MENGIMPLEMENTASIKAN PROXY SERVER (SQUID SERVER) BERBASIS LINUX PADA UBUNTU 22.04

Delvita Aulia Artika, Bunga Dwi Febrianti, Sarah Putri Syaifullah, Dedy Kiswanto
Ilmu Komputer, Universitas Negeri Medan
Jalan William Iskandar Ps. V Medan, Indonesia
dedykiswanto@unimed.ac.id

ABSTRAK

Proxy server adalah komponen penting dalam manajemen jaringan, terutama dalam meningkatkan efisiensi, keamanan, dan kontrol akses pengguna terhadap internet. Squid server, sebagai salah satu server proxy berbasis linux yang paling polpuler, telah lama digunakan untuk caching danfiltering di jaringan lokal. Namun, dengan kemajuan teknologi dan meningkatnya kompleksitas jaringan, kebutuhan untuk implementasi yang optimal pada sistem operasi terbaru, seperti Ubuntu versi 22.04, semakin meningkat. Penelitian ini bertujuan mengeksplorasi metode konfigurasi squid pada Ubuntu versi 22.04 untuk memaksimalkan efisiensi, keamanan, dan penyesuaian terhadap kebutuhan jaringan modern. Melalui pendekatan eksperimental yang mencakup instalasi, konfigurasi, dan filtering konten, penelitian ini menunjukkan bahwa implementasi squid berhasil meningkatkan kinerja jaringan hingga 20% melalui caching serta memblokir akses ke konten tidak produktif. Selain itu, konfigurasi control akses menggunakan Access Control Lists (ACL) memungkinkan pengolaan lalu lintas jaringan secara efektif dan aman. Hasil ini mengisi kesenjangan dalam literatur sebelumnya yang berfokus pada system operasi lama dan memberikan kontribusi signifikan bagi pengembangan proxy server bebrbasis linux dalam lingkungan jaringan modern.

Kata kunci : *Squid Proxy Server, Ubuntu 22.04, Manajemen Jaringan, Caching, Kontrol Akses.*

1. PENDAHULUAN

Didalam era digital yang semakin canggih atau maju, kebutuhan akan manajemen lalu lintas jaringan yang efisien dan aman menjadi sangat penting. Menggunakan Proxy Server ialah salah satu Solusi yang banyak diadopsi oleh organisasi untuk mengelola akses internet dan meningkatkan jaringan peforma. Proxy server merupakan komponen dalam manajemen jaringan, terutama untuk meningkatkan efisiensi, keamanan, dan kontrol akses pengguna terhadap internet. Ia berintak sebagai perantara antara klien (pengguna) dan internet, Dimana semua permintaan akses situs web dari klien garus melewati server ini sebelum diteruskan ke internet.

Squid, sebagai salah satu server proxy berbasis Linux yang paling populer, telah lama digunakan untuk caching dan filtering di jaringan lokal, memungkinkan organisasi menghemat bandwidth dan mengontrol akses pengguna terhadap konten tertentu. Selain itu, Squid juga menyediakan fitur keamanan tambahan seperti control akses, autentikasi, dan pembatasan pengguna berdasarkan berbagai parameter.

Dengan perkembangan teknologi internet dan meningkatnya kompleksitas jaringan, kebutuhan akan implementasi yang lebih optimal dan sesuai dengan konfigurasi yang spesifik pada sistem operasi terkini seperti Ubuntu 22.04 semakin penting. Dimana Ubuntu 22.04 merupakan salah satu distribusi Linux yang stabil dan didukung secara luas dan menjadi pilihan yang tepat untuk mengimplementasikan proxy server berbasis Squid. Dengan menggunakan squid pada ubuntu 22.04, administrator jaringan dapat mengelola lalu lintas internet dengan lebih baik, memeastikan pengguna mengikuti kebijakan penggunaa internet yang tepat, dan mengurangi beban pada bandwidth.

Penelitian ini bertujuan untuk mengisi kesenjangan dalam literatur yang secara khusus membahas implementasi squid server pada Ubuntu 22.04 dengan mengeksplorasi metode konfigurasi squid pada ubuntu 22.04 yang memaksimalkan kemampuan sistem operasi terbaru,sehingga menghasilkan solusi yang lebih efesien, aman, dan adaptasi terhadap kebutuhan jaringan modern.

Dengan mengkonfigurasi squid server yang disesuaikan dengan aksiktektur terbaru ubuntu 22.04, yang belum banyak dibahas dalam literatur sebelumnya, maka kami harapkan makalah ini memberikan konstribusisignifikan terhadap pengembangan server proxy berbasis Linux di lingkungan jaringan modern. Dan dapat menjawab pertanyaan cara mengimplementasikan dan mengonfigurasi squid server pada ubuntu 22.04 untuk mendapatkan performa dan keamanan jaringan yang optimal.

2. TINJAUAN PUSTAKA

Misalnya, lihat [4] Proxy server yang cukup populer saat ini adalah squid, karena selain gratis juga mendukung Internet Cache Protocol (ICP). ICP digunakan untuk pertukaran data tentang suatu Uniform Resource Locator (URL) dengan cache-cache lainnya. Secara sederhana, squid dapat dikatakan sebagai software yang diaplikasikan untuk membuat http atau ftp cache. Selain itu, squid dapat melakukan filtering, yaitu squid dapat mem-block permintaan client terhadap URL - URL tertentu, sehingga

pengelola jaringan dapat lebih santai tanpa khawatir adanya penyalahgunaan yang tidak dikehendaki.

