EFEKTIVITAS *CLOUDFLARE GATEWAY* DALAM MEMBATASI AKSES PORNOGRAFI SERTA PENGARUHNYA PADA KETERSEDIAAN *BANDWIDTH*

Ismail Puji Saputra
Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro, ismailpujisaputra@gmail.com

ABSTRAK

Internet merupakan kebutuhan utama dalam sebuah organisasi. Namun, kebutuhan akan internet tidak selalu sebanding dengan bandwidth yang tersedia. Bandwidth yang terbatas harus diawasi untuk mencegah penyalahgunaan, seperti akses ke konten pornografi. Penelitian ini bertujuan untuk mengevaluasi efektivitas Cloudflare Gateway dalam memblokir situs pornografi dan dampaknya terhadap penggunaan bandwidth. Metode penelitian dilakukan dengan mengimplementasikan DNS Cloudflare Gateway ke dalam router Mikrotik, menguji pemblokiran terhadap 10 situs pornografi terpopuler, dan menghitung perbedaan penggunaan bandwidth sebelum dan sesudah implementasi. Hasil penelitian menunjukkan bahwa Cloudflare Gateway berhasil memblokir 100% situs yang diuji dan menurunkan penggunaan bandwidth sekitar 1,197%. Penelitian ini juga menemukan bahwa penggunaan internet pada objek yang diuji cukup sehat (tidak menyalahgunakan internet untuk pornografi). Sebaliknya, jika penurunan bandwidth sangat signifikan, hal ini mungkin mengindikasikan tingkat penyalahgunaan internet untuk pornografi yang tinggi pada objek yang diuji.

Keyword: Cloudflare Gateway, Cyber Security, Firewall, Pornografi

1 PENDAHULUAN

Internet merupakan kebutuhan yang sangat mendasar bagi sebuah organisasi [1,2]. Sebagian besar organisasi telah memanfaatkan internet untuk menunjang pekerjaan seperti mengirim email, bertukar data, pemasaran, komunikasi dan sebagainya [3,4]. Penggunaan internet yang tidak semestinya (*misuse*) akan menimbulkan efek domino bagi sebuah organisasi, misalnya internet yang memiliki *bandwidth* terbatas digunakan sebagian kecil untuk bekerja dan sebagian besar sisanya disalahgunakan untuk menonton konten video, hal ini dapat menimbulkan kerugian bagi organisasi yaitu dapat menghambat pekerjaan yang disebabkan oleh penyalahgunaan *bandwidth*.

Penyalahgunaan *bandwidth* dapat mengganggu ketersediaan data *(availability), availability* merupakan salah satu penyusun dari *CIA TRIAD (Confidentiality, integrity and Availability)* yang menjadi tujuan utama dari keamanan komputer yaitu kerahasiaan, integritas dan ketersediaan sumberdaya [5,6,7]. Degan ketersediaan *bandwidth* yang terbatas, diperlukan mekanisme dalam mencegah penyalahgunaan sehingga *bandwidth* dapat digunakan secara maksimal untuk kepentingan pekerjaan [8,9,10].

Mekanisme pengamanan jaringan dalam meningkatkan efisiensi *bandwidth* telah dilakukan dengan berbagai cara, salah satunya adalah menggunakan *UTM (unified threat management), UTM* melakukan efisiensi *bandwidth* sekitar 4,66%, efisiensi *bandwidth* didapatkan melalui proses *filtering* konten dan *caching* konten [11]. Penggunaan *software firewall* pfSense juga dilakukan untuk memblokir konten negatif yang dapat mengurangi kepadatan trafik dan menghemat *bandwidth* [12].

Penelitian ini akan berfokus pada mekanisme pemblokiran akses konten pornografi, pornografi adalah konten dengan aduan paling tinggi yang dicatat oleh Kementrian Komunikasi dan Informatika dengan total 1.142.010 aduan[13], proses pemblokiran konten pornografi akan memanfaatkan layanan *Cloudflare Gateway*. Penelitian ini akan menemukan efektifitas *Cloudflare gateway* dalam memblokir konten pornografi serta melihat pengaruhnya pada kepadatan trafik (penggunaan *bandwidth*) pada jaringan.

