

**PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT)
UNTUK PERLINDUNGAN AKSES JARINGAN
MENGUNAKAN *CISCO PACKET TRACER***

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



Disusun Oleh

ALIF MIFTAKHUL FIRDAUS

22.83.0816

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

**PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT)
UNTUK PERLINDUNGAN AKSES JARINGAN
MENGUNAKAN *CISCO PACKET TRACER***

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



Disusun Oleh
ALIF MIFTAKHUL FIRDAUS
22.83.0816

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026**

HALAMAN PERSETUJUAN

SKRIPSI

**PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT)
UNTUK PERLINDUNGAN AKSES JARINGAN
MENGUNAKAN *CISCO PACKET TRACER***

yang disusun dan diajukan oleh

ALIF MIFTAKHUL FIRDAUS

22.83.0816

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Mei 2026

Dosen Pembimbing,



Senie Destya, S.T., M.Kom.
NIK. 190302312

HALAMAN PENGESAHAN
SKRIPSI
PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT)
UNTUK PERLINDUNGAN AKSES JARINGAN
MENGGUNAKAN *CISCO PACKET TRACER*

yang disusun dan diajukan oleh

ALIF MIFTAKHUL FIRDAUS

22.83.0816

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Mei 2026

Susunan Dewan Penguji

Nama Penguji

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

Muhammad Kopravi, S.Kom., M.Eng.
NIK. 190302454

Senie Destya, S.T., M.Kom.
NIK. 190302312

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Mei 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **ALIF MIFTAKHUL FIRDAUS**
NIM : **22.83.0816**

Menyatakan bahwa Skripsi dengan judul berikut:

PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT) UNTUK PERLINDUNGAN AKSES JARINGAN MENGGUNAKAN *CISCO PACKET TRACER*

Dosen Pembimbing : **Senie Destya, S.T., M.Kom.**

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian **SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat **orang** lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab **SAYA**, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini **SAYA** buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka **SAYA** bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Mei 2026

Yang Menyatakan,



ALIF MIFTAKHUL FIRDAUS

KATA PENGANTAR

Alhamdulillah, puji dan syukur penulis panjatkan ke hadirat Allah SWT atas berkat Rahmat, Hidayah, serta Karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Penerapan *Network Address Translation* (NAT) untuk Perlindungan Akses Jaringan Menggunakan Cisco Packet Tracer”. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan pada Program Studi S1 Teknik Komputer.

Dalam penyusunannya, penulis menyadari bahwa tidak sedikit hambatan dan kesulitan yang dihadapi. Namun berkat banyaknya bantuan, bimbingan, motivasi, serta dukungan dari berbagai pihak, sehingga skripsi ini dapat selesai pada waktunya. Oleh karena itu, penulis menyampaikan terima kasih kepada :

