PANDUAN PENGGUNAAN

F I R E W A L L

GOV-CSIRT (Government Computer Security Insident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah

Direktorat Kemanan Informasi

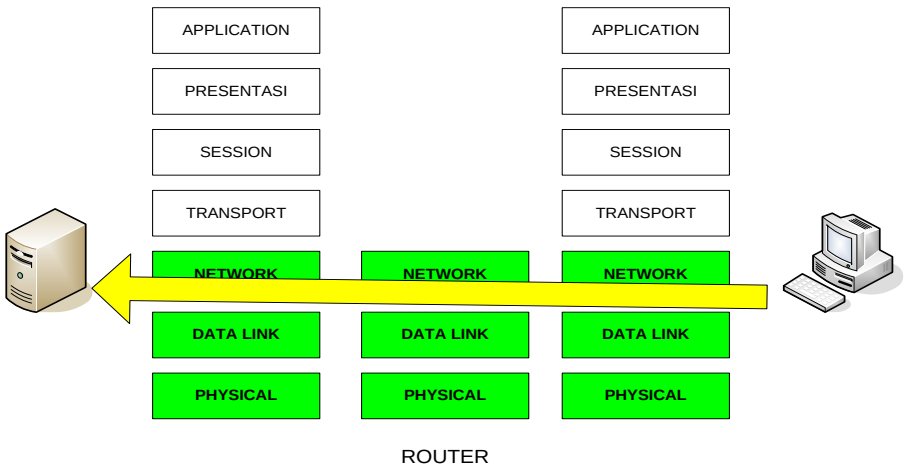
Kementerian Komunikasi dan Informatika Republik Indonesia

Overview Firewall

Firewall merupakan sebuah mekanisme pengamanan yang dilakukan dengan cara melakukan kegiatan penyaringan (filtering) paket data yang masuk dan keluar jaringan.Hanya paket yang diijinkan saja yang diperbolehkan melewati firewall untuk menjangkau jaringan tertentu. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak untuk dapat menyaring paket data.

Teknologi Firewall ➔ Penyaringan Paket

Pada awalnya, teknologi penyaringan paket hanya memeriksa paket hingga ke layer network. Adapun keempat buah layer diatasnya tidak akan diperiksa dan akan langsung memperkenankan paket-paket tersebut memasuki jaringan internal. Terakhir, mengingat bahwa sudah mulai banyak perangkat router yang dapat memeriksa paket-paket hingga ke layer transport, maka kemampuan teknologi ini pun ikut ditingkatkan hingga ke layer transport juga tentunya. Artinya, bahwa teknologi ini pun akan mampu memeriksa asal dan tujuan alamat IP, nomor protokol serta dalam penanganan kasus UDP dan TCP dapat mencapai hingga ke nomor portnya. Biasanya, teknologi ini dibangun secara built-in di dalam pabrikasi perangkat router seperti hal yang sama akan dapat juga dijumpai pada beberapa modus kernel sistem UNIX. Jadi, teknologi penyaringan paket dapat memeriksa setiap paket data yang masuk maupun keluar dari suatu jaringan dan menerima ataupun menolak paket-paket data tersebut berdasarkan pada aturan yang telah ditentukan sebelumnya.Teknologi ini pun cukup efektif dan transparan bagi para user. Jadi, ada suatu keterbatasan dari jenis teknologi penyaringan paket ini, yaitu berupa ketidakmampuan dalam menyediakan sistem keamanan bagi hampir semua sistem protokol dasar.



Gambar 1 Lintasan paket data dalam pada teknologi penyaringan paket

Keunggulan teknologi penyaringan paket (filtering packets) adalah :

- Biaya rendah,
- Lebih cepat daripada teknologi gateway layer aplikasi.

Kelemahan teknologi penyaringan paket (filtering packets) adalah :

- Tingkat keamanan cukup rendah,
- Akses terbatas hanya pada bagian header dari paket,
- Pemeriksaan terbatas hanya pada layer network atau diatasnya,
- Kemampuannya sangat terbatas dalam memanipulasi informasi,
- Mekanisme logging dan alerting yang tersedia kurang memadai,
- Tidak mampu mengatasi aktifitas IP spoofing.

