Sistematika Penyusunan Materi Pembelajaran (Daring)

MATA PELAJARAN : Administrasi Infrastruktur Jaringan (AIJ)

KOMPETENSI KEAHLIAN : TKJ

KELAS/SEMESTER : 4 (Empat)

PERTEMUAN KE : 1

KOMPETENSI DASAR : Mengevaluasi permasalahan *routing* dinamis

MATERI : Konfigurasi Routing Static dan Dinamis

Konfigurasi Routing Static dan Dinamis

Routing, adalah sebuah proses untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah internetwork. Routing juga dapat merujuk kepada sebuah metode penggabungan beberapa jaringan sehingga paket-paket data dapat hinggap dari satu jaringan ke jaringan selanjutnya.

Untuk melakukan hal ini, digunakanlah sebuah perangkat jaringan yang disebut sebagai router. Router-router tersebut akan menerima paket-paket yang ditujukan ke jaringan di luar jaringan yang pertama, dan akan meneruskan paket yang ia terima kepada router lainnya hingga sampai kepada tujuannya.

Static routing (Routing Statis) adalah sebuah router yang memiliki tabel routing statik yang di setting secara manual oleh para administrator jaringan. Routing static pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statik murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut.

Penggunaan routing statik dalam sebuah jaringan yang kecil tentu bukanlah suatu masalah, hanya beberapa entri yang perlu diisikan pada forwarding table di setiap router. Namun Anda tentu dapat membayangkan bagaimana jika harus melengkapi forwarding table di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar.

Dynamic Routing (Router Dinamis) adalah sebuah router yang memiliki dan membuat tabel routing secara otomatis, dengan mendengarkan lalu lintas jaringan dan juga dengan saling berhubungan antara router lainnya.

Protokol routing mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi forwarding table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan data ke arah yang benar.

Dengan kata lain, routing dinamik adalah proses pengisian data routing di table routing secara otomatis.

Dynamic routing mempelajari sendiri Rute yang terbaik yang akan ditempuhnya untuk meneruskan paket dari sebuah network ke network lainnya. Administrator tidak menentukan rute yang harus ditempuh oleh paket-paket tersebut.

Administrator hanya menentukan bagaimana cara router mempelajari paket, dan kemudian router mempelajarinya sendiri. Rute pada dynamic routing berubah, sesuai dengan pelajaran yang didapatkan oleh router.

Perbedaan Static Routing dan Dynamic Routing

Pada dasarnya perbedaan antara routing statis dengan routing dinamis adalah cara mengenalkan alamat networknya.

1. Routing dinamis pada prinsipnya hanya mengenalkan network yang berhubungan dengan router yang bersangkutan (tanpa mengetahui subnet masknya). Sedangkan Routing Statis harus mengenalkan setiap alamat pada setiap network yang ingin dituju, jadi harus tahu semua alamat network yang ingin dituju. Semakin luas jaringannya, maka table routenya pun semakin banyak dan lebih rumit dibandingkan dengan Routing Dinamis.

2. Routing Dinamis sangat cocok untuk topologi jaringan yang lingkupnya besar (terhubung ke banyak network). Sedangkan routing statis cocok untuk topologi jaringan yang simple.

Kelebihan Routing Statis

1. Beban kerja router terbilang lebih ringan dibandingkan dengan routing dinamis. Karena pada saat konfigurasi router hanya mengupdate sekali saja ip table yang ada.
2. Pengiriman paket data lebih cepat karena jalur atau rute sudah di ketahui terlebih dahulu.
3. Deteksi dan isolasi kesalahan pada topologi jaringan lebih mudah

Kekurangan Routing Statis

Harus tahu semua alamat network yang akan dituju beserta subnet mask dan next hoopnya (gateway nya)

Kelebihan Routing Dinamis

1. Hanya mengenalkan alamat network yang terhubung langsung dengan routernya.
2. Tidak perlu mengetahui semua alamat network yang ada.
3. Bila terjadi penambahan suatu network baru tidak perlu semua router mengkonfigurasi. Hanya router-router yang berkaitan.

