ANALISA DAN IMPLEMENTASI DNS SERVER SEBAGAI FILTERING KONTEN NEGATIF MENGGUNAKAN METODE RPZ (RESPONSE POLICY ZONE) DI PT. TIME EXCELINDO

Sani Muhlison[1)], Kusnawi[2)]

[1,2)]Teknik Informatika STMIK AMIKOM Yogyakarta
email : sani.m@students.amikom.ac.id[1)], khusnawi@amikom.ac.id[2)]

Abstract

Internet today has become an important requirement for the community. The increased use of the internet, it is also popping up more and more sites with content that can have negative effects for society. To create a clean and comfortable internet, it is necessary to filtering of the domain that has a negative content. PT. Time Excelindo as one of the internet service providers (ISPs), shall perform the blocking of websites that contain negative content. This is reinforced by the MINISTER OF COMMUNICATION AND INFORMATION OF THE REPUBLIC OF INDONESIA NUMBER 19 OF 2014 Article 8, paragraph 1, Internet Access Service Provider shall perform the blocking of sites contained in the TRUST + Positive. In this thesis, the author will analyze and implement the DNS Server As Negative Content Filtering Using RPZ (Response Policy Zone) method at PT. Time Excelindo. So that filtering can run up, the client may be forced to use the DNS server with the help of a router.

The method used is the analysis, installation, configuration, testing and evaluation. DNS servers, can perform filtering of the domain are allowed and which are not allowed to be accessed by the client. By using RPZ, can register a particular client for a free from the filtering process on the DNS server. In addition, in order to force the client through the process of filtering, use the router. With the blocking of negative sites, the authors hope to civilize healthy internet for a better Indonesia.

***Keywords*:**
Filtering, Negative Content, DNS Server, Response Policy Zone (RPZ)

Pendahuluan

Situs negatif saat ini sudah semakin menyebar luas di masyarakat. Hal ini membuat tugas pemerintah dalam memberikan akses internet yang bersih dan nyaman semakin berat. Menurut data trafik filtering lewat jaringan DNS Nawala, tiap hari tercatat satu juta akses ke halaman situs negatif yang diblokir di Indonesia. "Itu artinya, kurang lebih ada satu juta orang yang meminta akses ke situs negatif," kata direktur pelaksana DNS Nawala M Yamin di Jakarta[1].

PT. Time Excelindo sebagai salah satu penyelenggara jasa internet di Indonesia, diwajibkan melakukan pemblokiran terhadap situs-situs yang terdapat dalam TRUST+Positif. Hal ini sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 Pasal 8 Ayat (1). Dengan adanya peraturan ini, diharapkan dapat menjauhkan masyarakat dari dampak negatif internet.

Dari hasil observasi yang penulis lakukan pada PT. Time Excelindo, penulis tidak menemukan pemblokiran pada situs - situs yang terdapat pada TRUST+Positif. Oleh karena itu, penulis memiliki ide untuk melakukan pemblokiran terhadap situs negatif menggunakan salah satu dns server pada PT.Time Excelindo. Pemblokiran dilakukan dengan menggunakan DNS *Server* dan metode yang digunakan adalah RPZ *(Response Policy Zone).*

DNS (*Domain Name System*) adalah *Distribute Database System* yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan TCP/IP (*Transmission Control Protocol/ Internet Protocol*) [2]. *Response Policy Zone* adalah metode yang memungkinkan administrator name server untuk mengkustom informasi diatas DNS global untuk memberikan tanggapan alternatif atas pertanyaan [3]. Ketika sebuah komputer menggunakan DNS Server ini, maka akan ditampilkan halaman peringatan ketika mengakses situs negatif, sehingga dengan adanya pemblokiran ini diharapkan dapat membantu masyarakat dalam menjaga perilaku penyimpangan dan mewujudkan Indonesia yang bersih, aman dan sehat dalam berinternet.

Tujuan utama dari penelitian ini yaitu dapat memblokir situs-situs dengan konten negative di PT. Time Excelindo menggunakan DNS *server* dengan metode RPZ (*Response Policy Zone*).

