PERTEMUAN 20

KEAMANAN INFRASTRUKTUR JARINGAN

A. TUJUAN MATERI KEAMANAN INFRASTRUKTUR JARINGAN

Setelah mempelajari materi ini, diharapkan pembaca mampu :

5.1 Memahami dan mengerti Keamanan Infrastruktur Jaringan

5.2 Menjelaskan apa itu Keamanan Infrastruktur jaringan

5.3 Mengetahui prinsip keamanan jaringan

5.4 Jenis Serangan Terhadap Keamanan infrastruktur Jaringan

5.5 Macam-macam Ancaman Terhadap Infrastruktur Jaringan serta metoda yang dipakai untuk mengatasinya

B. URAIAN MATERI

5.1 Konsep Keamanan Infrastruktur Jaringan

Keamanan Infrastruktur Jaringan Komputer sebagai salah satu bagian dari sistem informasi berperan sangat penting guna menjaga suatu integritas dan validitas data juga menjamin ketersediaan layanan bagi setaip usernya. Sistem haruslah dilindungi dari segala macam jenis serangan, pemindaian atau penyusupan dari pihak yang tidak bertanggungjawab.

Komputer yang terhubung ke dalam jaringan rentan mengalami ancaman keamanan lebih besar dibandingkan host yang tidak terubung kemana-mana. Dengan mengendalikan keamanan jaringan, risiko ancaman tersebut dapat kurangi. Namun demikian keamanan jaringan biasanya bertolakbelakang dengan akses jaringan, kenapa demikian? karena jika akses jaringan semakin mudah, keamanan infrastruktur jaringan akan semakin rawan di retas. Bila keamanan jaringan semakin baik, akses kedalam jaringan makin terbatas. Suatu jaringan dirancang sebagai komunikasi data *highway* yang bertujuan meningkatkan akses ke sistem komputer, sementara *security* (keamanan) dirancang untuk mengontol akses ke dalam suatu jaringan. Penyedia

keamanan jaringan adalah sebagai aksi pennyeimbang antara *security* dengan *open access.*

Infrastruktur jaringan merupakan sekumpulan komponen-kompnen fisik dan logika yang memberikan pondasi keamanan, konektifitas, routing, akses, manajemen, dan bermacam-macam fitur integral jaringan. Misalkan jika jaringan yang kita gunakan terhubung kedalam internet, maka akan lebih banyak menggunakan protocol TCP/IP suite yang umumnya paling banyak di pakai pada jaringan.

1. Infrastruktur Fisik

   Sesuai dengan namanya (fisik), maka akan lebih banyak berhubungan dengan komponen-komponen fisik suatu jaringan komputer seperti :

   a. Berhubungan dengan masalah jaringan perkabelan, yaitu jaringan perkabelan yang sesuai dengan jaringan topology yang dipakai. Misalkan jika dalam sebuah jaringan memakai *backbone Gigabite Ethernet* maka seharusnya sudah memakai kabel CAT5e yang bisa mensupport kecepatan jaringan tersebut.
   b. Semua kelengkapan jaringan seperti:
      - Router yang memungkinkan komunikasi antar jaringan lokal yang berbeda segmen.
      - *Switches, bridges* yang digunakan untuk menghubungkan host ke jaringan.
      - Servers, yaitu seperti exchange server, server data file, DNS server, layanan

        IP address dari DHCP server dan sebagainya dan juga host.
   c. Infrastruktur fisik terdiri dari beberapa alat fisik seperti teknologi Ethernet dan standar Wireless 802.11a/b/n, jaringan telpon umum (PTSN), ATM (*Asynchronous Transfer Mode)* dan semua metode komunikasi dan jaringan fisik lainnya.
   d.

