Materi firewall

Karakteristik Firewall

Karakteristik Firewall atau ciri-ciri dari firewall adalah:

- Firewall harus dapat lebih kuat dan tangguh terhadap serangan di luar. Hal ini artinya sistem operasi komputer akan lebih aman dan penggunaan sistem bisa diandalkan.
- Yang dapat melakukan hubungan adalah aktivitas yang dikenal atau terdaftar pada jaringan. Dalam hal ini dilaksanakan dengan cara setting policy pada konfigurasi keamanan lokal.
- Seluruh kegiatan yang asalnya dari dalam ke luar harus melalui firewall lebih dulu. Hal ini dilaksanakan dengan memberikan batasan atau meblokir setiap akses kepada jaringan lokal, terkecuali jika melalui firewall terlebih dahulu.

Teknologi firewall

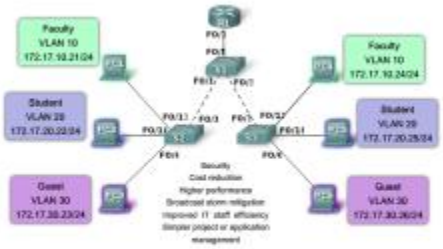
- Packet-filtering firewall; sebuah teknologi firewall yang bekerja pada titik-titik tempat pertemuan berbagai perangkat.

- Circuit-level gateway; sebuah teknologi firewall yang mengawasi seluruh pergerakan informasi melalui protokol internet di seluruh jaringan untuk menentukan terpercaya atau tidaknya sebuah koneksi.
- Stateful inspection firewall; sebuah teknologi firewall yang tidak hanya memeriksa isi dari sebuah paket informasi, melainkan riwayat paket tersebut dalam hubungannya dengan protokol atau jaringan-jaringan terdahulu yang perndah terdeteksi.
- Application-level gateway; sebuah teknologi firewall dalam bentuk proksi yang menggabugnkan kemampuan packet filtering dan circuit-level gateway firewall. Teknologi ini menentukan tingkat kepercayaan sebuah koneksi berdasarkan layanan yang dituju.
- Next-generation firewall; sebuah teknologi firewall yang memeriksa setiap isi dari paket data yang masuk atau keluar, termasuk sesi penelusuran internet yang sedang berjalan, bahkan jika dikombinasikan dengan koneksi dari sebuah perangkat jaringan HTTPS.

- **Pengertian dan Konfigurasi VLAN**
- Kinerja sebuah jaringan sangat dibutuhkan oleh organisasi terutama dalam hal kecepatan dalam pengiriman data. Salah satu kontribusi teknologi untuk meningkatkan kinerja jaringan adalah dengan kemampuan untuk membagi sebuah broadcast domain yang besar menjadi beberapa broadcast domain yang lebih kecil dengan menggunakan VLAN. Broadcast domain yang lebih kecil akan membatasi device yang terlibat dalam aktivitas broadcast dan membagi device ke dalam beberapa grup berdasar fungsinya, se[erti layanan databasse untuk unit akuntansi, dan data transfer yang cepat untuk unit teknik.
- Teknologi VLAN (Virtual Local Area Network) bekerja dengan cara melakukan pembagian network secara logika ke dalam beberapa subnet. VLAN adalah kelompok device dalam sebuah LAN yang dikonfigurasi (menggunakan software manajemen) sehingga mereka dapat saling berkomunikasi asalkan dihubungkan

dengan jaringan yang sama walaupun secara fisikal mereka berada pada segmen LAN yang berbeda. Jadi VLAN dibuat bukan berdasarkan koneksi fisikal namun lebih pada koneksi logikal, yang tentunya lebih fleksibel. Secara logika, VLAN membagi jaringan ke dalam beberapa subnetwork. VLAN mengijinkan banyak subnet dalam jaringan yang menggunakan switch yang sama.