Landasan Teori

Dalam jurnal yang berjudul "Membangun jaringan *internet wifi* yang sehat di Dinas Pendidikan, Pemuda dan Olahraga Daerah Istimewa Yogyakarta". Peneliti tersebut melakukan pemblokiran situs porno dengan menggunakan dns dari nawala dan *squid*. DNS Nawala digunakan sebagai *name server* dari *proxy*. Sehingga ketika komputer klien tersebut mengakses situs porno, akan diblokir oleh dns nawala. *Squid* digunakan untuk memblokir situs yang mengandung kata-kata yang ditentukan oleh admin. Ketika dalam sebuah

website mengandung kata-kata yang telah ditentukan tersebut, maka situs tersebut akan diblokir. [4]

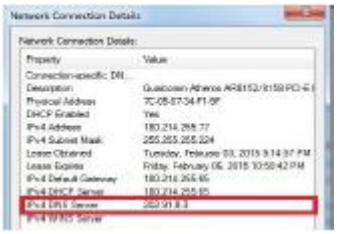
Dalam jurnal yang berjudul "Perancangan dan Implementasi *Proxy Server* Untuk *Filtering* Berdasarkan Alamat Situs dan Alamat IP". Dalam jurnal tersebut, peneliti melakukan *filtering* situs dengan memblokir situs negatif menggunakan *proxy server (Squid)*. Situs negatif didaftarkan kedalam sistem, ketika ada komputer klien yang mengakses situs yang terdaftar dalam sistem, akan diblok sehingga komputer klien tidak bisa mengakses situs tersebut. [5]

Dalam skripsi yang berjudul "Pengaruh Situs Porno Internet Terhadap Perilaku Menyimpang Remaja Wonocolo Gang Lebar Surabaya". Dalam penelitian ini, peneliti melakukan penelitian dengan metode *angket* (*kuisioner*) dan *interview*. Dari hasil penelitian tersebut didapat hasil bahwa situs porno internet sangat berpengaruh terhadap perilaku menyimpang remaja Wonocolo gang lebar Surabaya. [6]

Pembahasan

Analisis Masalah

Langkah awal yang dilakukan adalah menganalisis kondisi dari jaringan di PT. Time Excelindo dengan cara melakukan pengujian. Sebelum dilakukan pengujian, pastikan menggunakan IP DNS yang ada pada PT. Time Excelindo, yaitu 202.91.8.3 seperti yang terlihat pada gambar 1.



Gambar 1. IPv4 DNS Server Primary

Setelah itu, barulah dilakukan pengujian. Beberapa cara yang dapat digunakan untuk mengetahui apakah sudah dilakukan pemblokiran atau belum adalah dengan melakukan uji ping, traceroute, nslookup dan juga melalui web browser. Ada beberapa parameter yang menjadi acuan apakah pemblokiran sudah berhasil dilakukan atau belum. Parameter tersebut dapat dilihat pada tabel 1 :

Tabel 1. Parameter Pemblokiran Situs

Nama Situs (diambil dari TRUST Positif)	PARAMETER			
	ping	traceroute	nslookup	Akses browser
	Apakah situs terblokir ?			
www.latexas.com	Ya/ Tidak	Ya/ Tidak	Ya/ Tidak	Ya/ Tidak
Allaboutgambling.com	Ya/ Tidak	Ya/ Tidak	Ya/ Tidak	Ya/ Tidak

Keterangan :

Parameter *ping*

Ya :Jika computer *client* dapat terkoneksi ke alamat IP situs.

Tidak :Jika computer *client* tidak dapat terkoneksi ke alamat IP situs.

Parameter *traceroute*

Ya :Alamat IP akhir tidak sesuai dengan IP situs.

Tidak :Alamat IP akhir sesuai dengan IP situs.

Parameter *nslookup*

Ya : *name* dan *address* tidak sesuai seperti di http://whois.domaintools.com

Tidak : *name* dan *address* sesuai seperti di http://whois.domaintools.com

Parameter *akses browser*

Ya : Apabila situs tidak dapat dibuka (free cache)

Tidak : Apabila situs dapat dibuka (free cache)

Sebelum uji coba dilakukan, akan dicari tahu dulu alamat ip dari kedua situs tersebut di whoisdomaintools.com.

