ISSN: 2654-2617 (Cetak)
Jurnal Teknologi Informatika (J-TIFA) V.8.No.2 September 2025 ISSN: 2654-2633(Online)
Website : jurnal.ummu.ac.id/index.php/J-TIFA

J-TIFA
(Jurnal Teknologi Informatika)
|Teknologi Informasi | Jaringan Komputer | Data Mining |

Penerapan Transparent Dns, Pencegahan Akses Proxy Dan Vpn Dengan Metode Layer 7 Protocol Untuk Filtering Pengguna Internet Di Universitas Muhammadiyah Maluku Utara

M. Al'Aidin. Hi . Abd. Mutalib, Salim Albaar, Sakina Sudin
Teknik Informatika, Universitas Muhhamdiyah Maluku Utara, Kota Ternate, Indonesia
email: muhammadalaidinmutalib@gmail.com

Abstrak

Penelitian ini membahas penerapan Transparent DNS dan metode Layer 7 Protocol untuk mencegah akses proxy dan VPN di Universitas Muhammadiyah Maluku Utara. Metode ini efektif dalam meningkatkan keamanan jaringan dengan mengarahkan permintaan DNS melalui server universitas dan mendeteksi penggunaan proxy serta VPN pada lapisan aplikasi. Hasilnya menunjukkan peningkatan performa jaringan dan kepuasan pengguna, memberikan solusi pengendalian akses internet yang optimal di lingkungan akademik.

Kata Kunci : *DNS, Proxy, Vpn, Layer 7 Protokol & Filtering*

Abstract

This study examines the implementation of Transparent DNS and Layer 7 Protocol methods to prevent proxy and VPN access at Universitas Muhammadiyah Maluku Utara. These methods effectively enhance network security by routing DNS requests through the university's servers and detecting proxy and VPN usage at the application layer. The results demonstrate improved network performance and user satisfaction, providing an optimal internet access control solution in an academic environment.

Keywords: DNS, Proxy, Vpn, Layer 7 Protokol & Filtering

1. Pendahuluan

Di era digital saat ini, akses internet telah menjadi kebutuhan esensial dalam berbagai aktivitas, khususnya di lingkungan akademik. Universitas sebagai institusi pendidikan memegang peranan penting dalam menyediakan akses internet yang aman, cepat, dan andal bagi mahasiswa serta staf pengajar. Namun, tantangan muncul ketika pengguna memanfaatkan layanan proxy dan VPN untuk melewati pembatasan akses yang diterapkan oleh institusi, sehingga perlu adanya mekanisme pengelolaan dan pengawasan yang efektif untuk menjaga keamanan jaringan kampus.

Salah satu solusi yang diterapkan di Universitas Muhammadiyah Maluku Utara adalah penggunaan Transparent DNS yang mengarahkan seluruh permintaan DNS melalui server yang dikelola universitas, serta metode Layer 7 Protocol untuk

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)

mendeteksi dan memblokir akses melalui proxy dan VPN. Metode Layer 7 Protocol memungkinkan inspeksi paket data pada lapisan aplikasi, sehingga dapat secara akurat mengenali dan memfilter lalu lintas yang menggunakan protokol proxy atau VPN, termasuk yang menggunakan port standar. Penerapan ini tidak hanya meningkatkan keamanan jaringan tetapi juga mengoptimalkan penggunaan sumber daya jaringan dan produktivitas pengguna.

Penelitian ini bertujuan untuk mengkaji efektivitas penerapan Transparent DNS dan metode Layer 7 Protocol dalam mengontrol akses internet, khususnya dalam memblokir penggunaan proxy dan VPN di lingkungan Universitas Muhammadiyah Maluku Utara. Selain itu, penelitian ini juga menilai dampak dari penerapan metode tersebut terhadap kinerja jaringan dan kepuasan pengguna. Hasil penelitian diharapkan dapat memberikan kontribusi signifikan dalam pengelolaan keamanan jaringan akademik yang lebih baik dan penerapan kebijakan penggunaan internet yang lebih efektif di lingkungan universitas

2. Teori

1. Transparent DNS (Domain Name System) adalah sistem yang menerjemahkan nama domain yang mudah diingat menjadi alamat IP yang digunakan oleh komputer. Transparent DNS merupakan konfigurasi jaringan di mana permintaan DNS dari klien secara otomatis dialihkan (*redirected*) ke server DNS yang telah ditentukan oleh administrator jaringan, tanpa memerlukan konfigurasi manual pada setiap perangkat klien. Mekanisme Kerja: Dalam konteks Mikrotik, implementasi ini umumnya dilakukan dengan aturan NAT (*Network Address Translation*) atau Firewall Mangle yang menangkap semua paket DNS (Port 53) yang ditujukan ke luar jaringan dan mengarahkannya kembali ke DNS lokal (ISP atau DNS *filtering* yang ditentukan). Keuntungan: Memastikan konsistensi kebijakan *filtering* konten di seluruh jaringan dan mencegah upaya *bypass* kebijakan melalui penggunaan DNS eksternal (seperti Google DNS 8.8.8.8 atau OpenDNS).

