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

Pardan Jamaludin[1], Irfan Dwiguna Sumitra[2]

[1,2] Program Studi Teknik Informatika – Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
E-mail : pardan14263@email.unikom.ac.id[1], irfan_dwiguna@email.unikom.ac.id[2]

ABSTRAK

Para siswa di sekolah membutuhkan teknologi untuk membantu mereka dalam melakukan kegiatan belajar ketika berada di sekolah. Diluar itu, akan ada segelintir siswa yang menggunakan internet untuk hal yang tidak-tidak seperti contohnya membuka situs negatif. Meskipun pemerintah dan ISP di Indonesia sudah menerapkan keamanan untuk menyaring situs negatif tersebut, tetapi masih ada celah dari keamanan tersebut untuk dengan mudahnya dilewati *(Bypass)*. Oleh karena itu penulis membuat sebuah jaringan tentang keamanan untuk mengoptimalkan penyaringan *website* yang sudah ditetapkan oleh pemerintah dan ISP di Indonesia untuk membangun sistem internet yang sehat. Pengoptimalan keamanan ini menggunakan *Transparent* DNS dan *Firewall Layer 7 Protocol* Mikrotik. *Transparent* DNS adalah sebuah metode keamanan dimana setiap paket data yang melewati router akan dikirim ke DNS ISP terlebih dahulu. Dengan begitu, walaupun *client* menganti DNS miliknya, paket data yang lewat akan dikirim ke DNS milik ISP terlebih dahulu. Sedangkan *Layer 7 protocol* adalah pencarian pola beberapa pola paket data yaitu ICMP, TCP, dan UDP. Tujuan digunakannya *Transparent* DNS adalah untuk mencegah siswa menggunakan DNS Eksternal diluar DNS *default* milik ISP sehingga situs negatifpun bisa terbuka atau dengan kata lain menjadi tidak terblokir. Sedangkan tujuan digunakannya *firewall layer 7 protocol* Mikrotik adalah untuk mencegah penggunakan *Proxy* dan VPN yang juga digunakan untuk mengakses situs berkonten negatif.

Kata Kunci : Keamanan Jaringan, *Transparent DNS, Layer 7 Protocol*, Mikrotik

1. PENDAHULUAN

Internet Service Provider (ISP) atau penyedia layanan internet di Indonesia, harus melakukan pemblokiran terhadap situs-situs yang mengandung unsur negatif. Hal ini sesuai dengan Peraturan Menteri KOMINFO Republik Indonesia Nomor 19 Tahun 2014 Pasal 8 Ayat (1). Dengan adanya peraturan ini, diharapkan dapat menjauhkan masyarakat dari dampak negatif internet.

Dari hasil wawancara penelitian yang penulis lakukan di SMA Negeri 27 Bandung, disana sudah melakukan pemblokiran pada situs - situs yang terdapat pada *TRUST+Positif* melalui keamanan dari ISP yang mereka gunakan yaitu Indihome. Akan tetapi, disana tidak melakukan keamanan tambahan yang menyebabkan masih ada celah untuk melewati keamanan internet positif yang diberlakukan oleh ISP. Oleh karena itu, penulis memiliki ide untuk melakukan keamanan jaringan tambahan untuk mengoptimalisasikan pemblokiran terhadap situs berkonten negatif.

Dalam mencegah hal diatas dibuatlah sebuah mekanisme dalam upaya menjaga keamanan jaringan atau biasa disebut dengan *Firewall*. *Firewall* adalah sistem yang mengizinkan lalu lintas jaringan yang tidak aman. Biasanya, *firewall* diimplementasikan dalam sebuah gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. *Firewall* juga biasanya digunakan untuk mengontrol akses terhadap siapa saja yang mempunyai akses terhadap jaringan dari pihak luar.

Keamanan yang akan penulis terapkan disana yaitu dari sisi DNS, *Proxy*, dan juga VPN. Keamanan dari sisi DNS menggunakan *Transparent* DNS yang dimana setiap paket data yang melewati *router* akan dikirim ke DNS ISP terlebih dahulu. Dengan begitu, walaupun *client* menganti DNS miliknya, paket data yang lewat akan dikirim ke DNS milik ISP terlebih dahulu. Ibaratnya seperti kita memaksa *client* untuk masuk ke DNS milik ISP.

Selain dari DNS, celah lain untuk melakukan *bypass* internet positif adalah dengan menggunakan *Proxy* dan juga VPN. Oleh karena itu, penulis juga akan mencoba menerapkan pemblokiran penggunaan *Proxy* serta VPN dengan menggunakan *firewall L7 Protocol* dari Mikrotik untuk mencegah *client* mengakses konten internet negatif.