Gambar 2. Alamat IP www.latexas.com

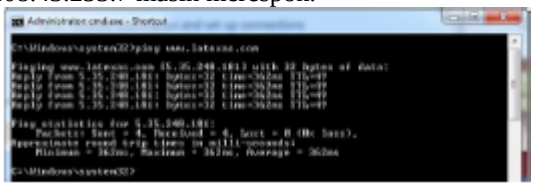
Gambar 2 menunjukkan bahwa alamat IP dari situs www.latexas.com adalah 5.35.248.181.

Gambar 3. Alamat IP allaboutgambling.com

Gambar 3 menunjukkan bahwa alamat IP dari situs allaboutgambling.com adalah 208.43.253.7.

Uji Ping

Salah satu cara untuk menguji koneksi ke situs yang dituju adalah dengan ping. Hasil uji ping menunjukkan IP address www.latexas.com dan allaboutgambling.com seperti yang terdapat pada *whoisdomaintools* yaitu 5.35.248.181 dan 208.43.253.7 masih merespon.

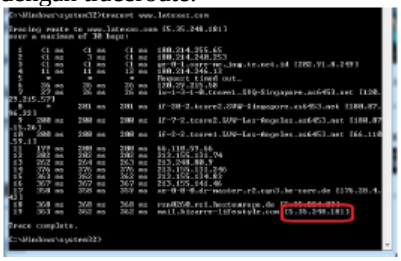


Gambar 4. Uji Coba Ping ke www.latexas.com

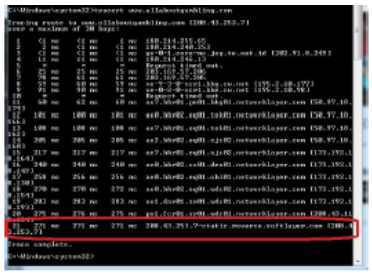
Gambar 5. Uji Coba Ping ke allaboutgambling.com

Uji Traceroute

Salah satu cara untuk mengetahui rute yang dilalui untuk menuju ke alamat IP sebuah domain adalah dengan traceroute.



Gambar 6. Uji Coba Traceroute ke www.latexas.com



Gambar 7. Uji Coba Traceroute allaboutgambling,com

Dari hasil uji coba tracert, jalur yang dilalui menuju ke alamat IP dari domain www.latexas.com dan allaboutgambling.com yaitu 5.35.248.181 dan 208.43.253.7.

Uji Nslookup

Salah satu cara untuk mengetahui alamat IP dari sebuah domain adalah dengan nslookup.

Gambar 8. Uji Coba nslookup ww.latexas.com

Gambar 9. Uji Coba nslookup allaboutgambling.com

Dari hasil uji coba nslookup, nama domain dan alamat IP sesuai dengan yang terdapat pada whoisdomaintools.

Uji Akses Browser

Setelah uji ping, traceroute dan nslookup dilakukan, Langkah selanjutnya adalah membuka situs negatif tersebut melalui browser untuk membuktikan apakah situs tersebut sudah diblokir atau belum.

Gambar 10. Uji akses www.latexas.com melalui browser

Gambar 11. Uji akses allaboutgambling.com melalui browser

Hasil uji coba akses melalui browser menunjukkan halaman dari situs www.latexas.com dan allaboutgambling.com masih dapat dibuka. Hal ini menunjukkan situs tersebut belum terblokir.

Hasil Uji Coba

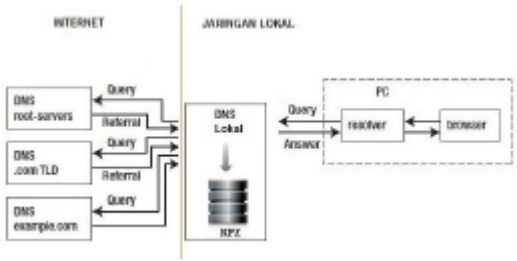
Setelah pengujian selesai dilakukan, akan didapat hasil. Dari hasil tersebut akan diketahui apakah pada PT. Time Excelindo telah dilakukan pemblokiran terhadap situs yang ada pada TRUST+Positif. Hasil uji coba dapat dilihat pada tabel 2 berikut.

Tabel 2. Hasil uji Coba Sebelum Pemblokiran

Nama Situs	PARAMETER			
	ping	traceroute	nslookup	Akses browser
	Apakah situs terblokir ?			
www.latexas.com	Tidak	Tidak	Tidak	Tidak
Allaboutgambling.com	Tidak	Tidak	Tidak	Tidak

Perancangan Sistem

Perancangan dilakuakan di PT. Time Excelindo, dan salah satu DNS server (202.91.10.38) akan digunakan sebagai filtering konten negatif menggunakan metode *Response Policy Zone*. Cara kerja dari sistem yang akan dirancang dapat dilihat pada gambar 12.



Gambar 12. Rancangan Sistem

Dari gambar tersebut dapat dijelaskan dengan menggunakan contoh sebagai berikut.

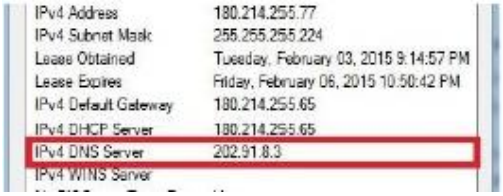
Misalnya client dari PT. Time Excelindo mengakses sebuah situs misalnya www.example.com menggunakan browser (missal : google chrome, mozila firefox, dan lain lain) dan *browser* akan mengirimkan permintaan (*query*). Permintaan pertama kali akan ditanyakan ke cache browser. Ketika cache tersebut memilik data yang telah diakses sebelumnya dari permintaan yang diajukan browser, maka cache akan memberikan apa yang diminta browser. Tetapi jika cache tersebut tidak memiliki jawabannya, maka browser akan memanggil resolver. Jika resolver tidak memiliki jawaban atas permintaan tersebut, maka resolver akan mengirimkan jawaban ke DNS Resolver atau DNS server. Jika resolver memiliki jawabannya, browser akan langsung mengontak server yang dituju menggunakan alamat IP dari www.example.com yang didapat dari resolver. *DNS Resolver* yang dituju akan disesuaikan dengan alamat *DNS Server primary* yang digunakan komputer *client* tersebut. Jika client menggunakan *DNS server* yang disediakan dari pihak PT. Time Excelindo, maka *DNS server* tersebut akan mengecek ke zona RPZ dan *cache* dari server DNS tersebut. Jika situs yang dituju terdapat dalam daftar situs yang terdapat pada zona RPZ, maka DNS server akan mengirimkan jawaban ke client. jika tidak menemukan jawabannya, *DNS server* tersebut akan bertanya ke *DNS server* lain atau mencarikan jawaban ke server *authoritative* (sesuai dengan konfigurasi yang ada di server tersebut). Server *authoritative* tersebut yaitu *root* (.), TLD (.com), dan SLD (example.com), dan situs yang dituju / *hostname* (www.example.com). Setelah menemukan jawaban dari pertanyaan tersebut, jawaban akan dikirimkan ke client. Jika ternyata pertanyaan yang diajukan tidak ada (situs tidak terdaftar), maka akan dikirimkan pesan eror ke client.

Uji Coba Setelah Adanya Filtering

Uji coba dilakukan pada salah satu komputer yang terdapat pada jaringan PT. Time Excelindo. Uji coba akan dilakukan dengan beberapa skenario. Skenario pertama, uji coba untuk client yang memasang DNS (202.91.10.38) secara manual. Skenario kedua, uji coba untuk client yang menggunakan DNS google (8.8.8.8 dan 8.8.4.4) secara manual dan memaksa client tersebut menggunakan DNS (202.91.10.38). dan Skenario yang ketiga, uji coba untuk client yang dibebaskan dari proses filtering oleh DNS server (202.91.10.38).

Uji Coba Skenario 1

Uji coba scenario 1 yaitu memasang DNS (202.91.10.38) secara manual seperti yang terlihat pada gambar 13, kemudian melakukan pengaksesan situs menggunakan ping, traceroute, nslookup dan melalui browser.



Gambar 13. Input DNS Manual

Uji Ping

Dengan menggunakan ping, akan diketahui berapa alamat IP yang merespon dari situs yang diuji coba.

Hasil uji coba *ping* menunjukkan bahwa alamat IP yang merespon dari situs www.latexas.com dan allaboutgambling.com adalah 202.91.10.38. Ini membuktikan bahwa situs tersebut berhasil diblokir.

Uji Traceroute

Dengan menggunakan traceroute, akan diketahui jalur yang dilalui dan berapa alamat IP tujuan. Hasil uji coba traceroute menunjukkan bahwa IP address terakhir atau tujuan adalah IP DNS server yang telah dibuat (202.91.10.38). Ini membuktikan bahwa situs tersebut berhasil diblokir.

Uji Nslookup

Dengan nslookup, dapat diketahui berapa alamat IP dari sebuah nama domain. Hasil uji coba nslookup,menunjukkan bahwa alamat IP dari situs www.latexas.com dan allaboutgambling.com adalah alamat IP dari DNS server yang telah dibuat (202.91.10.38). Ini membuktikan bahwa situs tersebut berhasil di blokir.

Uji Akses Browser

Untuk lebih memastikan lagi bahwa pemblokiran berhasil atau tidak dapat diuji dengan mengakses situs melalui browser.

Gambar 14. Akses kedua situs melalui browser

Hasil uji coba akses melalui browser tersebut menunjukkan bahwa kedua situs tersebut tidak dapat dibuka dan diganti dengan halaman peringatan. Ini membuktikan kedua situs tersebut berhasil diblokir.

Uji Coba Skenario 2

Skenario kedua, yaitu uji coba untuk client yang menggunakan DNS google (8.8.8.8 dan 8.8.4.4) dan memaksa client tersebut menggunakan DNS (202.91.10.38).

Uji Ping

Dengan menggunakan ping, akan diketahui berapa alamat IP yang merespon dari situs yang diuji coba. Hasil uji coba *ping* menunjukkan bahwa alamat IP yang merespon dari situs www.latexas.com dan allaboutgambling.com adalah 202.91.10.38. Ini membuktikan bahwa situs tersebut berhasil diblokir.

Uji Traceroute

Dengan menggunakan traceroute, akan diketahui jalur yang dilalui dan berapa alamat IP tujuan. Hasil uji coba traceroute menunjukkan bahwa IP *address* terakhir atau tujuan adalah IP *address* DNS server yang telah dibuat (202.91.10.38). Ini membuktikan bahwa kedua situs tersebut berhasil diblokir.

Uji Nslookup

Dengan nslookup, dapat diketahui berapa alamat IP dari sebuah nama domain. Hasil uji coba *nslookup* menunjukkan bahwa alamat IPv4 dari situs www.latexas.com dan allaboutgambling.com adalah IPv4 dari DNS server yang telah dibuat (202.91.10.38). Ini membuktikan bahwa situs tersebut berhasil di blokir.

Uji Akses Browser

Untuk lebih memastikan lagi bahwa pemblokiran berhasil atau tidak dapat diuji dengan mengakses situs melalui browser.

Gambar 15. Akses kedua situs melalui browser

Hasil uji coba akses melalui browser menunjukkan kedua situs tersebut tidak dapat dibuka dan ditampilkan halaman peringatan. Ini membuktikan kedua situs tersebut berhasil diblokir.

Uji Coba Skenario 3

Skenario yang ketiga, yaitu uji coba untuk client yang dibebaskan dari proses filtering oleh DNS server (202.91.10.38). Meskipun client menggunakan DNS server (202.91.10.38) sebagai DNS server primary, client tersebut akan terbebas dari pemblokiran.

Uji Ping

Dengan menggunakan ping, akan diketahui berapa alamat IP yang merespon dari situs yang diuji coba. Hasil uji coba *ping* menunjukkan bahwa alamat IP yang merespon dari situs www.latexas.com dan allaboutgambling.com sama dengan yang ada pada whoisdomaintools. Ini membuktikan bahwa situs tersebut tidak diblokir.

Uji Traceroute

Dengan menggunakan traceroute, akan diketahui jalur yang dilalui dan berapa alamat IP tujuan. Hasil uji coba *traceroute* menunjukkan bahwa IP address terakhir atau tujuan sama seperti yang ada pada whoisdomaintools. Ini membuktikan bahwa situs tersebut tidak diblokir.

Uji Nslookup

Dengan nslookup, dapat diketahui berapa alamat IP dari sebuah nama domain. Hasil uji coba menunjukkan bahwa alamat IPv4 dari situs www.latexas.com dan allaboutgambling.com sama seperti yang ada pada whoisdomaintools. Ini membuktikan bahwa situs tersebut tidak diblokir.

Uji Akses browser

Untuk lebih memastikan lagi bahwa pemblokiran berhasil atau tidak dapat diuji dengan mengakses situs melalui browser.

Gambar 16. Akses browser www.latexas.com

Gambar 17. Akses browser allaboutgambling.com

Hasil uji coba akses melalui browser tersebut menunjukkan bahwa kedua situs tersebut dapat diakses. Ini membuktikan kedua situs tersebut tidak diblokir.

Hasil Uji coba setelah filtering

Hasil akhir yang didapat setelah semua proses uji coba dilakukan, dapat dilihat di table 3, 4 dan 5.

Tabel 3. Hasil Uji Coba Skenario 1

Nama Situs	PARAMETER			
	ping	traceroute	nslookup	Akses browser
	Apakah situs terblokir ?			
www.latexas.com	Ya	Ya	Ya	Ya

Allabout gambling.com	Ya	Ya	Ya	Ya

Tabel 4. Hasil Uji Coba Skenario 2

Nama Situs	PARAMETER			
	ping	traceroute	nslookup	Akses browser
	Apakah situs terblokir ?			
www.latexas.com	Ya	Ya	Ya	Ya
Allabout gambling.com	Ya	Ya	Ya	Ya

Tabel 5. Hasil Uji Coba Skenario 3

Nama Situs	PARAMETER			
	ping	traceroute	nslookup	Akses browser
	Apakah situs terblokir ?			
www.latexas.com	Tidak	Tidak	Tidak	Tidak
Allabout gambling.com	Tidak	Tidak	Tidak	Tidak

Kesimpulan

Dari hasil uji coba didapat kesimpulan bahwa dengan menggunakan DNS Server dan menggunakan metode RPZ (*Response Policy Zone*) dapat memblokir situs dengan konten negatif yang ada pada TRUST+Positif. Dengan bantuan router mikrotik, client yang menggunakan DNS server yang mebebaskan dari proses filtering, akan dipaksa untuk menggunakan DNS server filtering, dan metode RPZ (*Response Policy Zone*) dapat membebaskan client dari proses filtering sehingga beberapa client dapat terbebas dari proses filtering.

Saran yang dapat disampaikan pada penelitian ini adalah penelitian dapat dikembangkan sehingga dapat melakukan pemblokiran terhadap konten yang ada di *google image*, dapat berfungsi untuk client yang menggunakan koneksi VPN (*Virtual Private network*), dan dapat dibuat sistem laporan pemblokiran.

Daftar Pustaka

[1] Chandrataruna, M. Ngazis, AN. 1 Juta Kali/Hari, Pengguna Internet RI Akses Situs Negatif, http://teknologi.news.viva.co.id/news/read/426514-1-juta-kali-hari--pengguna-internet-ri-akses-situs-negatif, diakses tanggal 2 Desember 2014.

[2] Syafrizal, M. 2005, *Pengantar Jaringan Komputer*. Yogyakarta. Penerbit Andi.

[3] https://dnsrpz.info/ diakses pada tanggal 27 januari 2015.

[4] Suryaningrum, F. Suraya. Rachmawati, Y. 2013. *Membangun Jaringan Internet Wifi yang Sehat di Dinas Pendidikan, Pemuda dan Olahraga Daerah Istimewa Yogyakarta*. Journal IST AKPRIND Yogyakarta. Yogyakarta.

[5] Lurio. Lestariningati, SI. 2013, *Perancangan dan Impementasi Proxy Server Untuk Filtering Berdasarkan Alamat Situs dan Alamat IP*. Journal Universitas Komputer Indonesia. Bandung.

[6] Huda, MS. 2009, *Pengaruh Situs Porno Internet Terhadap Perilaku Menyimpang Remaja Wonocolo Gang Lebar Surabaya*.Skripsi IAIN Sunan Ampel Surabaya. Surabaya.