Kekurangan Routing Dinamis

1. Beban kerja router lebih berat karena selalu memperbarui ip table pada tiap waktu tertentu.
2. Kecepatan pengenalan network terbilang lama karena router membroadcast ke semua router hingga ada yang cocok.
3. Setelah konfigurasi harus menunggu beberapa saat agar setiap router mendapat semua Alamat IP yang ada.
4. Susah melacak permasalahan pada suatu topologi jaringan lingkup besar

PENUGASAN

Petunjuk Mengerjakan :

1. **Kerjakanlah soal – soal berikut ini di buku catatan masing-masing**
2. **Tugas dikumpulkan dengan cara fotolah hasil dari mengerjakan di poin 1 dan dikumpulkan di group kelas masing-masing.**
3. **File foto tugas berilah nama : nama siswa_routing**

SOAL

1. Bagaimanakah cara kerja router?
2. Apakah yang dimaksud routing statis?
3. Apakah yang Anda ketahui tentang routing dinamis?
4. Apakah perbedaan antara routing statis dengan routing dinamis?
5. Apakah kelebihan routing dinamis?

Sistematika Penyusunan Materi Pembelajaran (Daring)

MATA PELAJARAN : Administrasi Infrastruktur Jaringan (AIJ)

KOMPETENSI KEAHLIAN : TKJ

KELAS/SEMESTER : 4 (Empat)

PERTEMUAN KE : 2

KOMPETENSI DASAR : Mengevaluasi *firewall* jaringan

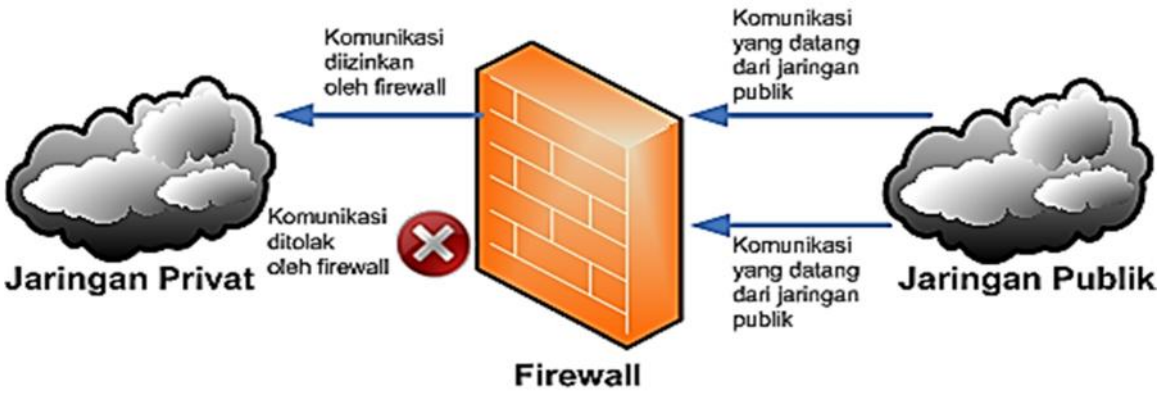
MATERI : *Firewall* jaringan

URAIAN MATERI

Untuk pembahasan kali ini kami akan mengulas mengenai Firewall yang dimana dalam hal ini meliputi pengertian, fungsi, cara kerja, karakteristik dan manfaat, nah agar lebih dapat memahami dan dimengerti simak ulasan selengkapnya dibawah ini.

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar. Firewall merupakan suatu cara untuk memastikan bahwa data pada komputer atau server Web yang terhubung tidak akan bisa diakses siapa saja di Internet.

Pihak lain yang mengakses informasi pribadi atau mengubah situs Web anda akan di blokir oleh Firewall. yaitu seperangkat program yang saling terhubung, yang beerada di server gateway jaringan, yang berfungsi untuk melindungi sumber daya dari jaringan pribadi dari pengguna dari jaringan lain.