Sesuai kesepakatan dengan kepala sekolah serta *staff* IT disana, mereka ingin bisa melihat akses apa saja yang dilakukan oleh siswa yang menggunakan internet di SMA Negeri 27 Bandung. Sehingga, jika masih ada yang terlihat menggunakan internet untuk hal yang tidak wajar, bisa ditindaklanjuti dengan hukuman seperti pemberhentian akses internet

selama waktu yang ditentukan atau bisa ditegur oleh pihak yang terkait.

Berdasarkan latar belakang masalah diatas maka penulis bermaksud mengambil topik tugas akhir ini dengan judul "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"

Maksud dari penelitian ini adalah meningkatkan keamanan jaringan dari sisi client agar lebih optimal. Sedangkan tujuan dari dilakukannya penelitian ini adalah sebagai berikut :

a. Menerapkan *Transparent* DNS agar *client* tetap menggunakan DNS milik ISP meskipun mengganti pengaturannya
b. Memblokir situs-situs penyedia layanan *Proxy* dan VPN *Service* menggunakan *L7 Protocol* Mikrotik
c. Menerapkan pemutusan akses internet kepada *client* selama 1 menit jika masih mencoba menggunakan internet untuk membuka situs negatif

2. ISI PENELITIAN

2.1 Tinjauan Pustaka

Berikut adalah teori yang dijadikan refrenensi pada penelitian ini.

2.1.1 Jaringan Komputer

Jaringan komputer adalah dua ataupun lebih system yang terpisah, melalui media komunikasi untuk melakukan komunikasi data dari satu sumber dengan sumber yang lain untuk saling berbagi sumber daya.

Sedangkan jaringan komputer menurut Harry Prihanto adalah sekumpulan komputer yang berjumlah lebih dari satu atau banyak yang terpisah, tetapi saling berhubungan dalam mengerjakan tugasnya atau saling terkoneksi satu sama lain. [1]

Berdasarkan Pengertian tersebut dapat di simpulkan bahwa jaringan komputer adalah sistem yang terpisah untuk melakukan komunikasi agar dapat bertukar informasi.

2.1.2 Firewall

Firewall adalah perangkat yang bertugas untuk memeriksa paket data yang dapat masuk ataupun keluar dari sebuah jaringan. Dengan kata lain, *firewall* berperan dalam melindungi jaringan dari serangan yang berasal dari bukan jaringan local atau jaringan luar (*outside network*). [2]

Firewall mengimplementasikan packet filtering dan juga fungsi keamanan yang digunakan untuk mengelola aliran data dari, ke, dan melalui *router*. Contohnya, *firewall* digunakan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang datang dari Internet. Selain untuk melindungi jaringan, *firewall* juga digunakan untuk melindungi komputer pengguna atau *host (host firewall).* [2]

2.1.3 DNS (Domain Name System)

Setiap *network interface* yang terhubung pada TCP/IP *network* diidentifikasi melalui alamat IP. Suatu nama (*hotsname*) juga dapat diberikan pada setiap perangkat yang memiliki alamat IP seperti: *server*, *router*, *terminal*, dan sebagainya. Perangkat lunak jaringan tidak memerlukan nama untuk berhubungan. Namun, kita sebagai pengguna jaringan atau *network* memerlukan hal tersebut karena lebih mudah diingat dan diketik daripada alamat IP yang diperlukan komputer. Penamaan setiap komputer yang terhubung satu sama lain. Pada Internet, setiap perangkat diberi nama yang informatif. Dengan melihat nama dari suatu perangkat, setidaknya kita dapat membayangkan dimana perangkat itu berada dan *service* apa yang diberikan. Bentuk domain situs yang digunakan pada Internet mirip dengan *IP Address*, yakni terdiri dari beberapa segmen. Setiap segmen berupa nama atau singkatan yang memberikan sebuah informasi. [3]

2.1.4 Proxy

Proxy bertindak sebagai gerbang terhadap dunia Internet ini untuk setiap komputer klien. *Proxy* tidak terlihat oleh komputer klien, dengan kata lain, seorang pengguna yang berinteraksi dengan Internet menguunakan sebuah *proxy* tidak akan mengetahui bahwa sebuah *proxy* sedang menangani permintaan yang dilakukannya. *Web* yang menerima permintaan dari *proxy* akan menginterpretasikan permintaan-permintaan tersebut seolah-olah permintan itu datang secara langsung dari komputer klien, bukan dari sebuah *proxy*. [4]

2.1.5 VPN (Virtual Private Network)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam suatu jaringan itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. [5]