2. Infrastruktur Logical

   Infrastruktur logika dari sebuah jaringan komputer adalah komposisi dari banyak macam elemen software yang saling berhubungan, mengamankan dan mengatur host pada jaringan. Infrastruktur logika ini berfungsi agar terjadinya komunikasi antar satu atau lebih komputer melalui jaringan fisik yang sesuai

dengan topology yang dipakai. Sebagai contoh dari sebuah infrastruktur logika adalah komponen -komponen berikut ini :

a. *Domain System Name* (DNS), yang merupakan sistem untuk memberikan resolusi nama dari sebuah permintaan resolusi nama client.

b. *Directory Services,* yaitu layanan directory untuk meng-autentifikasi dan authorisasi user atau pengguna untuk menggunakan resource dan masuk ke dalam jaringan.

c. Protocol-protocol jaringan yaitu protocol TCP/IP, salah satu paling banyak di pakai dan sangat populer sebagai protocol jaringan dari berbagai platfrom jaringan baik berplatfrom windows, linux, unix, dan lainnya.

d. System kemanan jaringan seperti :

1) Jika menggunakan jaringan windows server, mestinya sudah dilengkapi dengan sistem *update patch* yang sudah di deploy secara otomatis kepada host dalam sebuah jaringan seperti *Windows System Update Service*s (WSUS).
2) System keamanan terhadap virus, jika untuk kepeningan jaringan yang besar sudah seharusnya membangun sebuah sistem antivirus corporate edition dimana semua klien akan terhubung ke server tersebut untuk mendownload secara otomatis signature datanya.
3) Sistem keamanan terhadap berbagai macam ancaman jaringan yang juga berhubungan dengan infarstruktur fisik seperti firewall, pemakainan IPSec yang terdapat pada remote VPN connection dan lainnya.
4) Berbagai macam *policy dan guidelines* dari corporate tentang penggunaan resource jaringan sama tidak kalah pentingnya. Sperti policy tentang penggunaan email dalam company yang tidak mengurangi untuk pemakain pribadi seperti mailing list yang memungkinkan banyaknya spam email dalam system exchange.
5) Software client yang menghubungkan ke dalam server

Setelah terbentuknya infrastruktur logical, sebagai administrator kita perlu memiliki pengetahuan untuk dapat bisa memahami berbagai macam aspek teknologi yang ada didalamnya. Seperti halnya harus dapat membuat desain IPaddress agar bisa di

terapkan berdasarkan jaringan fisik yang tersedia, memberikan IP-address sebagai identitas masing-masing host pada jaringan dan harus juga bisa melakukan trobleshooting jika terjadi permasalahan jaringan berhubungan dengan addressing, konektivitas, security, access, maupun masalah resolusi nama (*name resolution*).

5.2 Prinsip Keamanan Jaringan

Dibagi menjadi 5, yaitu :

1. *Secrecy* (Kerahasiaan)

   Secrecy berhubungan dengan sebuah hak akses membaca data dan informasi dari suatu sistem komputer. Dalam hal ini sebuah sistem komputer dapat dikategorikan aman jikalau suatu informasi atau data hanya dapat di akses oleh pihak yang sudah diberi hak akses secara legal.

2. *Integrity* (Integritas)

   Integritas berhubungan dengan wewenang atau hak akses untuk mengubah informasi dan data dari sebuah sistem komputer. Jika dalam *Secrecy* itu hak akses untuk membaca, lain dengan *Integrity*. Karena dalam hal ini sebuah sistem komputer sudah dikatakan aman jika suatu informasi dan data hanya dapat diubah oleh pihak yang diberi hak dan wewenang untuk mengubah secara legal.

3. *Availability* (Ketersediaan)

   Ketersediaan berhubungan dengan *availability* data atau informasi pada saat yang dibutuhkan oleh user. Dalam hal ini suatu system komputer dapat dikategorikan aman jika informasi atau data yang terdapat pada system komputer sesuai dengan apa yang dibutuhkan dan dapat digunakan oleh pihak yang berhak.

4. *Authentication* (Autentifikasi)

   Aspek ini berhubungan dengan metode untuk menyatakan bahwa sebuah informasi betul-betul original, orang yang memberikan dan mengakses informasi adalah benar orang yang dituju dan tidak mengada-ngada, atau server yang dihubungi adalah server asli.

5. *Access Control* (Akses Kontrol)

Merupakan fitur-fitur keamanan yang mengontrol bagaimana user berkomunikasi dengan sistem. Akses kontrol melindungi sistem dari akses yang ilegal dan umumnya menentukan tingkat otorisasi setelah prosedur autentikasi berhasil dilengkapi.

