PERTEMUAN 17

FOTIGATE FIREWALL

A. TUJUAN PEMBELAJARAN

Pada bab ini akan dijelaskan mengenai Fortigate Firewall

B. URAIAN MATERI

1. Macam-macam Proteksi Keamanan Sistem

a. Firewall

Firewall dapat diartikan sebagai suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman.

Istilah firewall ini berasal dari bahasa inggris yaitu fire yang berarti api dan wall yang berarti dinding. Jadi, menurut bahasa, arti dari firewall adalah dinding api. Sedangkan fungsi dari sebuah dinding adalah melindungi sesuatu yang ada di dalam dari sesuatu yang ada dari luar. Begitu pula firewall yang mempunyai fungsi untuk melindungi suatu jaringan atau komputer dari akses lain yang tidak memiliki hak akses atas jaringan atau computer lokal.

Firewall dapat berarti suatu mekanisme/sistem/cara yang diterapkan baik terhadap suatu sistem pada jaringan, software, atau hardware itu sendiri dengan tujuan melindungi (membatasi, menyaring, dan menolak) suatu kegiatan pada jaringan yang sifatnya pribadi dengan jaringan luar yang tidak pada ruang lingkupnya.

Secara mendasar, fungsi dari firewall adalah sebagai berikut :

1. Mengatur dan mengontrol lalu lintas jaringan
2. Melakukan autentikasi terhadap akses
3. Melindungi sumber daya dalam jaringan privat
4. Mencatat semua kejadian, dan melaporkan kepada administrator

Beberapa karakteristik dari firewall

1. Firewall harus lebih kuat dan kebal terhadap serangan luar. Hal ini berarti bahwa Sistem Operasi akan relatif lebih aman dan penggunaan sistemnya dapat dipercaya.
2. Hanya aktivitas atau kegiatan yang dikenal/terdaftar saja yang dapat melewati atau melakukan hubungan. Hal ini dilakukan dengan menyetting policy pada konfigurasi keamanan lokal.
3. Semua aktivitas atau kegiatan dari dalam ke luar harus melewati firewall. Hal ini dilakukan dengan membatasi atau memblok semua akses terhadap jaringan lokal, kecuali jika melewati firewall terlebih dahulu.

Sedangkan untuk jenis-jenis firewall dapat dibagi menjadi 2 macam, yaitu :

1. Personal Firewall

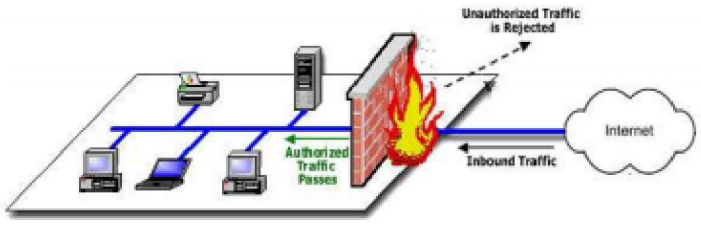
Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.

Contoh : Microsoft Windows Firewall (yang telah terintegrasi dalam sistem operasi Windows XP Service Pack 2, Windows Vista dan Windows Server 2003 Service Pack 1), Symantec Norton Personal Firewall, Kerio Personal Firewall, dan lain-lain.

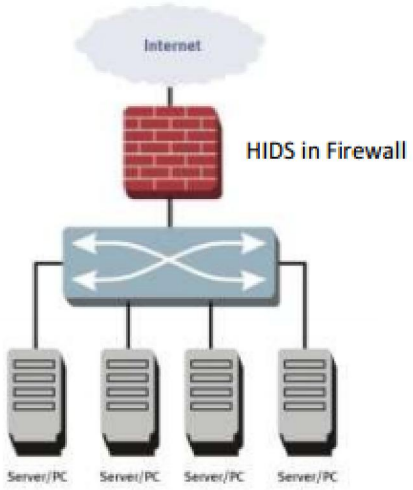
2. Network Firewall

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 : Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, dan produk Fortinet.



b. Intrusion Detection System (IDS)



Intrusion Detection System adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Ada dua jenis IDS, yaitu:

1. Network-based Intrusion Detection System (NIDS): Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.
2. Host-based Intrusion Detection System (HIDS): Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