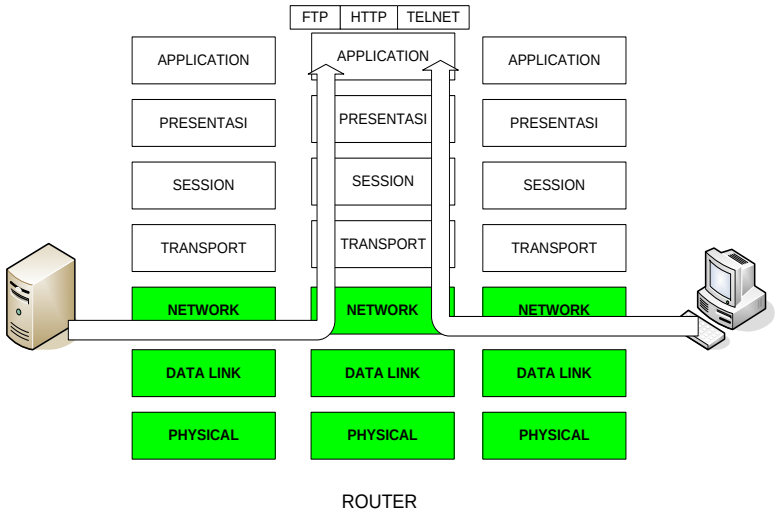
Penyaringan paket data, awalnya diterapkan pada perangkat router, yaitu menyaring content berdasarkan hasil definisi user, contohnya alamat IP. Teknologi ini akan memeriksa suatu paket pada layer network dan aplikasi secara bebas, yang kemudian mengizinkan paket-paket ini untuk dikirimkan dengan kinerja dan skalabilitas yang baik. Akan tetapi, teknologi ini dianggap masih kurang aman karena masih kurang memadai untuk mengatasi hal-hal yang terjadi di layer aplikasi. Teknologi ini tidak dapat mengatasi konteks isi dari suatu komunikasi yang sedang berlangsung sehingga dapat memudahkan para user yang tak punya kewenangan untuk menembusnya.

Oleh karena teknologi penyaringan paket tidak dapat memeriksa paket di atas layer network dan transport, ada beberapa hal tidak dapat dilakukan oleh teknologi ini, yaitu :

- Tidak dapat menyediakan layanan content security. Contohnya, pemeriksaan dan penyaringan virus pada pengaksesan situs-situs dan halaman web tertentu.
- Tidak dapat menyediakan layanan otentikasi. Contohnyaadalah hanya para user yang memiliki kewenangan yang boleh menggunakan suatu service.
- Tidak mampu membuka dan menutup port-port aplikasi secara dinamis pada saat dibutuhkan. Hal ini akan menyebabkan tidak memungkinkannya penerapan aplikasi seperti aplikasi RealAudio, FTP dan H.323.
- Tidak mampu memvalidasi suatu port khusus bagi pemakaian suatu layanan tertentu. Contohnya, menjamin bahwa hanya trafik HTTP yang sah yang boleh melewati nomor port 80.

Teknologi Firewall ➔Application Layer Gateways

Teknologi Application Layer Gateways atau proxy akan mengimplementasikan firewall pada layer aplikasi. Proxy selalu akan menerima permintaan dari suatu klien, kemudian menghubungkannya dengan suatu server atas nama klien tersebut. Dalam beberapa kasus, klien akan secara eksplisit melakukan koneksi ke server proxy. Dalam kasus yang lain, proxy akan mencegat koneksi melalui bantuan sistem operasi di bawahnya atau arsitektur jaringan. Aplikasi proxy secara spesifik tertuju pada suatu layanan jaringan tertentu, maka ia dapat mamahami secara penuh suatu session. Artinya, proxy dapat melakukan pemeriksaan muatan, menyediakan otentikasi dan menjamin bahwa hanya services tertentu yang boleh digunakan. Contohnya, suatu proxy HTTP dapat menjamin bahwa hanya trafik HTTP yang akan diijinkan untuk lewat, atau ia bisa juga menyediakan layanan aplikasi khusus seperti halnya penyimpanan pada memori caching. Proxy dapat juga menyediakan suatu koneksi yang telah mapan terbentuk ke suatu server yang berada di belakang firewall, hal ini karena perangkat proxy selalu membuka koneksi atas nama klien yang memintanya.