2. Pencegahan Akses Proxy dan VPN

Proxy dan VPN (Virtual Private Network) sering dimanfaatkan pengguna untuk menyembunyikan alamat IP asli, melewati pembatasan geografis atau *filtering* konten, dan mengenkripsi lalu lintas jaringan. Meskipun berguna untuk privasi, dalam jaringan institusional, penggunaannya dapat menyebabkan masalah keamanan, penyalahgunaan *bandwidth*, dan pelanggaran kebijakan. Pencegahan akses melibatkan identifikasi dan pemblokiran lalu lintas yang berasal dari layanan ini.

3. Metode Layer 7 Protocol

Layer 7 Protocol merujuk pada lapisan aplikasi dalam model OSI (Open Systems Interconnection). Metode Layer 7 Protocol Filtering merupakan teknik inspeksi paket yang canggih yang bekerja dengan menganalisis isi sebenarnya dari paket data (payload), bukan hanya *header* IP atau *port*.

1. Prinsip Kerja: Mikrotik RouterOS menggunakan fitur Layer 7 Protocol untuk mendefinisikan pola (menggunakan *Regular Expression* / RegEx) yang unik dan menjadi ciri khas dari protokol atau layanan tertentu (misalnya, *signature* koneksi VPN atau Proxy tertentu).

Keefektifan: Metode ini sangat efektif untuk mendeteksi layanan Proxy dan VPN yang mencoba bersembunyi di balik *port* standar (misalnya Port 80 atau 443), karena ia memeriksa pola data pada lapisan aplikasi memastikan deteksi yang lebih akurat dan granular terhadap layanan yang dicurigai.

4. Metode Penelitian

Penelitian ini menggunakan kerangka konsep yang mengacu pada siklus pengembangan jaringan dan melibatkan analisis masalah, perumusan solusi, implementasi, dan analisis hasil.

1. Permasalahan: Sistem jaringan lama UMMU menggunakan *firewall* dasar dan *filtering* IP/port konvensional, yang tidak efektif dalam mencegah *bypass* melalui Proxy dan VPN, sehingga mengakibatkan akses ke konten negatif dan mengganggu keamanan/produktivitas.
2. Pemecahan Masalah: Diusulkan penerapan Transparent DNS untuk memaksakan *filtering*

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)

ISSN: 2654-2617 (Cetak)
Jurnal Teknologi Informatika (J-TIFA) V.8.No.2 September 2025 ISSN: 2654-2633(Online)

DNS dan Firewall Layer 7 Protocol (Mikrotik) untuk mendeteksi serta memblokir pola lalu lintas Proxy dan VPN.

3. Analisis Hasil: Hasil implementasi dianalisis berdasarkan efektivitas pencegahan akses Proxy/VPN, serta dampak terhadap jaringan (kecepatan, *latensi*, *throughput*) dan pengalaman/kepuasan pengguna.

2. Metode Pengembangan Jaringan (NDLC)

Penelitian dan implementasi sistem yang diusulkan ini mengikuti model *Network Development Life Cycle* (NDLC) yang adaptif, yang terdiri dari tahapan utama berikut:

a. Analisis: Dilakukan studi literatur (Tinjauan penelitian terkait Layer 7 Protocol dan Transparent DNS) dan identifikasi kebutuhan spesifik UMMU (kebutuhan akan keamanan, efisiensi *bandwidth*, dan pencegahan *bypass*).
b. Desain: Merancang arsitektur jaringan yang diusulkan, yang meliputi penentuan lokasi penempatan *router* Mikrotik utama, perencanaan *subnetting* untuk memisahkan *traffic*, dan perumusan aturan Firewall NAT untuk Transparent DNS dan aturan Layer 7 Protocol untuk mendeteksi Proxy/VPN.
c. Simulasi: ASPengujian konfigurasi *Layer 7* dan *Transparent DNS* pada lingkungan pengujian terkendali sebelum diimplementasikan ke jaringan utama UMMU, untuk memverifikasi fungsionalitas dan dampaknya.
d. Implementasi: Penerapan konfigurasi yang telah diverifikasi pada *router* Mikrotik utama UMMU.
e. Pemantauan: Memantau lalu lintas jaringan, mencatat upaya akses Proxy/VPN, dan mengukur kinerja jaringan setelah penerapan (*latency*, *throughput*).
f. Evaluasi: Menganalisis data pemantauan untuk menilai efektivitas sistem dan dampaknya terhadap pengalaman pengguna (menggunakan kuesioner atau survei kepuasan).

