RANCANGAN PENGELOLAAN IP DENGAN FIREWALL DI LAPAN PUSAT

Oleh

Suwardi
Peneliti Bidang Informasi
Pusat Analisis dan Informasi Kedirgantaraan

RINGKASAN

Saat ini penggunaan internet telah berkembang sangat pesat. Internet tidak saja digunakan sebagai sarana "pertukaran" data tetapi telah dimanfaatkan untuk sarana menjalankan semua aplikasi *triple play* (*data,voice and video*). Sejak tahun 1986 LAPAN telah terkoneksi dengan internet dan telah dimanfaatkan dalam penyebaran data dan informasi hasil penelitian dan pengembangan kedirgantaraan. Sepanjang perjalanan itu tidak sedikit kendala yang di hadapi dalam mengelola jaringan. Selain bandwidth dan konektifitas, keamanan jaringan terhadap hacker juga masih merupakan kendala yang harus segera diselesaikan oleh LAPAN.

Pusat analisi dan informasi kedirgantaraan (Pussisfogan) sebagai salah satu pusat yang menangani jaringan komputer LAPAN berupaya menangkal akses hacker terhadap jaringan LAPAN Pusat dengan mengoptimalkan fasilitas firewall dan melakukan manajemen terhadap IP address. Dengan cara ini diharapkan akan diperoleh keamanan jaringan dan rancangan *network plan* dengan benar.

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat telah mengubah cara untuk mendapatkan informasi. Kini informasi yang dibutuhkan telah tersedia dan dapat diakses dengan cepat melauli internet. Kebutuhan akan koneksi internet semakin terasa sangat dibutuhkan baik untuk sekedar *browsing* mencari informasi yang dibutuhkan ataupun sebagai penunjang aktifitas kantor sehari-hari misalnya pengiriman email, pemutakhiran informasi hasil

penelitian pada web dan pengiriman aplikasi online antar lembaga atau instansi.

Hal yang sangat mendasar dan dibutuhkan agar dapat terkoneksi dengan internet melalui Internet Service Provider (ISP) adalah IP. Internet Protokol (IP) merupakan tulang punggung internet. Jumlah IP yang diberikan oleh ISP sangat terbatas dan berbanding lurus dengan besarnya jasa yang harus dibayarkan. Untuk itu diperlukan pengelolaan IP dengan benar dalam suatu network sehingga dapat memberikan banyak manfaat diantaranya adalah kecepatan akses, kemudahan dalam keamanan dan pengelolaan jaringan.

1.2 Maksud dan Tujuan

Tulisan ini dimaksudkan untuk memberikan suatu rancangan dalam mengelola IP address dengan tujuan agar lebih mendayagunakan penggunaan IP sehingga memberikan manfaat dalam perancangan suatu *network plan* dengan benar agar tercipta keamanan jaringan yang handal.

1.3 Metode Penelitian

Metode yang digunakan dalam penulisan ini adalah metode eksperimental semu (*quasi-experimental research*) atau disebut sebagai penelitian simulasi yaitu dengan melakukan simulasi pengelolaan ip pada beberapa server dan client dengan menggunakan *firewall* yang ditunjang dengan data-data literature sehingga diperoleh hasil *network plan* yang benar dimana dimungkinkan untuk diterapkan pada jaringan intranet LAPAN.