5.3 Jenis Serangan Terhadap keamanan Jaringan

Serangan terhadap suatu data atau informasi dalam sebuah jaringan dapat dikategorikan menjadi dua, yaitu :

1. Serangan aktif

Merupakan serangan yang mencoba memodifikasi atau merubah data dan mendapatkan otentifikasi dengan mengirim paket-paket data yang keliru ke dalam stream data atau dengan cara memodif paket-paket yang melewati *stream* data. Serangan aktif sangat sulit untuk dihindari karena untuk melakukannya dibutuhkan perlindungan fisik bagi keseluruhan fasilitas komunikasi dan juga jalur-jalurnya setiap saat. Dan yang dapat kita dilakukan adalah hanya mendeteksi dan memulihkan keadaan yang disebabkan dari serangan ini.

2. Serangan Pasif

Serangan pasip yaitu serangan pada sistem otentifikasi yang tidak menyelipkan data ke dalam sebuah aliran data, akan tetapi hanya memantau pengiriman informasi ke sumber tujuan. Informasi ini biasanya digunakan oleh seseorang yang tidak bertanggung jawab. Serangan pasif yang mengambil sebuah unit data kemudian memakainya untuk memasuki sesi otentikasi dengan berpura-pura berperan sebagain pengguna asli yang disebut sebagai *Replay attack.* Beberapa otentifikasi seperti data *biometric* atau *password* yang dikirim menggunakan transmisi elektronik dapat direcord dan selanjutnya digunakan untuk pemalsuan data yang sesungguhnya. Serangan ini sulit didetect karena penyerang samasekali tidak melakukan pengubahan data. Oleh karena itu untuk mengatasi serangan ini lebih ditekankan pencegahannya daripada pendeteksiannya.

5.4 Ancaman Infrastruktur Jaringan Dan Metode Yang Umum digunakan

Berikut ini adalah macam-macam Ancaman peretasan atau metoda peretasan yang dipakai terhadap keamanan jaringan .

1. Memaksa masuk dan juga kamus password

   Ancaman keamanan infrastruktur jaringan ini lebih familiar disebut dengan *Brute Force and Dictionary*, jenis serangan ini adalah upaya untuk memasuki sistem jaringan dengan menyerang basis data password atau login promt yang sedang aktif. Serangan ini adalah suatu bentuk upaya untuk menemukan kata sandi dari akun pengguna secara sistematis dan mencoba berbagai macam kombinasi huruf, angka, atau simbol. Sementara serangan dengan metode kamus password yaitu sebuah bentuk upaya untuk menemukan kata sandi dengan mencoba berbagai macam kata sandi yang mungkin biasa di pakai oleh pengguna secara umum dengan memakai daftar atau kamus password yang telah didefinisikan sebelumnya.

   Untuk mengatasi serangan tersebut, kita semestinya mempunyai suatu policy tentang penggunaan password yang kuat diantaranya untuk pantang memakai password dekat dengan identitas kita misal : nama kita, nama anak, tanggal lahir, dsb. Semakin panjang sebuah password dan kombinasi hurufnya semakin susah untuk di pecahkan. Akan tetapi dengan waktu yang cukup, nantinya password akan tetap di temukan dengan metode brute force ini.

2. *Denial Of Services*

   DoS (Denial of Services) yaitu termasuk kedalam ancaman keamanan jaringan yang mengakibatkan layanan jaringan jadi macet, serangan yang mengakibatkan jaringan kita tidak bisa di akses dan menjadikan sistem kita tidak dapat merespon terhadap permintaan atau trafik layanan objek dan resource jaringan. DoS terbagi menjadi beberapa bagian antara lain:

   a. *Distributed Denial of Services* (DoS), terjadi saat peretas berhasil meng-kompromi dengan system layanan dan mempergunakannya sebagai pusat untuk menyebarkan peretasan terhadap korban lain.
   b. *Distributed Reflective Denial of Services* (DRDoS), memanfaatkan layanan internet, seperti router dan protocol update DNS. DRDoS ini meretas fungsi dengan mengirim sesi, update dalam jumlah yang amat besar kepada

bermacam - macam layanan server atau router dengan memakai address spoofing kepada korban yang di targetkan.

