

OTOMATISASI PEMBAHARUAN IP PADA DOMAIN ITICMALANG.NO-IP.ORG UNTUK AKASES GATEWAY DI PT.INDONESIAN TOBACCO

Achmad Rony Syafrudin, Antonius Duty Susilo, Mahmud Yunus

Program Studi Teknik Informatika
STMIK PPKIA Pradnya Paramita Malang
Jl. Laksda Adi Sucipto 249 A, Malang
ronyachmad91@gmail.com

ABSTRACT

The need for access to data across the network has now become one of the primary needs PT. Indonesian Tobacco. Purposes of data access can be realized if the company has a public IP functioned to access internal applications, vpn and cctv. The problem occurs because the public IP obtained from the internet provider is dynamic (always changing) so the impact on the configuration of the client-side gateway. the method that implemented is to change the public IP address to a fixed domain, the domain used is a domain that is free with no-ip.org with address iticmalang.no-ip.org. Configuration is configured in the router includes a domain update script and scheduler, if the public IP changes and scheduler are met then the router will request to change the IP domain domain with a public IP configured on the router

Key words : mikrotic, CCTV, VPN, domain, gateway

PENDAHULUAN

Komunikasi lintas jaringan dewasa ini telah menjadi kebutuhan primer, penggunaannya tidak sebatas pada korporasi di bidang IT, industri manufaktur juga mulai memanfaatkan teknologi ini untuk mendukung operasional, salah satunya adalah PT. Indonesian Tobacco. Penggunaan intens aplikasi internal serta kebutuhan akses data perusahaan, ditambah dengan tingginya mobilitas karyawan yang menggunakan aplikasi dan data tersebut, implementasi VPN (*Virtual Private Network*) merupakan salah satu solusi yang efektif untuk PT. Indonesian Tobacco.

PT. Indonesia Tobacco membutuhkan sebuah IP publik untuk keperluan akses

aplikasi internal, VPN dan CCTV (*Closed Circuit Television*) yang dapat di akses oleh klien dimanapun. PT. Indonesia Tobacco menggunakan layanan ISP (*Internet Service Provider*) yang menyediakan satu IP publik, tetapi IP publik yang diberikan oleh ISP bersifat dinamis dimana akan mempengaruhi terhadap layanan VPN dan CCTV, dimana IP CCTV dan VPN akan berubah mengikuti IP Publik dari provider.

VPN dan CCTV dapat diakses oleh user dengan cara mengeset IP gateway pada device mereka. Hal ini tentu merepotkan user yang harus melakukan konfigurasi ulang. Diperlukan sebuah mekanisme untuk merubah agar IP publik yang berubah tersebut dapat diakses secara mudah. Solusinya merubah IP

publik menjadi domain yang bersifat statis. Penelitian ini menerapkan metode **"Otomatisasi Pembaharuan IP Pada Domain Iticmalang.no-ip.org Untuk Akses Gateway di PT. Indonesian Tobacco"** guna menangani terjadinya perubahan IP Publik secara dinamis yang digunakan sebagai gateway VPN dan CCTV di jaringan internal PT. Indonesian Tobacco

Rumusan Masalah

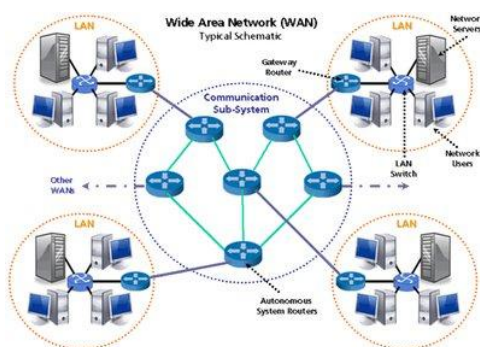
Berdasarkan latar belakang yang telah dijelaskan pada sub bab 1.1, dapat dirumuskan permasalahan sebagai berikut, Bagaimana membangun mekanisme pemetaan alamat IP dinamis menjadi fixed address.

Tujuan Penelitian

Susunan ini bertujuan untuk Membangun mekanisme pemetaan alamat IP menjadi fixed address sehingga konfigurasi pada perangkat user tidak berdasarkan alamat IP.