2 LITERATUR REVIEW

2.1 *Cloudflare Gateway*

Cloudflare merupakan sebuah perusahaan yang bergerak pada jasa keamanan berbasis *cloud* [14], salah satu produk yang ditawarkan *cloudflare* yaitu *cloudflare gateway* yang dapat dimanfaatkan dengan menggunakan *DNS (domain name server)*. Dengan memasangkan *DNS* dari layanan *cloudflare gateway* pada perangkat router, dapat memfilter konten tanpa harus melakukan konfigurasi yang sulit, penerapan *cloudflare gateway* sudah pernah dilakukan dan berhasil untuk memfilter *malware cryptojacking* (*malware* yang digunakan untuk menambang *crypto*) [15].

2.2 Pornografi

Menurut undang-undang nomor 44 tahun 2008 tentang pornografi, dijelaskan bahwa pornografi merupakan sketsa, ilustrasi, foto, tulisan, suara, bunyi, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lain melalui berbagai bentuk media komunikasi dan atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitas seksual yang melanggar norma kesusilaan [16]. Akses pornografi banyak dilakukan melalui media internet, menurut data Kementrian Komunikasi dan Informatika pornografi merupakan konten dengan aduan tertinggi [13]. Pornografi dapat menyebabkan kecanduan, selain itu kecanduan pornografi dapat mengakibatkan kerusakan otak yang fatal, memicu kejahatan dan keburukan lainya [17].

2.3 Ketersediaan *Bandwidth*

Bandwidth merupakan lebar data yang dapat diproses pada media tansmisi suatu jaringan internet [18]. Umumnya jumlah *bandwidth* akan mempengaruhi biaya yang harus dikeluarkan kepada penyedia jasa, sehingga semakin tinggi *bandwith* yang

dimiliki, maka biaya yang harus dikeluarkan akan semakin besar, maka diperlukan manajemen *bandwidth* untuk memaksimalkan fungsionalitas *bandwith* guna mencapai tujuan suatu organisasi.

3 METODOLOGI

metode penelitian ini merupakan tahapan yang akan dilakukan untuk mencapai tujuan penelitian yaitu efektifitas *Cloudflare gateway* dalam memblokir konten pornografi dan melihat pengaruhnya terhadap trafik pada jaringan. Berikut ini gambar 1 yaitu tahap penelitian:

Gambar 1 Tahap Penelitian

Setiap tahap pada gambar 1 dapat dijelaskan sebagai berikut:

3.1 Persiapan

Tahap persiapan adalah tahap menyiapkan *hardware* dan *software* serta melakukan implementasi *DNS cloudflare gateway* pada router. Berikut ini tabel 1 yaitu daftar *hardware* dan *software* yang diperlukan dalam penelitian ini.

Tabel 1 daftar *hardware* dan *software*

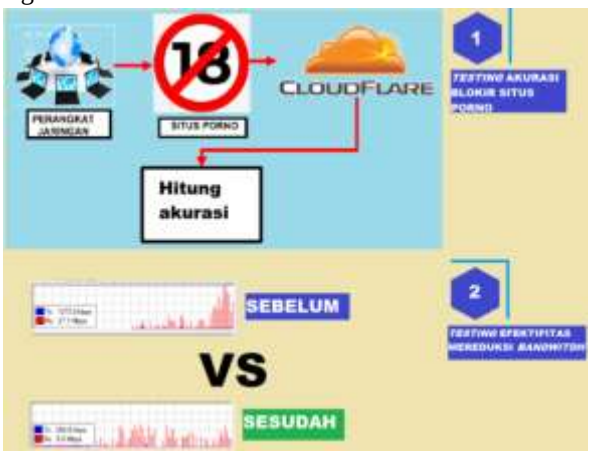
No	*Hardware*	Fungsi
1	*Mikrotik Routerboard*	Perangkat keras yang digunakan untuk mengatur jaringan dan menjadi tempat implementasi *DNS cloudflare gateway*

No	*Software*	Fungsi
2	*Mikrotik RouterOS*	Sistem operasi pada *Mikrotik Routerboard*
3	*Cloudflare Gateway*	Layanan *Software as service* yang disediakan oleh *cloudflare* guna memblokir akses konten tertentu, dalam hal ini pornografi

Setelah daftar *hardware* dan *software* pada tabel 1 telah dipersiapkan, maka selanjutnya *hardware* dan *software* tersebut dikonfigurasi guna dilakukan proses *testing*.