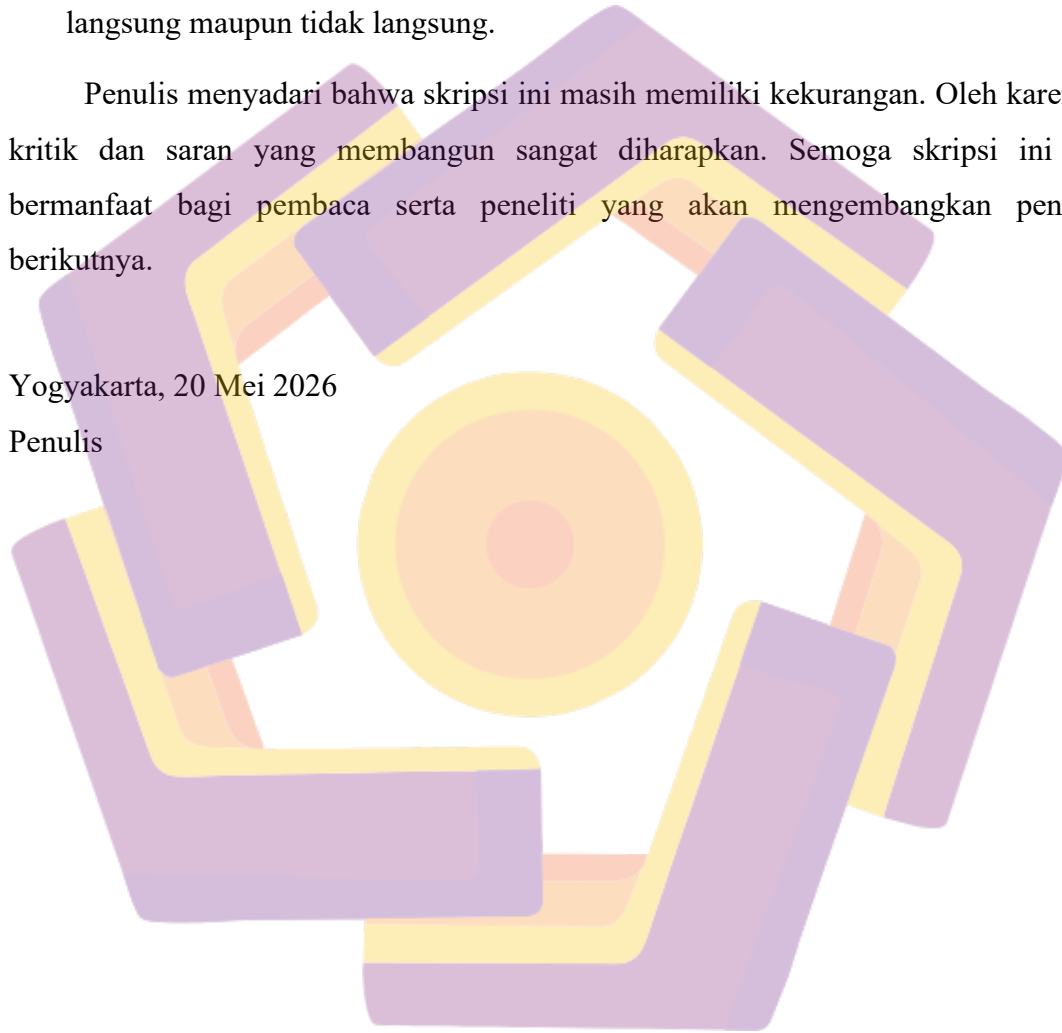
1. Ibu Senie Destya, S.T., M.Kom. selaku dosen pembimbing yang telah meluangkan waktu yang tidak ternilai harganya serta memberikan ilmu, arahan, bimbingan, kritik, serta saran selama penyusunan skripsi ini.
2. Kedua orang tua penulis, Bapak Parluji, M.Pd. dan Ibu Suprantini, S.Si., yang senantiasa memberikan motivasi, do'a, dukungan, serta kasih sayang yang tiada henti. Kehadiran, pengorbanan, dan perhatian Bapak dan Ibu menjadi sumber semangat bagi penulis dalam menyelesaikan skripsi ini dengan sebaik-baiknya.
3. Seluruh Dosen Pengajar di Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta yang telah memberikan begitu banyak ilmu serta motivasi kepada penulis selama menempuh pendidikan di Universitas AMIKOM Yogyakarta.
4. Teman-teman kelas seperjuangan 22TK01 yang tidak dapat penulis sebutkan satu-persatu namanya.
5. Nurkumala, Mugni Saleh Maheswara, Lia Shintya Mu'in, Khent Harianto Sandang, serta Abisag Kartika Sari, yang telah memberikan dukungan secara mental, arahan, motivasi, serta semangat dalam proses penyusunan.
6. Alvino Dean Saputra, Rayhand Tirtadistira Mile, Jordy Valentino Kalelo, serta teman kos lain yang tidak dapat disebutkan namanya satu-persatu.
7. Hanin Aqila Mukhlisin serta Elza Salsabila Rachmawati yang telah memberikan penulis dukungan serta motivasi dan semangat dalam penyusunan skripsi selama di Semarang.

8. Akhmad Iqra' Pangarsa, Aryant Barbaryant A., serta Rey Subekti selaku teman dekat penulis.
9. Raditya Naufal yang menemani penulis selama penyusunan skripsi dari awal hingga akhir.
10. Teman-teman Roblox yang tidak dapat penulis sebutkan satu-persatu namanya.
11. Seluruh pihak yang telah terlibat membantu dalam penyusunan skripsi secara langsung maupun tidak langsung.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan. Semoga skripsi ini dapat bermanfaat bagi pembaca serta peneliti yang akan mengembangkan penelitian berikutnya.

