JURNAL TEKNIK KOMPUTER AMIK BSI

Vol. II, No. 2, Agustus 2016

Implementasi DNS Filtering Unbound Menggunakan Centos 6.7 di Jaringan VSAT pada PT. Indopratama Teleglobal

Taufik Rahman[1], Irfan Maulana[2]

Abstract— *Current information can be found in cyberspace in this case the Internet, either negative or positive information, one of its information can be accessed through the website and accessible through the browser on the device used. The purpose of this study is to apply the rules and laws issued by the government is obliged to comply with the Internet service provider or website content filtering rules in order to realize a healthy internet for the people of Indonesia. There are many methods that can be applied to filtering websites that are considered to contain elements of pornography, gambling, phishing, and sara. One of them using software Unbound. After implementing Unbound on Vsat network PT.Indo Primary Teleglobal can conclude that the use unbound for filtering websites that is considered harmful both to the network at the client and at the VSAT network, from the client side does not require any special configuration to take advantage of unbound, because all packages requested by the client, will automatically be redirected by Mikrobits Router using nat rule, unbound itself is an Open Source software that is validating, recursive, and caching DNS resolver and the client will be faster to access websites.*

Intisari— *Saat ini informasi dapat diperoleh di dunia maya dalam hal ini internet, baik informasi negatif atau positif, Salah satu nya informasi dapat diakses melalui website dan diakses melalui browser pada perangkat yang digunakan. Tujuan dari penelitian ini adalah untuk menerapkan peraturan dan undang-undang yang di keluarkan oleh pemerintah yaitu penyedia jasa internet wajib mematuhi peraturan memfilter konten atau website agar terwujud internet sehat bagi rakyat indonesia. Ada banyak metode yang bisa di aplikasikan untuk melakukan filtering website-website yang dianggap mengandung unsur-unsur pornografi, judi, Phising, dan Sara. Salah satunya menggunakan software Unbound. Setelah melakukan implementasi Unbound pada jaringan Vsat PT.Indo Pratama Teleglobal dapat menyimpulkan bahwa penggunaan unbound untuk filtering website-website yang di anggap berbahaya baik untuk jaringan di client dan jaringan di sisi vsat, dari sisi client tidak memerlukan konfigurasi khusus untuk menggunakan fasilitas unbound, karena semua paket yang direquest oleh client, otomatis akan diredirect oleh Router Mikrobits dengan menggunakan rule nat, unbound sendiri adalah sebuah software Open Source yang bersifat memvalidasi, rekursif, dan caching DNS resolver dan client akan lebih cepat untuk mengakses website-website.*

Kata Kunci: *Filter, DNS, Unbound.*

[1] *Program Studi Manajemen Informatika, AMIK BSI Jakarta, Jl. Rs. Fatmawati No.24 Pondok Labu, Jakarta , Telp. (021)7500282 email: taufik.tkr@bsi.ac.id*

[2] *Program Studi Teknik Informatika, STMIK Nusa Mandiri Jakarta, Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan email: irfan.virgo84@gmail.com*

PENDAHULUAN

Saat ini informasi dapat diperoleh di dunia maya dalam hal ini internet, baik informasi negatif atau positif. Salah satu nya informasi dapat diakses melalui website dan diakses melalui browser pada perangkat yang digunakan.

Dalam tulisan ini, sistem kontrol klien yang dirancang untuk mencegah pelanggaran pengembangan sistem. Dengan kata lain, terinfeksi file berbahaya pada komputer Anda dengan menggunakan pengembangan berpusat pengguna dan keamanan sistem informasi melalui desain sistem kontrol menggunakan DNS client kontrol firewall akses ke situs acak untuk tindakan untuk mencegah under-teknik pemecahan. Kontrol desain sistem klien diklasifikasikan sebagai intrusi dinamis sistem pencegahan desain modul, desain domain sistem pelayanan nama tertanam modul, Hendak layanan DNS desain modul dan modul desain Cert & Analysis. Akhirnya, melalui simulasi, rata-rata 14% yang diukur dengan rasio paket yang abnormal[2].