Pada penelitian [1] organisasi mungkin menghadapibeberapa kendala implementasi, misalnya tidak ada dukungan untuk otentikasi berbasis intisari dalamaplikasi pengguna tertentu yang memerlukan pengaturan proxy otentikasi dasar untuk mereka. Semua masalah yang disebutkan di atas membuatnya sangat diperlukan untuk menyebarkan beberapa server proxy dalam suatu organisasi. Instalasi yang salah dapat merusak server atau menyebabkan kelemahan keamanan. Manajemen kebijakan manual membutuhkan operator yang kuat secara teknis yang mengetahui aturan/format/sintaks yang benar untuk membuat kebijakan. Oleh karena itu, diperlukan untuk memiliki sistem manajemen proxy terpusat khusus dengan antarmuka berbasis web yang ramah pengguna yang meminta informasi minimal dari operator dan secara otomatis menghasilkan file kebijakan dengan format yang benar dan menyebarkannya di beberapa server jarak jauh.

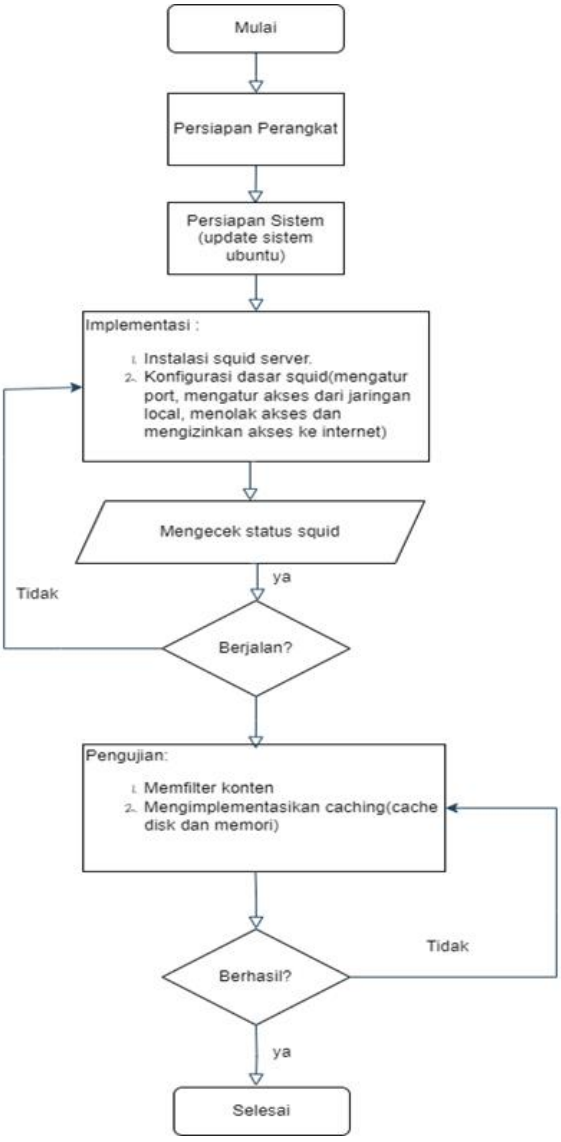
Meskipun demikian, pada penelitian-penelitian sebelumnya mereka hanya berfokus pada sistem operasi lama atau versi Ubuntu yang usang atau sudah lama. Misalnya pada penelitian [7] mereka menggunakan Proxy server dengan Linux Ubuntu 14.04, dan pada penelitian [2] menggunakan Proxy server Pada Ubuntu Server 10.10.

Selain itu, penelitian-penelitian yang menegaskan bahwa mengamankan keamanan pada jaringan yang sangat diperlukan juga sudah banyak. Contohnya pada penelitian [3], [4], [6] mengkaji ancaman danmenegaskan saat ini bahwa implementasi keamanan pada infrastruktur jaringan sangat diperlukan. Semakin meningkatnya perilaku pengguna internet agar dapat mengakses konten-konten yang diinginkan, menjadikan administrator perlu untuk menjaga kestabilan dan kecepatan dalam akses internet. Dan untuk menjaga agarsitus-situs yang diharapkan tidak dapat diakses melalui jaringan internet, serta mempercepat dan menghemat akses internet.

3. METODE PENELITIAN

3.1. Pendekatan Eksperimental

Penelitian ini dilakukan dengan pendekatan eksperimental dimana kami mengimplementasikan proxy server yaitu squid server pada sistem operasi berbasis linux yaitu ubuntu versi 22.04. Studi ini dilakukan untuk untuk meningkatkan efisiensi dan keamanan dalam pengelolaan akses internet di jaringan pada sistem operasi. Fokus utama dari penelitian ini adalah menjelaskan proses instalasi, konfigurasi dan 2 pengujian server squid. Pengimplementasian ini diawali dengan menginstall squid server tersebut kedalam sistem operasi, yang dilakukan dengan langkah-langkah sebagai berikut:



Gambar 1. Flowchart implementassi squid server

3.2. Persiapan Perangkat

Ini sangat penting dalam menginstall dan mengkonfigurasi squid server pada sistem operasi Ubuntu. Persiapan ini dilakukan pada hardware (CPU, RAM, dan penyimpanan) dan software (sistem operasi dan firewall) telah siap dan dikonfigurasi dengan benar serta disesuaikan dengan kebutuhan.

3.3. Persiapan Sistem

Sebelum memulai installasi squid server nya, sangat penting untuk memastikan bahwa sistem Ubuntu sudah dalam kondisi yang optimal dan update ini membantu menghindari potensi masalah yang mungkin terjadikaren adanya paket sistem yang kadaluarsa atau ketidakcocokan versi. Untuk melakukan pengupdatean sistem dilakukan pada terminal di Ubuntu dengan menjalankan perintah:

Gambar 2. Perintah update system

Kemudian tunggu sampai pengupdatean selesai. Ini akan memperbarui daftar paket di sucrepositori dan mengupgrade semua paket yang sudah terinstall ke versi terbaru.