Implementasi dan cara kerja :

1. Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.
2. Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan false positive. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan false positive yang muncul.
3. Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

c. Intrusion Prevention System (IPS)

Intrusion Prevention System merupakan kombinasi antara fasilitas blocking capabilities dari Firewall dan kedalaman inspeksi paket data dari Intrusion Detection System (IDS). IPS diciptakan pada awal tahun 1990-an untuk memecahkan masalah serangan yang selalu melanda jaringan komputer. IPS membuat akses kontrol dengan cara melihat konten aplikasi, dari pada melihat IP address atau ports, yang biasanya

dilakukan oleh firewall. IPS komersil pertama dinamakan BlackIce diproduksi oleh perusahaan NetworkIce, hingga kemudian berubah namanya menjadi ISS(Internet Security System). Sistem setup IPS sama dengan sistem setup IDS. IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Secara logic IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi sistem call.

Jenis-jenis IPS:

1. Host-based Intrusion Prevention System. Host Based IPS (HIPS) bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi secara konstan. Hal ini disebut dengan Application Binary Interface (ABI). Hampir tidak mungkin untuk membajak sebuah aplikasi tanpa memodifikasi Application Binary Interface, karena konvensi ini bersifat universal di antara aplikasi-aplikasi yang dimodifikasi. HIPS merupakan sebuah system pecegahan yang terdiri dari banyak layer, menggunakan packet filtering, inspeksi status dan metode pencegahan intrusi yang bersifat real-time untuk menjaga host berada di bawah keadaan dari efisiensi performansi yang layak. Mekanisme kerjanya yaitu dengan mencegah kode-kode berbahaya yang memasuki host agar tidak dieksekusi tanpa perlu untuk mengecek threat signature.
2. Network Intrusion Prevention System. Network Based IPS (NIPS), yang juga disebut sebagai "In-line proactive protection", menahan semua trafik jaringan dan menginspeksi kelakuan dan kode yang mencurigakan. Karena menggunakan in-line model, performansi tinggi merupakan sebuah elemen krusial dari perangkat IPS untuk mencegah terjadinya bottleneck pada jaringan. Oleh karena itu, NIPS biasanya didesain menggunakan tiga komponen untuk mengakselerasi performansi bandwidth, yaitu :
   - Network Chips (Network processor)
   - FPGA Chips
   - ASIC Chips

   Network Based IPS (NIPS) biasanya dibangun dengan tujuan tertentu, sama halnya dengan switch dan router. Beberapa teknologi sudah diterapkan pada NIPS, seperti

signature matching, analisa protocol dan kelainan pada protocol, identifikasi dari pola trafik, dan sebagainya. NIPS dibuat untuk menganalisa, mendeteksi, dan melaporkan seluruh arus data dan disetting dengan konfigurasi kebijakan keamanan NIPS, sehingga segala serangan yang datang dapat langsung terdeteksi.

Kebijakan keamanan NIPS sendiri terdiri dari :

- Content based Intrusion Prevention System, yang bertugas mengawasi isi dari paket-paket yang berlalu lalang dan mencari urutan yang unik dari paket-paket tersebut, berisi virus worm, trojan horse, dll.
- Rate based Intrusion Prevention System, bertugas mencegah dengan cara memonitor melalui arus lalu lintas jaringan dan dibandingkan dengan data statistic yang tersimpan dalam database. Apabila RBIPS mengenali paket-paket yang tidak jelas, maka langsung mengkarantina paket tersebut. Baik host based maupun network IPS memiliki kelebihan dan kekurangannya masing-masing. HIPS dapat mengatasi semua jenis jaringan yang terenkripsi dan dapat menganalisa semua kode, sedangkat NIPS tidak menggunakan prosesor dan memori di client maupun host. NIPS tidak selalu bagus, kadang bisa gagal dalam mendeteksi serangan, kadang bisa langsung mendeteksi serangan. Keuntungan NIPS adalah administrasinya yang gampang.

Cara kerja IPS:

- Formula yang umum digunakan untuk mendefinisikan IPS adalah: IPS = IDS + Firewall.

