

MEMBANGUN RT / RW – NET

“SITE BLOCKING”

Disusun guna melengkapi tugas Mata Kuliah Jaringan Komputer



Disusun Oleh:

SYAIFULLOH AMIEN

MUHAMMAD MAHMUD RAGIL

MUH.SETIAWAN

MULYONO

M.CAHYA ADI NUGRAHA

MUHAMMAD DIKA P

NUR KOSIM FADILLAH

PENGKU RAJO KURNIAWAN S

TEKNIK INFORMATIKA

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2010/2011

PENDAHULUAN

Seperti kita ketahui di zaman kecanggihan Informasi sekarang ini kita dapat memperoleh berbagai macam informasi atau kebutuhan yang kita butuhkan di internet. Mulai News, Education, Hiburan, Shopping, dan berbagai macam kebutuhan dan informasi lainnya tanpa batas di Internet. . Namun dengan kehadiran Internet ini tentunya tak lepas juga dari hal negatif. Antara masih banyaknya situs yang berbau negatif, yang mengandung content seperti Sara, Pornografi, Explicit, Phising dan Exploit. Tentunya hal ini juga cukup mengawatirkan terutama bila website yang merugikan semacam itu bila diakses oleh kalangan yang belum matang jiwanya seperti kalangan Pelajar yang belum cukup dewasa. .

Menurut temuan Kemenkominfo dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), total pengguna Internet di Indonesia saat ini menembus 40 juta pengguna. Dari angka itu, 64 persen adalah remaja. "Dari laporan terakhir yang saya dapat, pengguna Internet di dunia sudah menembus angka 1,7 miliar. Di Indonesia sendiri sudah mencapai 40 juta pengguna," ujar Djoko Agung, Sekretaris Dirjen Aptel (aplikasi telematika), di sela Talkshow Internet Sehat di Ponsel, Jakarta, Kamis 26 Agustus 2010. "Artinya, Internet saat ini memegang peranan penting bagi generasi masa depan Indonesia. Pengaruhnya sangatlah besar," imbuhnya. Untuk itu, kata Djoko, perlu ada pemanfaatan teknologi yang tepat mulai dari sekarang. Selain sosialisasi program Internet sehat, sisi pemerintah perlu melakukan beberapa upaya preventif, seperti misalnya pemblokiran akses situs porno.

Internet memang sangat dibutuhkan untuk memajukan pendidikan para pelajar, namun kita harus selalu aktif mengawasi penggunaan internet untuk para pelajar dibawah umur tersebut. Sebenarnya kita bisa mengurangi dampak negatif internet dengan cara membatasi atau memblokir beberapa situs yang mengandung hal hal yang tidak bermanfaat, sehingga internet lebih aman untuk semua kalangan terutama untuk menciptakan Internet yang aman untuk para pelajar, sekaligus menghindarkan komputer kita dari website yang berisi virus dan spyware.

PEMBAHASAN

Site Blocking atau pemblokiran website merupakan suatu cara untuk mencegah suatu website dapat diakses orang lain. Tujuan utamanya sudah jelas yaitu mencegah user mengakses situs-situs yang berbau negatif seperti pornografi, phishing, exploit dan lain-lain. Selain itu juga melindungi pengguna dalam membuka suatu website yang terdapat banyak virus, malware, spyware dan lain-lain.

Beberapa cara melakukan site blocking

1. Melakukan blokir berdasarkan URL

Cara ini cukup bagus namun memiliki banyak kelemahan, karena website pornografi setiap hari bertambah banyak. Butuh waktu yang lama dan banyak data yang harus di input untuk melakukan blokir berdasarkan alamat website dan URL. Selain itu, masih banyak website yang bisa lolos dari pemblokiran. Sebagai contoh “Google Image Search”, website ini memiliki banyak manfaatnya dan seringkali terlewatkan oleh operator atau mungkin sengaja di lewat karena manfaatnya tadi. Namun dari website ini pun, buat orang yang punya otak “ngeres” bisa mencari gambar-gambar porno yang di sukainya.