LANDASAN TEORI

WAN (Wide Area Network)



Gambar 1 Simulasi jaringan WAN

WAN (Wide Area Network) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan

komputer yang membutuhkan router dan saluran komunikasi publik. Internet merupakan contoh dari jaringan WAN ini. Jika Wide Area Network sudah mencakup area intercontinental maka disebut jaringan informasi global atau internet. (Stiawan, Deris, 2009)

Disamping pengiriman paket secara datagram, dalam jaringan IP juga dikenal pengiriman paket secara connection oriented dimana sebelum paket dikirim, dilakukan setup koneksi logika dari tempat asal ke tujuan oleh proses packet control dengan request logical connection agar paket suatu informasi menempuh rute yang sama. Mode koneksi ini disebut virtual circuit, tetapi tidak seperti pada jaringan circuit switched yang menduduki kanal (bandwidth/resources) secara monopoli, dalam virtual circuit penggunaan resources masih dalam pola sharing. Dengan cara demikian urutan paket bisa dijamin, tetapi tingkat kontinuitas real time tidak dijamin, sangat bergantung pada kapasitas dan tingkat kepadatan trafik dalam jaringan. Dengan mode virtual circuit ini memungkinkan suatu kelompok organisasi/perusahaan memiliki jaringan privat (semacam jaringan PBX) secara virtual (disebut IP VPN / Virtual Private Network), atau semacam jaringan PBX (Private Branch Exchange) tetapi lingkup area tidak terbatas seperti PABX karena jaringan yang dibangun dalam IP VPN bukan secara fisik melainkan secara logika dan pembentukan jaringan hanya saat diperlukan saja sehingga lingkup jaringan pribadi IP VPN dapat mencakup area nasional bahkan internasional.

Jaringan berbasis packet switched lain yang banyak dikembangkan di AS adalah jaringan ATM (Asynchronous Transfer Mode). Perbedaannya dengan jaringan IP, bahwa pada jaringan ATM mode koneksi secara keseluruhan menggunakan virtual circuit, sedangkan pada jaringan IP, virtual circuit hanya bersifat option. Perbedaan lain, paket pada jaringan ATM disebut cell selalu tetap yakni 53 oktet (Byte) yang terdiri dari 48 oktet payload, 5 oktet header. Sedangkan dalam jaringan IP, ukuran paket tidak tetap.

Teknologi ATM banyak dikembangkan di Amerika Serikat (tidak dibahas disini). Satu hal lagi, bahwa jaringan ATM dirancang berbasis layanan broadband dan dapat mengakomodasi layanan VBR (Variable Bit Rate) selain CBR (Constant Bit Rate). Sedangkan rancangan awal jaringan IP berbasis Narrow Band dan layanan CBR. (Stiawan, Deris 2009)

Router

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu Local Area Network (LAN). (Muslim, Much Aziz, 2007)

Sebagai ilustrasi perbedaan fungsi dari router dan switch merupakan suatu jalanan, dan router merupakan penghubung antar jalan. Masing-masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu. Dengan cara yang sama, switch menghubungkan berbagai macam alat, dimana masing-masing alat memiliki alamat IP sendiri pada sebuah LAN

Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan IP Router. Selain IP Router, ada lagi AppleTalk Router, dan masih ada beberapa jenis router lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP.

Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa subnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda (seperti halnya router wireless yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel UTP), atau berbeda arsitektur jaringan, seperti halnya dari Ethernet ke Token Ring.

Router juga dapat digunakan untuk menghubungkan LAN ke sebuah layanan telekomunikasi seperti halnya telekomunikasi

leased line atau Digital Subscriber Line (DSL). Router yang digunakan untuk menghubungkan LAN ke sebuah koneksi leased line seperti T1, atau T3, sering disebut sebagai access server. Sementara itu, router yang digunakan untuk menghubungkan jaringan lokal ke sebuah koneksi DSL disebut juga dengan DSL router. Router-router jenis tersebut umumnya memiliki fungsi firewall untuk melakukan penapisan paket berdasarkan alamat sumber dan alamat tujuan paket tersebut, meski beberapa router tidak memilikinya. Router yang memiliki fitur penapisan paket disebut juga dengan packet-filtering router. Router umumnya memblokir lalu lintas data yang dipancarkan secara broadcast sehingga dapat mencegah adanya broadcast storm yang mampu memperlambat kinerja jaringan. (Muslim, Much Aziz, 2007)

Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang digunakan untuk memfungsikan komputer sebagai *router*. *PC router* tersebut dilengkapi dengan berbagai fasilitas dan alat, baik untuk jaringan kabel maupun nirkabel. Mikrotik sekarang ini banyak digunakan oleh ISP, *penyedia hotspot*, ataupun oleh pemilik warnet. Pada standar perangkat keras berbasis *Personal Computer (PC)* mikrotik dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses *route* atau lebih dikenal dengan istilah *routing*. Sedangkan aplikasi yang

dapat diterapkan dengan Mikrotik selain *routing* adalah aplikasi kapasitas akses (*bandwidth*), manajemen, *firewall*, *wireless access point (WiFi)*, *backhaul link*, *sistem hotspot*, *Virtual Private Network (VPN) server* dan masih banyak lainnya. (Saputro, Daniel T, Kustanto. 2008. Membangun Server Internet dengan Mikrotik OS. Gava Media: Yogyakarta)

➤ Jenis – jenis mikrotik

- a. MikroTik RouterOS yang berbentuk software. Dapat diinstal pada komputern rumah (PC).
- b. *BUILT-IN* Hardware MikroTik. Dalam bentuk perangkat keras yang khusus dikemas dalam board router, yang didalamnya sudah terinstal MikroTik RouterOS.