Gambar 2 Lintasan paket data dalam teknologi gateway layer aplikasi (proxy)

Keunggulan teknologi proxy atau application layer gateways, yaitu :

- Menyediakan tingkat keamanan yang lebih baik dibandingkan packet filtering
- Mampu manangani permasalahan secara penuh pada layer aplikasi.

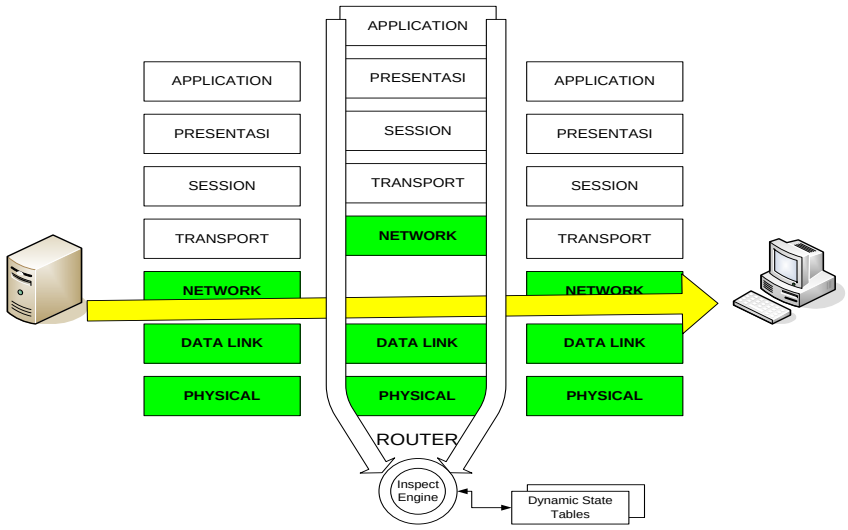
Kelemahan teknologi proxy atauapplication layer gateways, yaitu :

- Hanya dapat mengatasi secara parsial kondisi informasi yang salah dari suatu komunikasi dan secara penuh mengatasi kondisi informasi yang berasal dari suatu aplikasi.
- Implementasi pada tingkat aplikasi tentu akan cukup mengganggu kinerjanya.
- Mengabaikan muatan informasi pada layer yang lebih rendah.
- Biaya performansinya cukup mahal.

Teknologi Firewall ➔Statefull Inspection

Teknologi stateful inspection menggabungkan beragam fitur terbaik dari teknologi penyaringan Paket dan teknologi application layer gateways.Engine dari teknologi stateful inspectiondiletakkan di antara layer datalink dan layer network yang dalam kasus ini diletakkan antara network interface card dengan driver TCP/IP.Teknologi stateful inspectiondapat melihat keseluruhan paket dan membuat suatu keputusan terhadap kebijakan keamanan berdasarkan isi dari paket tersebut.Teknologi ini juga akan menjaga jejak perjalanan setiap koneksi aktif ke dalam suatu tabel kondisi. Untuk beberapa layanan seperti FTP, ia juga mampu secara dinamis membuka port-port antara dua buah host sehingga komunikasi bisa berhasil dan setelah itu akan menutupnya jika memang sudah selesai.

Teknologi inspeksi seluruh kondisi (stateful inspection) membutuhkan sedikit lebih besar memori dan siklus CPU daripada teknologi penyaringan paket karena ia harus melakukan lebih banyak aktivitas.