2. Melakukan blokir berdasarkan kata.

Cara ini sangat beresiko untuk melakukan blokir besar-besaran, karena akan memiliki dampak tertutupnya website yang tidak seharusnya kita tutup. Contoh website yang akan menjadi korban cara blokir dengan sistem ini adalah website “Jangan Bugil didepan kamera”, padahal jelas-jelas website ini mengedukasi masyarakat untuk tidak bugil didepan kamera, tapi karena website ini mengandung salah satu kata “haram” yaitu kata “bugil” sehingga website ini berpotensi ikut-ikutan di blokir.

Sebagai pengembangan dari cara kedua adalah berdasarkan “weight” atau berat. Melakukan blokir dengan cara ini cukup efektif, karena berdasarkan jumlah kata “haram” yang dimasukkan didalam blacklist yang dibuat administrator. Cara ini akan meloloskan website yang mengandung kata “haram” yang di blokir oleh administrator selama kata tersebut belum memenuhi jumlah tertentu. Sangat efektif, namun kembali lagi cara ini memiliki masalah, cara ini akan memblok website pencarian seperti google, yahoo dan website lain apabila digunakan untuk mencari topik yang mengandung kata “haram” tersebut. Ada kata yang sebenarnya tidak memiliki arti porno namun banyak disalahgunakan oleh pembuat website porno. Contoh: kata “cewek” apabila kita melakukan pencarian di Google Images kata “cewek” ini akan memunculkan banyak sekali gambar-gambar yang mengandung unsur pornografi. Padahal tidak semua website dengan kata “cewek” isinya gambar porno. Sedangkan apabila kita lakukan bloking berdasarkan jumlah kata, pencarian ini akan turut terblok.

3. Melakukan blokir berdasarkan “regular expression” (regex).

Cara ini memblok berdasarkan “kata” yang ada didalam URL. Cara ini masih beresiko namun bisa cukup meminimalisir. Kekurangan dari cara pemblokiran ini yaitu semakin banyak kata “haram” yang kita masukkan kedalam blacklist akan semakin banyak website tidak bersalah yang turut ke blok, namun bukan websitenya tapi URL linknya. Contohnya, misalnya ada website dengan link www.namasitus.com/jangan-bugil.htm mau tidak mau link tersebut akan menjadi korban, tapi kita masih bisa mengakses www.namasitus.com nya. Cara blokir sistem regex inipun akan sangat bermanfaat untuk menangani kasus yang baru-baru ini terjadi, yaitu rencana pemerintah untuk melakukan blokir terhadap situs Youtube.com mengenai kasus film Fitna. dengan cara ini kita dapat melakukan blokir hanya link Youtube.com yang mengandung kata Fitna, bukan Youtube.com nya sehingga kita masih bisa melakukan pencarian yang lebih bermanfaat di website Youtube.com tanpa harus memblokirnya secara keseluruhan.

Blocking menggunakan Antamedia

Antamedia HotSpot memiliki kemampuan untuk melacak dan memblokir situs web yang tidak diinginkan. Situs Web akan secara otomatis diblokir jika kata kunci spesifik muncul di alamat url. Dengan menggunakan software ini Anda dapat mencegah akses ke situs porno, dan situs web lainnya yang tidak sesuai dengan persyaratan penggunaan Anda. Untuk membuat sebuah blocking, silakan tentukan kata kunci dalam software HotSpot dengan cara - Setup - URL - URL Filtering site.

Memblokir website dengan Antamedia HotSpot adalah tugas yang sangat sederhana. Fitur terletak di HotSpot - Setup – fitering site. Untuk memblokir situs web yang diinginkan, silakan masukkan alamat URL di kolom URL situs Blok dan tekan tombol Add URL. Silakan mengetik URL tanpa http://. Apabila kita mencoba membuka situs yang telah kita blokir, pada halaman browser akan muncul pemberitahuan bahwa situs tersebut telah terblokir.