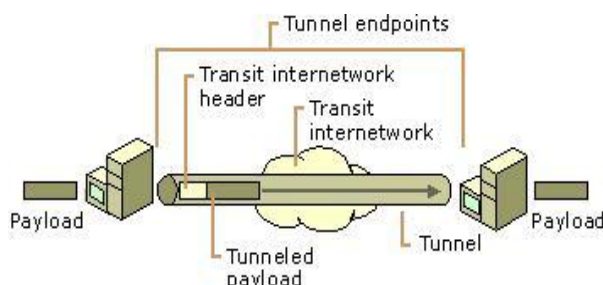
VPN (Virtual Private Network)

VPN adalah sebuah jaringan komputer dimana koneksi antar perangkatnya (node) memanfaatkan jaringan public sehingga yang diperlukan hanyalah koneksi internet di masing-masing site. Ketika mengimplementasikan VPN, interkoneksi antar node akan memiliki jalur virtual khusus di atas jaringan public yang sifatnya independen. Metode ini biasanya digunakan untuk membuat komunikasi yang bersifat secure, seperti system ticketing online dengan database server terpusat



Gambar 2 VPN melewati jaringan publik Internet

VPN merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang, *telecommuters*, *suppliers*, dan rekan bisnis lainnya, ke dalam suatu jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode enkripsi tertentu sebagai media pengamanannya (Kevin, 2001). VPN merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan *public* seperti Internet. Data yang dilewatkan akan dienkapsulasi (*encapsulation*) (*dibungkus*) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya.



Gambar .3 Tunneling VPN di Interkoneksi Jaringan

Tunneling adalah salah satu metode yang digunakan untuk mentransfer data melewati infrastruktur interkoneksi jaringan dari satu jaringan ke jaringan lainnya seperti jaringan internet, data yang ditransfer (*payload*) dapat berupa frames (atau paket) dari protokol yang lain. Tunnel menggambarkan paket data secara logika yang

di *encapsulation* (*dibungkus*) melewati interkoneksi jaringan. Proses tunnelingnya meliputi proses *encapsulations*, transmisi, dan *decapsulations* paket. (Microsoft, VPN with windows 2003, 2003 : 9)

Peningkatan penggunaan koneksi VPN dari tahun ke tahun karena mudahnya infrastruktur yang dibutuhkan oleh VPN serta mudahnya dalam instalasi, maka koneksi ini lebih efisien dibandingkan dengan metode WAN. Jaringan VPN dikoneksikan oleh ISP lewat *router*nya ke *router-router* lain dengan menggunakan jalur Internet yang telah dienkripsi antara dua titik, dengan menggunakan *leased line* untuk hubungan jarak jauh dengan VPN, perusahaan dapat menghemat 20 sampai 40% dari biaya WAN.

➤ Jenis-jenis VPN

- a. **Access VPN** : membuat koneksi jarak jauh untuk mengakses ke jaringan intranet atau ekstranet pelanggan dan pengguna bergerak dengan menggunakan infrastruktur PSTN dial-up, ISDN, DSL, atau Mobile IP untuk membuat koneksi yang aman bagi mobile user, telecommuters dan kantor cabang.
- b. **Intranet VPN** : menghubungkan kantor pusat, kantor cabang, dan remote user ke dalam jaringan internal dengan menggunakan infrastruktur koneksi Dedicated
- c. **Extranet VPN** : menghubungkan dengan pihak luar seperti pelanggan, supplier, rekan bisnis, atau suatu komunitas ke dalam jaringan internal dengan menggunakan koneksi *dedicated*. Koneksi

ini menghubungkan jaringan internal dengan jaringan di luar perusahaan. Sistem keamanan di VPN menggunakan beberapa metode lapisan sistem keamanan, diantaranya ;

- a. **Metode tunneling** (terowongan), membuat terowongan virtual diatas jaringan publik menggunakan protocol seperti *Point to Point Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Generic Routing Encapsulation* (GRE) atau *IP Sec*. PPTP dan L2TP adalah layer 2 tunneling protocol. keduanya melakukan pembungkusan payload pada frame *Point to Point Protocol* untuk di lewatkan pada jaringan. IP Sec berada di layer 3 yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.
- b. **Metode Enkrpsi** untuk *Encapsulations* (membungkus) paket data yang lewat di dalam tunneling, data yang dilewatkan pada pembungkusan tersebut, data disini akan dirubah dengan metode algoritma kriptography tertentu seperti DES, 3DES, atau AES
- c. **Metode Otentikasi User**, karena banyak user yang akan mengakses biasanya digunakan beberapa metode otentikasi user seperti *Remote Access Dial In User Services* (RADIUS) dan *Digital Certificates*.
- d. **Integritas Data**, paket data yang dilewatkan di jaringan publik perlu penjaminan integritas data / kepercayaan data apakah terjadi perubahan atau tidak.

Metode VPN menggunakan HMA C-MD5 atau HMA C-SHA1 untuk menjadi paket tidak dirubah pada saat pengiriman

CCTV (*Closed Circuit Televison*)

CCTV adalah alat perekam yang menggunakan satu atau lebih kamera video dan menghasilkan data video ataupun audio. Standard TV mengirimkan sinyal broadcast secara terbuka. Sedangkan cara kerja kamera CCTV yaitu mengirimkan sinyal secara tertutup lewat melalui wireless ataupun kabel. (www.jurnas.com/halaman/5/2012-03-19/202810, hal5)

Prinsip kerja CCTV tidak jauh berbeda dengan kamera video. Hanya saja CCTV lebih cenderung digunakan dengan alasan keamanan suatu tempat dan membantu mengurangi tingkat kejahatan. Saat ini sudah banyak tempat umum menggunakan prinsip kerja CCTV. Hal ini dikarenakan harga kamera CCTV tidaklah terlalu mahal dan harga pengoperasiannya dapat disesuaikan oleh keuangan masing-masing pemilik. Yang paling berbeda adalah bentuk kamera CCTV yang kecil dan dipasang diatas atap atau menempel ditembok. Perbedaan dari kamera video, kamera CCTV lebih sering menangkap gambar dengan kecepatan rendah sekitar 15fps (frame per second). Ada beberapa CCTV yang dapat bergerak kekanan,kekiri, keatas, atau kebawah dan bahkan digerakkan lewat jarak jauh.

Kabel yang digunakan untuk CCTV biasanya adalah kabel coaxial yang sering digunakan oleh TV analog untuk menangkap sinyal broadcast dari antenna TV. Sedangkan

jika menggunakan sinyal wireless menggunakan frekuensi 2.4 Gigahertz. CCTV biasanya digunakan untuk mengawasi sebuah tempat berkaitan dengan masalah keamanan ataupun kerahasiaan tempat, misalnya digunakan di toko, bank, ataupun tempat publik yang ramai.

Cara penyimpanan video bisa menggunakan dua metode penyimpanan. Tape adalah media penyimpanan yang paling mudah dan hemat. Kemudian metode lainnya adalah dengan menggunakan DVR (Digital Video Recorders). DVR dibagi menjadi stand-alone DVR yaitu DVR yang mempunyai kamera dan tempat penyimpanan sendiri. Sedangkan yang lainnya yaitu PC-based DVR yang media penyimpanannya disambungkan ke sistem komputer.

Pentaplex CCTV yaitu cara kerja kamera CCTV yang dapat melakukan 5 aktivitas seperti siaran langsung, menyimpan, playback / akses lihat data video sebelumnya, backup / penyimpanan video lama, dan terhubung langsung jaringan komputer sehingga mudah diakses. (Agung, I Putu Suhada, 2009).

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini terdiri dari beberapa tahap, yaitu :

- a. Studi literatur.
Mengumpulkan informasi dan referensi serta mempelajari tentang konsep jaringan , *scripting* mikrotik dan *dynamic IP* publik.
- b. Analisis dan perancangan sistem.

Melakukan analisis pada konfigurasi jaringan WAN yang terkonfigurasi IP publik dinamis di PT. Indonesian Tobacco dan merancang metode untuk akses gateway jaringan internal dengan kondisi IP publik yang bersifat dinamis dengan memanfaatkan domain.

- c. Implementasi sistem.
Menerapkan metode dengan merubah IP publik dinamis menjadi *fixed address domain*. Konfigurasi dilakukan di router dengan mengeksekusi script yang mengecek perubahan ip publik dan merubah ip domain sesuai dengan ip publik yang terkonfigurasi di router. Domain tersebut digunakan sebagai *gateway user* untuk akses jaringan internal.
- d. Pengambilan data dan analisis hasil pengukuran.
Menjalankan metode dengan rebooting router dan pergantian ip otomatis dari *provider* dan mengukur tingkat keberhasilan metode dalam merubah ip domain dengan ip yang terkonfigurasi di router
- e. Penarikan kesimpulan
Dari hasil analisis dari tahap sebelumnya ditarik kesimpulan mengenai merubah ip publik dinamis ke bentuk *domain* untuk akses *gateway user* ke jaringan internal.