2. Penerpan perancangan sistem
Perancangan sistem dalam penelitian ini bertujuan untuk menciptakan sebuah mekanisme pengelolaan dan pengamanan akses internet yang efektif di lingkungan akademik. Sistem dirancang dengan menggunakan metode Transparent DNS untuk mengarahkan seluruh permintaan DNS pengguna ke server DNS universitas, sehingga menghindari penggunaan DNS eksternal yang berpotensi membuka akses tidak sah. Selain itu, penerapan Layer 7 Protocol dalam sistem memungkinkan inspeksi paket data secara mendalam pada lapisan aplikasi, yang berfungsi mendeteksi dan memblokir lalu lintas proxy dan VPN. Seluruh komponen ini diintegrasikan dalam sebuah sistem pengendalian akses internet yang dapat diuji melalui berbagai skenario untuk memastikan efektivitas serta kestabilan jaringan, guna mendukung keamanan dan kenyamanan pengguna di lingkungan kampus.

Penerapan perancangan sistem dalam penelitian ini meliputi:

1. pengembangan sistem dengan integrasi Transparent DNS untuk memastikan seluruh permintaan DNS dialihkan ke server universitas sehingga menghilangkan akses DNS eksternal yang tidak diizinkan.
2. implementasi metode Layer 7 Protocol yang mampu melakukan inspeksi paket data pada lapisan aplikasi guna mendeteksi dan memblokir penggunaan proxy dan VPN secara efektif.
3. pengujian sistem secara menyeluruh melalui berbagai skenario akses internet untuk memastikan efektivitas filtering dan kestabilan jaringan dalam lingkungan akademik.
4. Sistem yang diusulkan untuk Universitas Muhammadiyah Maluku Utara mencakup penerapan Transparent DNS dan penggunaan metode Layer 7 Protocol untuk meningkatkan filtering pengguna internet. Transparent DNS akan memastikan bahwa semua permintaan DNS dari pengguna diarahkan melalui server DNS yang dikelola oleh universitas, memungkinkan pemantauan dan pengendalian akses ke situs web yang tidak diinginkan. Metode Layer 7 Protocol akan digunakan untuk menganalisis dan

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)

mengidentifikasi pola lalu lintas jaringan pada lapisan aplikasi, memungkinkan deteksi dan pemblokiran akses melalui proxy dan VPN yang sering digunakan untuk melewati pembatasan jaringan. Dengan kombinasi teknologi ini, sistem yang diusulkan akan memberikan kontrol yang lebih ketat dan efektif terhadap penggunaan internet di kampus, meningkatkan keamanan jaringan, dan memastikan penggunaan internet yang lebih aman dan terfokus pada tujuan akademik.

5. Sistem yang berjalan di Universitas Muhammadiyah Maluku Utara saat ini menggunakan metode konvensional untuk pengelolaan dan pengawasan akses internet, yang mencakup firewall dasar dan aturan akses yang terbatas pada filtering alamat IP dan port. Namun, sistem ini kurang efektif dalam mencegah penggunaan proxy dan VPN yang digunakan oleh beberapa pengguna untuk melewati pembatasan akses. Akibatnya, banyak konten yang tidak diinginkan atau tidak relevan tetap dapat diakses, yang mengganggu keamanan dan produktivitas lingkungan akademik. Sistem saat ini juga tidak menerapkan Transparent DNS dan metode

Layer 7 Protocol, yang lebih canggih dan mampu melakukan inspeksi paket data secara mendalam untuk mengidentifikasi dan memblokir penggunaan proxy dan VPN secara lebih efektif. Implementasi teknologi ini diharapkan dapat meningkatkan keamanan dan kontrol atas penggunaan internet di kampus, memastikan akses yang lebih aman dan teratur.

5. Hasil Penelitian

Penelitian menunjukkan bahwa penerapan Transparent DNS dan metode Layer 7 Protocol secara signifikan mampu mencegah akses melalui proxy dan VPN di lingkungan Universitas Muhammadiyah Maluku Utara. Data pengujian menampilkan penurunan akses ke situs yang tidak diinginkan dan perbaikan kestabilan jaringan yang signifikan. Hal ini menunjukan peningkatan keamanan serta optimalisasi penggunaan bandwidth di kampus.