c. *Ping of Death,* yaitu peretasan dengan memakai tool khusus, peretas dapat melakukan pengiriman paket ping yang sangat besar kepada korban. Dalam banyak kasus sistem yang di serang mencoba memproses data tersebut, error terjadi menyebabkan *system crash, freeze* atau *reboot. Ping of Death* ini semacam serangan *Buffer overflow* akan tetapi karena sistem yang di serang sering menjadi down, maka disebut DoS attack. Stream Attack terjadi saat banyaknya jumlah paket yang besar dikirim menuju ke dalam port pada sistem korban.

3. *Spoofing*

Istilah spoofing biasanya digunakan untuk merujuk kepada header pemalsuan, penyisipan data palsu atau menyesatkan dalam netnews header atau e-mail. Header dipalsukan dan dipakai untuk menyesatkan penerima atau jaringan aplikasi mengenai asal daripada pesan tersebut.

4. Serangan *Man-In-The-Middle*

Man-in-the-middle terjadi saat user yang bertujuan untuk merusak dapat menempatkan posisi diantara kedua titik link komunikasi. Para peretas ini tidak terlihat pada dua sisi link komunikasi dan bisa merubah data dan arah traffic. Dengan metode ini para peretas bisa memperoleh logon credensial bahkan bisa merubah isi pesan dari dua titik komunikasi ini.

5. Spamming

Spamming merupakan salah satu metode penyalahgunaan teknologi e-mail yang sangat umum dan paling sering di temui pengguna fasilitas e-mail. *spam product* hasil spamming, dapat di definisikan sebagai pesan e-mail yang di inginkan oleh pengguna yang sebagian besar adalah pesan komersil walaupun tingkat ancamannya dapat di bilang tergolong rendah jika dibandingkan dengan e-mail worm atau pun phising.

6. Sniffer

Sniffer (snooping attack) adalah kegiatan user untuk merusak dan bertujuan agar mendapatkan informasi tentang trafic atau jaringan lewat jaringan tersebut. *Sniffer* adalah program penangkap paket yang bisa mengcopy isi paket yang melewati media jaringan kedalam file. Serangan *sniffer* sering di targetkan pada koneksi awal antara *client* dan *server* untuk mendapatkan *logon credential* dan *password.*

7. *Crecker*

Crecker adalah panggilan untuk seseorang yang masuk ke dalam sistem komputer orang lain dan *cracker* lebih bersifat destruktif di dalam jaringan komputer, dan mem-*bypass* lisensi dan password program komputer, dengan sengaja melawan keamanan komputer, mengubah halaman muka web (*Deface*) milik orang lain bahkan hingga menghapus data milik orang, hingga yang lebih parah mencuri data dan umumnya melakukan cracking untuk keuntungan pribadi, bermaksud jahat, atau karena sebab sepele seperti ada tantangan. Beberapa proses peretasan dilakukan untuk menunjukan lemahnya keamanan sistem.

5.5 Implementasi Keamanan Infrastruktur Jaringan

Berikut beberapa teknik atau cara mengamankan sebuah infrastruktur jaringan, yaitu :

1. *Firewall*

Firewall adalah teknik yang sangat penting dan berguna dalam mengamankan sebuah jaringan, dan *Firewall* merupakan suatu sistem atau mekanisme mode yang diterapkan baik pada perangkat *Software, Hardware,* ataupun pada sistem itu sendiri yang bertujuan untuk menaungi, baik dengan membatasi, menyaring, atau bahkan menolah satu atau semua hubungan segmen kegiatan pada jaringan pribadi beserta jaringan luar yang notabene bukan merupakan ruang lingkupnya, segmen tersebut dapat berupa *server, workstation, router,* dan jaringan LAN.

Untuk dapat terkoneksi dengan jaringan lain (Internet) maka harus masuk kedalam server *firewall* bisa secara remote atau langsung. Intinya software yang mengizinkan traffic jaringan yang sudah dianggap aman agar bisa melaluinya dan mencegah lalulintas jaringan yang dirasa tidak aman. Umumnya, tembok api

(*firewall)* diterapkan dalam sebuah *gateway* (gerbang) antara jaringan local dengan jaringan internet.