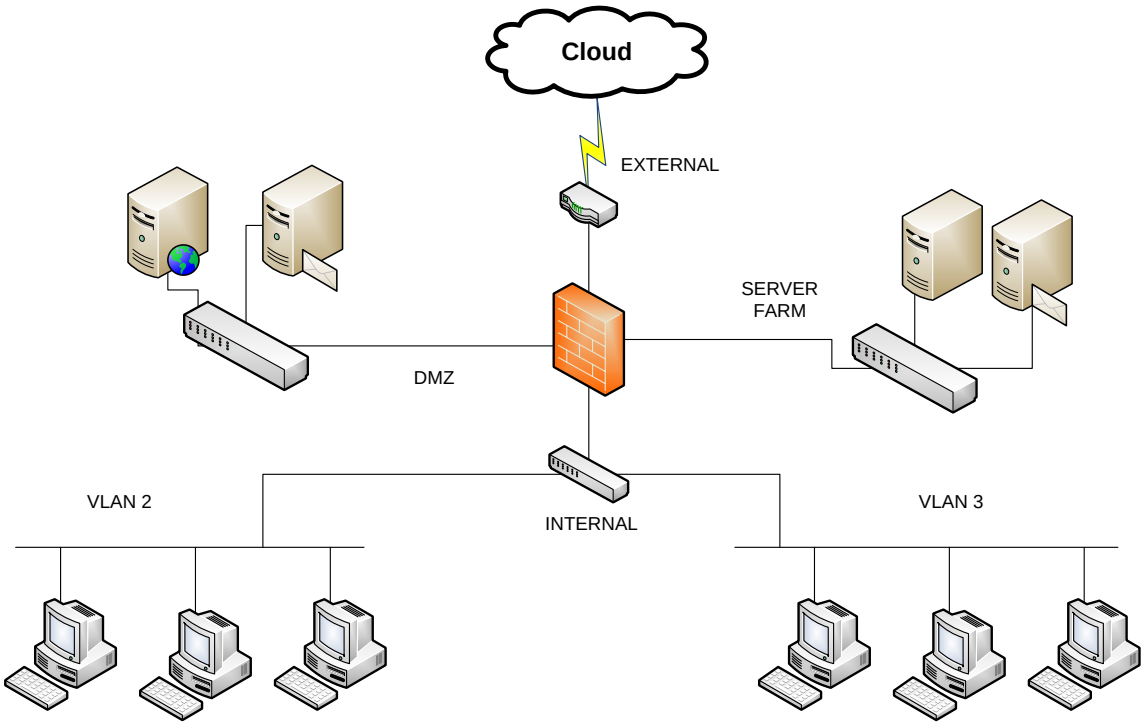


Gambar 3 Lintasan aliran paket pada teknologi Stateful Inspection

Keunggulan teknologi Stateful Inspection adalah sebagai berikut :

- Memiliki tingkat keamanan yang jauh lebih baik.
- Mampu menangani secara penuh permasalahan pada layer aplikasi.
- Memiliki kinerja yang tinggi.
- Memiliki skalabilitas yang jauh lebih baik.

Arsitektur jaringan komputer dan firewall



Gambar 4 Topologi single firewall

Salah satu lapisan pengamanan yang diperlukan adalah melakukan segmentasi jaringan. Segementasi jaringan sebaiknya terdiri dari :