2.1.6 Jenis Konten Negatif

Konten negatif kini begitu bertebaran di internet. Internet bukan hanya milik segelintir orang namun milik kita semua apa jadinya jika konten konten negatif bertebaran di internet namun kita tidak bisa bertindak karena tidak memiliki kuasa. Konten negatif yang dimaksudkan didalam penelitian ini yaitu seperti pornografi, Judi online, dan lain sebagainya. Adapun list dari konten-konten negatif tersebut terdapat di database situs Trust+Positif kominfo yaitu: https://trustpositif.kominfo.go.id/

2.1.7 Mikrotik

Mikrotik adalah sistem operasi dan juga *software* yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk jaringan *wireless* maupun IP *Network*. Mikrotik diciptakan untuk mudah digunakan dan sangat baik untuk keperluan pengontrolan jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks atau besar sekalipun [6]

2.2 Metode Penelitian

Metode penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, di mana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Metode penelitian yang digunakan adalah metode analisis deskriptif yang memiliki dua tahap yaitu pengumpulan data dan pengembangan jaringan.

2.2.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penulisan skripsi ini sebagai berikut.

a. Studi Literatur

Mempelajari buku, artikel dan paper yang berkaitan dengan topik tugas akhir.

b. Perancangan Sistem

Perancangan yang dilakukan antara lain perancangan topologi jaringan, mempersiapkan kebutuhan perangkat, dan pemasangan sistem operasi dan aplikasi yang digunakan untuk melakukan optimalisasi sehingga dapat berjalan dengan baik pada sistem.

c. Implementasi

Implementasi yang dilakukan yaitu berupa implementasi sistem dan konfigurasi *Transparent* DNS, Pemblokiran *Proxy* dan VPN untuk mengoptimalkan *filtering* konten negatif yang diberlakukan ISP

d. Pengujian

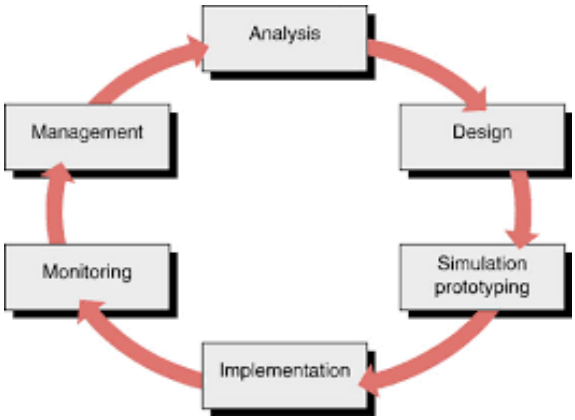
Pengujian dilakukan dengan melakukan penggunaan DNS *default* yang diberikan oleh ISP, menggunakan DNS Eksternal, serta menggunakan Proxy dan VPN

e. Analisa dan Kesimpulan

Setelah melakukan pengujian pada DNS, *Proxy*, dan VPN dapat diambil kesimpulan

2.2.2 Metode Pengembangan Jaringan

Metode yang digunakan pada penelitian ini adalah model NDLC. *Network Development Life Cycle* (NDLC) merupakan sebuah model yang bergantung pada proses model siklus hidup jaringan dengan konsep NDLC yaitu, Analisis Kebutuhan (*Analysis*), Perancangan (*Design*), Simulasi (*Simulation Prototype*), Implementasi (*Implementation*), *Monitoring*, dan *Management*. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan. Berikut ini adalah tahapan dari NDLC. [7]



Gambar 1 Network Development Life Cycle (NDLC)

a. Analisis Kebutuhan (Analysis)

Tahap ini dibutuhkan analisis permasalahan yang muncul, analisis keinginan user serta kebutuhan hardware yang akan digunakan dan analisis topologi jaringan yang sudah ada saat ini.

b. Perancangan (Design)

Design atau perancangan bisa berupa struktur topologi, design akses data, desain tata *layout* perkabelan dan sebagainya yang akan memberikan gambaran jelas tentang *project* yang akan dibangun.

c. Simulasi (*Simulation Prototype*)

Pada tahap simulasi penulis membangun sebuah jaringan sederhana pada *project* yang akan dibangun menggunakan semua alat yang nantinya akan digunakan pada penerapan.

d. Implementasi (*Implementatiton*)

Pada tahap implementasi penulis akan mengkonfigurasi sebuah jaringan LAN dan juga *Wireless*. Implementasi ini diawali dengan pengaturan dasar

e. Monitoring

Model pengawasan sistem jaringan NDLC mengkategorikan proses pengujian pada tahap *monitoring*. Hal ini dikarenakan pengawasan sistem yang sudah dibangun atau dikembangkan. Proses pengujian yaitu untuk menjamin apakah sistem yang dibangun atau dikembangkan dapat berjalan dan sesuai dengan keinginan. Pada tahap ini penulis memantau *user* menggunakan Mikrotik. Langkah dilakukan dengan tujuan memastikan jaringan berjalan dengan baik.

f. Management

Selanjutnya adalah *management* atau pengelolaan. Fase ini meliputi aktifitas dan pemeliharaan dari seluruh sistem yang sudah dibangun. Tahap *management* ini akan dilakukan setelah sistem ini berjalan dengan baik pada jaringan yang telah dibangun. Pada tahap *management* penulis akan melakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yag diharapkan.