3.2 *Testing*

Proses *testing* dilakukan untuk melihat apakah *cloudflare gateway* mampu mendeteksi aktifitas pornografi dan memblokir aktifitas tersebut, dengan melakukan pengujian mengakses beberapa alamat situs porno dan melihat respon yang ditampilkan oleh situs. Selanjutnya proses *testing* juga akan melihat trafik pada jaringan, apakah *filtering* yang dilakukan *cloudflare gateway* mampu menekan trafik *(bandwidth)* pada jaringan. Berikut ini merupakan gambar 2 yaitu gambar alur testing:



Gambar 2 Alur *Testing*

Pada gambar 2 ditunjukan *testing* dilakukan untuk mengukur akurasi *cloudflare gateway* dalam mendeteksi serangan, proses pengukuran akurasi menggunakan formula 1 [19] dibawah ini:

$$\text{Akurasi} = (\text{jumlah keberhasilan deteksi} / \text{jumlah total pengujian}) * 100 \quad (1)$$

Setelah menemukan akurasi dari *cloudflare gateway* dalam memblokir akses situs pornografi, selanjutnya adalah melihat hubungan antara aktifitas pemblokiran tersebut terhadap trafik, apakah trafik menurun ketika jaringan menerapkan *filtering* menggunakan *cloudflare gateway.* Untuk mengukur persentase perbedaan antara sebelum dan sesudah penerapan *cloudflare gateway* dapat menggunakan formula 2 dibawah ini:

$$\text{Persentase Perbedaan} = ((\textit{Bandwith}\ \text{Sebelum} - \textit{Bandwith}\ \text{Sesudah}) / \text{bandwith sebelum}) * 100 \quad (2)$$

Dengan menggunakan formula 2 diatas maka akan didapatkan nilai kuantitatif, seberapa efektif *cloudflare gateway* dalam mengurangi penggunaan trafik (*bandwidth*) pada jaringan. Penelitian ini dibatasi untuk tidak melihat karakteristik pengguna, sehingga kemungkinan saja efektifitas tersebut dipengaruhi juga oleh karakteristik pengguna pada suatu lokasi tertentu.

3.3 Analisis

proses analisis akan melihat hasil dari *testing*, menghitung akurasi dan efektifitas *cloudflare gateway* dalam menurunkan penggunaan *bandwidth*, serta menyajikanya dalam bentuk grafik.

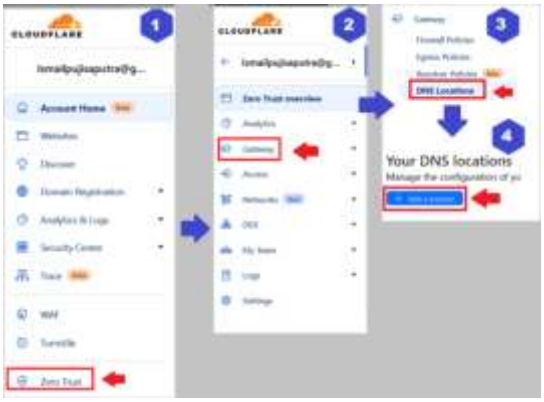
3.4 Hasil

Proses ini akan menyimpulkan hasil dari analisis yang telah dilakukan terhadap *testing*, hasil sendiri akan terdiri dari 2 bagian yaitu berapa akurasi *cloudflare gateway* dalam memblokir situs porno serta berapa nilai penurunan penggunaan bandwith pada jaringan internet.