Yogyakarta, 20 Mei 2026

Penulis



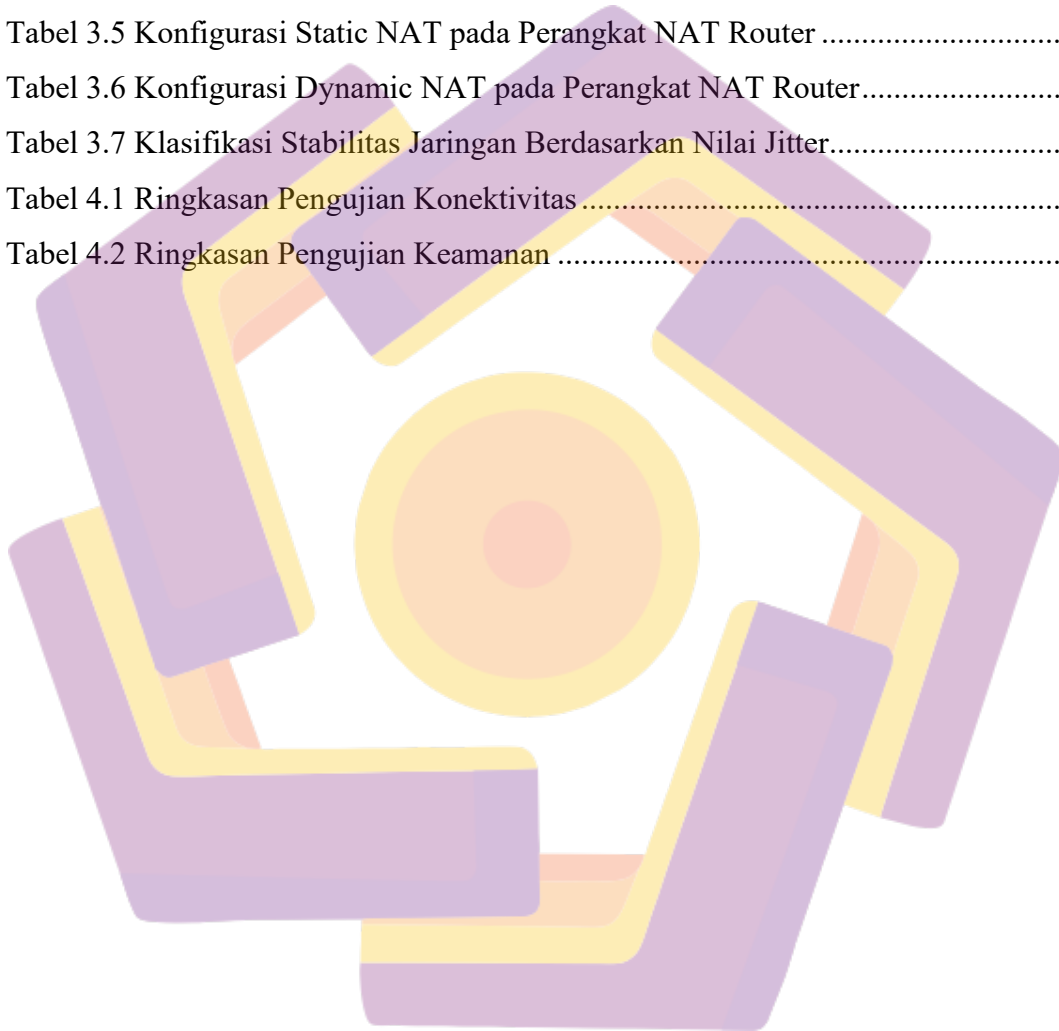
DAFTAR ISI

HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
KATA PENGANTAR.....	vi
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMBANG DAN SINGKATAN	xiii
DAFTAR ISTILAH	xiv
INTISARI	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	4
2.1 Studi Literatur	4
2.2 Dasar Teori.....	9
2.2.1 Jaringan Komputer	9
2.2.2 <i>Internet Protocol</i> (IP).....	10
2.2.3 Keamanan Jaringan	11
2.2.4 <i>Network Address Translation</i> (NAT).....	12
2.2.5 <i>Cisco Packet Tracer</i>	14
BAB III METODE PENELITIAN	15
3.1 Alur Penelitian	15
3.2 Alat dan Bahan.....	17
3.2.1 Alat Penelitian.....	17