2.3 Hasil dan Pembahasan

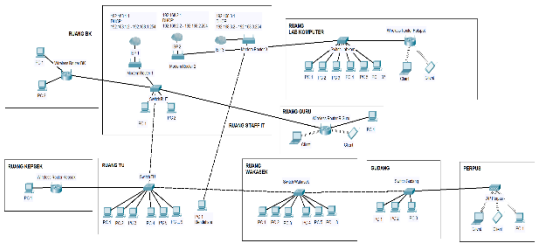
Berikut adalah pembahasan penelitian yang akan dibangun beserta hasilnya.

2.3.1 Analisis Sistem

Analisis adalah suatu tindakan yang dilakukan untuk mengetahui lebih detil tentang objek yang akan diteliti. Pada bagian ini akan diuraikan analisis kebutuhan , analisis perancangan jaringan dan konfigurasi sistem. Tahapan awal dilaksanakan analisis kebutuhan-kebutuhan pokok dari konfigurasi yang akan dibangun. Pada saat ini keamanan internet positif di ISP Indonesia hanya dilakukan dari sisi DNS mereka saja. Bila pengguna mengganti pengaturan DNS menggunakan DNS selain yang diberikan oleh ISP, maka keamaan internet positif pun akan terlewati (*bypassed*). Selain itu juga masih ada jalan lain seperti menggunakan *proxy* dan VPN. *Administrator* jaringan di SMAN 27 Bandung belum bisa membatasi penggunaan DNS Eksternal, *proxy*, dan juga VPN di lingkungan SMAN 27 Bandung

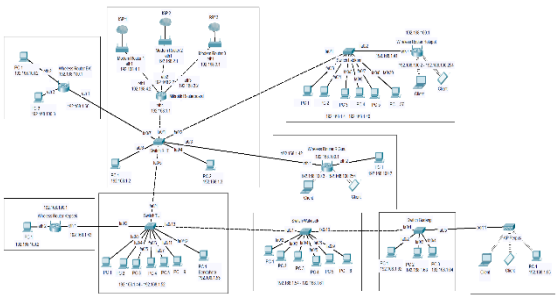
2.3.2 Arsitektur Jaringan

Berikut adalah arsitektur jaringan yang saat ini berjalan di SMA Negeri 27 Bandung.



Gambar 2 Arsitektur Jaringan Saat Ini

Lalu arsitektur jaringan untuk implementasi ini adalah bagaimana suatu Mikrotik Routerboard dapat mencegah terbukanya situs berkonten negatif dan telah dikonfigurasi agar dapat menghentikan koneksi internet penggunanya yang tetap mencoba membuka situs tersebut sesuai dengan waktu yang ditentukan. Berikut ini gambaran dari arsitektur jaringan setelah implementasi.



Gambar 3 Arsitektur Jaringan Setelah Implementasi

Selain itu, terdapat alokasi IP address yang digunakan di SMAN 27 Bandung. IP public yang digunakan dari ISP untuk SMAN 27 Bandung bersifat dynamic dan IP untuk jaringan lokal bersifat static. Berikut ini alokasi IP address di SMAN 27 Bandung.

Tabel 1 Alokasi IP Address

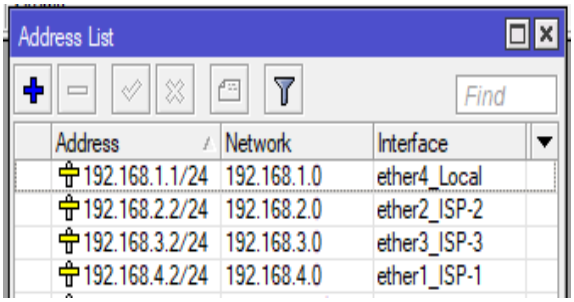
Device	IP Address	Gateway	Interface
Wireless Router ISP 1	(IP Dynamic)	(IP Dynamic)	ether1
	192.168.4.1/24	-	ether2
Wireless Router ISP 2	(IP Dynamic)	(IP Dynamic)	ether1
	192.168.2.1/24	-	ether2
Wireless Router ISP 3	(IP Dynamic)	(IP Dynamic)	ether1
	192.168.3.1/24	-	ether2
Mikrotik Routerboard	192.168.4.2/24	192.168.4.1	ether1
	192.168.2.2/24	192.168.2.1	ether2
	192.168.3.2/24	192.168.3.1	ether3
	192.168.1.1/24	-	ether4