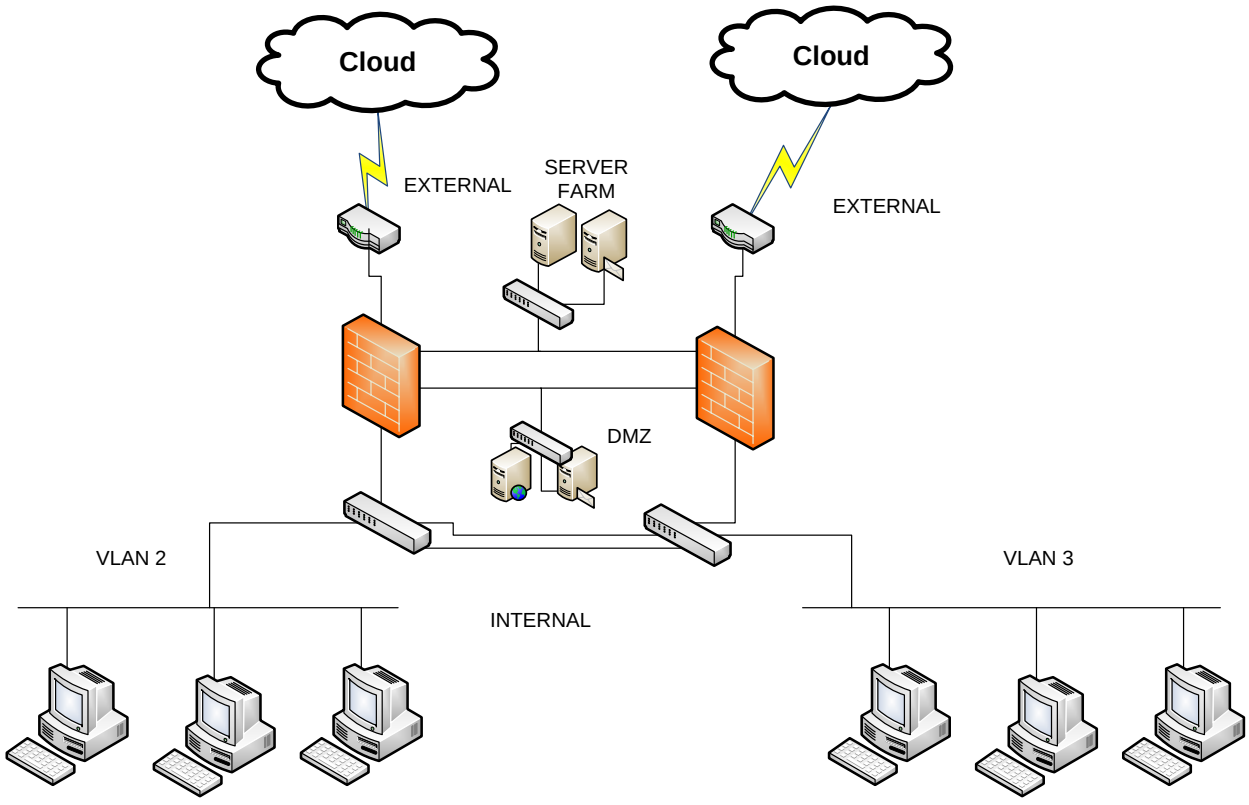
- Zone Eksternal (public), merupakan zone public yang terhubung dengan jaringan internet.

- DeMilitary Zone, merupakan zone yang diisi oleh server-server yang dapat berkomunikasi dengan wilayah internal dan eksternal. Contohnya web server yang berisi company profile perusahaan.

- Zone Server Farm, merupakan zone dimana tempat terinstall server-server yang dibutuhkan oleh internal. Contohnya server kepegawaian, server keuangan dan sebagainya.

- Zone Internal (private), wilayah internal pun sebaiknya di segmentasi menggunakan teknologi VLAN untuk membagi jaringan berdasarkan broadcast domain yang berbeda untuk setiap bagian (departemen)

Pada organisasi yang besar dan menerapkan kebijakan load balancing dan fail over pada sistem jaringannya, dapat menerapkan topologi berikut pada sistem firewall nya.



Gambar 5 Topologi multiple firewall

Penerapan Kebijakan Firewall

Kebijakan berbasis hubungan antar zone

Setelah dilakukan proses segmentasi , langkah berikutnya adalah menetapkan kebijakan hubungan antar segment (wilayah) :

- Routing atau NAT (Network Address Translation)

	Eksternal	Internal	DMZ	Server Farm
Eksternal		x	NAT/Routing	x
Internal	NAT		Routing	Routing
DMZ	NAT/Routing	Routing		Routing
Server Farm	x	Routing	Routing	

Pilihan NAT atau Routing pada relasi antara DMZ dan Eksternal tergantung ketersediaan IP Publik, tetapi Lebih disarankan untuk memanfaatkan fitur NAT jika aplikasi yang digunakan mendukung mekanisme NAT.