Dengan intranet suatu perusahaan memungkinkan pekerjanya mengakses ke Internet lebih luas menginstal firewall untuk mencegah orang luar mengakses sumber daya pribadi untuk mengendalikan data.

Firewall, pada dasarnya bekerja sama dengan program router yang memeriksa setiap paket jaringan supaya dapat menentukan apakah akan maju ke arah tujuannya. Firewall juga bekerja dengan proxy server yang membuat permintaan jaringan atas nama pengguna workstation.

Komputer yang dirancang khusus terpisah dari sisa jaringan sering diinstal Firewall, sehingga tidak ada permintaan yang masuk bisa langsung pada sumber daya jaringan pribadi.

Fungsi Firewall

1. Mengontrol dan mengawasi arus paket data yang mengalir di jaringan.
2. Firewall berfungsi juga dalam mengaturm memfilter dan mengontrol lalulintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :
   - Alamat IP dari komputer sumber
   - Port TCP/UDP sumber dari sumber.
   - Alamat IP dari komputer tujuan.
   - Port TCP/UDP tujuan data pada komputer tujuan
   - Informasi dari header yang disimpan dalam paket data.
   - Melakukan autentifikasi terhadap akses kejaringan.
   - Applikasi firewall mampu memeriksa lebih dari sekedar header dari paket data.

Manfaat penggunaan Firewall

1. Menjaga informasi rahasia dan berharga yang menyelinap keluar tanpa sepengetahuan.
2. Sebagai filter yang digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan.
3. Memodifikasi paket data yang data di firewall, proses tersebut *Network Address Translation (NAT).*
4. Sebagai Akurasi data seperti informasi keuangan, spesifikasi produk, harga produk dll.

Cara Kerja Firewall

1. Sistem firewall bekerja dengan cara menganalisis paket data yang keluar dan masuk ke dalam lingkungan aman yang dilindungi oleh sistem firewall tersebut. Paket data yang tidak lolos analisis akan ditolak untuk masuk ataupun keluar jaringan atau komputer yang dilindungi.
2. Penyaring atau filter firewall akan bekerja melakukan pemeriksaan sumber dari paket data yang masuk dengan kebijakan yang dibuat untuk mengontrol paket dari mana

saja yang boleh masuk. Sistem juga dapat melakukan pemblokiran pada jenis jaringan tertentu serta melakukan pencatatan pada lalu lintas paket data yang mencurigakan.

Jenis-Jenis Firewall

Berikut ini terdapat beberapa jenis-jenis firewall, diantaranya adalah:

1. Personal Firewall

Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya.

2. Network Firewall

Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server.

Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. yang dibundel dalam sistem operasi Solaris.

Network Firewall secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh personal firewall (packet filter firewall dan stateful firewall), Circuit Level Gateway, Application Level Gateway, dan juga NAT Firewall. Network Firewall umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

3. IP Filtering Firewall : Sebuah IP Filtering firewall bekerja pada level paket
4. Proxy Server : Cara kerja proxy server, terlihat saat user terhubung dengan proxy server dengan perangkat lunak client, proxy server akan menduplikasi komunikasi tersebut.

PENUGASAN

Petunjuk Mengerjakan :

1. **Kerjakanlah soal – soal berikut ini di buku catatan masing-masing**
2. **Tugas dikumpulkan dengan cara fotolah hasil dari mengerjakan di poin 1 dan dikumpulkan di group kelas masing-masing.**
3. **File foto tugas berilah nama : nama siswa_firewall**

SOAL

1. Apakah yang dimaksud firewall?
2. Apakah fungsi firewall?
3. Bagaimanakah cara kerja firewall?
4. Sebutkan manfaat penggunaan firewall!
5. Sebutkan kriteria firewall dalam melewatiu paket data!
6. Jelaskan Jenis-jenis Firewall !