2.3.3 Konfigurasi Mikrotik

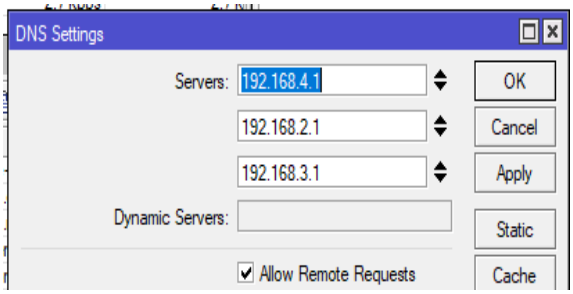
Konfigurasi routerboard adalah tahapan dilakukannya pengaturan-pengaturan pada beberapa parameter yang terdapat pada routerboard agar dapat melakukan optimalisasi internet positif. Adapun parameter-parameter yang akan di konfigurasi pada mikrotik routerboard adalah sebagai berikut :

a. Tahap konfigurasi IP Address
b. Tahap Konfigurasi DNS
c. Tahap Konfigurasi IP Route
d. Tahap konfigurasi IP firewall NAT Address
e. Tahap cek koneksi
f. Tahap konfigurasi firewall NAT untuk Transparent DNS
g. Tahap konfigurasi firewall Layer7 Protocols untuk
h. pemblokiran Proxy dan VPN

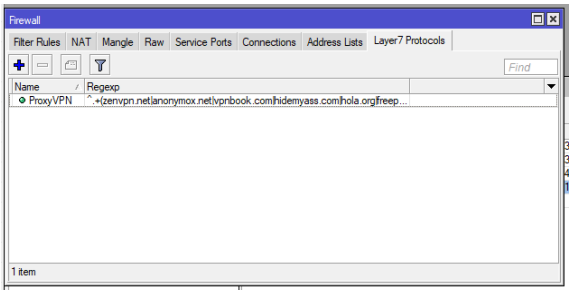
Tahapan konfigurasi diatas dilakukan secara bertahap sehingga apabila terjadi kesalahan dapat dengan mudah untuk memperbaikinya. Berikut adalah gambar pengkonfigurasian Mikrotik secara bertahap.