4 HASIL DAN PEMBAHASAN

4.1 Konfigurasi *Cloudflare Gateway*

Anda harus mendaftar ke *cloudflare*, selanjutnya *login* menggunakan akun *cloudflare* anda, setelah login anda akan diarahkan ke halaman *dashboard*, selanjutnya anda akan melihat beberapa menu, seperti pada gambar 3 dibawah ini:



Gambar 3 Halaman *dashboard cloudflare zero trust*

Untuk menambahkan *DNS* yang akan kita gunakan pada *router* yaitu langkah pertama adalah klik menu *zero trust* seperti yang ditunjukan di angka 1 pada gambar 3. Setelah masuk ke menu *zero trust*, klik menu *gateway* seperti yang ditunjukan angka 2 pada gambar 3, selanjutnya klik menu *DNS Locations* seperti yang ditunjukan pada angka 3 gambar 3, selanjutnya tekan tombol *Add a Location* seperti yang ditunjukan pada angka 4 gambar 3. Setelah itu anda akan diarahkan ke halaman tambah *DNS Location* seperti pada gambar 4 dibawah ini:

Gambar 4 Halaman Add *DNS endpoints*

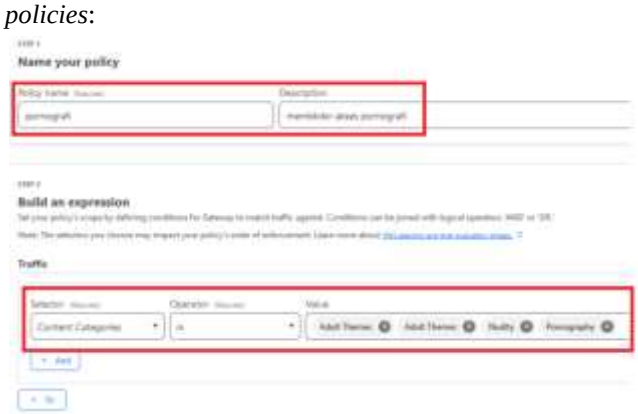
Pada gambar 4 terdapat beberapa *form* yang anda isi, untuk *location name* bisa anda isi dengan nama yang ingin anda gunakan. Aktifkan tombol *IPv4* jika anda ingin menggunakan *DNS* yang memiliki *type IPv4*, terdapat isian form *select IPv4 DNS endpoints* yang memiliki alamat *IP* 172.64.36.1 / 172.64.36.2 yang merupakan *DNS* yang diberikan *cloudflare* untuk dipasangkan pada *router* yang ada pada jaringan internet.

Selanjutnya adalah optional, jika anda ingin mengaktifkan *DNS* IPv6, *DNS over TLS (DoT) DNS over HTTPS (DoH)* dan sebagainya, anda dapat mengikuti gambar 4 sebagai contoh dalam menambahkan *DNS Locations.* Untuk melanjutkan langkah konfigurasi tersebut klik tombol *continue*, maka anda akan diarahkan ke halaman *protect endpoint* seperti pada gambar 5 dibawah ini:

Gambar 5 Halaman *protect endpoints*

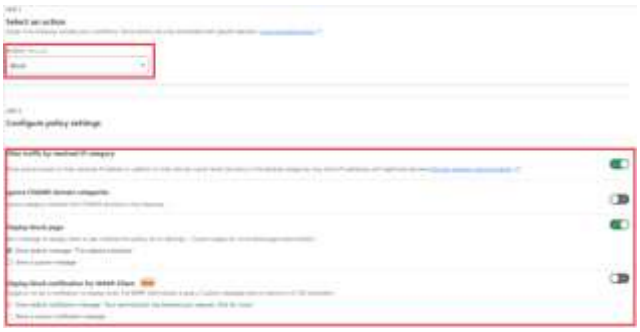
Pada gambar 5, terdapat tulisan "*To modify your Source IPv4 address, upgrade to an Enterprise plan*" yang artinya adalah jika anda ingin memodifikasi *IPv4* alamat *IP* anda maka anda disarankan untuk memilih paket *enterprise* (berbayar), karena pada kasus ini adalah tidak berbayar, maka *IPv4* yang tertera pada *form* tersebut tidak dapat diubah, alamat *IP* tersebut merupakan alamat *IP public* yang digunakan sebagai *gateway* jaringan internet yang kita gunakan, maka sebaiknya menggunakan *IP Public static* yang tidak berubah-ubah. Selanjutnya adalah menekan tombol *continue* dan melihat detail konfigurasi dan mengkonfirmasi apabila konfigurasi telah sesuai dan terakhir tekan tombol *Done*.

Setelah *DNS Location* telah ditambahkan, selanjutnya adalah membuat *firewall policies*, berikut ini gambar 6 yaitu langkah 1 dan 2 dalam membuat *firewall policies*:



Gambar 6 *Step* 1 dan 2 membuat *firewall policies*

Pada langkah 1 terdapat isian *form* nama dan deskripsi *policy*, selanjutnya pada langkah 2 pilih *selector* dengan *content categories*, *operator* dengan isian in dan *value adult themes, nudity* dan *pornography*. Selanjutnya terdapat langkah 3 dan 4 yang ditunjukan dengan gambar 7 dibawah ini:



Gambar 7 Konfigurasi *DNS* pada *router* Mikrotik

Pada langkah 3 terdapat isian *form action* isi dengan *Block*, hal ini berarti konten yang masuk kategori *adult themes* akan di blokir, selanjutnya step 4 aktifkan *filter traffic by resolved IP category* yang artinya pemblokiran tidak hanya pada *domain* saja, melainkan juga *IP Address* nya. Pada langkah 4 juga terdapat *display block page* sehingga apabila situs diblokir, pengguna akan diarahkan pada halaman *block cloudflare gateway*. Untuk menyimpan konfigurasi klik tombol *create policy*.

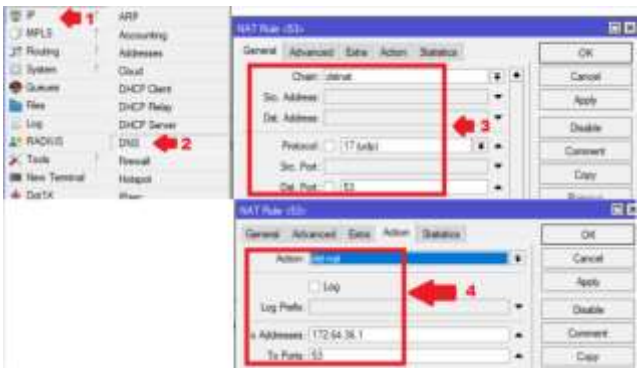
4.2 Konfigurasi Router Mikrotik

Setelah *firewall policies* berhasil ditambahkan, selanjutnya adalah mengkonfigurasi *DNS* yang telah dibuat sebelumnya, *DNS* yang diberikan *cloudflare* yaitu 172.64.36.1 / 172.64.36.2, dipasangkan pada *router Mikrotik*, berikut ini gambar 8 yang menunjukan langkah konfiguras *DNS* pada *router* Mikrotik.

Gambar 8 Konfigurasi *DNS* pada *router* Mikrotik

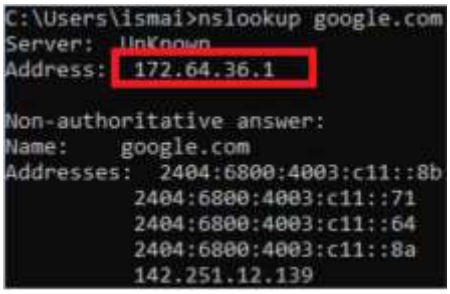
Pada *router* Mikrotik klik menu *IP* pilih *DN*S dan isikan *servers DNS* dengan *DNS* yang didapatkan dari proses pada gambar 4, selanjutnya klik OK untuk menyimpan konfigurasi.

Setelah *DNS* cloudflare terpasang pada router Mikrotik, selanjutnya adalah memaksa pengguna yang ada pada jaringan untuk menggunakan *DNS* tersebut dengan menambahkan *NAT (network address translation)* pada *router* Mikrotik, berikut ini merupakan langkah menambahkan *NAT* untuk memaksa pengguna menggunakan *DNS cloudflare*.



Gambar 9 Konfigurasi *NAT* pada *router* Mikrotik

Dengan konfigurasi *NAT* pada gambar 9 diatas, maka pengguna akan selalu menggunakan *DNS cloudflare*, karena *port UDP* 53 yaitu *port default DNS* selalu diarahkan ke alamat *DNS cloudflare*. Berikut ini gambar 10 yaitu hasil *nslookup* pada komputer *windows* yang digunakan untuk mengkonfirmasi *DNS cloudflare* telah terpasang pada jaringan:



Gambar 10 Hasil *nslookup* pada komputer *windows*

4.3 Testing Akurasi *Cloudflare Gateway* pada situs pornografi

Beberapa situs pornografi akan coba diakses menggunakan *browser*. Berikut ini tabel 2 yaitu tabel hasil *testing* blokir situs pornografi.

Tabel 2 testing akurasi

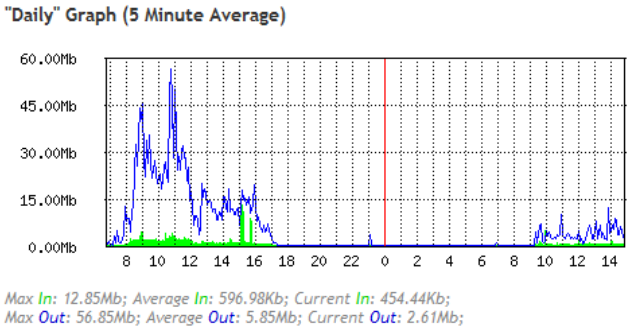
No	Situs Pornografi	Hasil
1	Xvideos	Berhasil diblokir
2	Pornhub	Berhasil diblokir
3	Xhamster	Berhasil diblokir
4	Xnxx	Berhasil diblokir
5	Xhamsterdesi	Berhasil diblokir
6	Stripchat	Berhasil diblokir
7	Chaturbate	Berhasil diblokir
8	Spankbang	Berhasil diblokir
9	Eporner	Berhasil diblokir
10	redtube	Berhasil diblokir

Hasil testing akurasi pada tabel 2 yaitu ke 10 situs pornografi yang paling sering dikunjungi di dunia versi similarweb [20] namun untuk pemsrv *down* pada saat pengujian maka diganti dengan redtube. Tabel 2 menunjukan hasil yang sangat baik *cloudflare gateway* dapat memblokir 10 situs pornografi tersebut. Hal ini juga dapat dibuktikan dari *dashboard cloudflare gateway* pada menu *analytics* yang menunjukan daftar list situs-situs yang terblokir oleh *DNS Cloudflare*. Berikut ini gambar 11 yaitu daftar domain yang terblokir:

Gambar 11 Domain yang terblokir *DNS cloudflare gateway*

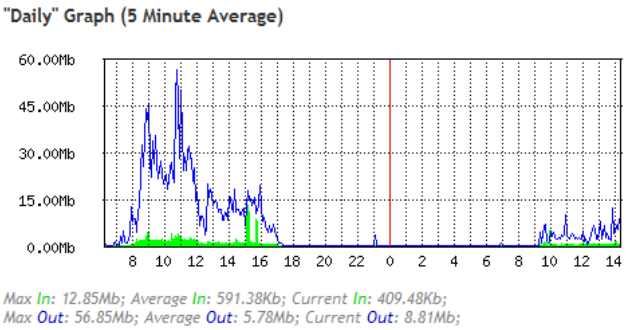
4.4 Testing penggunaan *bandwidth* sebelum dan sesudah penggunaan *Cloudflare Gateway*

Proses *testing* dilakukan menggunakan *tool graphs* pada *router Mikrotik*, *graphs* di konfigurasi untuk melakukan perhitungan statistik setiap 5 menit, berikut ini merupakan statistik penggunaan *bandwidth* sebelum penggunaan *DNS cloudflare gateway*:



Gambar 12 statistik penggunaan *bandwidth* sebelum implementasi

Gambar 12 menunjukan *Average Out* (rata-rata *bandwidth* yang digunakan untuk mengakses internet) dengan jumlah 10,64 Mb. Selanjutnya adalah gambar 12 yaitu setelah penggunaan *DNS cloudflare gateway:*



Gambar 13 statistik penggunaan *bandwidth* setelah implementasi

Gambar 13 menunjukan *average out* setelah implementasi menurun menjadi 5.78Mb lebih kecil dari sebelum implementasi.

4.5 Analisis Testing

Proses *testing* akurasi memberikan hasil sebagai berikut:

Akurasi = (10/10)*100 = 100%

Hasil perhitungan akurasi menunjukan *DNS Cloudflare gateway* berhasil 100% dalam memblokir 10 situs pornografi terpopuler versi similarweb.

Selanjutnya proses menghitung persentase perbedaan penggunaan *bandwidth* sebelum dan sesudah *penggunaan DNS cloudflare gateway* adalah sebagai berikut:

Persentase Perbedaan = ((*5.85 – 5.78*) / 5.85) * 100 = 1,197%

Persentase perbedaan antara sebelum dan sesudah menggunakan *DNS Cloudflare gateway* tidak terlalu signifikan, hal ini dapat dipengaruhi beberapa faktor yang tidak menjadi fokus pada penelitian ini, namun dengan adanya *DNS cloudflare gateway* trafik internet menurun. Hal ini juga dapat menjadi indikator bahwa objek penelitian (pengguna internet) tidak signifikan dalam mengakses situs pornografi.

4.6 Hasil

Hasil testing akurasi menunjukan bahwa *cloudflare gateway* mampu memblokir 100% situs porno yang diujikan, namun hasil ini tidak serta merta menunjukan akurasi yang sangat sempurna dari *cloudflare gateway* karena terdapat situs porno yang tidak hanya menggunakan domain saja namun juga menggunakan alamat IP dan tentunya masih dapat dikunjungi meskipun menggunakan *cloudflare gateway*.

Hasil *testing* persentase perbedaan menunjukan bahwa trafik menurun sekitar 1,197% setelah implementasi *cloudflare gateway*, hasil ini juga menjadi indikator bahwa pengguna internet cukup sehat dalam memanfaatkan fasilitas internet, sehingga metode pengukuran ini dapat dijadikan tolak ukur dalam melihat kesehatan pengguna dalam menggunakan internet pada suatu instansi, semakin besar hasil persentase maka semakin tidak sehat pengguna internetnya.

5 KESIMPULAN

Cloudflare gateway mampu memblokir 100% situs pornografi yang diuji dalam tabel 2, perlu dicatat bahwa tidak semua situs porno mampu diblokir dengan metode ini, karena nyatanya banyak situs porno yang menggunakan alamat *IP address* yang masih dapat dibuka meskipun menggunakan *DNS cloudflare gateway*.

Penurunan *bandwidth* hanya sekitar 1,197% setelah mengimplementasikan *cloudflare gateway* dan tidak menurunkan trafik internet secara signifikan, hasil ini mengindikasikan bahwa penggunaan internet pada objek yang diuji cukup sehat (tidak menyalahgunakan internet untuk pornografi), apabila penurunan *bandwidth* sangat signifikan kemungkinan penyalahgunaan internet untuk pornografi pada objek yang diuji sangat tinggi.

Secara keseluruhan *cloudflare gateway* cukup efektif dalam memblokir akses ke situs pornografi yang populer, serta menurunkan penggunaan *bandwidth* sebesar 1,197%, diharapkan penelitian selanjutnya dapat menggunakan metode ini untuk menguji penyalahgunaan internet pada bidang lain selain pornografi (*malware, game*, perjudian dan lainya).

REFERENSI

Arief Budi Pratomo. (2023). PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS. Bulletin of Network Engineer and Informatics/Bulletin of Network Engineer and Informatics, 1(2), 51–51. https://doi.org/10.59688/bufnets.v1i2.10.

Ali Akbar Rismayadi. (2023). IMPLEMENTASI HIERRARCHICAL TOKEN BUCKET (HTB) DENGAN METODE DYNAMIC QUEQUE UNTUK EFEKTIFITAS PENGGUNAAN BANDWITH. Jurnal Responsif : Riset Sains Dan Informatika, 5(2), 205–305. https://doi.org/10.51977/jti.v5i2.1275

Karina, M., Fery Hernaningsih, & Rinto Rivanto. (2022). STRATEGI PEMASARAN DENGAN PEMANFAATAN FENOMENA VIRAL DAN KOMUNIKASI ELECTRONIC WORD OF MOUTH MELALUI SOSIAL MEDIA DI INDONESIA. Jurnal Ilmiah Manajemen, Ekonomi, Dan Akuntansi, 6(3), 924–942. https://doi.org/10.31955/mea.v6i3.2506

Komalasari, R. (2020). MANFAAT TEKNOLOGI INFORMASI DAN KOMUNIKASI DI MASA PANDEMI COVID 19. TEMATIK, 7(1), 38–50. https://doi.org/10.38204/tematik.v7i1.369

Arogundade, O. R. (2023). Network security concepts,

dangers, and defense best practical. Computer Engineering and Intelligent Systems, 14(2). https://doi.org/10.7176/ceis/14-2-03

Arnav Aditya, Deepti Vidyarthi, & Nene, M. J. (2024). A Study of Common Vulnerabilities in IoT Devices. https://doi.org/10.1109/icrito61523.2024.10522155

Noluntu Mpekoa. (2024). An Analysis of Cybersecurity Architectures. Proceedings of the ... International Conference on Information Warfare and Security/˜ the œProceedings of the ... International Conference on Information Warfare and Security, 19(1), 200–207. https://doi.org/10.34190/iccws.19.1.2115

IBRAS INDARO, M. U. H. A. M. M. A. D. (2021). IMPLEMENTASI MANAJEMEN BANDWIDTH INTERNET MENGGUNAKANROUTER MIKROTIK PADA KANTOR POS METRO (Doctoral dissertation, https://ummetro. ac. id/).

Doni, A., Amalia, L., & Putri, V. Y. (2023). Optimalisasi Bandwidth Menggunakan Metode Queue Tree Dan Web Filtering Berbasis Router Mikrotik Pada SMK Assa'adah. BINER: Jurnal Ilmu Komputer, Teknik dan Multimedia, 1(2), 187-207.

Hadinagoro, A. R. G., & Handa, I. B. (2023). Manajemen Jaringan Internet Klinik Dr. Sri Ningsih Menggunakan Mikrotik (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

Hidayat, M. R., Saragih, R., Basuki, S., Charisma, A., & Setiawan, A. D. (2024). IMPLEMENTASI THREAT MITIGATION DAN TRAFFIC POLICY MENGGUNAKAN UTM PADA JARINGAN TCP/IP. Jurnal Teknologi Informasi dan Ilmu Komputer, 11(2), 437-446.

Athallah, A. A., & Prihanto, A. (2024). Simulasi Keamanan Jaringan Komputer Penerapan Internet Positif. Journal of Informatics and Computer Science (JINACS), 199-209.

(2024). Kominfo.go.id. https://www.kominfo.go.id/statistik

About us. (n.d.). Cloudflare. Retrieved 2024, from https://www.cloudflare.com/about-overview/

Adhar, S., & Saprudin, U. (2023). Implementasi Cloudflare Zero Trust Dalam Mendeteksi Aktivitas Cryptojcking Pada Jaringan Komputer. JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi), 6(1), 23-28.

Hukum, K. (2008). Undang-Undang Republik Indonesia nomor 44 Tahun 2008 tentang Pornografi. Jakarta: Kementrian Hukum dan Hak Asasi Manusia Republik Indonesia, 1-13.

Prawitasari, I. (2022). FAKTOR-FAKTOR NARKOLEMA (KECANDUAN PORNOGRAFI) DAN IMPLIKASINYA PADA REMAJA. Jurnal Guru Indonesia, 2(1), 1-10.

Darmadi, E. A. (2019). Manajemen Bandwidth Internet Menggunakan Mikrotik Router Di Politeknik Tri Mitra Karya Mandiri. IKRA-ITH Teknologi Jurnal Sains dan Teknologi, 3(3), 7-13.

Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.

Suryakusumah, I. (n.d.). 10 situs Dewasa Paling Sering Dikunjungi di Dunia. inilah.com. https://www.inilah.com/10-situs-dewasa-paling-sering-dikunjungi-di-dunia