- Dengan menggunakan VLAN, kita dapat melakukan segmentasi jaringan switch berbasis pada fungsi, departemen atau pun tim proyek. Kita dapat juga mengelola jaringan kita sejalan dengan kebutuhan pertumbuhan perusahaan sehingga para pekerja dapat mengakses segmen jaringan yang sama walaupun berada dalam lokasi yang berbeda. Contoh penerapan teknologi VLAN diberikan dalam Gambar 1.



-

- gambar 1

- Beberapa keuntungan penggunaan VLAN antara lain:
- 1. *Security* – keamanan data dari setiap divisi dapat dibuat tersendiri, karena segmennya bisa dipisah secara logika. Lalu lintas data dibatasi segmennya.
- 2. *Cost reduction* – penghematan dari penggunaan bandwidth yang ada dan dari upgrade perluasan network yang bisa jadi mahal.
- 3. *Higher performance* – pembagian jaringan layer 2 ke dalam beberapa kelompok broadcast domain yang lebih kecil, yang tentunya akan mengurangi lalu lintas packet yang tidak dibutuhkan dalam jaringan.
- 4. *Broadcast storm mitigation* – pembagian jaringan ke dalam VLAN-VLAN akan mengurangi banyaknya device yang berpartisipasi dalam pembuatan broadcast storm. Hal ini terjadinya karena adanya pembatasan broadcast domain.
- 5. *Improved IT staff efficiency* – VLAN memudahkan manajemen jaringan karena

pengguna yang membutuhkan sumber daya yang dibutuhkan berbagi dalam segmen yang sama.

- 6. *Simpler project or application management* – VLAN menggabungkan para pengguna jaringan dan peralatan jaringan untuk mendukung perusahaan dan menangani permasalahan kondisi geografis.
- Untuk memberi identitas sebuah VLAN digunakan nomor identitas VLAN yang dinamakan VLAN ID. Digunakan untuk menandai VLAN yang terkait. Dua range VLAN ID adalah:
- a. Normal Range VLAN (1 – 1005)
- – digunakan untuk jaringan skala kecil dan menengah.
- – Nomor ID 1002 s.d. 1005 dicadangkan untuk Token Ring dan FDDI VLAN.
- – ID 1, 1002 – 1005 secara default sudah ada dan tidak dapat dihilangkan.
- – Konfigurasi disimpan di dalam file database VLAN, yaitu vlan.dat. file ini disimpan dalam memori flash milkik switch.

- – VLAN trunking protocol (VTP), yang membantu manaejemn VLAN, nanti dipelajari di bab 4, hanya dapat bekerja pada normal range VLAN dan menyimpannya dalam file database VLAN.
- b. Extended Range VLANs (1006 – 4094)
- – memampukan para seervice provider untuk memperluas infrastrukturnya kepada konsumen yang lebih banyak. Dibutuhkan untuk perusahaan skala besar yang membutuhkan jumlah VLAN lebih dari normal.
- – Memiliki fitur yang lebih sedikit dibandingakn VLAN normal range.
- – Disimpan dalam NVRAM (file running configuration).
- – VTP tidak bekerja di sini.
- Switch catalys 2960 mendukung 255 normal range dan extended range.
- Berikut ini diberikan beberapa terminologi di dalam VLAN.
- a. VLAN Data
- VLAN Data adalah VLAN yang dikonfigurasi hanya untuk membawa data-data yang

digunakan oleh user. Dipisahkan dengan lalu lintas data suara atau pun manajemen switch. Seringkali disebut dengan VLAN pengguna, User VLAN.