1.4. Ruang Lingkup

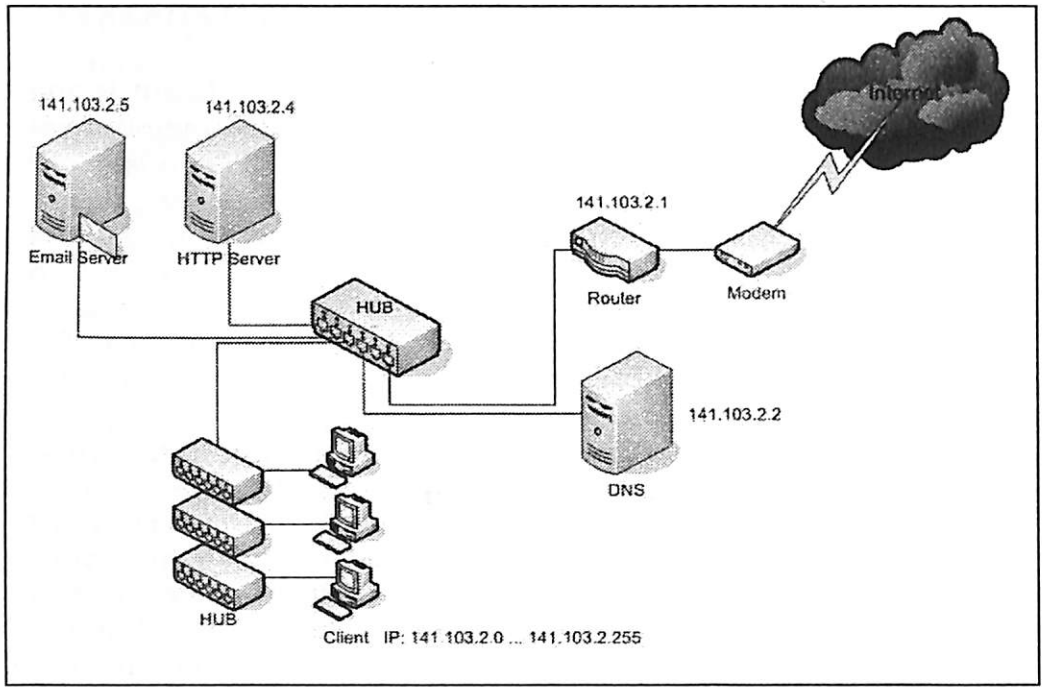
Lingkup penulisan dibatasi hanya pada pembahasan sisi yang ditimbulkan dengan penggunaan firewall jenis *hardware* yaitu pengaturan penggunaan IP pada server-server dan IP untuk masing-masing client.

2. JARINGAN LAPAN PUSAT DAN PERMASALAHANNYA

IP Adders adalah identitas satu komputer dalam jaring computer / internet, seperti halnya rumah kita memupnyai nomer rumah yang tertempel pada dinding. Penulisan IP Adders terbagi 4 kelompok 8 bit yang dituliskan dalam bilangan biner. Dimana setiap kelompok dalam IP Adders dipisahkan oleh titik (Dot). Nilai terbesar dari bilangan biner 8 bit adalah 255. Oleh karena itu jumlah IP Adders yang tersedia ialah 255.255.255.255 IP Adders yang sebanyak ini harus dibagi bagikan keseluruh pengguna jaringan komputer / internet di seluruh dunia.

LAPAN terkoneksi dengan 'dunia' internet tahun1986 mendapat nomor IP yang cukup banyak. Sekitar satu *subnet Mask* IP yang dipakai pada jaringan Local Area Network (LAN) LAPAN Pusat. Masing-masing *client* menggunakan penomoran IP address publik agar dapat tekoneksi dengan internet. Ada sekitar 254 *hosts* atau *client* yang dapat terkoneksi. Kondisi jaringan yang seperti gambar 2.1 ini sangat tidak efektif dan efisien dalam pengelolaan dan pemeliharaan (maintanance) jaringan oleh administrator jaringan. Terkait dengan kondisi diatas ada beberapa hal yang pernah antara lain:

a) Serangan virus terhadap server web. *Open Network* yang digunakan pada jaringan LAPAN Pusat sangat beresiko terhadap serangan *hacker* yang berpotensi merusak operating system (OS) dan aplikasi yang terinstall didalam server.
b) Penggunan nomor IP pada jaringan LAN dengan IP Publik untuk masing-masing *client* berdampak negatif terhadap setiap *client* yang terhubung dengan LAN tersebut. *Client* mudah terserang virus *Adware, Browser hijacker,* dan *Spyware.* Komputer yang terinfeksi virus tersebut akan mengirim informasi yang ada pada setiap komputer *client* dan akan mudah diakses oleh pihak lain melalui internet
c) Kesulitan dalam pengelolaan dan pemeliharaan jaringan. Sering terjadi penggunaan ip yang sama pada *client,* sehingga *client* tersebut tidak dapat terkoneksi internet.
d) Banyaknya penggunaan IP Publik yang dipakai pada *client* mempersulit administrator jaringan dalam pengelolaan jaringan LAN yang lebih besar yaitu *Wide Are Network* (WAN).