Tembok Api (*Firewall)* dipakai untuk mengontol atau membatasi akses terhadap siapa saja yang memiliki perizinan untuk mengaksees terhadap jaringan pribadi dari pihak luar. Saat ini istilah *firewall* menjadi istilah awam yang merujuk pada sistem yang mengatur alur komunikasi antara dua macam jaringan terhubung yang berbeda. Saat ini hampir semua instansi yang mempunyai akses ke internet dan tentu saja jaringan yang mempunyai landasan hukum didalamnya, maka haruslah ada perlindungan terhadap seluruh perangkat digital instansi tersebut dari ancaman serangan para hacker, pencuri data, ataupun mata-mata, dan sebagainya.

Firewall terbagi menjadi 2 bagian , yaitu sebagai berikut :

a. *Personal Firewall*

Personal *firewall* dirancang untuk melindungi komputer yang terhubung ke dalam jaringan yang di akses secara ilegal. *Firewall* jenis ini sekarang berevolusi menjadi sekumpulan program yang berfungsi untuk mengamankan sebuah komputer secara menyeluruh, dengan di tambah beberapa fitur pengamanan seperti perangkat proteksi terhadap serangan virus, anti-spam, anti-*spyware* dan lain-lain. Bahkan beberapa produk *firewall* yang lainnya dilengkapi dengan fitur deteksi gangguan keamanan jaringan (*intrusion detection system*) . Beberapa contoh *firewall* jenis ini yaitu *Microsoft Windows Firewall* yang sudah terintegrasi dalam operation system Windows vista, Windows Server 2003 servis pack 1, OS Windows XP servis pack 2, Kerio *Personal Firewall, Symentec Norton Personal Firewall,* dan sebagainya. Personal *Firewall* memiliki 2 fitur utama, yaitu *Stateful Firewall,* dan *Packet Filter Firewall.*

b. *Network Firewall*

Network Firewall didesain agar bisa melindungi jaringan secara total dan menyeluruh dari berbagai serangan dan peretasan. Umumnya ditemui dalam 2 bentuk, yakni sebuah software terdedikasi atau sebuah software yang diinstalasikan ke dalam server. Contoh *firewall* ini adalah Cisco PIX, Watch Guard, Cisco ASA, Fortigate, Juniper SRX, *Microsoft Internet*

Security dan *Accelelator Server* (ASA *server*), PF dalam keluarga sisitem operasi Linux BSD, IPTables dalam sisitem operasi GNU/Linux, serta SunScreen dai SunMicrosustem, Inc. dalam sistem operasi Solaris.

Secara mendasar, *firewall* dapat menjalankan hal-hal sebagai berikut :

1) Melakukan autentifikasi terhadap akses
2) Mengatur dan mengontrol lalulintas sebuah jaringan
3) Melindungi sumber daya dalam suatu jaringan pribadi atau privat.
4) Mencatat seluruh kejadian, dan melakukan pelaporan kepada administrator.

Gambar 1. Firewall

2. *Rule and Policy*

Rule and policy adalah teknis utama dalam sebuah *firewall* yang dimana melalui *Rule and policy* seorang *network administrator* mengontrol sistem kerja sebuah *firewall* dan dapat melakukan monitoring secara dinamis dan memaksimalkan produktifitas kinerja perangkat jaringan.

3. *Port Interface*

Interface (Antarmuka) yaitu mekanisme komunikasi antar *user* (pengguna) dengan *system. Interface* (antarmuka) dapat menerima informasi dari *user* (pengguna) untuk membantu mengarahkan lajur penelusuran suatu masalah sampai ditemukan sebuah solusi.

Interface berfungsi untuk memasukan pengetahuan yang baru kedalam basis pengetahuan *Expert System* (Sistem pakar), dengan menyajikan penjelasan sistem dan juga memberikan panduan pemakaian sistem *step by step* atau secara menyeluruh sehingga user mengerti apa yang akan dilakukan terhadap sistem. Yang paling penting yaitu kemudahan dalam menggunakan dan menjalankan

sistem, serta interaktif, dan juga komunikatif, akan tetapi kesulitan dalam membangun atau mengembangkan suatu program jangan terlalu di perlihatkan.