- b. VLAN Default
- Semua port switch pada awalnya menjadi anggota VLAN Default. VLAN Default untuk Switch Cisco adalah VLAN 1. VLAN 1 tidak dapat diberi nama dan tidak dapat dihapus.
- c. Native VLAN
- Native VLAN dikeluarkan untuk port trunking 802.1Q. port trunking 802.1Q mendukung lalu lintas jaringan yang datang dari banyak VLAN (*tagged traffic*) sama baiknya dengan yang datang dari sebuah VLAN (*untagged traffic*). Port trunking 802.1Q menempatkan *untagged traffic* pada Native VLAN.
- d. VLAN Manajemen
- VLAN Manajemen adalah VLAN yang dikonfigurasi untuk memanajemen switch. VLAN 1 akan bekerja sebagai Management VLAN jika kita tidak mendefinisikan VLAN khusus sebagai VLAN Manajemen. Kita dapat memberi IP address dan subnet mask

pada VLAN Manajemen, sehingga switch dapat dikelola melalui HTTP, Telnet, SSH, atau SNMP.

- e. VLAN Voice
- VLAN yang dapat mendukung Voice over IP (VoIP). VLAN yang dikhusukan untuk komunikasi data suara.
- Terdapat 3 tipe VLAN dalam konfigurasi, yaitu:
- a. Static VLAN – port switch dikonfigurasi secara manual.
- Konfigurasi:
- SwUtama#config Terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- SwUtama(config)#VLAN 10
- SwUtama(config-vlan)#name VLAN_Mahasiswa
- SwUtama(config-vlan)#exit
- SwUtama(config)#Interface fastEthernet 0/2
- SwUtama(config-if)#switchport mode access
- SwUtama(config-if)#switchport access VLAN 10

- b. Dynamic VLAN – Mode ini digunakan secara luas di jaringan skala besar. Keanggotaan port Dynamic VLAN dibuat dengan menggunakan server khusu yang disebut VLAN Membership Policy Server (VMPS). Dengan menggunakan VMPS, kita dapat menandai port switch dengan VLAN? secara dinamis berdasar pada MAC Address sumber yang terhubung dengan port.
- c. Voice VLAN – port dikonfigurasi dalam mode voice sehingga dapat mendukung IP phone yang terhubung.
- Konfigurasi:
- SwUtama(config)#VLAN 120
- SwUtama(config-vlan)#name VLAN_Voice
- SwUtama(config-vlan)#exit
- SwUtama(config)#Interface fastEthernet 0/3
- SwUtama(config-if)#switchport voice VLAN 120
- Berikut ini diberikan sedikit command untuk konfigurasi dasar VLAN pada Swicth Cisco Catalyst
- **Langkah 1:Membuat VLAN**

- (secara default, hanya ada satu VLAN, yaitu VLAN 1)
- syntax
- Switch#configure terminal
  Switch(config)#vlan NomorVLAN
  Switch(config-vlan)#name NamaVLAN
- contoh: untukmembuat VLAN dengan ID nomor 10 nama marketing.
- Switch#configure terminal
  Switch(config)#vlan 10
  Switch(config-vlan)#name marketing
  Switch(config-vlan)#end
- **Langkah 2: Verifikasi VLAN yang sudah dibuat:**
- Command: Switch#sh vlan brief
- **Langkah 3: Memasukkan Port menjadi anggota suatu VLAN**
- (secara default semua port dalam switch menjadi anggota VLAN 1)
- Contoh: memasukkan Port Fa0/1 menjadi anggota VLAN 10:
- Switch#configure terminal
  Switch(config)#interface fa0/1
  Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10
Switch(config-if)#end

- Jika Anda ingin memasukkan beberapa port bersama-sama menjadi anggota port 10, bisa juga menggunakan interface range. misal Anda ingin memasukkan port Fa0/1 sampai dengan Fa0/6, maka urutan perintahnya adalah:
- Switch#configure terminal
  Switch(config)#interface range fa0/1 – fa0/6
  Switch(config-if-range)#switchport mode access
  Switch(config-if-range)#switchport access vlan 10
- **Langkah 4: Verifikasi Pengaturan Port Menjadi anggota VLAN:**
- Switch#sh vlan brief
- VLAN Name Status Ports
  —- ——————————– ——— ———
  ——————————-
  1 default active Fa0/7, Fa0/8, Fa0/9, Fa0/10
  Fa0/11, Fa0/12, Fa0/13, Fa0/14
  Fa0/15, Fa0/16, Fa0/17, Fa0/18
  Fa0/19, Fa0/20, Fa0/21, Fa0/22
  Fa0/23, Fa0/24, Gig1/1, Gig1/2