Sistematika Penyusunan Materi Pembelajaran (Daring)

MATA PELAJARAN : Administrasi Infrastruktur Jaringan (AIJ)

KOMPETENSI KEAHLIAN : TKJ

KELAS/SEMESTER : 4 (Empat)

PERTEMUAN KE : 3 (Tiga)

KOMPETENSI DASAR : Menganalisis permasalahan *firewall* jaringan

MATERI : Permasalahan *Firewall* jaringan

URAIAN MATERI

Permasalahan pada firewall jaringan dapat mengakibatkan terancamnya keamanan pada system jaringan komputer. Untuk mencegah permasalahan itu timbul,seorang administrator jaringan sebaiknya melakukan pemeriksaan firewall jaringan secara berkala.

Permasalahan pada Firewall jaringan

Firewall pada jaringan memiliki permasalahan yang sedikit rumit. Sebelum melakukan pemeriksaan terhadap firewall jaringan,kita sebaiknya memahami dulu konsep firewall yang kita gunakan.

Hal ini juga berlaku pada firewall iptables. Pahami firewall iptables berikut.

a. Rule/aturan dimulai dari atas turun kebawah. Kecuali diperintahkan untuk membuat sebaliknya.
b. Sebuah rule atau aturan yang sama,apabila kita tidak memberikan informasi secara lengkap,paket yang tidak diinginkan akan tetap menyelinap masuk.
c. Setelah menerima,menolak,atau memblokir paket,iptables tidak akan memprosesrula/aturan lebih lanjut.

Setelah memahami konsep firewall, untuk melakukan pemeriksaan langkah selanjutnya adalah mengerti permasalahan umum yang sering terjadi pada firewall tersebut.

Permasalahan umum yang sering terjadi pada firewall iptables adalah sebagai berikut.

a. Tidak menerima lalu lintas yang seharusnya diizinkan
b. Menerima lalu lintas yang seharusnya tidak diizinkan.Jika server secara acak memblokir atau menerima lalu lintas, hal ini memerlukan lebihbanyak pemecah masalah. Pemecahaan masalah adalah proses yang memakan waktu dan butuh kesabaran

Saat anda ingin mensetting firwall pada komputer anda tampil pesan Due to an unidentified problem, Windows cannot display Windows Firewall settings, apa yang terjadi, menurut informasi dari microsoft adalah sbb :

- Windows Firewall/Internet Connection Sharing (ICS) is not displayed in the Services list in Control Panel.
- Windows Firewall/Internet Connection Sharing (ICS) is displayed in the Services list, but you cannot start this service.
- anda menerima pesan galat “Due to an unidentified problem, Windows cannot display Windows Firewall settings.” ketika anda mencoba mengakses setting windows firewall

Permasalahan:

Masalah ini disebabkan file SharedAccess.reg hilang atau rusak. sebuah File yang mewakili SharedAccess.reg layanan Windows Firewall.

Penyelesaian:

Untuk mengatasi masalah ini, gunakan salah satu metode berikut :

Metode 1:

Cari “Setup API InstallHinfSection” fungsi untuk menginstal Windows Firewall
Untuk menginstal windows firewall ikuti langkah-langkah ini

- klik start, klik run, ketik cmd, kemudian klik ok
- pada prompt perintah, ketik baris berikut
- Rundll32 setupapi,InstallHinfSection Ndi-Steelhead 132 %windir%\inf\netrass.inf kemudian tekan ENTER
- Restart Windows,
- klik start, klik run, ketik cmd, kemudian klik ok
- pada prompt perintah, ketik baris berikut Netsh firewall reset kemudian tekan ENTER.
- klik start, klik run, ketik firewall.cpl dan kemudian tekan ENTER. Dalam kotak dialog Windows Firewall, klik On (disarankan), dan kemudian klik OK.

Metode 2:

Karena untuk metode ke 2 ini sedikit bermain dengan regsitry, jadi saya sarankan anda untuk memabaca lebih detail pada situs microsoft itu sendiri klik disini untuk mulai membaca.
Informasi tambahan:
Untuk memverifikasi bahwa Layanan Windows Firewall telah berjalan, ikuti langkah berikut

- klik start, klik run, ketik services.msc , kemudian klik ok
- Dalam daftar layanan, cari Windows Firewall / Internet Connection Sharing (ICS). Perhatikan bahwa status layanan Started tandanya windows firewall sudah aktif.