4. *Routing*

Routing yakni proses untuk memilih path (jalur) yang mesti dilalui oleh paket. Dan Jalur yang baik bergantung pada beban sebuah jaringan, *type of service requested*, pola trafik, dan panjang datagram.

Secara umum skema routing sekedar mempertimbangkan lajur paling pendek (*the shortest path).*

Bentuk routing terbagi menjadi 2, yakni :

a. *Direct Routing* atau direct delivery yaitu paket dikirim dari salah satu mesin ke mesin lainnya secara langsung (host ada pada jaringan fisik yang sudah aman) sehingga tidak harus melalui gateway atau mesin lainnya.
b. *Indirect Routing* (*indirect Delivery*) yaitu paket dikirim melalui salah satu mesin ke dalam mesin lainnya secara tidak langsung yang berbeda jaringan sehingga paket akan melalui satu atau lebih network atau gateway yang lainnya sebelum sampai ke mesin yang kita tuju.

Router merekomendasikan jalur yang dipakai untuk melewati paket berdasarkan data atau informasi yang dimiliki oleh Tabel Routing.

Informasi yang dimiliki oleh tabel routing bisa diperoleh secara routing statis melalui perantara admin dengan cara mengisi tebel routing secara manual atau dinamik routing dan menggunakan protocol routing, yang dimana setiap router berhubungan saling bertukar data atau informasi routing supaya dapat mengetahui alamat tujuan dan juga memelihara tabel routing.

Tabel Routing berisi beberapa informasi, antaralain :

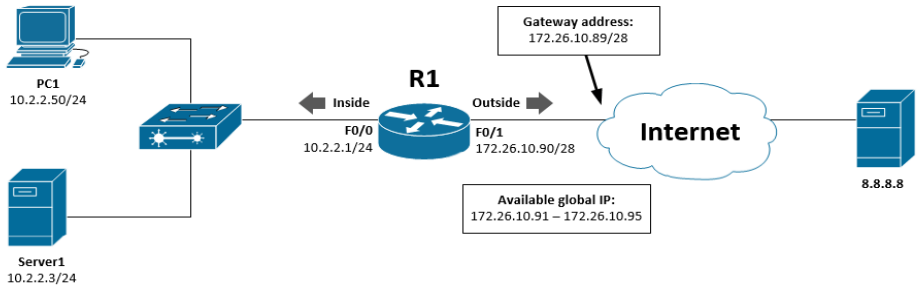
a. Alamat *Network* yang dituju.
b. *Interface Router* yang terdekat dengan network tujuan.
c. Matric, yaitu sebuah nilai yang menunjukan sebuah jarak untuk mencapai network yang dituju. Matric tersebut memakai teknik berdasarkan jumlah lompatan (*Hop Count).*

5. Network Address Translation (NAT)

Network Address Translation atau sering disingkakt NAT dan bisa pula di bilang penafsiran alamat jaringan merupakan suatu metoda untuk menghubungkan satu atau lebih komputer ke dalam jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini dikarenakan ketersediaan alamat IP yang sangat terbatas, kebutuhan akan *Security*(Keamanan), dan serta fleksibilitas didalam administrasi sebuah jaringan.