Gambar 2-1: LAN LAPAN Pusat

3. ANALISA DAN PEMECAHANNYA

3.1. Firewall

Ada beberapa definisi yang dapat menggambarkan fungsi dari firewall, antara lain :

1. *A firewall is a system or group system that enforce an access control policy between two network (http://www.clark.net/pub/mjr/pubs/fwfaql)*
2. *The main purpose of firewall ystem is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated (http://www.csrc.ncsl.nist.gov/initpubs/800-10/node31.html)*

Dari definisi diatas terlihat bahwa fungsi utama dari filewall adalah sistem yang mengatur layanan jaringan dari dan ke mana, melakukan apa, siapa saja yang diperbolehkan, kapan dan berapa besar/banyak traffic atau lalulintas yang melalui firewall tersebut.

Firewall dirancang untuk menjaga sistem komputer dari askses pihak luar yang tidak berhak. Firewall dapat

diimplementasikan dalam hardware, software atau gabungan keduanya. Firewall banyak digunakan untuk menjaga pengguna pengguna internet yang tidak berhak mengakses jaringan privat yang terhubung internet, khususnya intranet.

3.2. Firewall dari sisi Software

Suatu jaringan dengan koneksi intranet yang sekaligus dapat membolehkan akses internet biasanya menginstall firewall untuk menjaga sumber daya data dari akses pihak luar dan mengontrol sumber daya luar (internet) yang dapat diakses dari dalam (oleh karyawan). Semua pesan yang masuk dan keluar intranet melewati firewall yang akan memeriksa apakah setiap pesan tidak sesuai dengan kriteria keamanan sistem. Ada beberapa teknik software yang dipakai sebagai firewall:

a) *Packet filter.* Dengan teknik ini setiap paket yang masuk dan keluar jaringan akan diterima atau ditolak berdasarkan aturan yang telah dibuat sebelumnya. Penyaringan paket ini cukup efektif dan transparan tetapi sulit untuk menkonfirgurasinya.
b) *Application gateway.* Teknik ini mengaplikasikan mekanisme keamanan untuk aplikasi khusus, sperti FTP dan Telnet server. Teknik ini sangat efektif tetapi dapat menyebabkan penurunan kinerja.
c) *Proxy server.* Teknik ini menagkap semua pesan yang keluar dan masuk jaringan. Proxy server menyembunyikan alamat jaringan sebenarnya.

Dalam praktek firewall diimplementasikan menggunakan beberapa teknik sekaligus.

3.2 Firewall dari sisi Hardware

Selain firewall yang dibangun secara software, ada beberapa firewall yang bersifat *plug and play.* Firewall ini pada umumnya berupa *hardware* yang relatif lebih mudah untuk dikonfigurasi dalam penggunaannya sesuai kebutuhan. Firewall jenis ini dapat dikonfigurasi menjadi 3 zone batas pemisahan pengamanan:

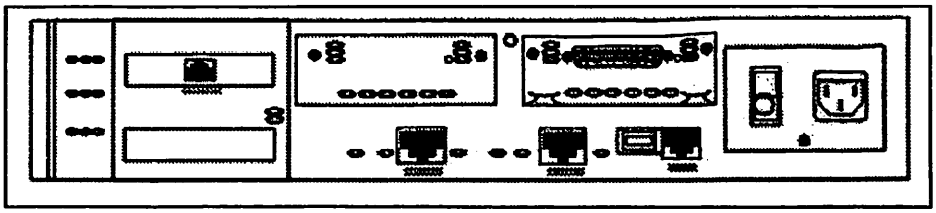
a) De-militarised Zone (DMZ). Digunakan untuk melindungi system internal yang berhubungan dengan serangan *hack (hacker attack).* Secara umum DMZ dibangun berdasarkan tiga buah konsep, yaitu NAT (*Network Address Translation*), PAT (*Port Addressable Translation*), dan *Access List.*

b) Inside Zone. Zone ini digunakan untuk melindungi server-server dan memisahkan jaringan *client* dan server dari akses internal (*back door attack*) terhadap server.
c) Outside Zone. Ini adalah zone terluar dimana berhadapan langsung dengan 'dunia' internet. Biasanya perangkat jaringan yang berada disisi ini adalah modem dan router.