3.2.2 Bahan Penelitian	18
3.3 Rancangan Topologi dan Pengalamatan Jaringan	18
3.3.1 Topologi Jaringan	18
3.3.2 Pengalamatan Jaringan.....	18
3.4 Alur Sistem	19
3.5 Skenario Penelitian	20
3.6 Konfigurasi Jaringan	21
3.6.1 Konfigurasi <i>Static</i> NAT	21
3.6.2 Konfigurasi <i>Dynamic</i> NAT.....	21
3.6.3 Konfigurasi Tanpa NAT	22
3.7 Metode Pengujian	22
3.8 Teknik Analisis Data.....	23
BAB IV HASIL DAN PEMBAHASAN	26
4.1 Pengujian Konektivitas	26
4.2 Pengujian Keamanan.....	33
4.3 Ringkasan Hasil Pengujian	46
4.3.1 Analisis Kinerja Jaringan.....	46
4.3.2 Analisis Keamanan Jaringan.....	47
BAB V PENUTUP	49
5.1 Kesimpulan	49
5.2 Saran.....	50
REFERENSI.....	51

DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian	6
Tabel 3.1 Spesifikasi Perangkat yang Digunakan	17
Tabel 3.2 Skema Perangkat	18
Tabel 3.3 Skema Pengalamatan IP Untuk Ketiga Skenario.....	19
Tabel 3.4 Pemetaan One-To-One Static NAT	21
Tabel 3.5 Konfigurasi Static NAT pada Perangkat NAT Router	21
Tabel 3.6 Konfigurasi Dynamic NAT pada Perangkat NAT Router.....	22
Tabel 3.7 Klasifikasi Stabilitas Jaringan Berdasarkan Nilai Jitter.....	24
Tabel 4.1 Ringkasan Pengujian Konektivitas	46
Tabel 4.2 Ringkasan Pengujian Keamanan	47