a. Pengertian NAT satatis

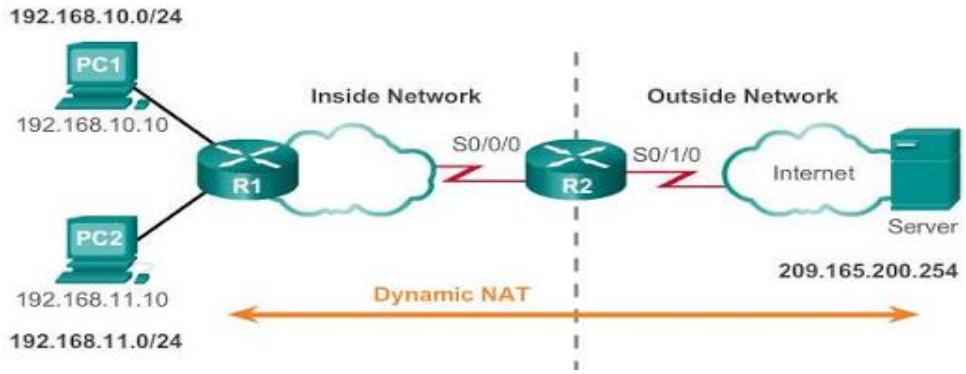
NAT Statis memakai *table routing* yang tetap, atau lokasi translasi alamat ip address ditetapkan sesuai dengan alamat asal atau source ke alamat yang dituju, sehingga mungkin akan terjadi pertukaran data dalam sebuah alamat ip bilamana translasi alamat ipnya belum di terdaftar dalam table nat. Translasi statik terjadi ketika *inside* (alamat local) dipetakan ke sebuah outside (alamat global/internet). Alamat local dan global dipetakan satu lawan satu secara statik. NAT statis akan melakukan sebuah request atau pengiriman dan pengambilan paket data sesuai aturan yang sudah ditabelkan dalam sebuah NAT.



Gambar 2. NAT statis

b. Pengertian NAT dinamis

NAT dinamis menggunakan logika kesetaraan atau pengaturan beban, dimana dalam tabelnya itu sendiri telah dibenamkan logika kemungkinan dan pemecahan. Pada umumnya NAT dinamis dibagi menjadi 2 jenis yakni NAT sistem overload dan NAT sistem pool.



Gambar 3. NAT dinamis

6. Blocking/Filtering

Pada bentuk yang paling sederhana, *firewall* merupakan router atau komputer yang memiliki dua buah *Network Interface Card* (NIC), kartu antarmuka jaringan yang mampu melakukan penyaringan terhadap setiap paket yang masuk. Perangkat jenis ini pada umumnya dinamai dengan nama *packet-fitering router.*

Firewall jenis ini bekerja dengan melakukan perbandingkan antara sumber alamat dari semua paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam *Access Control List Firewall, dan router* itu akan mencoba memutuskan apakah akan meneruskan paket yang masuk tersebut ke yang dituju atau menghentikannya.

Pada bentuk yang lebih sederhana, *firewall* hanya dapat melakukan pengujian terhadap sebuah alamat IP address atau nama domain yang menjadi sumber paket dan menentukan apakah akan menolak atau meneruskan paket tersebut. Walaupun demikian, *packet fitering router* tidak bisa digunakan untuk memberi akses atau menolaknya dengan menggunakan basis hak-hak yang dimiliki seorang pengguna, contoh blocking/filtering dibagi 2 yaitu :

a. Blocking internal to internet
   1) Web Filtering
   2) Gateway Antivirus
   3) Intrusion Prevention Services (IPS)
   4) Aplication Control

b. Blocing External to Internal

1) Spam Blocker
2) DLP (Data Lost Prevention)
3) Quarantine Server
4) APT blocker

C. LATIHAN /TUGAS

1. Sebutkan dan jelaskan macam-macam infrastruktur jaringan?
2. Sebutkan prinsip keamanan jaringan minimal 3 ?
3. Serangan pasif adalah salah satu jenis serangan terhadap infrastruktur jaringan, coba anda jelaskan dengan dengan rinci?
4. Apa itu DoS dalam ancaman terhadap infrastruktur jaringan?
5. Network Address Translation dibagi menjadi 2, sebutkan dan jelaskan?

D. REFERENSI

1. Sugiyono. 2016. *Sistem Keamanan Jaringan Komputer Menggunakan Metode Wathguard Firebox pada PT Guna Karya Indonesia.* Jurnal Teknik Informatika STIKOM Cipta Karya Informatika. 9(2):1-8.
2. Alwafi, Fariz. 2015. *Analisia Dan Implementasi Keamanan Jaringan Pada PT.Dae Myung Highness Indonesia.* Jurnal Program Studi Informatika STMIK Nusa Mandiri, Bekasi. 3(1):1-10.
3. Rushadi, Syukron. 2018. *Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone.* ResearchGate [Internet]. [Di unduh 2020 Mar 30]; 1(1). Tersedia Pada : https://www.researchgate.net/publication/328130248