Tugas 4 Manajemen Jaringan

DNS Filtering untuk ISP (Harijanto Pribadi)

Nama: Ahmad Fitri Rashad

Kelas: SK7Pil-A

NIM: 09121001023

Pada presentasi tersebut, bapak Harijanto Pribadi menjelaskan bagaimana cara memfilter internet pada ISP. Cara untuk memfilter internet adalah dengan 2 cara, yaitu proxy dan DNS.

Proxy adalah adalah suatu server yang menyediakan layanan untuk meneruskan setiap permintaan kita kepada server lain di internet. Dengan proxy, maka identitas komputer anda berupa IP menjadi tersembunyi dikarenakan yang dikenali server yang direquest adalah IP dari server proxy anda. Proxy ini pada umumnya digunakan untuk kegiatan menyembunyikan identitas atau untuk menghindari pemblokiran akses ke suatu server.

Keunggulan dari Web Proxy adalah:

- Dapat menapis sampai level URL
- Dapat menapis sampai level file

Kerugian dari Web Proxy adalah:

- Tidak robust (kuat)
- Tidak cocok untuk menangani traffic data ISP yang volume dan trafficnya sangat besar
- Single point of failure
- Proxy bukan native Internet (tanpa proxy Internet bisa tetap berfungsi)

DNS adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet.

DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surat elektronik (email) untuk setiap domain.

DNS adalah (Domain Name System) yang juga memiliki arti untuk mengidentifikasi setiap komputer sebagai titik dalam suatu jaringan Internet yang menggunakan bantuan sistem protokol internet adress untuk menerjemahkan dari suatu nama domain ke IP dan begitu juga sebaliknya.

Keunggulan dari DNS adalah:

- DNS adalah native dari internet, tanpa DNS Internet bisa lumpuh
- DNS memang dirancang untuk menangani request query FQDN yang sangat cepat dengan primary dan secondary DNS yang robust
- Mesin DNS dapat bekerja menggunakan backend SQL Database

Kerugian dari DNS adalah:

- DNS hanya mengenai FQDN maka DNS tidak dapat menapis sampai level URL / file seperti Web Proxy
- Resiko SQL injection sistem keamanan tidak dijaga dengan baik dan benar yang mengakibatkan resiko Phising dengan fake server (**sangat berbahaya**)

PowerDNS adalah autoratif server uang mempunyai solusi kemampuan untuk melakukan penyimpanan dalam database. PowerDNS didukung database agar berfungsi dengan baik. Berikut database yang mendukung PowerDNS:

- ✓ MySQL
- ✓ PostgreSQL
- ✓ Oracle
- ✓ SQLite
- ✓ LDAP
- ✓ DB2
- ✓ Sybase
- ✓ Microsoft SQL Server
- ✓ ODBC Server
- ✓ Geographical Information System

PowerDNS adalah DNS server alternatif BIND. PowerDNS lebih dipilih oleh pengguna virtual private server karena memakan sumber daya yang relatif kecil. Selain itu, konfigurasi PowerDNS juga lebih mudah daripada BIND. PowerDNS menggunakan database MySQL untuk menyimpan catatan (records) domain. Dan yang terpenting semuanya tersedia secara opensource dan tidak membutuhkan lisensi (license) yang mahal, karena keduanya ada GPL (General Public License.)

DNS nasional dalam aturan kebijakan yang tertera dalam surat Menkominfo dengan nomor 283/KOMINFO/AI.02.02/03/2015 menjadikan DNS Trust+Positif sebagai DNS Nasional. Menurut Rudiantara (Menkominfo), kebijakan pemblokiran terhadap konten berbau pornografi sejatinya telah dilakukan oleh operator dan penyedia jasa internet dengan memanfaatkan database dari Trust+Positif milik Kementrian Kominfo. Namun hal tersebut kenyataannya tidak berjalan mulus, masih banyak situs – situs pornografi yang lolos dari filter. Hal ini dikarenakan banyaknya server dan ratusan ISP di Indonesia.

Berikut adalah rincian pelaksanaan DNS Nasional tersebut:

- o DNS Trust+Positif dijadikan sebagai DNS Nasional
- o Penyelenggara jaringan wajib melakukan sinkronisasi pada DNS Penyelenggara jaringan dengan DNS Trust+Positif

- Penyelenggara jaringan telekomunikasi wajib menjamin tearahnya akses internet oleh pengguna DNS Nasional. Oleh karena itu, penyelenggara jaringan wajib melakukan redirection seluruh trafik DNS dari pengguna akhir internet (pelanggan) menuju DNS Nasional.
- Pelaksanaan sinkronisasi dan redirection harus sudah diimplementasikan paling lambat pada tanggal 31 Mei 2015.
- ISP yang menggunakan jaringan dari penyelenggara jaringan wajib mengikuti proses redirection terhadap DNS Nasional di sisi penyelenggara jaringan.
- Pelaksanaan teknis penerapan DNS Nasional harus dikoordinasikan dengan Direktorat Jenderal Aplikasi Informatika.

SQL juga bisa memfilter / membuat daftar hitam konten negatif, berikut adalah kelebihannya:

- Sistem bisa dikembangkan secara robust dan aman;
- Kominfo cukup memastikan bahwa master basis data SQL blacklist berkekuatan hukum dan FQDN yang di-blacklist sudah melalui mekanisme yang jelas misal dengan adanya panel konten.
- Kominfo tidak perlu men-deploy DNS Nasional yang jumlahnya pasti akan sangat banyak untuk bisa menangani kebutuhan seluruh pengguna internet di Indonesia.
- Jika sampai master basis data SQL Kominfo tidak berfungsi, slave basis data SQL di ISP masih tetap berfungsi sambil menunggu update master basis data SQL berfungsi lagi.
- DNS penapis menjadi tanggung jawab ISP dengan mengacu pada blacklist berbasis data SQL dari master MySQL Kominfo.
- DNS penapis ISP tetap dapat melayani query FQDN sesuai best-path dari upstreamnya masing-masing sehingga akses website tetap responsif dan pengguna ISP terlindungi dari situs-situs negatif.