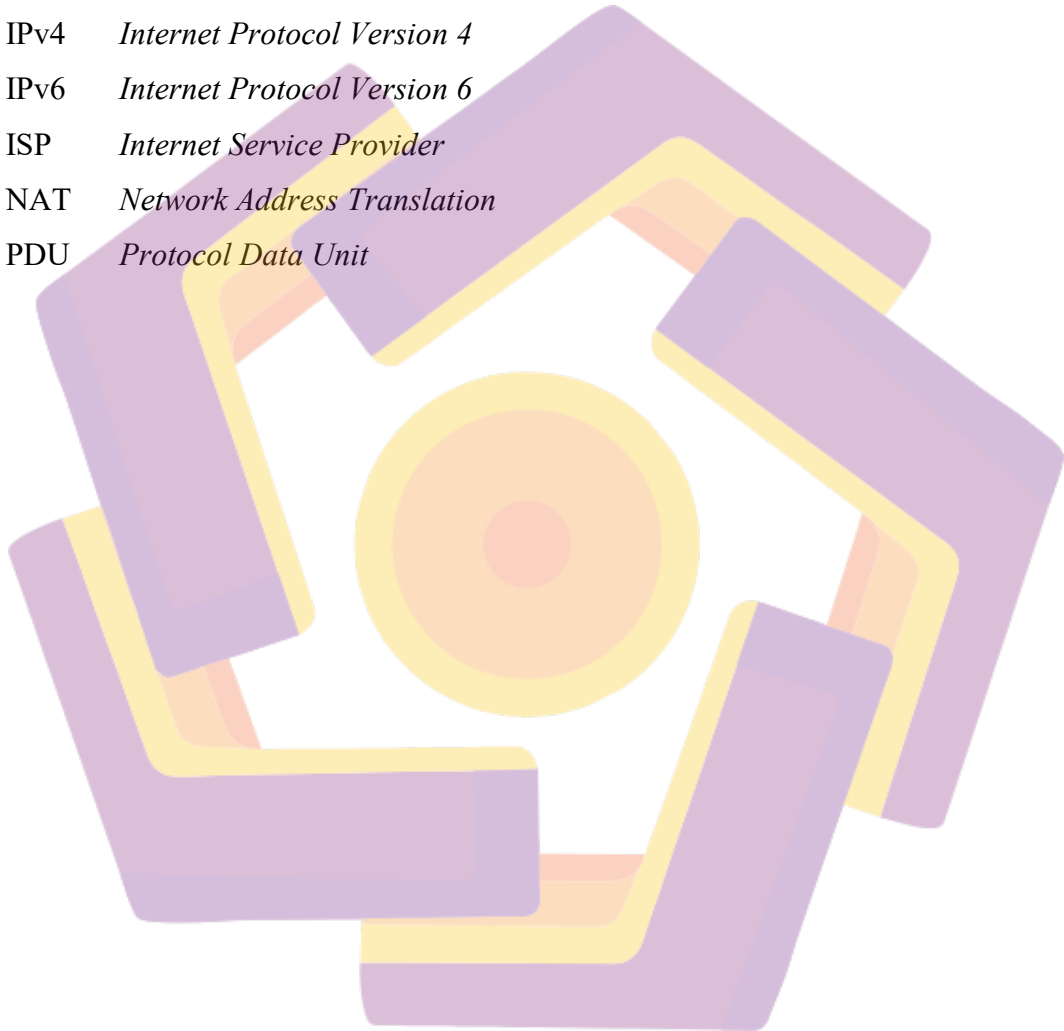
DAFTAR GAMBAR

Gambar 2.1 Topologi Jaringan PAN, LAN, MAN, dan WAN	10
Gambar 2.2 Contoh Pemetaan Alamat IPv4 Pada Static NAT	13
Gambar 2.3 Contoh Pemetaan Alamat IPv4 Pada Dynamic NAT	14
Gambar 3.1 Alur Penelitian	16
Gambar 3.2 Topologi NAT Jenis Star Untuk Ketiga Skenario	18
Gambar 3.3 Alur Sistem NAT	20
Gambar 4.1 Percobaan Ping 1 Sampai 6 Topologi Static NAT.....	26
Gambar 4.2 Percobaan Ping 7 Sampai 10 Topologi Static NAT.....	27
Gambar 4.3 Trace Route Perangkat PC1 Topologi Static NAT	27
Gambar 4.4 Trace Route Perangkat PC2 dan Laptop1 Topologi Static NAT	27
Gambar 4.5 Akses Web Server Pada Perangkat PC1 Topologi Static NAT	28
Gambar 4.6 Akses Web Server Pada Perangkat Lain Topologi Static NAT.....	28
Gambar 4.7 Percobaan Ping 1 Sampai 6 Topologi Dynamic NAT	29
Gambar 4.8 Percobaan Ping 7 Sampai 10 Topologi Dynamic NAT	29
Gambar 4.9 Trace Route Pada Perangkat PC1 Topologi Dynamic NAT.....	29
Gambar 4.10 Trace Route Pada PC2 dan Laptop1 Topologi Dynamic NAT.....	30
Gambar 4.11 Akses Web Server Pada Perangkat PC1 Topologi Dynamic NAT.....	30
Gambar 4.12 Akses Web Server Pada Perangkat Lain Topologi Dynamic NAT	30
Gambar 4.13 Percobaan Ping 1 Sampai 6 Topologi Tanpa NAT.....	31
Gambar 4.14 Percobaan Ping 7 Sampai 10 Topologi Tanpa NAT	31
Gambar 4.15 Trace Route Pada Perangkat PC1 Topologi Tanpa NAT	32
Gambar 4.16 Trace Route Pada PC2 dan Laptop1 Topologi Tanpa NAT	32
Gambar 4.17 Akses Web Server Pada Perangkat PC1 Topologi Tanpa NAT	32
Gambar 4.18 Akses Web Server Pada Perangkat Lain Topologi Tanpa NAT	33
Gambar 4.19 Informasi PDU PC1 Sebelum Sampai di NAT Router Static NAT.....	34
Gambar 4.20 Informasi PDU PC1 Setelah Translasi di NAT Router Static NAT	34
Gambar 4.21 Informasi PDU PC1 di Server ISP Static NAT	35
Gambar 4.22 Hasil Uji Filtering Dengan Ping Ke Alamat IP Internal Static NAT.....	35
Gambar 4.23 Informasi PDU Perangkat Eksternal pada NAT Router	36
Gambar 4.24 Informasi PDU Respon dari Perangkat PC1 pada NAT Router	37
Gambar 4.25 Informasi PDU Respon dari Perangkat PC2 pada NAT Router	37

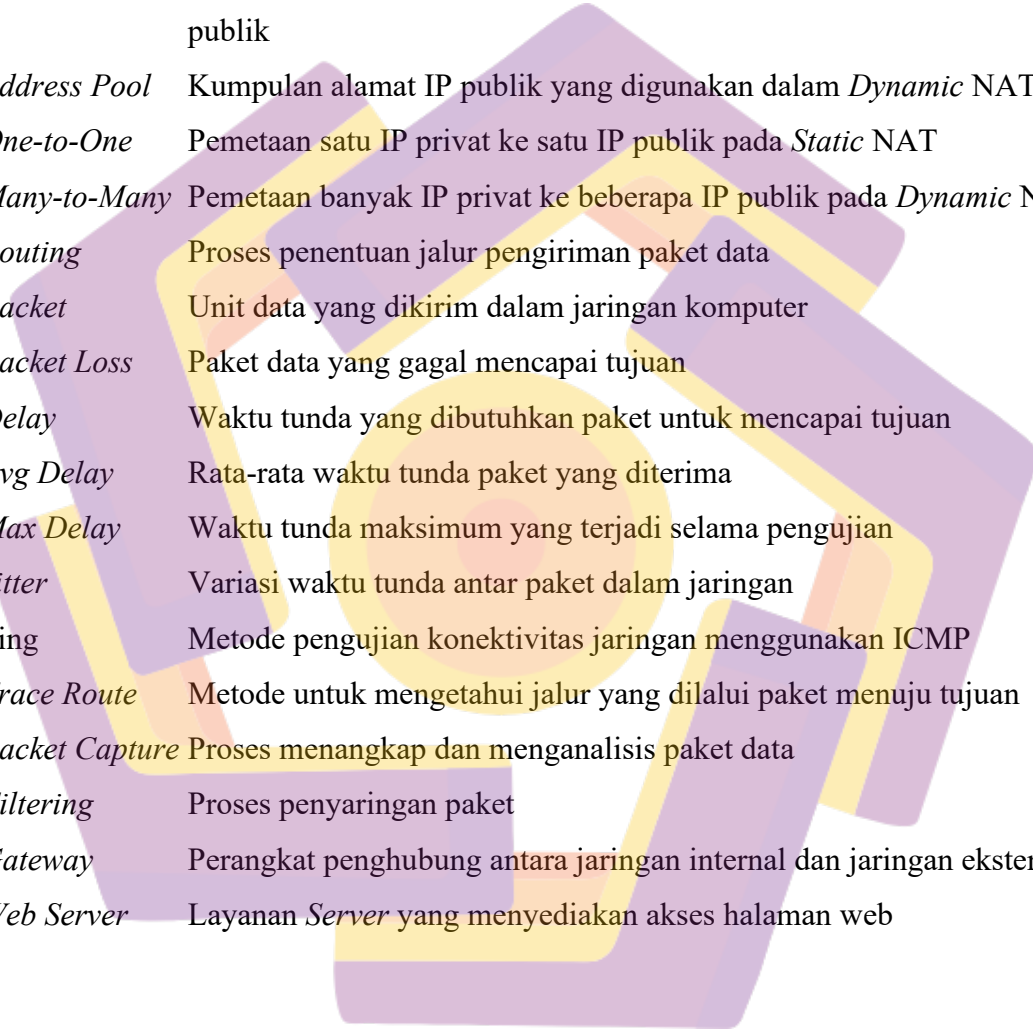
Gambar 4.26 Informasi PDU Respon dari Perangkat Laptop1 pada NAT Router.....	38
Gambar 4.27 Informasi PDU PC1 Sebelum Sampai di NAT Router Dynamic NAT	38
Gambar 4.28 Informasi PDU PC1 Setelah Translasi di NAT Router Dynamic NAT....	39
Gambar 4.29 Informasi PDU PC1 di Server ISP Dynamic NAT	39
Gambar 4.30 Hasil Uji Filtering Dengan Ping Ke Alamat IP Internal Dynamic NAT ..	40
Gambar 4.31 Informasi PDU Perangkat Eksternal pada NAT Router	40
Gambar 4.32 Informasi PDU Respon dari Perangkat PC1 pada NAT Router	41
Gambar 4.33 Informasi PDU Respon dari Perangkat PC2 pada NAT Router	41
Gambar 4.34 Informasi PDU Respon dari Perangkat Laptop1 pada NAT Router.....	42
Gambar 4.35 Informasi PDU PC1 Sebelum Sampai di NAT Router Tanpa NAT.....	42
Gambar 4.36 Informasi PDU PC1 Setelah Sampai di NAT Router Tanpa NAT	43
Gambar 4.37 Informasi PDU PC1 Sampai di Server ISP Tanpa NAT.....	43
Gambar 4.38 Hasil Uji Filtering Dengan Ping Ke Alamat IP Internal Dynamic NAT ..	44
Gambar 4.39 Informasi PDU Perangkat Eksternal pada NAT Router	44
Gambar 4.40 Informasi PDU Respon dari Perangkat PC1 pada NAT Router	45
Gambar 4.41 Informasi PDU Respon dari Perangkat PC2 pada NAT Router	45
Gambar 4.42 Informasi PDU Respon dari Perangkat Laptop1 pada NAT Router.....	46

DAFTAR LAMBANG DAN SINGKATAN

Σ	(Sigma) Penjumlahan
n	Jumlah paket valid
ACL	<i>Access Control List</i>
ICMP	<i>Internet Control Message Protocol</i>
IP	<i>Internet Protocol</i>
IPv4	<i>Internet Protocol Version 4</i>
IPv6	<i>Internet Protocol Version 6</i>
ISP	<i>Internet Service Provider</i>
NAT	<i>Network Address Translation</i>
PDU	<i>Protocol Data Unit</i>



DAFTAR ISTILAH



<i>Topologi Star</i>	Topologi jaringan dengan satu perangkat pusat sebagai penghubung
<i>IP Privat</i>	Alamat IP yang digunakan dalam jaringan internal
<i>IP Publik</i>	Alamat IP yang digunakan untuk komunikasi pada jaringan internet
<i>Static NAT</i>	Pemetaan tetap satu alamat IP privat ke satu alamat IP publik
<i>Dynamic NAT</i>	Pemetaan alamat IP secara dinamis menggunakan kumpulan alamat IP publik
<i>Address Pool</i>	Kumpulan alamat IP publik yang digunakan dalam <i>Dynamic NAT</i>
<i>One-to-One</i>	Pemetaan satu IP privat ke satu IP publik pada <i>Static NAT</i>
<i>Many-to-Many</i>	Pemetaan banyak IP privat ke beberapa IP publik pada <i>Dynamic NAT</i>
<i>Routing</i>	Proses penentuan jalur pengiriman paket data
<i>Packet</i>	Unit data yang dikirim dalam jaringan komputer
<i>Packet Loss</i>	Paket data yang gagal mencapai tujuan
<i>Delay</i>	Waktu tunda yang dibutuhkan paket untuk mencapai tujuan
<i>Avg Delay</i>	Rata-rata waktu tunda paket yang diterima
<i>Max Delay</i>	Waktu tunda maksimum yang terjadi selama pengujian
<i>Jitter</i>	Variasi waktu tunda antar paket dalam jaringan
<i>Ping</i>	Metode pengujian konektivitas jaringan menggunakan ICMP
<i>Trace Route</i>	Metode untuk mengetahui jalur yang dilalui paket menuju tujuan
<i>Packet Capture</i>	Proses menangkap dan menganalisis paket data
<i>Filtering</i>	Proses penyaringan paket
<i>Gateway</i>	Perangkat penghubung antara jaringan internal dan jaringan eksternal
<i>Web Server</i>	Layanan <i>Server</i> yang menyediakan akses halaman web