HASIL DAN PEMBAHASAN

Perancangan Uji Coba Sistem

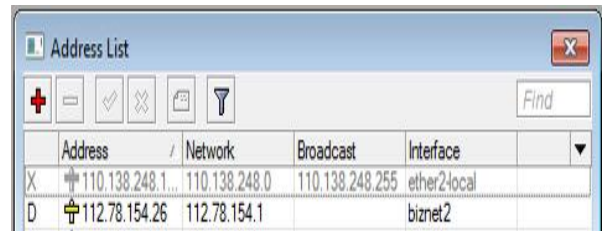
Metode ini dikonfigurasi pada router yang terhubung ke internet. *Script* update IP yang terdapat pada router akan di lakukan proses eksekusi secara terjadwal oleh *scheduler* di router setiap 5 menit.

Pada pengujian metode ini jika terjadi perubahan IP publik pada router dan proses scheduler telah mencapai interval waktunya, maka router akan melakukan eksekusi script yang meminta ke no-ip.org untuk merubah IP domain iticmalang.no-ip.org yang lama dengan IP domain yang baru.

Pada tahap pengujian ini dilakukan dengan cara melakukan *rebooting* router selama 8 kali dan menunggu proses pergantian IP publik secara otomatis dari provider sebanyak 2 kali, selanjutnya akan diuji tingkat kesuksesan dalam *update* konfigurasi IP pada domain iticmalang.no-ip.org. Pengujian lain yang dilakukan adalah membuka aplikasi internal dengan domain iticmalang.no-ip.org:887 serta melakukan akses VPN ke router.

Pengujian Sistem

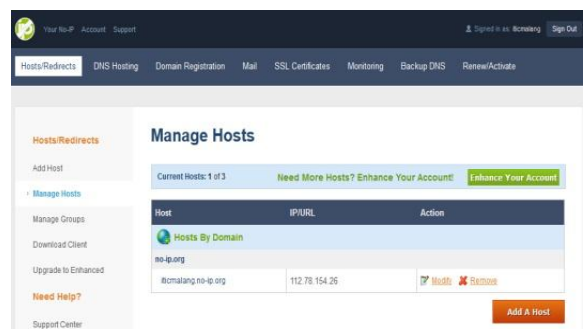
Pengujian Pada Router Dengan Melakukan *Rebooting*



| | Address | Network | Broadcast | Interface |
|---|------------------|---------------|-----------------|-------------|
| X | 110.138.248.1... | 110.138.248.0 | 110.138.248.255 | ether2local |
| D | 112.78.154.26 | 112.78.154.1 | | biznet2 |

Gambar 4 IP publik sebelum berubah.

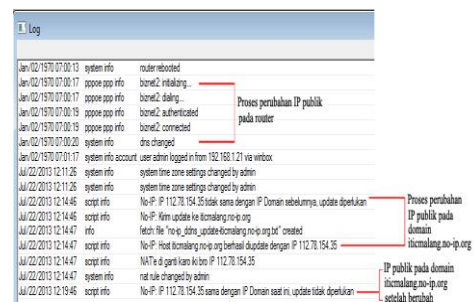
IP publik yang terdapat pada router yang dikonfigurasi pada interface biznet2 sebelum terjadi perubahan IP publik .



| Host | IP/URL | Action |
|----------------------|---------------|--------------------|
| iticmalang.no-ip.org | 112.78.154.26 | [Refresh] [Delete] |

Gambar 5 IP pada domain sebelum berubah

IP publik yang dikonfigurasi pada domain iticmalang.no-ip.org, sebelum terjadi perubahan IP domain



| Time | Message |
|----------------------|---|
| Jan/02/1970 07:00:13 | system info router rebooted |
| Jan/02/1970 07:00:17 | pppoe ppp info bond2: initiating... |
| Jan/02/1970 07:00:17 | pppoe ppp info bond2: dialing... |
| Jan/02/1970 07:00:19 | pppoe ppp info bond2: authenticated |
| Jan/02/1970 07:00:19 | pppoe ppp info bond2: connected |
| Jan/02/1970 07:00:20 | system info dns changed |
| Jan/02/1970 07:01:17 | system info user admin logged in from 192.168.1.21 via winbox |
| Jan/22/2013 12:11:25 | system info system time zone settings changed by admin |
| Jul/22/2013 12:14:46 | script info No-IP: IP 112.78.154.35 tidak sama dengan IP Domain sebelumnya, update diperlukan |
| Jul/22/2013 12:14:46 | script info No-IP: Form update ke iticmalang.no-ip.org |
| Jul/22/2013 12:14:47 | info No-IP: Host 'iticmalang.no-ip.org' created |
| Jul/22/2013 12:14:47 | script info No-IP: Host iticmalang.no-ip.org berhasil diupdate dengan IP 112.78.154.35 |
| Jul/22/2013 12:14:47 | script info NAT's di ganti kea kea IP 112.78.154.35 |
| Jul/22/2013 12:14:47 | system info nat rule changed by admin |
| Jul/22/2013 12:14:46 | script info No-IP: IP 112.78.154.35 sama dengan IP Domain saat ini, update tidak diperlukan |

Gambar 6 log pada mikrotik

Proses terjadinya perubahan IP publik dan proses perubahan ip domain dapat diketahui melalui logs router, pada gambar 4.3 dijelaskan proses terjadinya perubahan IP public dan proses perubahan IP publik pada domain iticmalang.no-ip.org

| | Address | Network | Broadcast | Interface |
|---|------------------|---------------|-----------------|--------------|
| X | 110.138.248.1... | 110.138.248.0 | 110.138.248.255 | ether2-local |
| X | 112.78.154.34 | 112.78.154.1 | 112.78.154.1 | ether1-WAN |
| D | 112.78.154.35 | 112.78.154.1 | | biznet2 |

Gambar 7 IP publik setelah berubah

IP publik yang terdapat pada router yang dikonfigurasi pada interface biznet2 setelah terjadi perubahan IP publik

| Host | IP/URL | Action |
|----------------------|---------------|---------------|
| Hosts By Domain | | |
| no-ip.org | | |
| iticmalang.no-ip.org | 112.78.154.35 | Modify Remove |

Gambar 8 IP pada domain setelah berubah

IP publik yang dikonfigurasi pada domain iticmalang.no-ip.org, setelah terjadi perubahan IP domain.

➤ Analisa pengujian

Pengujian dilakukan dengan melakukan *rebooting* router. IP publik pertama/sebelum berubah yang terkonfigurasi di router adalah 112.78.154.26 dan ip publik pertama/sebelum berubah yang terkonfigurasi di domain iticmalang.no-ip.org sama dengan yang terkonfigurasi di router yaitu 112.78.154.26. Proses pengujian metode dengan *rebooting* router dilakukan pada tanggal dan jam 22 juli 2013 jam 12:11:13 (waktu tidak sama dengan yang ada di logs karena jika router melakukan rebooting maka konfigurasi awal waktunya adalah 07:00:00) dan sukses melakukan dial up pppoe serta mendapat ip publik baru yaitu

112.78.154.35 pada jam 12:11:24. Pembaharuan ip domain tidak dapat langsung terjadi karena harus menunggu scheduler di router. Ip domain iticmalang.no-ip.org berhasil di perbaharui pada jam 12:14:47 dengan ip yang baru terkonfigurasi di router yaitu 112.78.154.35. Durasi waktu antara perubahan ip publik dirouter dengan perubahan ip domain adalah 3 menit 23 detik.

Pengujian Pada Router Dengan Perubahan IP Otomatis Dari Provider

| | Address | Network | Broadcast | Interface |
|---|------------------|---------------|-----------------|--------------|
| X | 110.138.248.1... | 110.138.248.0 | 110.138.248.255 | ether2-local |
| X | 112.78.154.34 | 112.78.154.1 | 112.78.154.1 | ether1-WAN |
| D | 112.78.154.150 | 112.78.154.1 | | biznet2 |

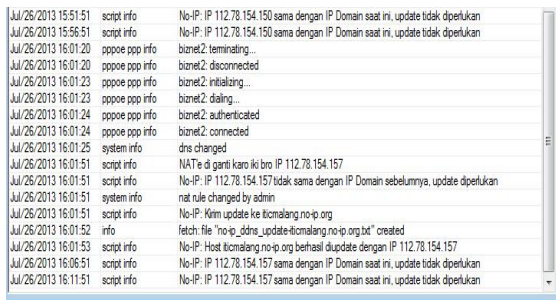
Gambar 8 IP publik sebelum berubah

IP publik yang terdapat pada router yang dikonfigurasi pada interface biznet2 sebelum terjadi perubahan IP publik.

| Host | IP/URL | Action |
|----------------------|----------------|---------------|
| Hosts By Domain | | |
| no-ip.org | | |
| iticmalang.no-ip.org | 112.78.154.150 | Modify Remove |

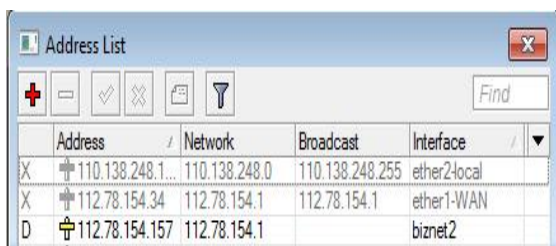
Gambar 9 IP pada domain sebelum berubah

IP publik yang dikonfigurasi pada domain iticmalang.no-ip.org, sebelum terjadi perubahan IP domain.



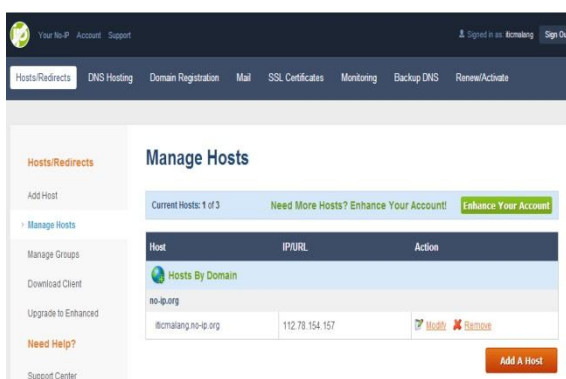
Gambar 10 log

Pada ini tidak dilakukan *rebooting* router tetapi menunggu proses pemutusan koneksi dan dial up ulang oleh provider. Proses terjadinya perubahan IP publik dan proses perubahan ip domain dapat diketahui melalui logs router, pada gambar 4.43 dijelaskan proses terjadinya perubahan IP public dan proses perubahan IP publik pada domain iticmalang.no-ip.org



Gambar 11 IP publik setelah berubah

IP publik yang terdapat pada router yang dikonfigurasi pada interface biznet2 setelah terjadi perubahan IP public pada pengujian ke-9.



Gambar 12 IP pada domain setelah berubah

IP publik yang dikonfigurasi pada domain iticmalang.no-ip.org, setelah terjadi perubahan IP domain pada pengujian ke-9.

➤ Analisa pengujian

Pengujian dilakukan dengan menunggu pergantian ip otomatis dari provider internet. IP publik pertama/sebelum berubah yang terkonfigurasi di router adalah 112.78.154.150 dan ip publik pertama/sebelum berubah yang terkonfigurasi di domain iticmalang.no-ip.org sama dengan yang terkonfigurasi di router yaitu 112.78.154.150. Proses pengujian metode dilakukan pada tanggal dan jam 26 juli 2013 jam 16:01:20 dan sukses terkoneksi ke jaringan via dial up pppoe dan mendapat ip publik baru yaitu 112.78.154.157 pada jam 16:01:24. Pembaharuan ip domain tidak dapat langsung terjadi karena harus menunggu scheduler di router. Ip domain iticmalang.no-ip.org berhasil di perbaharui dengan ip yang terdapat di router yaitu 112.78.154.157 pada jam 16:01:53. Durasi waktu antara perubahan ip publik di router dengan perubahan ip domain adalah 33 detik

Pengujian Metode Dengan Membuka Aplikasi Internal

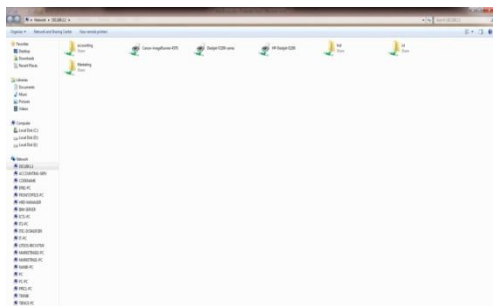
Pengujian metode dilakukan salah satunya dengan membuka aplikasi internal lewat domain iticmalang.no-ip.org:889.



Gambar 13 Pengujian metode dengan membuka aplikasi internal

Pengujian Metode Dengan Membuka Fileshare Melalui VPN

Pengujian metode dilakukan dengan membuka *fileshare* melalui akses VPN di klien.



Gambar 14 Pengujian metode dengan membuka *fileshare* melalui VPN

Analisa Hasil Pengujian

Konfigurasi dilakukan pada router mikrotik RB450G. Scheduler yang mengeksekusi script setiap interval 5 menit akan mengecek kondisi IP yang terkonfigurasi, jika terjadi perubahan IP publik maka script akan mengirim logs perubahan IP, logsnya adalah “No-IP: IP \$currentIP tidak sama dengan IP Domain sebelumnya, update diperlukan”. Selanjutnya script konfigurasi melakukan permintaan perubahan IP domain di no-ip.org untuk merubah IP domain

iticmalang.no-ip.org ke IP publik yang terbaru. Apabila proses perubahan IP domain sukses maka script akan mengirim logs yaitu “No-IP: Host \$host berhasil diupdate dengan IP \$currentIP”, jika *scheduler* mencapai intervalnya untuk melakukan eksekusi script dan tidak terjadi perubahan IP publik maka script akan mengirim logs yaitu “No-IP: IP \$previousIP sama dengan IP Domain saat ini, update tidak diperlukan”. *Script* juga akan mengirim logs jika *interface ethernet* pada router yang terdapat IP publik tidak aktif, logs yang dikirim adalah “No-IP: interface \$inetinterface tidak aktif, update tidak dapat dilakukan.” Kegagalan metode dapat diakibatkan oleh *interface* IP publik tidak aktif yang dikarenakan kegagalan router dalam melakukan dial up pppoe ke jaringan provider. Kegagalan pada metode juga bisa diakibatkan jika penyedia domain no-ip.org mengalami gangguan.

Percobaan selanjutnya adalah membuka aplikasi portal web aplikasi internal dengan mengakses alamat iticmalang.no-ip.org:889 dan membuka *sharefile* melalui koneksi VPN dengan *gateway* iticmalang.no-ip.org.

KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya, maka dapat diambil kesimpulan, Konversi IP publik dinamis ke domain

iticmalang.no-ip.org telah mencukupi kebutuhan perusahaan akan kebutuhan akses data antar jaringan serta kebutuhan akses data selama 24 jam, meskipun terdapat beberapa kelemahan yaitu terdapat penundaan waktu ketika proses perubahan alamat IP ke domain sehingga jika user terkoneksi ke jaringan dan terjadi perubahan ip domain maka koneksi user ke jaringan internal perusahaan akan terganggu. Percobaan metode dilakukan dengan rebooting router dan proses update ip publik otomatis dari provider dengan hasil 100% sukses. Kegagalan pada metode bisa diakibatkan jika router gagal dalam melakukan dial up pppoe sehingga menyebabkan *interface* IP publik tidak aktif atau terjadi kerusakan pada domain no-ip.org.

SARAN

Berikut adalah saran-saran untuk pengembangan lebih lanjut terhadap rancangan otomatisasi perubahan IP publik pada domain:

1. Mencari alternatif domain lain jika domain no-ip.org terjadi kerusakan.
2. Penundaan waktu ketika proses perubahan alamat IP publik ke domain dapat dikurangi dengan tidak mengganggu jaringan perusahaan.
3. Memberikan notifikasi ke user jika telah terjadi pergantian ip di domain
4. Disarankan manajemen PT. Indonesian Tobacco melakukan upgrade paket internet yang mendapatkan ip publik statik agar koneksi jaringan lebih stabil dan untuk kedepannya melakukan

upgrade perangkat router untuk mengantisipasi lalu lintas jaringan yang semakin padat.

Dalam penyusunan karya ilmiah ini masih ada beberapa kekurangan, untuk itu diharapkan dari para pembaca untuk dapat mengembangkan yang lebih baik.

DAFTAR PUSTAKA

1. Agung, I Putu Suhada, Desember 2009, "CCTV Berbasis Web Sebagai Sistem Keamanan", Jurnal Penelitian Seni Budaya. Volume 1, No. 2, <http://jurnal.isi-ska.ac.id/index.php/acintya/article/download/236/209> download tanggal 5 September 2013 pkl 10:00)
2. Handoyo, Joko, Juli 2011, "Kajian Penggunaan Mikrotik Router Ostm Sebagai Router Pada Jaringan Komputer". Jurnal Transformatika. Volume IX, No. 1, http://journal.usm.ac.id/elibs/USM_f949Article%20Joko%20Handoyo.pdf download tanggal 4 September 2013 pkl 19:30
3. Mikrotik.com. 2007. MikroTik RouterOS™ v2.9 Reference Manual (<http://www.mikrotik.com/testdocs/ros/2.9/refman2.9.pdf> tanggal 27 Februari 2013 pkl 16:00)
4. Muslim, Much Aziz, Januari 2007, "Analisa Teknis Perbandingan Router Linux dengan Router Mikrotik pada Jaringan Wireless". Jurnal Teknologi Informasi DINAMIK. Volume XII, No. 1, <http://www.unisbank.ac.id/ojs/index.php/fti1/article/download/45/40> download tanggal 4 September 2013 pkl 20:10)
5. Purbo, Onno w, Juli 2009, "Virtual Private Network (VPN) sebagai alternatif Komunikasi Data Pada Jaringan Skala Luas (WAN)". <http://kambing.ui.ac.id/onnopurbo/library/library-ref-ind/ref-ind->

3/network/VPN_Jurnal.pdf download
tanggal 4 September 2013 pkl 21:00)

6. Saputro, Daniel T, Kustanto. 2008. Membangun Server Internet dengan Mikrotik OS. Gava Media: Yogyakarta
7. Stiawan, Deris, Januari 2009, "Optimalisasi Interkoneksi *Virtual Private Network* (VPN) Dengan Menggunakan *Hardware Based* dan IIX. (Indonesia Internet Exchange) Sebagai Alternatif Jaringan Skala Luas". Jurnal Ilmiah Generic. Volume 4, No. 1, <http://eprints.unsri.ac.id/89/1/7.pdf> download tanggal 4 September 2013 pkl 19:30)
8. Yoga K, Adyatma. 2008. Konfigurasi VPN PPTP pada Mikrotik(http://www.mikrotik.co.id/artikel_lihat.php?id=43 tanggal 27 Februari 2013 pkl 17:00)