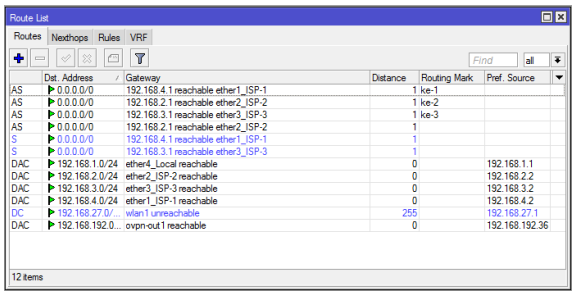
Gambar 4 Konfigurasi IP Address



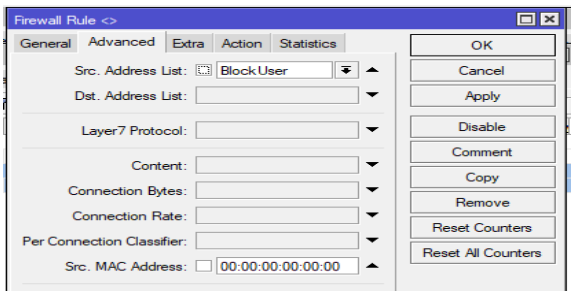
Gambar 5 Konfigurasi DNS



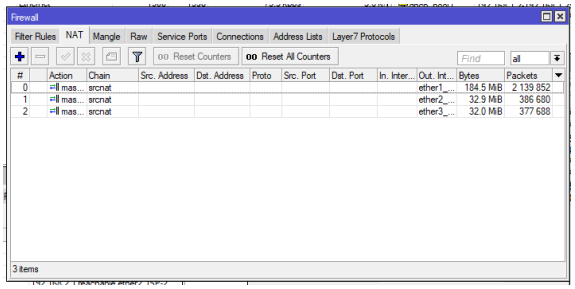
Gambar 10 Konfigurasi L7 Protocol



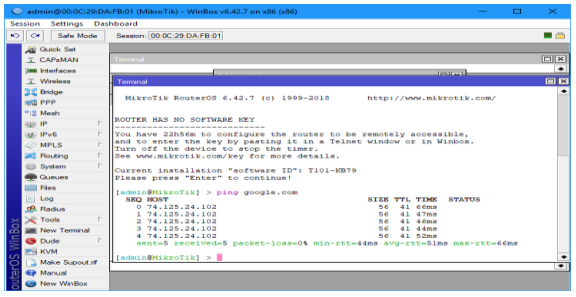
Gambar 6 Konfigurasi IP Route



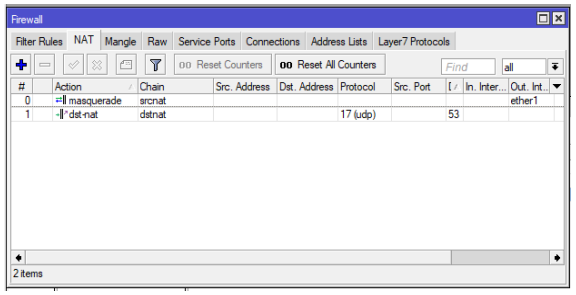
Gambar 11 Konfigurasi Block User



Gambar 7 Konfigurasi IP Firewall NAT



Gambar 8 Cek Koneksi



Gambar 9 Konfigurasi Transparent DNS

2.3.4 Skenario Pengujian

Skenario pengujian disini digunakan sebagai acuan pada saat melakukan proses pengujian hasil konfigurasi, adapun skenario pengujian yang akan dilakukan dibuat menjadi beberapa skenario uji yang terkait dengan konfigurasi yang di implementasikan. Skenario pengujian yang akan dilakukan fokus kepada konfigurasi sistem yang telah dilakukan di Mikrotik dan perintah-perintah yang akan digunakan pada medianya.

Berdasarkan parameter-parameter tersebut, maka akan dibuat lima skenario utama pengujian yang di implementasikan. Skenario-skenario yang diujikan adalah sebagai berikut.

a. Mengakses situs negatif dengan DNS:
   - Menggunakan DNS default tanpa konfigurasi Transparent DNS
   - Menggunakan DNS eksternal tanpa konfigurasi Transparent DNS
   - Menggunakan DNS default dengan konfigurasi Transparent DNS
   - Menggunakan DNS eksternal dengan konfigurasi Transparent DNS

b. Menguji penggunaan proxy:
   - Tanpa menggunakan konfigurasi L7 Protocols Mikrotik
   - Dengan menggunakan konfigurasi L7 Protocols Mikrotik

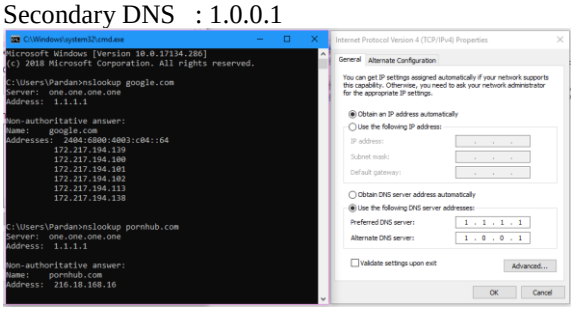
c. Menguji penggunaan VPN:
   - Tanpa menggunakan konfigurasi L7 Protocols Mikrotik
   - Dengan menggunakan konfigurasi L7 Protocols Mikrotik

2.3.5 Hasil Pengujian

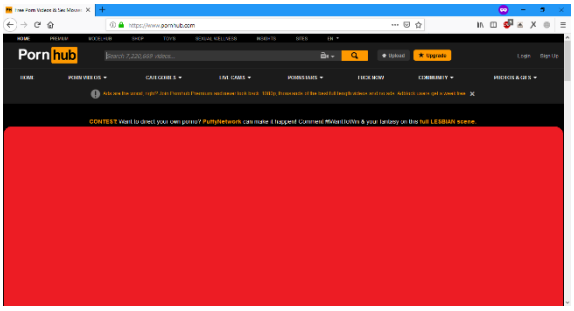
a. Pengujian DNS

Penulis mencoba merubah pengaturan DNS di perangkat *client* menggunakan DNS milik Cloudflare yaitu.