Gambar .1 Firewall NAT

Pada gambar di atas, terlihat antarmuka pengaturan firewall yang berfungsi untuk mengelola dan memblokir akses tertentu berdasarkan pola ekspresi reguler (regex). Terdapat dua entri utama yang ditunjukkan, yaitu block_doh dan block_vpn. Entri block_doh dirancang untuk memblokir alamat DNS yang dikenal menggunakan protokol DoH (DNS over HTTPS), seperti dns.google dan cloudflare-dns.com, yang dapat mengancam privasi pengguna dengan memungkinkan resolusi domain tanpa pengawasan. Sedangkan entri block_vpn bertujuan menutup akses ke berbagai layanan VPN dan proksi yang mungkin digunakan untuk menyembunyikan aktivitas internet, seperti ultrasurf dan hide.me. Konfigurasi ini menunjukkan pendekatan proaktif dalam pengelolaan keamanan jaringan, di mana administrator berusaha mencegah potensi pelanggaran keamanan serta menjaga integritas dan kebijakan akses dalam lingkungan jaringan yang

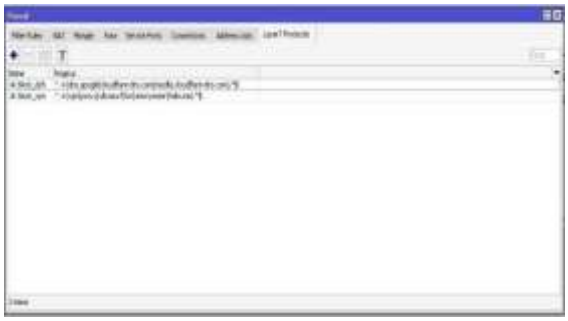
Gambar .2 NAT

Gambar yang disajikan menunjukkan antarmuka dari sistem firewall yang digunakan untuk mengelola pengaturan jaringan dan keamanan. Di bagian atas, terdapat menu yang memungkinkan pengguna untuk mengakses berbagai fitur, termasuk filter rules, NAT, mangle, dan lainnya. Di bawahnya, terlihat tabel yang mencakup informasi mengenai aturan firewall yang

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)

ISSN: 2654-2617 (Cetak)
Jurnal Teknologi Informatika (J-TIFA) V.8.No.2 September 2025 ISSN: 2654-2633(Online)

ada, di mana terdapat tiga entri dengan informasi mengenai tindakan (action), rantai (chain), alamat sumber dan tujuan (src/dst address), protokol, dan statistik terkait penggunaan data. Aturan pertama menunjukkan pengalihan (redirect) untuk DNS melalui UDP dengan ukuran byte 73,9 KiB dan total paket 1.093, sedangkan aturan kedua menunjukkan pengalihan untuk DNS menggunakan TCP dengan statistik yang masih kosong. Total penggunaan data untuk interface ether1 tercatat sebesar 2728,4 KiB dengan 13.171 paket. Data ini sangat penting untuk memastikan keamanan dan efisiensi operasional jaringan, serta



Gambar .2 . layar 7 protocol

Gambar tersebut menunjukkan konfigurasi pada firewall untuk membuat Layer 7 Protocol baru dengan nama "Facebook". Pada proses ini, pengguna menambahkan pola deteksi (regexp untuk mengidentifikasi trafik yang terkait dengan situs Facebook melalui pola ekspresi reguler **^.+(facebook.com).*$**. Dengan cara ini, firewall dapat mendeteksi dan memfilter paket data yang mengandung domain facebook.com, sehingga memungkinkan pengelolaan akses atau pembatasan terhadap situs Facebook berdasarkan aturan firewall yang telah dibuat. Setelah pengaturan selesai, pengguna bisa menyimpan konfigurasi dengan menekan tombol "OK" atau "Apply".