Pemasangan Access Rule antara Internal ➔ Eksternal (outgoing traffic)

- Identifikasi protocol dan port yang diperlukan diantara hubungan internal ke eksternal.
- Buat akses rule terhadap protocol dan port yang diperlukan agar protocol dan port tersebut dapat melewati firewall dari arah internal ke eksternal. Contoh port yang diperlukan diantara hubungan antara internal & eksternal adalah port HTTP & HTTPS.
- Aktifikan fitur proxy pada firewall, buat content filtering berdasarkan content dan URL untuk digunakan dalam penerapan access policy, guna mengatur hak akses user internal terhadap alamat tujuan internet.
- Terapkan access policy terhadap pengguna internet dengan memanfaatkan fitur content filtering yang sebelumnya sudah dibuat.

Pemasangan Access Rule antara Eksternal ➔ Internal (inbound traffic)

- Hindari pemasangan access rule dari eksternal ke internal.

Pemasangan Access Rule antara Internal ←→ Server Farm

- Identifikasi kebutuhan pengguna terhadap server – server yang terdapat di wilayah server farm
- Identifikasi port dan protocol yang dibutuhkan oleh pengguna terhadap masing-masing server yang terdapat di wilayah server farm
- Pasangkan access rule antara internal dan server farm sesuai dengan kebutuhan pengguna terhadap masing-masing server yang terdapat di wilayah server farm

Pemasangan Access Rule antara Internal ←→ DMZ

- Identifikasi kebutuhan akses pengguna terhadap server-server yang terdapat di wilayah DMZ
- Identifikasi port dan protocol yang dibutuhkan oleh pengguna terhadap masing-masing server yang terdapat di DMZ
- Pasangkan access rule antara internal dan DMZ sesuai dengan kebutuhan layanan bagi pengguna terhadap masing-masing server yang terdapat di wilayah server farm.

Pemasangan Access Rule antara DMZ ←→ Eksternal

- Identifikasi kebutuhan akses wilayah publik terhadap server yang terdapat di DMZ
- Identifikasi port dan protocol yang dibutuhkan oleh public terhadap masing-masing server
- Pasangkan access rule terhadap wilayah publik dengan server tertentu sesuai dengan port dan protokol yang dibutuhkan bagi public terhadap server masing-masing yang terdapat diwilayah DMZ.

Pemasangan Access Rule antara DMZ ←→ Server Farm

- Identifikasi kebutuhan akses wilayah DMZ terhadap server yang terdapat di Server Farm
- Identifikasi port dan protocol yang dibutuhkan oleh DMZ terhadap masing-masing server
- Pasangkan access rule terhadap masing-masing server yang terdapat di DMZ dengan server tertentu sesuai dengan port dan protokol masing-masing.

Pemasangan Access Rule antara Eksternal ←→ Server Farm

- Sebaiknya di hindari penyediaan akses dari eksternal ke Server Farm dan sebaliknya.

Kebijakan berbasis IP & Protokol

Kebijakan firewall yang berbasis alamat IP dan Protokol seharusnya hanya mengijinkan protokol IP yang perlu dilewatkan (dibutuhkan) saja. Beberapa protokol yang biasa digunakan pada protokol IP antara lain ICMP (1), TCP(6) dan UDP (17). Untuk protokol ICMP diijinkan hanya ketika diperlukan saja, dalam kondisi normal sebaiknya ICMP diblock.Protokol-protokol yang diijinkan seharusnya dibatasi ke host atau network yang diperlukan, semua protokol yang tidak perlu diblock secara default.