Print screen Input URL yang akan di block

Starting IP address

Ending IP address

Starting port
80

Ending port
80

Starting address	Ending address	Port from	Port to
69.63.181.11	69.63.181.11	80	80

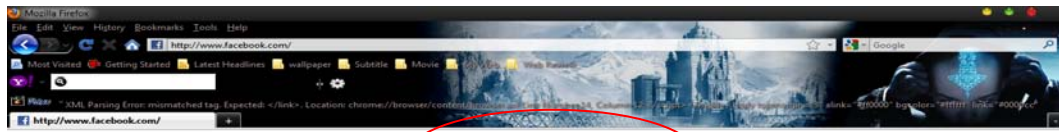
Redirect blocked website to IP

Redirect to port
80

Block website URL

Masukkan URL yang akan di Block

Print screen website yang berhasil diblock



URL is Blocked



KESIMPULAN

Berdasarkan pembahasan diatas, dapat diambil kesimpulan bahwa:

- Site Blocking atau pemblokiran website merupakan suatu cara untuk mencegah suatu website dapat diakses orang lain.
- Tujuan Site Blocking yaitu mencegah user mengakses situs-situs yang berbau negatif seperti pornografi, phishing, exploit dan lain-lain.
- Metode pemblokiran antara lain:
 - a) Melakukan blokir berdasarkan URL
 - b) Melakukan blokir berdasarkan kata.
 - c) Melakukan blokir berdasarkan “regular expression” (regex).
- Langkah-langkah pemblokiran website berdasarkan URL menggunakan Antamedia yaitu: HotSpot → Setup → fitering site.
Untuk memblokir situs web yang diinginkan, silakan masukkan alamat URL di kolom URL situs Blok dan tekan tombol Add URL.

Pertanyaan-pertanyaan

➤ Apa perbedaan http dan https?

HTTP berarti hyper text transfer protocol. Sedangkan HTTPS berarti hypertext transfer protocol secure. Sebuah halaman web atau homepage yang diawali dengan https:// merupakan sebuah web yang membutuhkan tingkat keamanan yang sangat tinggi terhadap data-data / informasi yang terdapat dalam web tersebut. Sehingga memberikan perlindungan kepada pemilik website atau pengunjung yang melakukan input informasi penting ke dalamnya.

Contoh website yang memiliki tingkat keamanan yang tinggi adalah PayPal (<https://www.paypal.com>). Menurut [Paypalindonesia](#), "PayPal merupakan salah satu alat pembayaran (Payment procesors) menggunakan internet yang terbanyak digunakan didunia dan teraman." Ternyata url yang berbeda memiliki tujuan dan maksud tertentu. Contoh lainnya adalah <https://www.google.com/adsense>.

➤ Bagaimana cara subnetting pada TP Link?

Untuk Setting Konfigurasi Akses Point TP-Link yang akan di jadikan Hotspot. Pastikan kita tau IP adres Akses point TP-Link bawaan dari pabrik, biasanya tertera dalam Akses point. Setelah ketemu IP WAN dari Akses Point TP Link, maka ketikkan IP tersebut di adres bar Internet Browser anda misal Mozilla Firefox lalu enter. Selanjutnya akan muncul tampilan Login, masukkan Username dan Pasword bawaan dari pabriknya, biasanya Username : admin Password : admin. Setelah sukses memasukkan username dan password, maka akan muncul tampilan awal dari TP Link. Pilih Menu Network dan isi alamat IP Address dengan alamat IP Akses Point. Misal alamat IP modem adalah 192.168.1.254, anda boleh mengisi Alamat IP adres dari 192.168.1.2 ----> 192.168.1.254, silahkan masukkan terserah anda pada range alamat IP tersebut yang belum terpakai. Subnet Mask isi dengan nilai 255.255.255.0. Default Gateway isi dengan alamat IP LAN yaitu : 192.168.1.15.

➤ **Dalam hotspot bagaimana cara mengantisipasi adanya Mac Address dan IP address yang sama??**

Untuk mengantisipasi adanya mac address yang sama coba security pake WPA (Wi-fi Protected Access), mac filter cuma allow mac address dari computer kilen, DHCP di tplink disable, pake ip statik di masing-masing komputer klien, ganti ip address tplink dan ip klien, hide ssid tplink.