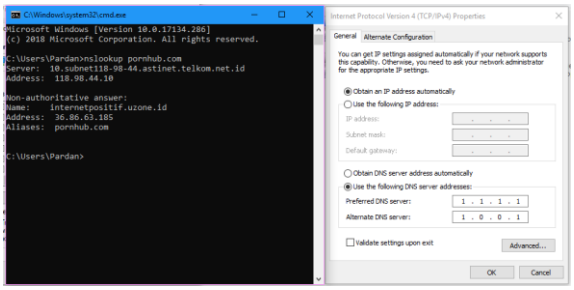
Primary DNS : 1.1.1.1
Secondary DNS : 1.0.0.1



Gambar 12 Mengubah Pengaturan DNS Tanpa Transparent DNS



Gambar 13 Membuka Situs Negatif Menggunakan DNS Cloudflare



Gambar 14 Mengubah Pengaturan DNS Dengan Transparent DNS

Gambar 15 Membuka Situs Negatif Menggunakan DNS Cloudflare Dengan Transparent DNS

Kesimpulan dari pengujian di tahap DNS ini dapat dilihat pada Tabel 2 berikut ini.

Tabel 2 Kesimpulan Pengujian DNS

Jenis Pengujian DNS	Situs Berkonten Negatif
DNS Default Tanpa Transparent DNS	Terblokir
DNS Eksternal (Cloudflare) Tanpa Transparent DNS	Tidak Terblokir
DNS Default Dengan Transparent DNS	Terblokir
DNS Eksternal (Cloudflare) Dengan Transparent DNS	Terblokir

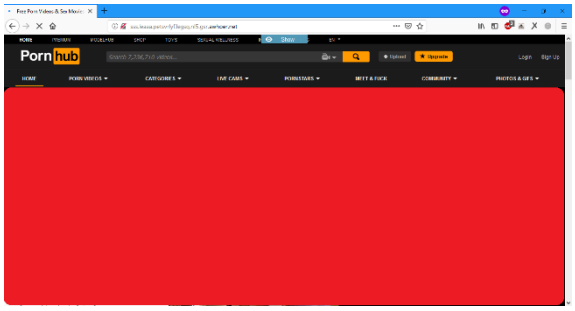
b. Pengujian Proxy

Pada tahap ini akan dilakukan pengujian penggunaan proxy untuk membuka pemblokiran situs konten negatif yang diberlakukan oleh ISP. Pengujian yang akan penulis lakukan dibagi menjadi dua tahap, yaitu penggunaan *proxy* tanpa konfigurasi *firewall L7 Protocols* Mikrotik dan dengan konfigurasi *firewall L7 Protocols* Mikrotik.

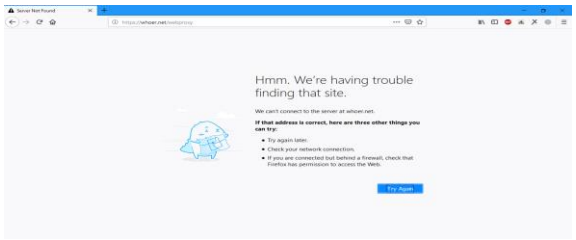
Pengujian ditahap ini akan dilakukan menggunakan *Web Proxy* dari https://whoer.net/webproxy

Gambar 16 Whoer.net Web Proxy

Meskipun sudah menerapkan sistem konfigurasi *Transparent* DNS, akan tetapi situs berkonten negatif masih bisa client akses. Salah satunya yaitu menggunakan *proxy* ataupun *web proxy* seperti whoer.net. Berikut adalah pengujian menggunakan whoer.net tanpa mengaktifkan konfigurasi *firewall layer 7 protocols* untuk mengakses situs berkonten negatif.



Gambar 17 Mengakses Situs Negatif Menggunakan Web Proxy Tanpa Firewall L7 Protocols Mikrotik



Gambar 18 Mengakses Situs Negatif Menggunakan Web Proxy Dengan Firewall L7 Protocols Mikrotik

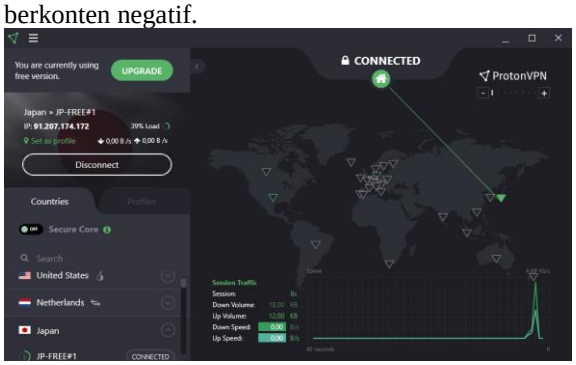
Kesimpulan dari tahap pengujian Proxy ini dapat dilihat pada Tabel 3 berikut ini.