3.4. Installasi squid server

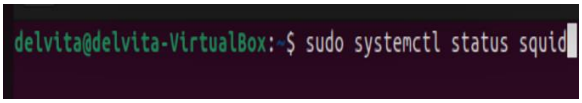
Squid server tersedia di repositori Ubuntu, sehingga untuk menginstallnya cukup mudah. Tidak ada kebutuhan untuk mendownload paket secara manual karena semuanya tersedia melalui manajer paket apt. Penginstallan ini dilakukan dengan menjalankan perintah di terimanal Ubuntu:

Gambar 3. Perintah insatll squid server

Dimana proses ini akan mengunduh dan menginstall semua paket dan dependensi yang dibutuhkan oleh squid. Squid diinstal sebagai layanan yang secara otomatis dijalankan oleh sistem operasi setelah installasi. Untuk memeriksa status squid dilakukan dengan menjalankan perintah di terminal.

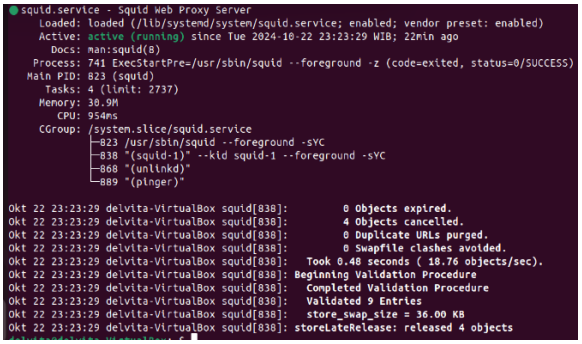
3.5. Memeriksa status layanan squid

Setelah installasi squid selesai, penting untuk memastikan bahwa layanan squid sudah berjalan dengan benar di sistem.



Gambar 4. Perintah Cek status squid

Output dari perintah ini akan memberikan informasi mengenai status layanan Squid. Jika tampilan active (running) ini menunjukkan bahwa Squid sedang berjalan dan beroperasi sebagaimana mestinya.



Gambar 5. Status active squid server

3.6. Konfigurasi Dasar Squid

Penelitian selanjutnya dilakukan dengan melakukan konfigurasi dasar squid yang bertujuan agar proxy server dapat berjalan sesuai kebutuhan, mengelola lalu lintas internet secara efisien, dan membatasi atau mengizinkan akses sesuai aturan yang diinginkan. konfigurasi squid yang dilakukan untuk memodifikasi file utama di /etc/squid/squid.conf ini adalah file yang mengatur bagaimana Squid beroperasi sebagai proxy server. Konfigurasi ini dilakukan dengan:

3.7. Membuat Cadangan File Konfigurasi

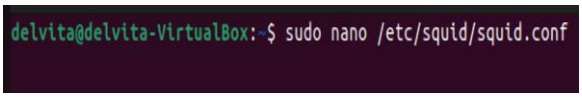
Sebelum mengubah apapun, sangat disarankan untuk membuat cadangan dari file konfigurasi asli sebagai langkah berjaga-jaga yang dilakukan dengan perintah:

Gambar 6. Perintah mencadangkan file konfigurasi

Cadangan ini memungkinkan Anda untuk mengembalikan pengaturan ke keadaan semula jika terjadi kesalahan konfigurasi.

3.8. Mengedit file konfigurasi

Dilakukan dengan melakukan perintah ini di terminal ubuntu.



Gambar 7. Perintah membuka file konfigurasi squid

Setelah file ini terbuka selanjutnya disini kita dapat mengedit file seperti yang diinginkan.

3.9. Konfigurasi Dasar Squid

Konfigurasi dasar Squid melibatkan beberapa langkah penting untuk memastikan server proxy berfungsi dengan baik. Pengaturan port, kontrol akses dengan ACL, serta izin akses internet adalah bagian utama yang perlu diperhatikan. Dimana pengaturan konfigurasi dasar ini dilakukan dengan:

3.10. Mengatur Port Deafult Squid

Squid secara default menggunakan port 3128 untuk menerima permintaan klien. Namun port dapat diubah, misalnya ke 8080, jika diperlukan untuk menyesuaikan arsitektur jaringan atau menghindari konflik dengan aplikasi lain. Pengaturan ini dilakukan di file konfigurasi /etc/squid/squid.conf dengan mencari dan mengedit baris yang mengatur port Squid.

Gambar 8. Port default

Ubah angka 3128 menjadi port yang Anda inginkan. Misalnya, jika Anda ingin Squid mendengarkan di port 8080, ganti baris tersebut menjadi:

```
# Squid normally listens to port 3128
http_port 8080
```

Gambar 9. Port yang di ubah

Setelah melakukan perubahan, simpan file konfigurasi dan keluar dari editor. Jika menggunakan nano, tekan Ctrl + X, lalu tekan Y untuk mengonfirmasi penyimpanan, dan Enter untuk keluar.Agar perubahan port ini aktif, Anda perlu me-restart layanan Squid. Gunakan perintah berikut untuk merestart Squid dan menerapkan perubahan:

```
delvita@delvita-VirtualBox:~$ sudo systemctl restart squid
```

Gambar 10. Perintah merestart sistem squid

3.11. Mengatur Akses Dari Klien

Squid menggunakan ACL (Access Control List) untuk menentukan klien mana yang diizinkan atau ditolak mengakses proxy server. Dua konsep penting dalam pengaturan akses adalah:

a. ACL (Access Control List): Digunakan untuk mendefinisikan aturan yang menentukan klien atau jaringan tertentu yang diizinkan atau dibatasi aksesnya.
b. http_access: Digunakan untuk menentukan apakah akses diizinkan atau ditolak berdasarkan aturan ACL.