Kebijakan Firewall seharusnya hanya mengijinkan alamat IP sumber dan alamat IP tujuan yang digunakan, sebagai rekomendasi sebagai berikut :

- Trafik yang berasal dari alamat-alamat sumber atau tujuan yang tidak sah seharusnya di block.Trafik yang masuk dengan menggunakan alamat sumber yang tidak sah atau trafik yang keluar dengan alamat tujuan yang tidak sah seharusnya di block. Trafik jenis ini sering ditimbulkan oleh malware, spoofing, serangan DoS(denial of services) atau kesalahan konfigurasi perangkat.

- Trafik arah masuk dengan alamat tujuan IP Private seharusnya di block. Firewall dapat melakukan translasi alamat untuk mengijinkan host internal berkomunikasi dengan wilayah publik, sehingga alamat private tidak perlu dilewatkan melalui perimeter jaringan.

- Trafik ke arah luar bagi alamat sumber yang tidak sah seharusnya di block. Sistem internal yang sudah terkena serangan oleh penyerang dapat dimanfaatkan untuk menyerang sistem lain yang terdapat di internet. Dengan melakukan blocking terhadap trafik jenis ini, firewall sangat membantu mengurangi efektifitas serangan.

- Trafik yang masuk dengan alamat tujuannya adalah alamat firewall seharusnya di block, kecuali firewall mengaktifkan layanan proxy.

- Trafik yang berisi informasi routing yang mengijinkan sistem untuk menetapkan rute yang akan paket lewati dari alamat sumber ke tujuan. Dengan kalimat lain tidak firewall tidak mengijinkan aktifitas traceroute dilakukan.

- Trafik dari arah luar jaringan yang berisi alamat broadcast yang mengarah ke jaringan internal seharusnya diblock.

Kebijakan berbasis pada aplikasi

Penerapan kebijakan firewall yang berbasis pada aplikasi dapat dilakukan jika sistem firewall yang digunakan memiliki sistem proxy. Penggunaan kebijakan berbasis pada aplikasi ini dapat digunakan dengan tahapan berikut :

- Aktifkan fitur proxy
- Definisikan content filtering yang diperlukan berdasarkan URL dan berdasarkan content.
- Manfaatkan content filtering tersebut melalui access policy
- Pasangkan policy tersebut kepada host atau network tertentu dapat juga dipasangkan terhadap user account jika firewall mendukung fitur otentikasi berbasis user account.

Kebijakan berbasis pada identitas user

Penerapan kebijakan firewall yang berbasis pada identitas user dilakukan jika firewall yang digunakan memiliki fitur otentikasi dan otorisasi berbasis user account.Pengaturan hak akses pengguna terhadap pengiriman trafik yang melalui firewall di atur berdasarkan user account.

Perencanaan dan implementasi Firewall

Perencanaan dan implementasi firewall dilakukan melalui pendekatan bertahap. Perencanaan firewall dan tahapan pelaksanaannya terdiri dari :

1. Perencanaan, tahap dimana organisasi menentukan firewall yang akan diterapkan dalam menetapkan kebijakan keamanan organisasi.
2. Konfigurasi, tahap instalasi perangkat keras maupun perangkat lunak firewall serta menyiapkan aturan untuk sistem.
3. Pengujian, tahap pengujian yang berfungsi untuk mengevaluasi fungsionalitas, kinerja, skalabilitas dan keamanan dan mengidentifikasi masalah
4. Deployment, tahap penerapan firewall yang telah dikonfigurasi dan melalui tahap pengujian.
5. Pengelolaan, tahapan ini dilakukan selama siklus hidup dari firewall ini, mencakup kegiatan perawatan komponen dan dukungan terhadap masalah operasional.

Perencanaan

Tahap perencanaan untuk memilih dan mengimplementasikan firewall harus dimulai hanya setelah sebuah organisasi telah menetapkan bahwa firewall diperlukan untuk menegakkan kebijakan keamanan organisasi. Ini biasanya terjadi setelah penilaian risiko dari sistem secara keseluruhan dilakukan.