Saat ini aplikasi memenuhi beragam kebutuhan tetapi sangat sangat berguna untuk lembaga pendidikan berusaha mewujudkan sistem mobile learning atau bagi perusahaan yang ingin meningkatkan bisnis mereka. Sebuah perusahaan / lembaga yang ingin melakukan penyaringan web, caching, pemantauan pengguna dll dan memungkinkan akses internet hanya setelah otentikasi mungkin menggunakan proxy eksplisit. Ia telah mengamati bahwa sebagian besar aplikasi yang harus terhubung ke Internet melalui proxy eksplisit, tidak bekerja sama sekali. Dalam tulisan ini, solusi telah diusulkan untuk mendapatkan aplikasi bekerja tanpa harus menghindari penggunaan server proxy. Solusi ini dikembangkan sekitar transparent proxy dan memanfaatkan captive portal untuk otentikasi. Oracle VM VirtualBox digunakan untuk mengembangkan test bed untuk percobaan dan pfSense digunakan sebagai firewall yang memiliki kedua server proxy dan layanan captive portal terintegrasi pada platform tunggal. Saat diuji, Windows 8 aplikasi serta aplikasi Ubuntu bekerja dengan baik tanpa mengorbankan layanan server proxy seperti penyaringan web. Solusi yang diusulkan adalah yang berlaku secara luas dan hemat biaya karena menggunakan software open source dan pada dasarnya perangkat keras yang sama

seperti yang digunakan untuk penyebaran proxy yang eksplisit[3].

Bagi banyak orang, mengakses Internet adalah berkat campuran; dalam kasus terburuk, dapat menciptakan masalah serius. Web Content Filtering adalah firewall untuk memblokir situs-situs tertentu dari sedang diakses. penyaringan konten dan produk yang menawarkan layanan ini dapat dibagi menjadi filtering Web, pemutaran situs Web atau halaman, dan e-mail filtering, penyaringan e-mail Keyword spam yang - filter berdasarkan Browser, atau konten yang dilarang lainnya. Makalah ini memberikan sebuah survei termasuk jenis utama, tugas, alat, proses, algoritma yang terlibat dalam penyaringan konten web dan juga menyarankan metodologi baru untuk disaring isi teks di Halaman Web dan membuat algoritma keputusan apakah halaman web diizinkan atau dilarang dari akses[4].

Nama resolusi menggunakan Domain Name System (DNS) adalah integral Internet saat ini. Resolusi nama domain seringkali tergantung pada namespace luar kendali pemilik domain. Dalam artikel ini kami meninjau protokol DNS dan beberapa implementasi server DNS. Berdasarkan pemeriksaan kami, kami mengusulkan model formal untuk menganalisis dependensi nama yang melekat dalam DNS, dan eksperimental memvalidasi model dengan nama domain yang sebenarnya. Dengan menggunakan model nama ketergantungan kita kita peroleh metrik untuk mengukur sejauh mana nama domain mempengaruhi nama domain lainnya. Hal ini ditemukan bahwa dalam kondisi tertentu, lebih dari setengah dari permintaan untuk nama domain dipengaruhi oleh ruang nama tidak tegas dikonfigurasi oleh administrator. Hasil ini berfungsi untuk mengukur tingkat kerentanan DNS karena ketergantungan yang administrator tidak menyadari. Ketika kita menerapkan metrik dari model kami data DNS produksi, kami menunjukkan bahwa kumpulan domain yang resolusi mempengaruhi nama domain yang diberikan jauh lebih kecil dari yang diperkirakan sebelumnya. Namun, perilaku seperti menggunakan alamat cache untuk query server otoritatif dan chaining nama domain alias meningkatkan jumlah dan keragaman domain berpengaruh, sehingga membuat infrastruktur DNS lebih rentan[1].

Tujuan dari penelitian ini adalah untuk menerapkan peraturan dan undang-undang yang di keluarkan oleh pemerintah yaitu penyedia jasa internet wajib mematuhi peraturan memfilter konten atau website agar terwujud internet sehat bagi rakyat indonesia.

BAHAN DAN METODE

PT.Indo Pratama Teleglobal merupakan salah satu vendor infrastruktur VSAT. Dimana VSAT merupakan salah satu perangkat koneksi jaringan skala luas maka PT. Indo Pratama Teleglobal menjadi salah satu Vendor yang melayani barang dan jasa dalam pemasangan atau Instalasi VSAT.

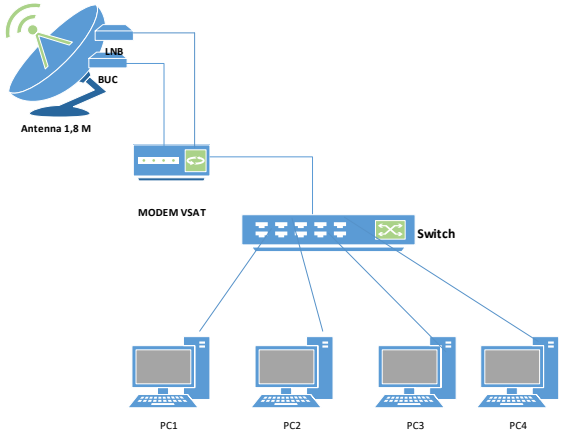
1. Manajemen Jaringan
   a) Topologi Jaringan

Topologi yang di gunakan pada PT. Indo Pratama Teleglobal untuk seluruh client/pelanggan yaitu topologi Star/bintang. Karena semua client / pelanggan terkoneksi melalui HUB Vsat. Setiap client mendapatkan 5 buah Public IP yang dapat digunakan di PC / Server, tetapi umumnya pelanggan yang hanya membutuhkan koneksi internet cukup diberikan Private IP kelas C, sementara proses NAT berada di sisi Modem.

b) Asitektur Jaringan

Arsitektur Jaringan Client atau pelanggan

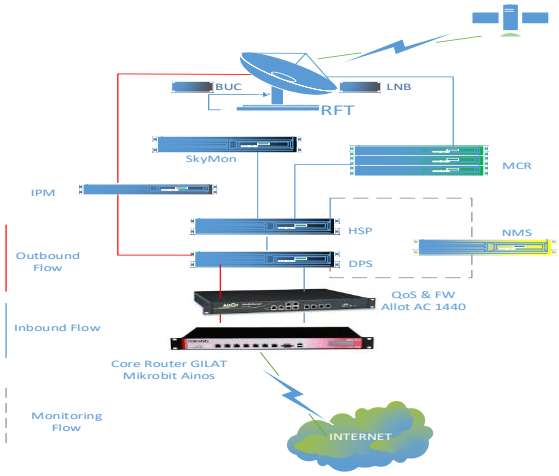
Hasil analisa, client rata-rata menggunakan 4 s/d 10 buah PC , dan sebuah Switch ataupun Router, berikut contoh gambar arsitektur jaringan client yang sudah terintegrasi dengan VSAT.



Gambar 1. Arsitektur jaringan pelanggan

c) Arsitektur jaringan HUB VSAT

Pada sistem jaringan HUB PT.Indo Pratama Teleglobal menggunakan VSAT HUB yang menghubungkan internet dengan client/pelanggan di remote site. Terdapat Core Router GILAT yang berfungsi mengatur alur routing dari dan untuk client/pelanggan. Setelah Router terdapat sebuah perangkat Allot yang berfungsi sebaga Bandwidth management dan Firewall, setelah itu data masuk ke DPS (Data Protocol Server), disini data yang lewat dirubah ke MPEG 2 frames atau disebut Backbone Packets, setelah di rubah ke Backbone Packet, selanjutnya dikonversikan menjadi LBand oleh IPM untuk kemudian di teruskan ke pelanggan melalui satelit.

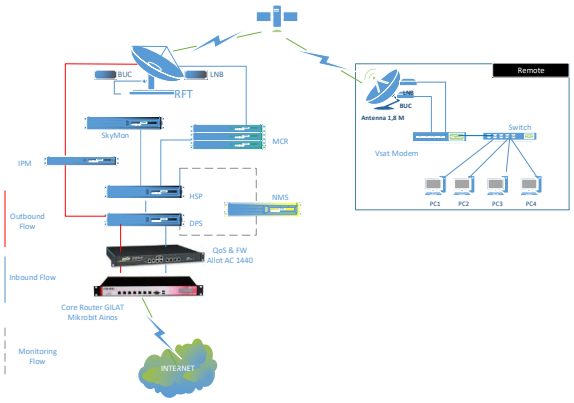


Gambar 2. Arsitektur Jaringan VSAT GILAT PT. indo Pratama Teleglobal

d) Skema Jaringan

Skema Jaringan VSAT Pada PT.Indo Pratama Teleglobal yang terhubung dengan Client/pelanggan.

Berikut adalah contoh gambar skema jaringan Client/ pelanggan yang sudah terinstallasi VSAT dan terkoneksi dengan HUB.



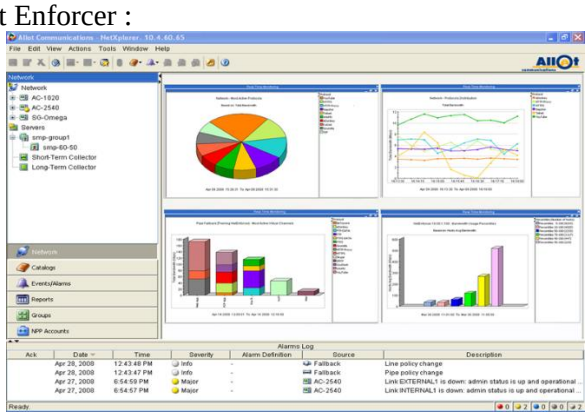
Gambar 3. Skema Jaringan VSAT ke pelanggan

2. Keamanan Jaringan

Berikut sistem keamanan yang diterapkan pada jaringan yang berjalan di sisi HUB yaitu PT.Indo Pratama Teleglobal, di HUB menggunakan sebuah perangkat yaitu Allot Net Enforcer. Dimana fitur Allot Net Enforcer antara lain :

1. Sebagai bandwidth management (Inbound QOS).
2. Pemantauan lalu lintas real-time dan alarm otomatis memungkinkan pemecahan masalah yang cepat dan akurat dengan kemampuan untuk proses Troubleshooting.
3. Sistem perlindungan all-in, dari level IP sampai dengan applikasi.

Contoh report realtime yang diberikan oleh Allot Net Enforcer :



Gambar 4. Report view allot netenforcer

Spesifikasi Hardware dan Software Jaringan

1. Hardware

Adapun beberapa hardware yang di gunakan antara lain:

a. Server

Tabel 1. Spesifikasi Komputer Server

No	HUB	Spesifikasi	Ip Address
1	Server NMS	Xeon QuadCore, Ram 8GB, HD 360 GB(Raid 5 Mode), OS: Windows 2003 Server SP2	172.16.x.x
2.	MRTG-Server	Xeon QuadCore, Ram 4GB, HD 360 GB(Raid 5 Mode) OS: Centos 5.1	202.55.x.x
3.	GILAT Hub Server	DPS,HSP,MCR,IPM Xeon QuadCore, Ram 8GB, HD 360 GB(Raid 5 Mode),	172.16.x.x
4	Bandwidth Management	Allot Netenforce AC-1440, Througput 2 Gbps	172.17.x.x

b. Antena

Tabel 2. Spesifikasi Antena

Antena	Spesifikasi
Client	1,8 meter
Hub	9 meter

c. Switch (Remote Site)

d. Modem GILAT (Remote Site)

Type SkyEdge IP.

Spesifikasi :

1) CPU : Power QUICC 133 Mhz,
2) Memory : Flash 16 MB, DDR2 64MB
3) Services : Support 2 Vlans, and 512 TCP Connection
4) Power Supply : (AC) 90-240V
5) IB Channel Rate : 128 s/d1536 Ksps (Kilo symbol per second)
6) Data Rate : UPLink, upto 1,2 Mbps, DownLink upto 7.5 Mbps

e. Perangkat Lunak (Software)

Perangkat lunak (software) yang digunakan pada HUB GILAT, terdiri dari sistrem operasi, dan juga perangkat lunak pendukung lainnya yang digunakan seperti:

a. Linux Distro Centos 6.7
b. SO server
   1.) Windows server 2003
c. SO NMS-Client
   1.) Windows XP

HASIL DAN PEMBAHASAN

Dari hasil analisa yang lakukan, terdapat beberapa kendala dalam pemberian data atau penyebaran internet ke planggan, yaitu:

a. Banyaknya alert atau event di NMS server karena dos-attack yang menyebabkan untuk access browsing jadi lambat dan tidak stabil.

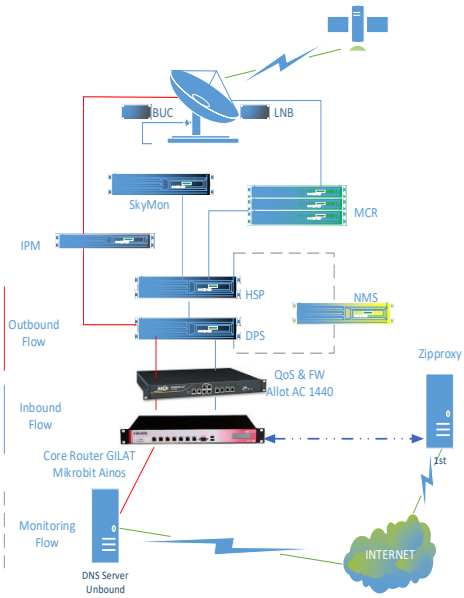
Gambar 5. Terdeteksi Virus yang broadcast sisi pelanggan

b. Dengan banyak website-website yang menggandung unsur pornografi dan website-website yang di anggap berbahaya baik untuk user sendiri atau dalam segi keamanan jaringan vsat.

3. Manajemen Jaringan implemen

a) Topologi Jaringan

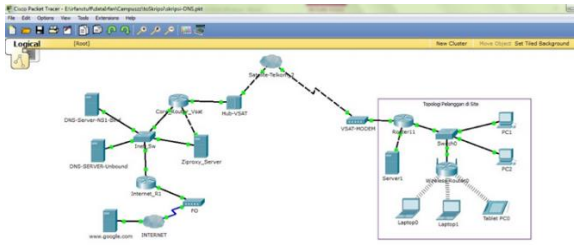
Topologi jaringan pada sistem implemen ini sama seperti pada sistem yang digunakan pada sistem jaringan berjalan, hanya disini menambahkan sebuah applikasi DNS Filtering dengan Unbound, yang diinstall di sebuah server.



Gambar 6. Topologi jaringan VSAT dengan DNS Server Unbound

b) Skema Jaringan

Berdasarkan topologi yang coba usulkan, maka mencoba menggambarkan implemen tersebut menggunakan Cisco Packet Tracer versi 6.0.1.0011. Dengan Software ini mencoba memberikan gambaran mengenai koneksi jaringan yang akan diimplementasikan di PT.Indo Pratama Teleglobal. Namun ada sedikit perbedaan mengenai device yang disediakan oleh Cisco Packet Tracer ini, dimana tidak adanya device Modem Vsat, dan Satelite. Sebagai gantinya mencoba menggambarkan koneksi Vsat dengan WAN Emulation, untuk modem vsat menggantinya dengan modem adsl. Dan berikut adalah konfigurasi jaringan implemen menggunakan software Cisco Packet Tracer:

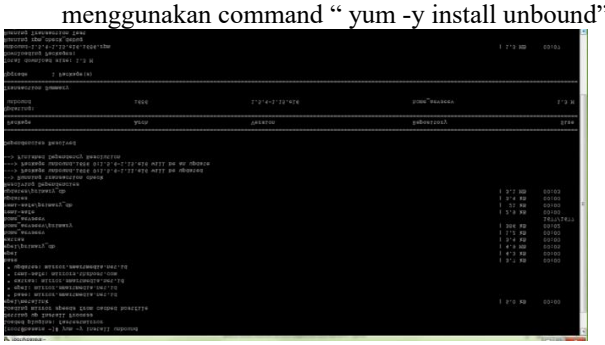


Gambar 7. Skema Jaringan VSAT Simulasi

Untuk DNS Unbound, diinstal pada OS Linux Centos Server 6.7. DNS Unbound adalah adalah memvalidasi, rekursif, dan caching DNS resolver. awalnya dikembangkan di C berdasarkan dari prototipe Java. Kode sumber menjadi sangat modular dalam desain, dan menjadi sangat ringan. Merancang sebuah solusi yang akan menjadi sekecil mungkin yang akan mencapai persyaratan minimal sebagai validator, resolver, dan server caching. Selain memenuhi persyaratan ini, mereka ingin server untuk mencapai kinerja tinggi sangat.

Berikut adalah tahapan proses installasi unbound pada Centos 6.7 :

1. Install Centos Server, ikuti panduan yang ada di website: lhttp://jurnalinux.blogspot.co.id/2013/12/step-by-step-install-centos-64.html
2. Install package Unbound dengan menggunakan command " yum -y install unbound"



Gambar 8. Instalasi paket unbound

3. Edit file konfigurasinya bisa menggunakan nano atau text editor lainnya (default file nya ada di /etc/unbound/unbound.conf), dan berikut adalah konfigurasi yang gunakan.

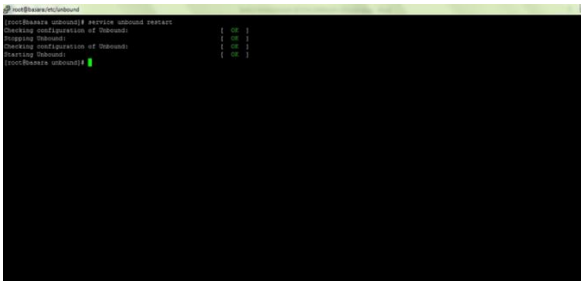
```
server:
        verbosity: 1
        statistics-interval: 120
        num-threads: 2
        interface: 0.0.0.0
        outgoing-range: 512
        num-queries-per-thread: 1024
        msg-cache-size: 32m
        rrset-cache-size: 64m
        msg-cache-slabs: 4
        rrset-cache-slabs: 4
        cache-max-ttl: 86400
        infra-host-ttl: 60
        infra-lame-ttl: 120
        infra-cache-numhosts: 10000
        infra-cache-lame-size: 10k
            # root key file, automatically updated
            #auto-trust-anchor-file: "/etc/unbound/root.key"
        do-ip4: yes
        do-ip6: no
        do-udp: yes
        do-tcp: yes
        do-daemonize: yes
        access-control: 0.0.0.0/0 allow
        #access-control: 192.168.0.0/16 allow
        #access-control: 172.16.0.0/12 allow
        #access-control: 10.0.0.0/8 allow
        #access-control: 127.0.0.0/8 allow
        #access-control: 0.0.0.0/0 refuse
            include: /etc/unbound/block.conf
```

```
        chroot: "/etc/unbound"
        username: "unbound"
        directory: "/etc/unbound"
        #logfile: "/var/log/unbound.log"
        logfile: ""
        use-syslog: no
        #pidfile: "/etc/unbound/unbound.pid"
        root-hints: "/etc/unbound/named.cache"
      identity: "DNS"
        version: "1.4"
        hide-identity: yes
        hide-version: yes
        harden-glue: yes
        do-not-query-address: 127.0.0.1/8
        do-not-query-localhost: yes
        module-config: "iterator"
      forward-zone:
      name: "."
          forward-addr: 202.55.169.200
          forward-addr: 202.55.172.7
      forward-addr: 8.8.8.8
    remote-control:
      control-enable: yes
      control-interface: 127.0.0.1
      control-interface: 202.55.172.19
          control-port: 953
      server-key-file: "/etc/unbound/unbound_server.key"
      server-cert-file: "/etc/unbound/unbound_server.pem"
      control-key-file: "/etc/unbound/unbound_control.key"
      control-cert-file: "/etc/unbound/unbound_control.pem"
```

4. File block.conf, bisa kita gunakan untuk memblock suatu websites, email dan iklan-iklan di website, berikut configureasi yang gunakan.

```
local-zone: "website.com" redirect
local-data: "website.com A 202.55.172.19"
local-data: "example.com. 3600 IN MX 5 127.0.0.1"
local-data: "example.com. 3600 IN A 127.0.0.1"
```

5. Lalu restart unbond dengan command "service unbound restart".



Gambar 9. restart service unbound

4. Keamanan Jaringan

Keamanan jaringan implemen tetap sama seperti pada sistem keamanan yang berjalan sekarang yaitu dengan menggunakan perangkat Allot Net-enforcer.

a) Pengujian Jaringan

Pengujian jaringan awal dilakukan dengan melakukan test koneksi internet menggunakan dengan jaringan Vsat existing. Awalnya sendiri melakukan pengujian dengan 1 buah Laptop. Dan melakukan test browsing ke beberapa alamat situs di internet yang di anggap tidak baik dan mengadung unsur sara, perjudian kekerasan atau pembajakan hak cipta dan website-website yang biasa di gunakan oleh user apakah bernasalah, antara lain :

1. http://www.google.com
2. http://www.22sinema.com
3. http://www.liputan6.com

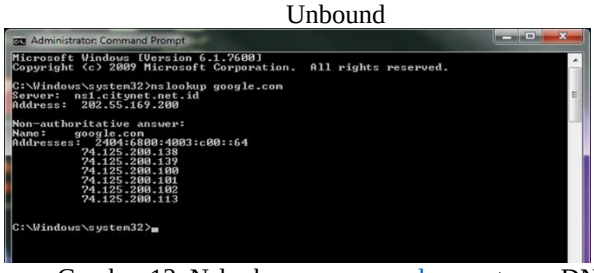
Berikut sample yang dapatkan selama pengujian jaringan awal dengan menggunakan 1 buah Laptop pada jaringan vsat, ke 5 alamat url diatas, sample yang diambil antara lain :

1. Test browsing ke website-website tersebut.
2. Nslookup website-website tersebut.

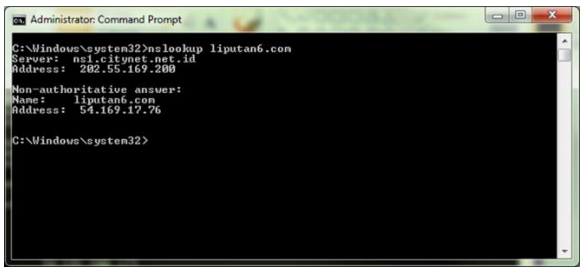
Gambar 10. Akses www.google.com tanpa DNS Unbound

Gambar 11. Akses www.22sinema.com tanpa DNS Unbound

Gambar 12. Browsing www.liputan6.com tanpa DNS Unbound



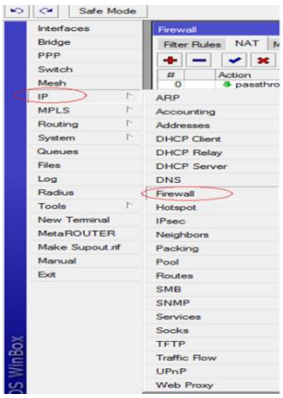
Gambar 13. Nslookup www.google.com tanpa DNS Unbound



Gambar 14. Nslookup www.lipitan6.com tanpa DNS Unbound

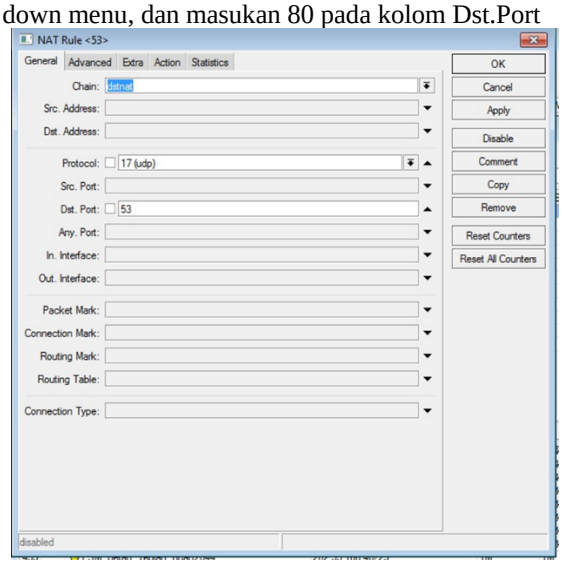
Pada Pengujian jaringan akhir ini dilakukan dengan melakukan percobaan menggunakan Unbound, dengan jaringan VSAT. Dalam tahap ini langsung melakukan perubahan rule didalam Core Router Gilat (Mikrobits Ainos), dengan meredirect semua traffic DNS dari semua remote Vsat yang Online ke Unbound DNS Server, caranya adalah sebagai berikut :

1. Setelah login sebagai admin pada mikrobits, lalu masuk ke menu ip > firewall.



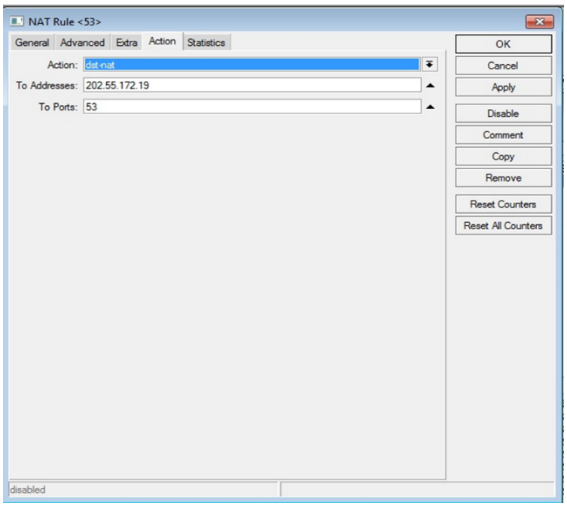
Gambar 15. Tampilan Winbox IP Firewall

2. Lalu klik Tab NAT, lalu add new
3. Pada TAB General, bagian Chain pilih dstnat dari drop down menu, lalu pada bagian Protocol pilih tcp dari drop down menu, dan masukan 80 pada kolom Dst.Port



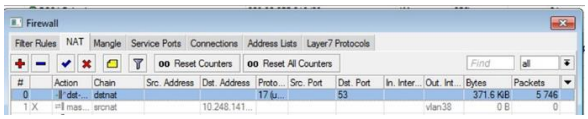
Gambar 16. Add rule nat, chain protocol dan dst port

4. Lalu pilih Tab Action, pilih dst-nat dari drop down menu pada kolom Action, lalu masukan IP server unbound pada kolom To.Addressess, dan masukan Unbound port pada kolom To.Ports.



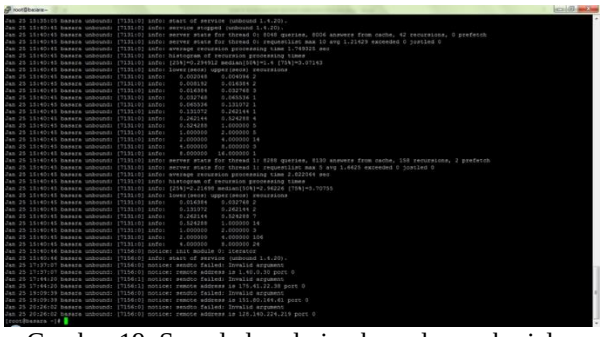
Gambar 17. add rule nat action

5. Klik Apply lalu OK, kemudian cek Bytes Counter dan Packets Counter, jika rule tersebut berjalan maka nilai counter akan bertambah.

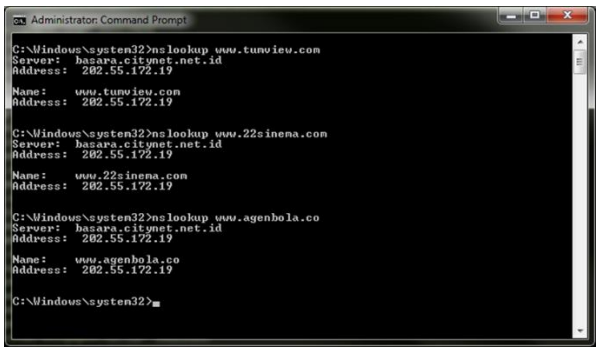


Gambar 18. nat rule packet counter dns unbound

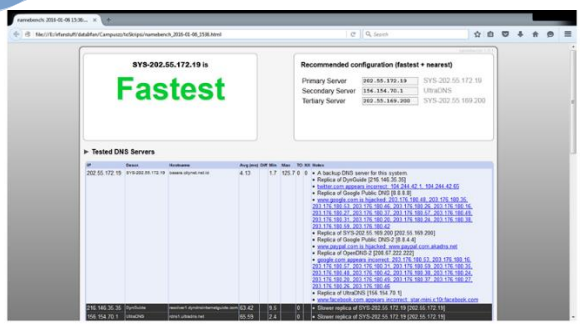
Untuk memastikan apakah data tersebut memang sudah melalui Unbound, melakukan analisa log yang berjalan dari unbound.



Gambar 19. Sample log dari unbound yang berjalan



Gambar 20. Nslookup ke website yang di filter pada Unbound

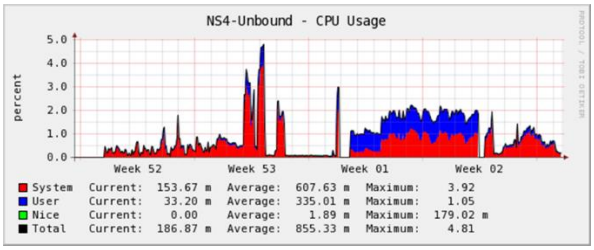


Gambar 21. Tes DNS Unbound dengan aplikasi namebench-1.3.1-windows

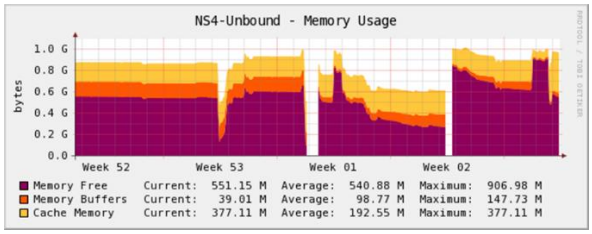
Gambar 22. Browsing ke website yang difilter Unbound

Dari gambar log diatas terlihat bahwa traffic untuk DNS sudah melalui unbound ,dan ketiga gambar selanjutnya menunjukan test untuk server unboun baik dengan aplikasi, nslookup dan mencoba browsing ke website-website yang di anggap tidak baik untuk customer dan jaringan vsat, setelah di implementasikannya ziproxy.

Dan berikut adalah memory dan CPU usage dari server Ziproxy tersebut.



Gambar 23. Utilisasi CPU Server Unbound



Gambar 24. Utilisasi memori (RAM server Unbound

KESIMPULAN

Dengan adanya peraturan dan undang-undang yang di keluarkan oleh pemerintah maka PT.Indo Pratama Teleglobal sebagai penyedia jasa internet wajib mematuhi peraturan yang ada. Ada banyak metode yang bisa di applikasikan untuk melakukan filtering website-website yang dianggap mengandung unsur-unsur pornografi, judi, Phising, dan Sara. Salah satunya menggunakan software Unbound. Setelah melakukan implementasi Unbound pada jaringan Vsat PT.Indo Pratama Teleglobal dapat menyimpulkan bahwa penggunaan unbound untuk filtering website-website yang di anggap berbahaya baik untuk jaringan di client dan jaringan di sisi vsat, dari sisi client tidak memerlukan konfigurasi khusus untuk menggunakan fasilitas unbound, karena semua paket yang direquest oleh client, otomatis akan diredirect oleh Router Mikrobits dengan menggunakan rule nat, unbound sendiri adalah sebuah software Open Source yang bersifat memvalidasi, rekursif, dan caching DNS resolver dan client akan lebih cepat untuk mengakses website-website.

REFERENSI

[1] Deccio, C., Sedayao, J., Kant, K., & Mohapatra, P. (2012, February 27). Quantifying DNS Namespace Influence. *Computer Networks*, *56*(2), 780-794. Diambil kembali dari http://dx.doi.org/10.1016/j.comnet.2011.11.005

[2] Kim, B.-H., & Park, Y.-G. (2013). Design and Analysis of Client Control System Using DNS Control Firewall. *International Journal of Smart Home*, *7*(5), 135-144.

[3] Sharma, P., & Benith, T. (2014). Design and Configuration of App Supportive Indirect Internet Access using a Transparent Proxy Server. *International Journal Of Modern Engineering Research (IJMER)*, *4*(10), 9-17.

[4] V.K.T.Karthikeyan. (2014). Web Content Filtering Techniques: A Survey. *International Journal of Computer Science & Engineering Technology (IJCSET)*, *5*(03), 203-208.

BIODATA PENULIS

Taufik Rahman, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informasi STMIK Nusa Mandiri Jakarta, lulus tahun 2008. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta, lulus tahun 2011. Saat ini menjadi Dosen di AMIK BSI Jakarta dan staff BTI network admin.