10 marketing active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

- **Menghapus VLAN**: Bila Anda Menghapus sebuah VLAN, Anda dapat menggunakan perintah “no vlan NomorVlan.
- contoh: perintah untukmenghapus VLAN 10:
- Switch#configure terminal
  Switch(config)#no vlan 10
- Apakah yang dimaksud dengan Intra-VLAN? Device apa saja yang dibutuhkan?Komunikasi antar host yang berada dalam VLAN ID yang sama dinamakan dengan Intra-VLAN. Komunikasi antar host dalam sebuah VLAN dengan host dalam VLAN yang lain dinamakan Inter-VLAN. Tentunya dalam komunikasi Inter-VLAN dibutuhkan sebuah Router karena mereka berbeda network.

- Switch layer 3 dapat membuat route di antara VLAN-VLAN dengan menggunakan teknologi *switch virtual interface* (SVI). SVI merupakan interface (secara logika) yang dikonfigurasi untuk suatu VLAN. SVI perlu dikonfigurasi untuk membuat route antar VLAN atau untuk memberikan koneksi IP dengan host. Secara default, SVI dibuat untuk VLAN 1 sehingga bisa dikelola secara remote.
- Sebuah VLAN Native ditandai dengan sebuah port trunk 802.1Q. Sebuah port trunk 802.1Q mendukung traffic dari banyak VLAN sama seperti traffic yang tidak berasal dari sebuah VLAN. Trunk adalah link point-to point diantara satu atau lebih interface ethernet device jaringan seperti router atau switch. Trunk Ethernet membawa lalu lintas dari banyak VLAN melalui link tunggal. Sebuah VLAN trunk mengijinkan kita untuk memperluas VLAN melalui seluruh jaringan. Jadi link Trunk digunakan untuk menghubungkan antar device intermediate. Dengan menggunakan port trunk, dapat digunakan sebuah link fisik

untuk menghubungkan banyak VLAN. Gambar 2 dan 3 memberikan perbandingan tanpa trunking dengan penggunaan link trunk.

- Sebuah Port pada Switch Cisco Catalyst mempunyai beberapa mode trunk. Mode trunking tersebut didefinisikan untuk negosiasi antar port yang saling berhubungan dengan menggunakan Dynamic Trunking Protocol (DTP). DTP merupakan sebuah protokol keluaran Cisco. Switch dari vendor lain tidak mendukung DTP. DTP mengatur negosiasi mode trunk hanya jika port switch dikonfigurasi dalam mode trunk yang mendukung DTP. DTP mendukung baik ISL maupun 802.1Q. Ada tiga mode trunk pada DTP, yaitu: Trunk, Access, Dynamic Auto dan Dynamic Desirable.
- **I.Definisi VLAN**
-
-
- Virtual Local Area Network (VLAN) adalah metode untuk menciptakan jaringan-jaringan yang secara logika tersusun

sendiri-sendiri. VLAN sendiri berada dalam jaringan Local Area Network (LAN), sehingga dalam jaringan (LAN) bisa terdapat satu atau lebih VLAN. Dengan demikian kita dapat mengambil kesimpulan bahwa dalam dalam suatu jaringan, kita dapat membuat lagi satu atau lebih jaringan (jaringan di dalam jaringan).
Konfigurasi VLAN itu sendiri dilakukan melalui perangkat lunak (software), sehingga walaupun komputer tersebut berpindah tempat, tetapi ia tetap berada pada jaringan VLAN yang sama.

- II. Manfaat VLAN
- Beberapa manfaat VLAN adalah ;
- 1. Performance.
  VLAN mampu mengurangi jumlah data yang dikirim ke tujuan yang tidak perlu. Sehingga lalu lintas data yang terjadi di jaringan tersebut dengan sendirinya akan berkurang.
- 2. Mempermudah Administrator Jaringan.
  Setiap kali komputer berpindah tempat, maka komputer tersebut harus di konfigurasi ulang agar mampu

berkomunikasi dengan jaringan dimana komputer itu berada. Hal ini membuat komputer tersebut tidak dapat dioperasikan langsung setelah di pindahkan.
Jaringan dengan Prinsip VLAN bisa meminimalkan atau bahkan menghapus langkah ini karena pada dasarnya ia tetap berada pada jaringan yang sama.

- 3. Mengurangi biaya.
  Dengan berpindahnya lokasi, maka seperti hal nya diatas, akan menyebabkan biaya instalasi ulang. Dalam jaringan yang menggunakan VLAN, hal ini dapat diminimallisira atau dihapuskan.
- 4. Keamanan
  VLAN bisa membatasi Pengguna yang bisa mengakses suatu data., sehingga mengurangi kemungkinan terjadinya penyalahgunaan hak akses.
- III. Jenis VLAN
- Berdasarkan perbedaan pemberian membership, maka VLAN bisa dibagi menjadi empat :
  1.Port based
  Dengan melakukan konfigurasi pada port

dan memasukkannya pada kelompok VLAN sendiri. Apabila port tersebut akan dihubungkan dengan beberapa VLAN maka port tersebut harus berubah fungsi menjadi port trunk (VTP)

- 2.MAC based
  Membership atau pengelompokan pada jenis ini didasarkan pada MAC Address . Tiap switch memiliki tabel MAC Address tiap komputer beserta kelompok VLAN tempat komputer itu berada
- 3.Protocol based
  Karena VLAN bekerja pada layer 2 (OSI) maka penggunaan protokol (IP dan IP Extended) sebagai dasar VLAN dapat dilakukan.
- 4.IP Subnet Address based
  Selaij bekerja pada layer 2, VLAN dapat bekerja pada layer 3, sehingga alamat subnet dapat digunakan sebagai dasar VLAN
- 5. Authentication based
  Device atau komputer bisa diletakkan secara otomatis di dalam jaringan VLAN yang didasarkan pada autentifikasi user

atau komputer menggunakan protokol 802.1x

- Sedangkan dari tipe koneksi dari VLAN dapat di bagi atas 3 yaitu :
  1. Trunk Link
  2. Access Link
  3. Hibrid Link (Gabungan Trunk dengan Access)
- IV. Prinsip kerja VLAN
  Terbagi atas
  1. Filtering Database
  Berisi informasi tentang pengelompokan VLAN. Terdiri dari
  A. Static Entries
  a.Static Filtering Entries:
  Mespesifisifikasikan apakah suatu data itu akan dikirim atau dibuang atau juga di masukkan ke dalam dinamic entries
- b.Static Registration Entries
  Mespesifisifikasikan apakah suatu data itu akan dikirim ke suatu jaringan VLAN dan port yang bertanggung jawab untuk jaringan VLAN tersebut
- B. Dynamic Entries
  a.Dynamic Filtering Entries

Mespesifisifikasikan apakah suatu data itu akan dikirim atau dibuang

- b.Group Registration Entries
  Mespesifisifikasikan apakah suatu data yang dikirim ke suatu group atau VLAN tertentu akan dikirim/diteruskan atau tidak
- c.Dynamic Registration Entries
  Menspesifikasikan port yang bertanggung jawab untuk suatu jaringan VLAN
- 2. Tagging
  Saat sebuah data dikirimkan maka harus ada yang menyatakan Tujuan data tersebut (VLAN tujuan). Informasi ini diberikan dalam bentuk tag header , sehingga:
- a. informasi dapat dikirimkan ke user tertentu saja (user tujuan)
  b. dan didalam nya berisi format MAC Address
- jenis dari tag header
  a. Ethernet Frame Tag Header
  b. Token Ring and Fiber Distributed Data Interface (FDDI) tag header