Seperti telah dikemukakan bahwa konsep dasar dari firewall adalah penggunaan NAT, PAT dan Access List. NAT berfungsi untuk menunjukan kembali paket-paket yang datang dari *"real address"* / IP Publik ke alamat internal, misalnya LAPAN memiliki *"real address"* 141.103.2.1 pada zone outside maka dalam bentuk NAT langsung data-data yang datang ke 192.168.1.1 untuk zone DMZ dan 10.10.10.1 untuk zone inside. Kemudian PAT berfungsi untuk menunjukan data yang datang pada *particular port* atau *range* sebuah *port* ke sebuah alamat internal IP. Sedangkan *Access List* berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan dalam suatu pertanyaan. Misalnya menolak atau memperbolehkan semua (Internet Control Message Protocol-ICMP) yang datang keseluruh alamat IP kecuali untuk sebuah ICMP yang tidak diinginkan.

Rancangan konfigurasi firewall yang sekarang diimplementasikan pada jaringan LAN di LAPAN Pusat adalah dengan menggunakan firewall jenis *hardware* yaitu Cisco Firewall PIX 515 E. Konfigurasi ini membawa dampak yang positif pada sisi pengelolaan IP jaringan baik pada sisi server maupun client. Sebelum rancangan ini dibuat, seluruh konfigurasi IP jaringan LAN LAPAN Pusat menggunakan IP Publik (gambar 2). Sifat *open network* yang demikian mengandung resiko yang besar terhadap serangan hacker (*hacker attack*), *spyware, adware* dan serangan *trojan* yang mengancam kerusakan sistem dan data yang ada pada server-server maupun *client* yang terhubung dengan internet. Untuk mengantisipasi serangan tersebut Pusat Analisis dan Informasi Kedirgantaraan melalui Bidang Pengembangan Informasi Kedirgantaraan melakukan analisan dan merancang sistem firewall yang dibangun secara *hardware*. Sistem ini dipilih karena memiliki kemudahan dan kelebihan pada *customize setting* yang dapat disesuaikan dengan perubahan arsitektur jaringan dimasa datang. Kelebihan ini tentunya harus 'dibayar' mahal jika dibandingkan dengan firewall yang

dibangun hanya secara *software*. Gambar 3.3.a adalah perangkat firewall Cisco PIX 515 E yang telah diuji coba penggunaannya pada jaringan LAN LAPAN Pusat.