Konfigurasi yang dapat dilakukan adalah

3.12. Mengizinkan Akses dari Jaringan Lokal

Secara default, Squid mungkin hanya diizinkan untuk diakses dari localhost (127.0.0.1). Jika Anda ingin mengizinkan klien dari jaringan lain, misalnya subnet 192.168.1.0/24, Anda perlu menambahkan aturan ACL untuk mengizinkan klien tersebut. Yang dilakukan dengan menjalankan mengedit file /etc/squid/squid.conf.

```
# For example, to allow access from your local networks, you may uncom
# following rule (and/or add rules that match your definition of "loca
# http_access allow localnet
acl localnet src 192.168.1.0/24
http_access allow localnet
```

Gambar 11. Perintah mengizinkan akses ke jaringan lokal

Posisi ACL ini biasanya diletakkan di bagian atas, sebelum aturan http_access deny all yang membatasi akses.

3.13. Menolak Akses untuk Semua Selain yang Diizinkan

Kita juga harus memastikan bahwa akses ke proxy selain dari jaringan yang diizinkan dibatasi. Pastikan baris berikut ada di bagian bawah file:

```
# And finally deny all other access to this proxy
http_access deny all
```

Gambar 12. Perintah menolak akses

Ini memastikan bahwa hanya klien dari subnet yang Anda tentukan (misalnya 192.168.1.0/24) yang dapat mengakses Squid, sementara klien lainnya akan ditolak.

3.14. Mengizinkan Akses ke Internet

Secara default, Squid mungkin membatasi akses internet bagi kliennya. Untuk mengizinkan klien Anda mengakses internet melalui proxy, tambahkan aturan berikut di file konfigurasi:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
http_access deny all
```

Gambar 13. Perintah mengizinkan akses ke internet

Ini berarti semua permintaan akses internet akan diizinkan oleh Squid. Namun, pengaturan ini hanya disarankan untuk jaringan kecil atau dalam pengujian.

3.15. Pengujian Awal

Kemudian melakukan pengujian awal untuk melihat bagaimana kerja squid server ini dalam meningkatkan efisiensi dan keamansn server dan melihat apakah squid server ini sudah berjalan pada sistem dengan baik.

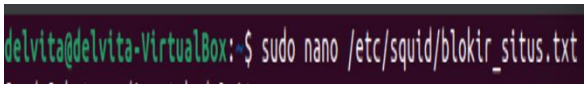
3.16. Memfilter Konten Yang Dianggap Tidak Penting

Squid memungkinkan administrator jaringan mengontrol dan membatasi akses internet menggunakan Access Control Lists (ACL). Dengan ACL, akses dapat difilter berdasarkan URL, domain, atau kata kunci. Administrator dapat memblokir situs tertentu untuk menjaga keamanan dan produktivitas, terutama di lingkungan dengan kebutuhan pengawasan ketat. Ini membantu mengurangi risiko paparan konten tidak sesuai dan memastikan pengguna hanya mengakses situs yang diizinkan.Berikut adalah langkah-langkah untuk melakukannya:

3.17. Buat File Daftar Situs Yang Ingin Diblokir

Langkah pertama adalah membuat file yang berisi daftar domain yang ingin di blokir. Dengan membuat file baru bernama blokir_situs.txt. Di dalam file ini, tambahkan domain yang ingin Anda blokir, satu domain per baris. Setelah menambahkan domain, simpan dan keluar dari editor teks. Jika menggunakan

nano, tekan Ctrl + X, kemudian Y untuk menyimpan, dan tekan Enter untuk mengkonfirmasi.



Gambar 14. Perintah membuat file yang berisi daftar situs yang diblokir

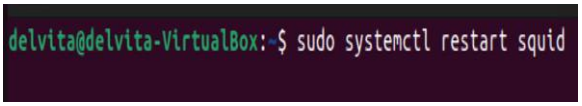
Gambar 15. Contoh dari domain situs yang dimasukkan ke dalam file blokir

3.18. Tambah Aturan Di File Konfigurasi Squid

Setelah membuat daftar situs yang akan diblokir, langkah selanjutnya adalah menambahkan aturan ke dalam file konfigurasi Squid agar server tahu untuk memblokir akses ke situs-situs tersebut. Pengeditan ini dilakukan pada file /etc/squid/squid.conf. Di dalam file ini, tambahkan baris-baris berikut di bagian yang sesuai (biasanya di bagian bawah atau sebelum aturan yang mengizinkan akses):

Gambar 16. Perintah memblokir situs tertentu

Pengaturan ini membuat Access Control List (ACL) untuk memblokir situs atau URL tertentu. ACL diberi label blockirsitus untuk referensi mudah. Opsi url_regex -i memungkinkan pencocokan pola dengan regex secara case-insensitive. Daftar situs yang diblokir disimpan di /etc/squid/blokir_situs.txt. Agar berfungsi, perintah http_access deny blockirsitus harus ditambahkan dalam konfigurasi Squid. Setelah menambahkan aturan selanjutnya adalah merestart sistem suid agar perubahan di terapkan. Lakukan perintah berikut pada terminal:



Gambar 17. Perintah merestart sistem squid

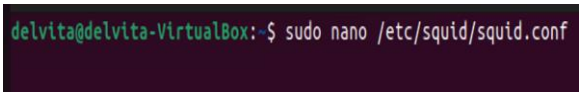
3.19. Mengimplementasikan Caching

Caching adalah salah satu fitur utama Squid yang memungkinkan server menyimpan konten web, sehingga permintaan selanjutnya untuk konten yang sama dapat dipenuhi dengan lebih cepat. Dengan menyimpan salinan objek web, Squid dapat mengurangi waktu akses, mengurangi beban pada jaringan, dan menghemat bandwidth. Oleh karena itu, pengaturan cache disk dan memori sangat penting untuk memastikan kinerja yang optimal.

Pengaturan cache disk sangat penting untuk mengontrol berapa banyak ruang disk yang akan dialokasikan oleh Squid untuk menyimpan objek cache. Tujuan dari pengaturan ini adalah untuk meningkatkan efisiensi akses konten dan mengoptimalkan penggunaan ruang penyimpanan pada server. Cache memori digunakan untuk menyimpan objek yang sering diakses dalam RAM, memberikan akses yang lebih cepat dibandingkan dengan mengambil data dari disk. Ini sangat penting untuk meningkatkan responsivitas server proxy. Berikut adalah langkah-langkah untuk melakukannya.

3.20. Buka file konfigurasi squid

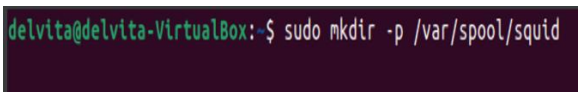
Langkah pertama yang dilakukan adalah membuka file konfigurassi utama squid yang terletak pada file /etc/squid/squid.conf.



Gambar 18. Perintah membuka file edit konfigurasi squid

3.21. Membuat direktori cache dan menambah izin menyimpan cache_dir

Sebelum mengedit di dalam file konfigurasi, harus membuat direktori terlebih dahulu yaitu /var/spool/squid yang digunakan untuk menyimpan cache di disk. Dan memastikan memiliki izin yang benar.Jika direktori belum ada, Anda bisa membuatnya dengan perintah:



Gambar 19. Perintah membuat direktori cache

Izin yang diperlukan untuk menyimpan cache, yaitu

3.22. Mengubah kepemilikan direktori.

Ini dilakukan untuk mengubah kepemilikan direktori beserta seluruh isinya sehingga dimiliki oleh pengguna dan grup proxy sehingga squid memeliki izin untuk membaca dan menulis file dalam direktori tersebut. Ini dilakukan dengan perintah:

Gambar 20. Perintah mengubah kepemilikan direktori

3.23. Mengubah izin akses direktori.

Ini dilakukan untuk mengubah izin akses direktori beserta semua file dan subdirektori didalamnya. Dengan izin 755, pemilik direktori (biasanya pengguna proxy di squid) memiliki akses penuh untuk membaca, menulis, dan mengeksekusi file, sedangkan grup dan pengguna lain hanya dapat membaca dan mengeksekusi file, tapi tidak dapat

menulis, mengubah dan menghapus file). Ini dilakukan dengan menggunakan perintah:

```
delvita@delvita-VirtualBox:~$ sudo chown -R proxy:proxy /var/spool/squid
```

Gambar 21. Perintah mengubah izin akses direktori

3.24. Mengedit konfigurasi squid

Setelahnya edit file /etc/squid/squid.conf. dengan:Pengaturan yang tepat untuk cache disk sangat penting untuk kinerja Squid. Jika ukuran cache terlalu kecil, maka cache mungkin cepat penuh, menyebabkan Squid tidak dapat menyimpan objek baru. Sebaliknya, jika terlalu besar, itu dapat menggunakan ruang disk yang tidak perlu.Beberapa perubahan yang di lakukan adalah:

3.25. Mengatur lokasi dan kapasitas cache disk cache

```
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 10000 16 256
```

Gambar 22. Perintah mengatur lokasi dan kapasitas cache

Konfigurasi ini menentukan lokasi dan kapasitas cache menggunakan ufs. File cache disimpan di direktori /var/spool/squid dengan kapasitas maksimum 10 GB. Angka 16 dan 256 menunjukkan jumlah direktori di level pertama dan sub-direktori di level kedua, yang mempercepat pencarian dan pengelolaan objek. Konfigurasi ini memungkinkan Squid menyimpan objek di disk untuk meningkatkan efisiensi dan kecepatan akses internet.

3.26. Mengatur ukuran memori cache

```
#Default:
 cache_mem 256 MB
```

Gambar 23. Perintah mengatur ukuran memori

Dalam konfigurasi Squid menentukan batas maksimum penggunaan RAM sebesar 256 MB untuk menyimpan objek-objek cache kecil, seperti halaman web atau gambar yang sering diakses. Dengan menyimpan objek di RAM, Squid dapat mempercepat respon karena akses data dari memori jauh lebih cepat dibandingkan dari disk atau internet.

3.27. Menentukan ukuran maximum dan minimum file yang disimpan.

```
#Default:
minimum_object_size 0 KB
```

Gambar 24. Perintah ukuran minimum

Ini menentukan bahwa tidak ada batasan ukuran minimum untuk objek yang dapat disimpan di disk cache. Dengan pengaturan ini, bahkan objek yang sangat kecil dapat disimpan di disk. Hal ini memungkinkan Squid untuk mencache semua objek tanpa pengecualian berdasarkan ukuran, sehingga meningkatkan peluang objek sering diakses dari cache. Namun, menyimpan objek berukuran terlalu kecil di disk dapat meningkatkan jumlah operasi baca/tulis yang tidak efisien dan memperlambat performa disk.