Tabel 3 Kesimpulan Pengujian Proxy

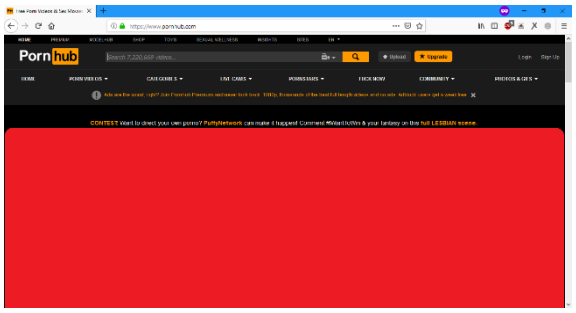
Jenis Pengujian Proxy	Keterangan
Menggunakan Web Proxy whoer.net tanpa konfigurasi Layer 7 Protocols Mikrotik	Tidak Terblokir
Menggunakan Web Proxy whoer.net dengan Layer 7 Protocols Mikrotik	Berhasil Terblokir

c. Pengujian VPN

Pada tahap pengujian ini, penulis akan menggunakan ProtonVPN untuk mengakses situs berkonten negatif.

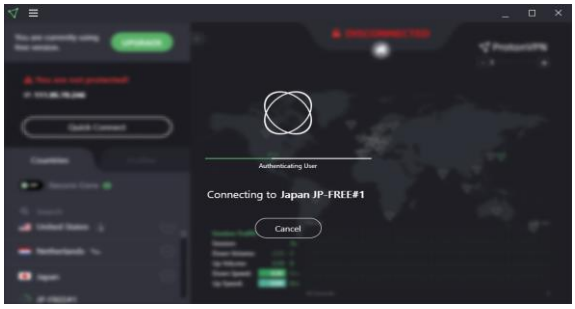


Gambar 19 ProtonVPN Berhasil Terkoneksi Tanpa Firewall L7 Protocols Mikrotik



Gambar 20 Situs Berkonten Negatif Terbuka Menggunakan ProtonVPN

Selanjutnya sama seperti sebelumya, pada pengujian ini penulis akan menggunakan ProtonVPN untuk mengakses situs berkonten negatif. Akan tetapi dengan mengaktifkan keamanan *Firewall Layer 7* tersebut



Gambar 21 ProtonVPN Tidak Bisa Terkoneksi Setelah Mengaktifkan Firewall L7 Protocols Mikrotik

Kesimpulan dari tahap pengujian VPN ini dapat dilihat pada Tabel 4 berikut ini.

Tabel 4 Kesimpulan Pengujian VPN

Jenis Pengujian VPN	Keterangan
Menggunakan ProtonVPN tanpa konfigurasi Layer 7 Protocols Mikrotik	Tidak Terblokir
Menggunakan ProtonVPN dengan Layer 7 Protocols Mikrotik	Berhasil Terblokir

3. PENUTUP

3.1 Kesimpulan

Setelah melakukan analisis perancangan,dan pengujian, maka dapat diperoleh kesimpulan sebagai berikut:

a. *Transparent* DNS membuat *client* menggunakan DNS *default* yang diberikan oleh ISP sehingga penggunaan internet akan lebih aman
b. *Layer 7 Protocol* adalah salah satu metode dalam pemblokiran situs, aplikasi, maupun ekstensi berkas.
c. Melalui *firewall*, suatu *address* tertentu yang diinputkan akan diblokir, sehingga jaringan tersebut tidak akan bisa terhubung dengan *address* tersebut

3.2 Saran

Berikut ini adalah uraian juga saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan penetilian ini, diantaranya:

a. Dapat dikembangkan untuk mengolah efektivitas penggunaan *Layer 7 Protocol* pada jaringan internet yang lebih besar
b. Memperbanyak list aplikasi Proxy dan juga VPN agar keamanan jaringan internet lebih optimal

c. Mencegah penggunaan DNS melalui jalur lain seperti DNS Over HTPS dan juga TLS

DAFTAR PUSTAKA

[1] Prihanto, Harry, Membangun Jaringan Komputer : Mengenal Hardware dan topologi Jaringan, Bandung, 2016.

[2] I. Riadi, Block Situs Dengan Mikrotik Layer 7 dan Web Proxy, Jakarta, 2015.

[3] Daryanto, Teknik Komputer Jaringan, Bandung: Alfabeta, 2010.

[4] Towidjojo, Rendra, Mikrotik Kungfu Kitab 3, Jakarta: Jasakom, 2013.

[5] Irawan Afrianto, Eko Budi Setiawan, "KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN DATA PADA JARINGAN KOMPUTER (Studi Kasus Jaringan Komputer Unikom)," *Majalah Ilmiah UNIKOM*, vol. 12, p. 1, 2014.

[6] Towidjojo, Mikrotik Kungfu Jilid 1, Jakarta: Jasakom, 2015.

[7] Herlambang, M.Linto, Membangun Sharing Koneksi Internet di Mikrotik, Yogyakarta: Andi, 2015.