Cara yang lain

- download file sharedaccess.reg
- setelah di download kemudian extract dulu,,
- double klik file sharedaccess.reg agar di merge dengan registry di windows
- kemudian restart komputer anda.
- setelah restart,
- pada run, ketik cmd
- muncul command console, ketik netsh firewall reset
- kemudian coba buka firewall

jika masih belum bisa

- pada run, jalankan command ini,
- rundll32 setupapi,InstallHinfSection Ndi-Steelhead 132 %windir%\inf\netrass.inf
- restart komputer
- setelah restart, pada run ketik cmd /k netsh firewall reset
- coba buka kembali firewall anda

belum bisa lagi

- pada run ketik, netsh winsock reset
- kemudian restart
- cek windows firewall anda.

Cara Mengatasi Windows Firewall yang tidak bisa dibuka (error)

Permasalahan:
Masalah ini disebabkan oleh SharedAccess.reg hilang atau file rusak. sebuah File yang mewakili SharedAccess.reg layanan Windows Firewall.

Penyelesaian:
Untuk mengatasi masalah ini, gunakan salah satu metode berikut Download file sharedaccess.reg, setelah di download kemudian extract dulu,, double klik file sharedaccess.reg agar di merge dengan registry di windows kemudian restart komputer anda.

Cara 1:
Panggil "Setup API InstallHinfSection" fungsi untuk menginstal Windows Firewall
Untuk menginstal windows firewall ikuti langkah-langkah ini

* klik start, klik run, ketik cmd, kemudian klik ok
* pada prompt perintah, ketik baris berikut :

Rundll32 setupapi,InstallHinfSection Ndi-Steelhead 132 %windir%\inf\netrass.inf kemudian tekan ENTER

* Restart Windows,

* klik start, klik run, ketik cmd, kemudian klik ok
* pada prompt perintah, ketik baris berikut Netsh firewall reset kemudian tekan ENTER.
klik start, klik run, ketik firewall.cpl dan kemudian tekan ENTER. Dalam kotak dialog Windows Firewall, klik On (disarankan), dan kemudian klik OK.

Cara 2:
Karena untuk metode ke 2 ini sedikit bermain dengan regsitry, jadi saya sarankan anda untuk memabaca
lebih detail pada situs microsoft itu sendiri klik disini untuk mulai membaca.

Informasi tambahan:
Untuk memverifikasi bahwa Layanan Windows Firewall telah berjalan, ikuti langkah berikut
* klik start, klik run, ketik services.msc , kemudian klik ok
* Dalam daftar layanan, cari Windows Firewall / Internet Connection Sharing (ICS). Perhatikan
bahwa status layanan Started tandanya windows firewall sudah aktif.
Jika masih belum bisa, ya berarti windows anda perlu di install ulang lagi

PENUGASAN

Petunjuk Mengerjakan :

1. **Kerjakanlah soal – soal berikut ini di buku catatan masing-masing**
2. **Tugas dikumpulkan dengan cara fotolah hasil dari mengerjakan di poin 1 dan dikumpulkan di group kelas masing-masing.**
3. **File foto tugas berilah nama : nama siswa_permasalahanfirewall**

SOAL

1. Bagaimanakah cara menyelesaikan permasalahan file shared access.reg hilang atau rusak?
2. Bagaimanakah cara memverifikasi firewall sudah berjalan?
3. Bagaimana cara mengatasi SharedAccess.reg hilang atau file rusak?
4. Bagaimanakah cara memverifikasi bahwa Layanan Windows Firewall telah berjalan?
5. Apakah yang harus dilakukan apabila sudah memverifikasi windows firewall tetapi tetap tidak berjalan?
6. Jelaskan permasalahan umum yang sering terjadi pada firewall iptables!