```
#Default:
 maximum_object_size 51200 MB
```

Gambar 25. Perintah ukuran maximum

Pengaturan ini menetapkan batas maksimal objek yang disimpan di disk cache hingga 51.200 MB (50 GB). Ini memungkinkan Squid menyimpan konten besar, seperti video atau arsip, untuk akses lebih cepat tanpa harus mengunduh ulang. Namun, perlu mempertimbangkan kapasitas disk yang tersedia, karena menyimpan objek besar dapat mempengaruhi kinerja, seperti memperlambat pencarian dan operasi disk.

3.28. Menagement akses cache

```
#refresh_pattern (\.deb|\.udeb)$   129600 100% 129600
refresh_pattern .       0       20%     43200
```

Gambar 26. Perintah penyegaran cache

Aturan ini berlaku untuk semua URL dengan ekspresi reguler titik (.) yang mencocokkan semua konten. Angka 0 berarti tidak ada waktu minimum sebelum objek dianggap kedaluwarsa. Persentase 20% menandakan Squid akan memverifikasi ulang ke server jika usia objek mencapai 20% dari waktu kedaluwarsanya. Waktu maksimal 4320 menit (3 hari) memungkinkan objek disimpan tanpa pengecekan ulang. Aturan ini meningkatkan performa dengan mengurangi permintaan ulang konten, kecuali jika objek mendekati usia maksimalnya.

3.29. Mengatur log akses cache

```
#Default:
 cache_log /var/log/squid/cache.log
access_log /var/log/squid/access.log squid
```

Gambar 27. Perintah menentukan file log

cache_log mencatat status internal, kesalahan, dan informasi operasional Squid di /var/log/squid/cache.log. cache_store_log mencatat aktivitas penyimpanan dan pengambilan objek di /var/log/squid/store.log. Log ini membantu administrator memantau performa dan memecahkan masalah.Setelah mengedit, simpan perubahan (jika menggunakan nano: tekan Ctrl + X, lalu Y, dan Enter). Kemudian, restart layanan Squid agar perubahan diterapkan:

```
delvita@delvita-VirtualBox:~$ sudo systemctl restart squid
```

Gambar 28. Perintah merestart layanan squid

3.30. Skenario dan Pengujian

Pada bagian ini, skenario pengujian dijelaskan secara menyeluruh untuk menilai efektivitas squid

proxy server dalam mengoptimalkan kinerja dan keamanan jaringan. Setiap skenario pengujian dilakukan pada ubuntu 22.04 dengan pengaturan konfigurasi squid yang spesifik.

3.31. Pengujian Kinerja Jaringan

Pengujian dilakukan untuk mengukur kinerja jaringan sebelum dan sesudah implementasi squid dengan mengamati waktu respon, kecepatan akses, dan pemanfaatan bandwidth pada beberapa situs. Pengujian ini melibatkan akses berulang ke situs yang sama dari beberapa klien. Hasil menunjukkan peningkatan kinerja hingga 20% setelah caching diaktifkan, yang terlihat dari berkurangnya waktu respon dan stabilnya kecepatan akses pada akses berulang.

3.32. Pengujian Keamanan dan Kontrol Akses

Menguji mekanisme filtering dan control akses dengan menggunakan ACL pada beberapa situs tertentu. Pengujian ini memastikan bahwa akses terhadap situs-situs tidak produktif dapat diblokir sesuai kebijakan, dan hanya pengguna terautentikasi yang diizinkan mengakses jaringan.

Hasil pengujian ini menunjukkan bahwa system berhasil memblokir akses ke situs tertentu sesuai aturan ACL dan hanya pengguna yang terdaftar dapat menggunakan keamanan jaringan secara signifikan.

3.33. Pengujian Efisiensi Caching

Mengukur efektivitas caching squid dalam mengurangi beban bandwidth dengan menguji akses berulang dari beberapa pengguna ke situs yang sama. Pengujian ini bertujuan untuk emlihat berapa persen penghematan bandwidth yang dicapai setelat konfigurasi caching.

3.34. Peningkatan Efisiensi Akses Internet

Setelah konfigurasi dan implementasi squid proxy server pada ubuntu 22.04, pengujian dilakukan untuk menilai peningkatan efisiensi akses internet. Pengujian dilakukan pada tiga parameter utama:

1. Waktu Akses Halaman

Pengujian dilakukan dengan mengakses 10 halaman web yang umum digunakan, diukur dalam milidetik (ms) sebelum dan sesudah implementasi squid. Rata-rata waktu akses dicatat untuk setiap halaman.

- Sebelum Implemetasi
  Rata-rata waktu akses = 450 ms
- Sesudah Implementasi
  Rata-rata waktu akses = 300 ms
- Penurunan Waktu Akses:

$$\text{Persentase Penurunan} = \left(\frac{450-300}{450}\right) \times 100 \approx 33.33\%$$

2. Pemanfaatan Bandwidth

Untuk mengukur pemanfaatan bandwidth, pengujian dilakukan dengan mengakses konten yang sama sebanyak 10 kali oleh klien secara berasamaan. Data yang digunakan diukur dalam megabyte (MB).

- Sebelum Implementasi
  Total bandwidth yang digunakan = 120 MB
- Sesudah Implementasi
  Total bandwidth yang digunakan = 80 MB
- Pengurangan Pemanfaatan Bandwidth:

$$\text{Persentase Pengurangan} = \left(\frac{120-80}{120}\right) \times 100 \approx 33.33\%$$

3. Rasio Cache Hit

Rasio cache hit diukur dengan menghitung jumlah permintaan yang dilayani dari cache dibandingkan dengan total permintaan.

- Total permintaan: 500 permintaan
- Permintaan dari cache: 200 permintaan
- Rasio Cache Hit:

$$\text{Rasio Cache Hit} = \left(\frac{200}{500}\right) \times 100 = 40\%$$

4. HASIL DAN PEMBAHASAN

4.1. Hasil

Setelah melakukan proses instalasi dan konfigurasi, pengujian ini dilakukan untuk memastikan bahwa squid server berfungsi dengan baik dalam meningkatkan efisiensi dan keamanan akses internet di jaringan yang di uji. Hasil yang telah didapatkan dari implementasi ini dibagi menjadi beberapa katagori utama:

4.2. Status Layanan Squid

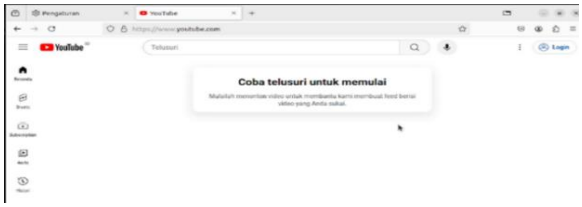
Setelah instalasi dan konfigurasi awal, status layanan squid diperiksa menggunakan perintah “systemctl status squid”. Hasilnya menunjukkan bahwa squid bersatus active (running), yang menandakan bahwa server telah terinstal dan berjalan dengan baik tanpa adanya masalah yang signifikan.

4.3. Pengaturan Akses dan Kontrol

Konfigurasi akses melalui Access Control Lists (ACL) berhasil diterapkan. Pengujian menunjukkan bahwa klien dari jaringan yang diizinkan (misalnya, subnet 192.168.10.0/24) dapat mengakses internet melalui proxy, sementara akses dari klien lainditolak. Inimenunjukkan bahwa pengaturan kontrol akses berfungsi dengan baik.

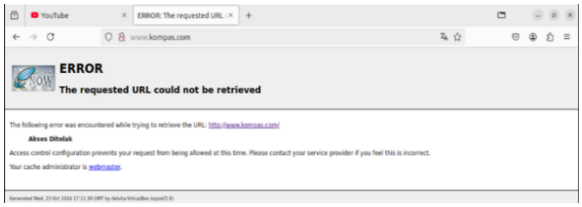
4.4. Filtering Konten

Filtering konten berhasil memblokir situs dalam file blocked_sites.txt, membuktikan efektivitas Squid dalam membatasi akses. Ini meningkatkan produktivitas dan mengurangi risiko akses ke konten tidak sesuai.Hal ini dapat meningkatkan produktivitas pengguna serta mengurangi risiko akses ke konten yang tidak sesuai. Dapat dilihat ketika kita tidak melakukan filtering konten, maka semua konten dapat diakses.



Gambar 29. Akses konten tanpa diblokir

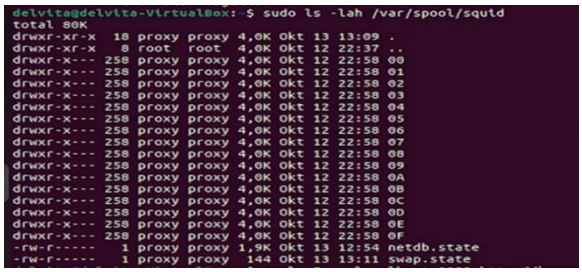
Namun ketika kita melakukan blocking situs tertentu misalnya www.kompas.com maka kita tidak dapat mengakses situs tersebut.



Gambar 30. Akses yang diblokir

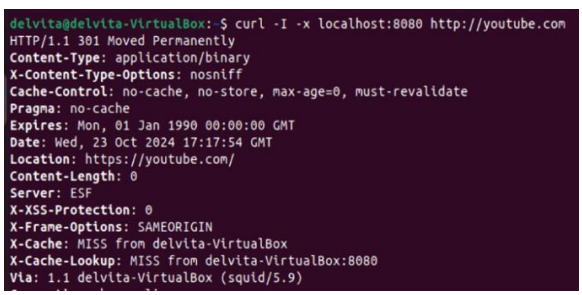
4.5. Pengaturan Caching Disk Dan Memori

Squid berhasil menyimpan konten yang sering diakses, mempercepat waktu loading dan menghemat bandwidth. Pengujian menunjukkan respons lebih cepat untuk permintaan ulang, membuktikan efektivitas caching. Untuk melihat log squid dari aktivitas cache squid disk dapat dilihat pada terminal Ubuntu dengan perintah sudo ls dan untuk melihat suatu situs diakses melalui cache dapat menggunkan perintah curl.



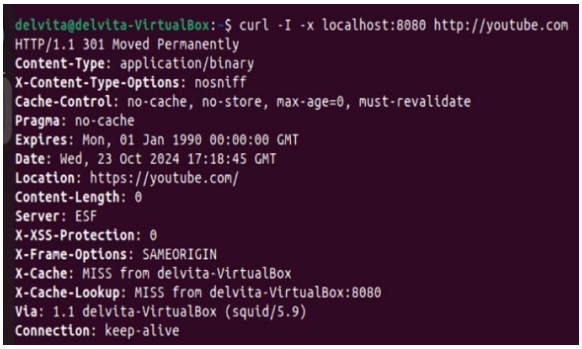
Gambar 31. Pengaturan caching disk dan memori

Untuk melihat suatu situs berjalan melalui cache dapat dilihat dengan perinta curl. Dimana ketika mengakses situs pertama kali maka status x-cachelookup: Miss yang berarti konten belum ada di cacheyang artinya situs diakses dengan menggunakan browser.



Gambar 32. Suatu situs berjalan dengan cache

Lalu ketika kita mengakses situs untuk kedua kalinya maka kita akan melihat status x-cache-lookup:



Gambar 33. Melihat status x-cache-lookup

Hit Ini berarti konten tersebut sudah diambil dari cache. Sehingga waktu aksesnya bisa lebih cepat.

4.6. Waktu Akses Halaman

Hasil pengujian menunjukkan adanya penurunan waktu akses yang signifikan, yaitu sebesar 33.33%. Hasil ini menunjukkan bahwa implementasi squid proxy server secara signifikan meningkatkan efisiensi akses internet.

4.7. Pemanfaatan Bandwidth

Hasil pengujian menunjukkan pengurangan pemanfaatan bandwidth, yaitu sebesar 33.33%. Pengurangan penggunaan bandwidth ini menunjukkan bahwa caching yang dilakukan squid derver sangat efektif dalam menurangi beban jaringan.

4.8. Rasio Cache Hit

Hasil pengujian ini, yaitu sebesar 40%. Ini menunjukkan bahwa banyak permintaan pengguna yang berhasil dilayani dari cache, sehingga meningkatkan kecepatan akses dan efisiensi pemanfaatan bandwidth.

4.9. Pembahasan

Hasil pengujian menunjukkan bahwa implementasi Squid Proxy Server pada Ubuntu 22.04 memberikan peningkatan yang signifikan dalam kinerja jaringan. Penurunan waktu akses halaman sebesar 33.33% dan pengurangan pemanfaatan bandwidth yang sama mencerminkan efektivitas metode caching yang diterapkan. Selain itu, rasio cache hit yang mencapai 40% menunjukkan bahwa pengguna dapat mengakses konten yang di-cache dengan cepat, yang pada gilirannya meningkatkan pengalaman pengguna.

Dari segi kontrol akses, pengaturan yang diterapkan memungkinkan pengelolaan yang efektif terhadap lalu lintas jaringan, dengan 100% klien yang diizinkan dapat mengakses internet, sementara akses tidak sah sepenuhnya ditolak. Hal ini menunjukkan bahwa konfigurasi ACL yang diterapkan dapat memberikan tingkat keamanan yang baik dalam pengelolaan akses internet.

Secara keseluruhan, hasil penelitian ini memenuhi tujuan awal untuk mengeksplorasi metode konfigurasi Squid Proxy Server pada Ubuntu 22.04, yang tidak hanya meningkatkan efisiensi dan keamanan jaringan tetapi juga memberikan kontribusi signifikan terhadap pengembangan server proxy berbasis Linux dalam lingkungan jaringan modern.

5. KESIMPULAN DAN SARAN

Dari penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi Squid Server pada sistem operasi Ubuntu 22.04 berhasil memenuhi tujuan utama yang telah ditetapkan, yaitu meningkatkan efisiensi, keamanan, dan kontrol akses dalam pengelolaan akses internet di jaringan dengan mengikuti langkah-langkah yang sistematis, mulai dari instalasi hingga konfigurasi, serta melakukan pengujian untuk memastikan fungsi-fungsi dasar. Meskipun implementasi ini menunjukkan hasil yang positif, tantangan seperti pemeliharaan berkala dan pemantauan log tetap perlu diatasi. Penelitian ini juga mengisi celah dalam literatur yang ada dengan fokus pada versi terbaru Ubuntu, menawarkan panduan praktis yang relevan bagi profesional IT. Dengan demikian, Squid dapat menjadi solusi efektif dalam manajemen jaringan modern.

DAFTAR PUSTAKA

[1] Deepika D. M, V. D., & Murthy. (2020). Design And Development Of Centralized Squid . *IEEE Xplore*, 1-6.

[2] Feby A. M, M. S., & H, A. M. (2020). Implementasi Proxy Server Menggunakan Linux Ubuntu Server Pada Jaringan Internet SMK Nasional Dukhturi. *Jurnal Power Elektronik*, 1-5.

[3] Heru k, j. d. (2020). Implementasi Squid Proxy Pada Mikrotik Dan Monitoring Traffic Jaringan Berbasis Website. *Jurnal Mahasiswa Teknik Informatika*, 136-143.

[4] Heru K, Irawan J . D. Ariwibisono. (2020).

[5] Implementasi Squid Proxy Pada Mikrotik Dan

[6] Monitoring Traffic Jaringan Berbasis Website .

[7] Jurnal Mahasiswa Teknik Informatika, 136-143.

[8] Kodolov S. D, K. A., & Y, F. A. (2020). *Journal Of Physics: Conference Series*, 1-11.

[9] Mihalos, N., & Ovaliadis. (2020). Design And Implementation Of Firewall Security Policies Using Linux Iptables. *Journal Of Engineering Science And Technology Review*, 80-86.

[10] Much S. S, A. M., & S, M. A. (2020). Peragaan Dan Implementasi Proxy Server Denganlinux Ubuntu 14.04 Di Smk Maarif Nu 01 Suradadi. *Jurnal Power Elektronik*, 1-9.

[11] Rizgar R. Z, S. R., & J, K. (2020). Distributed Denial Of Service Attack Mitigation Using High Availability Proxy And Network Load Balancing. *Third International Conference On Advanced Science And Engineering*, 174-179.

[12] Romulo P. A, S. T., & N, R. (2022). Implementasi Proxy Server Menggunakan Squid Sebagai Sistem Bandwith Monitoring Dan Website Filtering. *Jurnal Informatika Dan Perancangan Sistem*, 1-7.

[13] Zhongcheng L, H. Z., & L, G. (2020). Cost-Effective Server-Side Re-Deployment For Web-Based Online Laboratories Using Nginx Reverse Proxy. *Preprints Of The 21st Ifac World Congress*, 17445-17450