profile)# match identity remote address 20.20.20.2 255.255.255.255
R1 (config-ikev2-profile)# authentication remote pre-share
R1 (config-ikev2-profile)# authentication local pre-share
R1 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R1 (config-ikev2-profile)# exit
R1 (config)# interface Tunnel0
R1 (config-if)# ip address 172.16.1.1 255.255.255.252
R1 (config-if)# tunnel source 10.10.10.1
R1 (config-if)# tunnel destination 20.20.20.2
R1 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R1(config-if)# exit
R1(config)# end
R1# write memory
```

Lampiran Konfigurasi *Router* 2 Protokol OSPF

```
R2> enable
R2# configure terminal
R2 (config)# interface Serial1/1
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface Serial1/2
R2(config-if)# ip address 20.20.20.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# end
R2# write memory
```

Lampiran Konfigurasi *Router* 3 Protokol OSPF

```
R3> enable
R3# configure terminal
R3(config)# ip route 10.10.10.0 255.255.255.252 20.20.20.1
R3(config)# interface Serial1/1
R3(config-if)# ip address 20.20.20.2 255.255.255.252
R3(config)# interface FastEthernet0/0
R3(config-if)# ip address 192.168.50.1 255.255.255.0
R3(config-if)# exit
R3(config)# router ospf 3
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 172.16.1.0 0.0.0.3 area 0
R3(config-router)# network 192.168.50.0 0.0.0.255 area 0
R3(config-router)# exit
R3(config)# policy-map child-policy
R3(config-pmap)# class class-default
R3(config-pmap-c)# police 500000 250000 250000 conform-action transmit
exceed-action drop violate-action drop
R3(config-pmap-c)# fair-queue
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# policy-map SHAPE-TRAFFIC
R3(config-pmap)# class class-default
R3(config-pmap-c)# shape average 100000 10000 10000
R3(config-pmap-c)# service-policy child-policy
R3(config-pmap-c)# exit
R3(config-pmap)# exit
R3(config)# crypto ikev2 proposal IKEv2-PROPOSAL
R3(config-ikev2-proposal)# encryption aes-cbc-256
R3(config-ikev2-proposal)# integrity sha256
R3(config-ikev2-proposal)# group 14
R3(config-ikev2-proposal)# exit
R3(config)# crypto ikev2 policy IKEv2-POLICY
R3(config-ikev2-policy)# proposal IKEv2-PROPOSAL
R3(config-ikev2-policy)# exit
R3(config)# crypto ikev2 keyring IKEv2-KEYRING
R3(config-ikev2-keyring)# peer R1
R3(config-ikev2-keyring-peer)# address 10.10.10.1
R3(config-ikev2-keyring-peer)# pre-shared-key local cisco333
R3 (config-ikev2-keyring-peer)# pre-shared-key remote cisco111
R3 (config-ikev2-keyring-peer)# exit
R3 (config-ikev2-keyring)# exit
```

```
R3 (config)# crypto ikev2 profile IKEv2-PROFILE
R3 (config-ikev2-profile)# match identity remote address 10.10.10.1
255.255.255.255
R3 (config-ikev2-profile)# authentication remote pre-share
R3 (config-ikev2-profile)# authentication local pre-share
R3 (config-ikev2-profile)# keyring local IKEv2-KEYRING
R3 (config-ikev2-profile)# exit
R3 (config)# interface Tunnel0
R3 (config-if)# ip address 172.16.1.2 255.255.255.252
R3 (config-if)# tunnel source 20.20.20.2
R3 (config-if)# tunnel destination 10.10.10.1
R3 (config-if)# tunnel protection IPSec profile IPSEC-PROFILE
R3(config-if)# exit
R3(config)# end
R3# write memory
```