Dalam upaya menciptakan lingkungan internet yang aman, produktif, dan efisien di kampus, Universitas Muhammadiyah Maluku Utara (UMMU) dapat mengimplementasikan strategi *filtering* berlapis yang komprehensif, dimulai dengan penerapan transparent proxy yang secara otomatis mengarahkan seluruh lalu lintas HTTP/HTTPS dari pengguna internal melalui server *proxy* tanpa memerlukan konfigurasi manual pada setiap perangkat, sehingga memungkinkan manajemen terpusat, penghematan *bandwidth* melalui *caching*, serta kebijakan keamanan. Namun, karena pengguna yang canggih mungkin mencoba mengakali sistem *filtering* ini dengan menggunakan layanan *proxy* eksternal atau *Virtual Private Network* (VPN) untuk menyembunyikan identitas dan mengenkripsi lalu lintas mereka, UMMU perlu melengkapi *transparent proxy* dengan pencegahan yang lebih canggih menggunakan metode Layer 7 Protocol; pendekatan ini memungkinkan sistem keamanan untuk menganalisis isi sebenarnya dari paket data (*Deep Packet Inspection - DPI*) daripada hanya melihat alamat IP atau *port*, sehingga secara spesifik dapat mengidentifikasi dan memblokir *signature* atau pola perilaku unik dari protokol *proxy* dan *VPN* yang dikenal, bahkan jika mereka menggunakan *port* standar, memastikan bahwa semua aktivitas internet di lingkungan kampus sesuai dengan kebijakan yang ditetapkan, meningkatkan keamanan jaringan, dan mengoptimalkan penggunaan sumber daya internet untuk mendukung kegiatan akademik dan penelitian.

Kesimpulan

Penerapan Transparent DNS di Universitas Muhammadiyah Maluku Utara berhasil meningkatkan efektivitas pengelolaan akses internet dengan memudahkan proses filtering tanpa perlu konfigurasi manual pada perangkat pengguna. Metode Layer 7 Protocol Filtering terbukti efektif dalam mendeteksi dan memblokir akses melalui proxy dan VPN, sehingga dapat mencegah pengguna mengakses konten yang dibatasi atau tidak sesuai dengan kebijakan kampus. Kombinasi antara Transparent DNS dan filtering Layer 7 memberikan kontrol yang lebih granular terhadap jenis layanan dan aplikasi yang dapat diakses, meningkatkan keamanan dan produktivitas pengguna ini juga membantu dalam mengoptimalkan penggunaan bandwidth dan menjaga kualitas layanan internet bagi seluruh civitas akademika

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)

Daftar pustaka

Adhikari, M., et al. (2021). A Comparative Study of Layer 4 and Layer 7 Load Balancing in Microservices Architecture. *IEEE Transactions on Services Computing*, *14*(5), 872-885. https://doi.org/10.1109/TSC.2019.2926066

Albitz, P., & Liu, C. (2017). DNS and BIND (5th Edition). O'Reilly Media.

Alshammari, F., & Zincir-Heywood, A. N. (2018). A Comprehensive Survey of DNS Spoofing Attacks and Defense Mechanisms. *IEEE Communications Surveys & Tutorials*, *20*(2), 1342-1384.

Jamaludin, P. (2019). Penerapan Transparent DNS, Pencegahan Penggunaan Proxy Dan VPN Dengan Firewall Metode Layer 7 Protocol Mikrotik Untuk Optimalisasi Filtering

Konten Negatif Serta Implementasi Di SMAN 27 Bandung (Doctoral dissertation, Universitas Komputer Indonesia).

Jamaludin, P. (2019). Penerapan Transparent Dns, Pencegahan Penggunaan Proxy Dan Vpn Dengan Firewall Metode Layer 7 Protocol Mikrotik Untuk Optimalisasi Filtering Konten.

Iskandar, F., & Muslim, A. (2017). Analisis dan Implementasi Metode Layer 7 Protocol untuk Blocking Aplikasi Chatting Berbasis Android. Jurnal Teknik Informatika, 10(1), 45-52.

Kurniawan, D., & Wibowo, A. (2018). Implementasi Firewall Layer 7 untuk Pencegahan Akses VPN pada Jaringan Kampus. Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA), 2018, 231-236.

Setiawan, R., & Santoso, B. (2019). Transparent DNS Proxy dengan Metode Filtering untuk Meningkatkan Keamanan Jaringan. Jurnal Ilmiah Teknologi Informasi dan Komunikasi, 14(2), 89-96.

Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif.

RFC 1035 - Domain Names - Implementation and Specification.

RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1

Loid, A., & Nurhaeni, N. (2020). Implementasi Deep Packet Inspection (DPI) pada Firewall untuk Identifikasi dan Blocking Aplikasi VPN. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(3), 567-574.

Rahman, A., & Supriyanto, A. (2021). Analisis Perbandingan Efektivitas Metode Layer 7 Protocol dan Deep Packet Inspection dalam Mendeteksi Proxy dan VPN. Jurnal Sistem Informasi, 17(1), 123-130.

Riwayat Artikel: Menerima (10 Agustus 2025), Revisi (16 agustus 2025), Diterima (20 agustus 2025), Online (september 2025)