Penjelasan:

- IPS sebenarnya lebih dari sekedar IDS + firewall. IPS didesain sebagai sebuah embedded system yang membuat banyak filter untuk mencegah bermacam-macam serangan seperti hacker, worm, virus, Denial of Service (DoS) dan trafik berbahaya lainnya, agar jaringan enterprise tidak menderita banyak kerugian bahkan ketika security patch terbaru belum diterapkan. Pembangunan IPS didasarkan pada sebuah modul "in-line": data melewati perangkat IPS dari satu ujung dari kanal data tunggal, hanya data yang sudah dicek dan divalidasi oleh mesin IPS yang diperbolehkan untuk lewat menuju ujung lain dari kanal data.

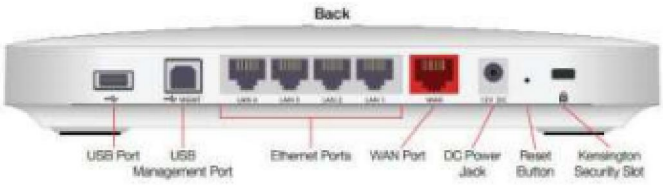
Setiap serangan yang mencoba mengeksploitasi kelemahan dari layer 2 sampai layer 7 OSI akan difilter oleh mesin IPS yang mana, secara tradisional, kemampuan firewall hanya terbatas sampai modul 3 atau 4 saja. Teknologi packet-filter dari firewall tradisional tidak menerapkan inspeksi untuk setiap byte dari segmen data yang bermakna tidak semua serangan dapat diidentifikasikan olehnya. Secara kontras, IPS mampu melakukan inspeksi tersebut dan semua paket data diklasifikasikan dan dikirim ke filter yang sesuai menurut informasi header yang ditemukan di segmen data, seperti alamat asal, alamat tujuan, port, data field dan sebagainya. Setiap filter bertanggung jawab untuk menganalisis paket-paket yang berkaitan, dan yang mengandung tanda-tanda membahayakan akan didrop dan jika dinyatakan tidak berbahaya akan dibiarkan lewat. Paket yang belum jelas akan diinspeksi lebih lanjut. Untuk setiap tipe serangan berbeda, IPS membutuhkan sebuah filter yang bersesuaian dengan aturan filtering yang sudah ditentukan sebelumnya. Aturan-aturan ini mempunyai definisi luas untuk tujuan akurasi, atau memastikan bahwa sebisa mungkin jangkauan aktifitas yang luas dapat terenkapsulasi di dalam sebuah definisi. Ketika mengklasifikasikan sebuah aliran data, mesin filter akan mengacu pada informasi segmen paket, menganalisa konteks dari field tertentu dengan tujuan untuk mengimprovisasi akurasi dari proses filtering.

2. Fortigate

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan Fortinet. Fortinet merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan Fortune Global 100 tahun 2009. Fortinet merupakan pemimpin pasar untuk unified threat management (UTM).

Unified Threat Management atau UTM adalah segmen produk jaringan yang dikhususkan untuk menangani fungsi keamanan jaringan secara terpadu. Pada produk UTM ini menghasilkan Fortigate yang memiliki fitur-fitur seperti firewall, Intrusion Prevention System, web filtering, antivirus yang digabungkan menjadi satu kesatuan dengan tambahan fitur jaringan lain seperti routing dalam satu box hardware.

Fortigate sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN sehingga tak dibutuhkan lagi router ataupun perangkat tambahan load balancing bila ada lebih dari satu koneksi WAN.

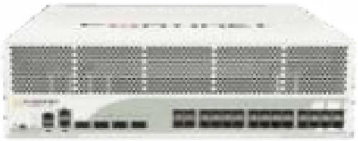


Fortigate 20C

Product Fortigate dari Fortinet terbagi menjadi 3 kategori yaitu :

- High-End (10GE & 40GE Interfaces)
  - FortiGate 5000 Series

  - FortiGate 3000 Series



  - FortiGate 1000 Series

- Mid-Range
  - FortiGate 800-600 Series

  - FortiGate 500-300 Series

  - FortiGate 200 Series

- Entry Level
  - FortiGate 100 Series

  - FortiGate/FortiWiFi 90-60 Series

  - FortiGate/FortiWiFi 30/20 Series

C. SOAL LATIHAN/TUGAS

D. DAFTAR PUSTAKA

Buku

Link and Sites: