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

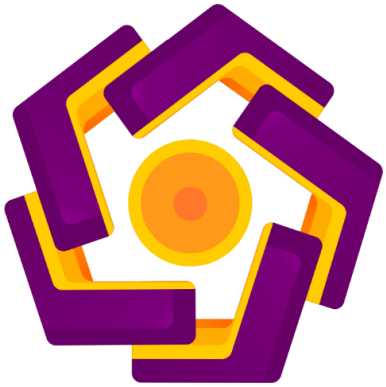
2026

PENERAPAN *NETWORK ADDRESS TRANSLATION* (NAT) UNTUK PERLINDUNGAN AKSES JARINGAN MENGGUNAKAN *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 MENGGUNAKAN *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	Tanda Tangan
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Senie Destya, S.T., M.Kom. **NIK. 190302312**	

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

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, 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 dihadapai. 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 Mukhlishin 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

$\sum$	(Sigma) Penjumlahan
n	Jumlah paket valid
ACL	*Access Control List*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
ISP	*Internet Service Provider*
NAT	*Network Address Translation*
PDU	*Protocol Data Unit*

DAFTAR ISTILAH

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