INTISARI

Keamanan jaringan menjadi aspek penting dalam menjaga integritas dan kerahasiaan data di tengah meningkatnya penggunaan teknologi digital. Salah satu permasalahan yang sering terjadi adalah keterbukaan alamat IP internal terhadap akses dari jaringan eksternal, yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan. Kondisi ini dapat menyebabkan kebocoran alamat IP internal, gangguan konektivitas, serta menurunkan tingkat keamanan sistem jaringan. Oleh karena itu, diperlukan mekanisme yang mampu melindungi jaringan internal tanpa menghambat proses komunikasi data antarperangkat.

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan simulasi jaringan menggunakan *Cisco Packet Tracer*. Proses penelitian dilakukan dengan merancang topologi jaringan dan mengimplementasikan tiga skenario, yaitu *Static NAT*, *Dynamic NAT*, dan tanpa NAT sebagai pembandingan. Pengujian dilakukan melalui uji konektivitas menggunakan *ping*, *trace route*, dan akses *web server*, serta uji keamanan melalui analisis translasi alamat, *filtering*, dan *packet capture*. Data yang diperoleh kemudian dianalisis secara komparatif untuk mengetahui perbedaan kinerja dan tingkat keamanan dari masing-masing skenario.

Hasil penelitian menunjukkan bahwa penerapan NAT, baik *Static NAT* maupun *Dynamic NAT*, mampu meningkatkan keamanan jaringan dengan menyembunyikan alamat IP internal dan membatasi akses langsung dari jaringan eksternal. *Static NAT* memberikan tingkat stabilitas terbaik berdasarkan nilai *delay* dan *jitter*, sementara *Dynamic NAT* menawarkan fleksibilitas dalam penggunaan alamat IP publik. Sebaliknya, tanpa NAT menunjukkan tingkat keamanan yang rendah karena alamat IP internal terekspos. Penelitian ini dapat dimanfaatkan oleh mahasiswa, teknisi jaringan, dan pengelola sistem sebagai referensi dalam menerapkan NAT untuk meningkatkan keamanan jaringan. Penelitian selanjutnya disarankan untuk menguji NAT pada skala jaringan yang lebih besar atau dikombinasikan dengan mekanisme keamanan lain.

Kata kunci: NAT, keamanan jaringan, alamat IP, simulasi jaringan, *Cisco Packet Tracer*

ABSTRACT

Network security has become an essential aspect in maintaining data integrity and confidentiality amid the increasing use of digital technology. One of the common problems that often occurs is the exposure of internal IP addresses to external network access, which can potentially be exploited by unauthorized parties to carry out attacks. This condition may lead to internal IP address leakage, connectivity disruptions, and a decrease in overall network system security. Therefore, a mechanism is needed to protect internal networks without disrupting the data communication process between devices.

This study employed a descriptive qualitative method with a network simulation approach using Cisco Packet Tracer. The research process was carried out by designing a network topology and implementing three scenarios, namely Static NAT, Dynamic NAT, and without NAT as a comparison. The testing process included connectivity tests using ping, traceroute, and web server access, as well as security tests through address translation analysis, filtering, and packet capture. The collected data were then analyzed comparatively to determine the differences in performance and security levels among each scenario.

The results of the study indicate that the implementation of NAT, both Static NAT and Dynamic NAT, is capable of improving network security by hiding internal IP addresses and limiting direct access from external networks. Static NAT provides the best level of stability based on delay and jitter values, while Dynamic NAT offers greater flexibility in the use of public IP addresses. In contrast, the scenario without NAT demonstrates a lower level of security because the internal IP addresses are exposed. This research can be utilized by students, network technicians, and system administrators as a reference in implementing NAT to enhance network security. Future studies are recommended to examine NAT implementation on larger-scale networks or combine it with other security mechanisms.

Keyword: NAT, network security, IP address, network simulation, Cisco Packet Tracer