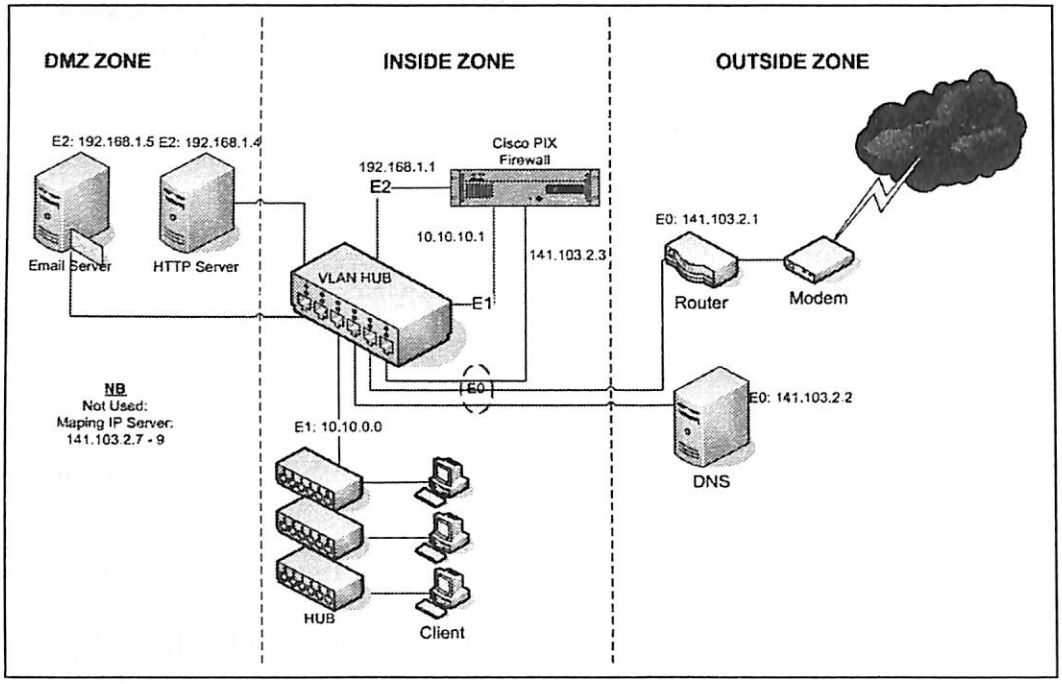
Gambar 3-3a: perangkat firewall Cisco

Firewall Cisco PIX 515 E secara *default* memiliki dua kartu ethernet card yang digunakan untuk inside zone dan outside zone. Untuk membangun zone DMZ diperlukan satu kartu ethernet tambahan. Zone DMZ digunakan untuk melindungi sistem internal terutama server-server dari serangan *hacker*. Ethernet card untuk zone inside ditandai dengan ethernet 0, zone outside ditandai dengan ethetnet 1 dan untuk zone DMZ diberikan pengenal ethetnet 2.

Berikut adalah tabel translasi IP yang digunakan pada firewall Cisco PIX 515 E:

Real IP Address	Gateway	Netmask	Interface	Zone
141.103.2.1	192.168.1.1	255.255.255.0	Ehernet 2	DMZ
	141.103.2.2	255.255.0.0	Ethernet 1	Outside
	10.10.10.1	255.255.255.0	Ethernet 0	Inside

Rancangan konfigurasi LAN yang dipakai dengan menggunakan firewall Cisco PIX 515 E pada sistem jaringan komputer LAPAN Pusat terlihat pada gambar 3.3.b. Output dari Cisco PIX 515 E dihubungkan pada hub *VLAN*. Hub ini berfungsi sebagai pembagi dan sekaligus sebagai penghubung perangkat-perangkat lain dengan firewall sesuai dengan pembagian zone yang telah direncanakan.



Gambar 3-3b: sistem jaringan komputer LAPAN Pusat

Terlihat jelas bahwa kini struktur IP yang digunakan lebih terorganisir dan tertata rapi sesuai dengan zone yang digunakan. Zone DMZ kini lebih *secure* dari serangan *hacker* baik dari luar (internet) maupun serangan yang bersifat *backdoor* (user attack). Zone Inside (*client*) kini menggunakan IP internal sehingga tidak mengganggu keamanan baik dari sisi *client* maupun server. Semua ini karena ada sistem NAT yang merupakan salah satu fungsi dari firewall.

4. KESIMPULAN

IP adalah protokol di internet atau jaringan yang menangani masalah pengalamatan dan pengaturan pengiriman paket data sehingga ia sampai ke alamat yang benar. Setiap komputer yang terkoneksi ke jaringan atau internet harus memiliki alamat yang unik yaitu IP. Satu IP hanya boleh dimiliki oleh satu komputer. Untuk melindungi server dan client yang terhubung dengan jaringan internet dari 'serangan' orang luar bisa ditempuh dengan jalan

memasang firewall baik berbentuk software maupun hardware.

Pusat Analisis dan Informasi Kedirgantaraan melalui bidang Pengembangan Informasi Kedirgantaraan telah merancang penggunaan firewall secara hardware untuk melindungi sistem jaringan komputernya di LAPAN Pusat. Firewall adalah salah satu sistem keamanan jaringan yang dipakai untuk melindungi jaringan komputer dari serangan luar tetapi yang perlu diperhatikan bahwa secanggih apapun teknologi keamanan jaringan yang dipakai kalau tidak didukung oleh kemampuan sumber daya manusianya hasil tidak optimal. Tetapi paling tidak program firewall akan menghambat craker dan hacker menembus suatu sistem jaringan.

DAFTAR RUJUKAN

Buku panduan instalasi Firewall Cisco PIX 515 E, Mei 2003

Indocisc, Security Tools Untuk Pengamanan, April 2004

Buku Pintar Internet TCP/IP oleh Onno W Prabowo, Adnan asamalah, Ismail Fahmi, dan Ahkmad Husni Thamrin ; Elex Media Komputindo Jakarta 2003