Sebuah penilaian risiko meliputi :

1. identifikasi ancaman dan kerentanan dalam sistem informasi,
2. dampak potensial atau besarnya bahaya bahwa hilangnya kerahasiaan, integritas ketersediaan, atau akan memiliki aset organisasi atau operasi (termasuk misi, fungsi, Citra, atau reputasi) ketika terjadi eksploitasi ancaman kerentanan diidentifikasi
3. identifikasi dan analisis kontrol keamanan untuk system informasi.

Prinsip dasar bahwa organisasi harus mengikuti dalam perencanaan penyebaran firewall meliputi:

Gunakan perangkat sesuai dengan fungsinya. Firewall jangan diimplementasikan pada perangkat yang bukan dimaksudkan untuk firewall. Sebagai contoh perangkat router disediakan untuk menangani fungsi routing, seharusnya router tidak dimanfaatkan untuk melakukan kegiatan filtering yang kompleks.Firewall tidak digunakan untuk menyediakan layanan-layanan lain seperti web server atau mail server.

Terapkan sistem pengamanan berlapis, dengan demikian resiko dapat dikelola dengan lebih baik. Firewall dapat dipasang di beberapa tempat (perimeter, pada bagian yang memiliki data sensitive, dan pada masing-masing computer pengguna). Firewall juga harus menjadi bagian

dari program keamanan secara keseluruhan yang juga mencakup produk seperti antimalware dan software intrusion detection.

Perhatikan ancaman internal. Ancaman ini mungkin tidak datang langsung dari orang dalam, tetapi dapat melibatkan host internal terinfeksi oleh malware atau dikompromikan oleh penyerang eksternal. Sistem internal penting harus ditempatkan di belakang firewall internal.

Dokumentasikan kemampuan firewall. Setiap jenis firewall memiliki kemampuan dan keterbatasan yang berbeda. Ini kadang-kadang akan mempengaruhi perencanaan kebijakan keamanan organisasi dan strategi penerapan firewall. Setiap fitur yang positif atau negatif mempengaruhi perencanaan ini harus ditulis ke dalam dokumen perencanaan secara keseluruhan.

Beberapa pertimbangan yang perlu dilakukan dalam memilih solusi firewall, antara lain :

- Kemampuan
    - Wilayah organisasi mana yang perlu dilindungi ?(perimeter, departemen internal, host dsb)
    - Jenis teknologi firewall mana yang sesuai untuk digunakan untuk melindungi ? (packet filtering, inspeksi stateful, gateway application proxy, dsb)
    - Fitur keamanan tambahan apa yang dimiliki oleh firewall ? (content filtering, VPN, IDS)
- Pengelolaan
    - Protokol apa yang digunakan untuk mendukung pengelolaan secara remote terhadap firewall, seperti HTTPS, SSH ?
      Apakah penggunaan protokol remote terhadap firewall diijinkan dan sesuai dengan kebijakan organisasi?
    - Apakah pengelolaan secara remote dibatasi pada interface firewall dan alamat IP sumber tertentu ?
- Kinerja
    - Berapa jumlah maksimum koneksi simultan, throughput yang disupport oleh firewall ?
    - Apakah kebutuhan load balancing dan fail over terhadap firewall diperlukan ?
    - Apakah menggunakan firewall berbasis software atau berbasis hardware ?
- Integrasi
    - Apakah ketika firewall terpasang, diperlukan perubahan pada area lain di jaringan ?
    - Apakah sistem logging firewall dapat saling beroperasi dengan sistem log yang sudah tersedia ?
    - Apakah firewall harus kompatibel dengan perangkat lain pada jaringan yang menyediakan sistem keamanan atau layanan lain?

- Lingkungan Fisik
    - Di mana firewall secara fisik ditempatkan untuk memastikan keamanan fisik dan perlindungan dari bencana?
    - Apakah ada rak yang memadai atau ruang rak di lokasi fisik di mana firewall akan ditempatkan?
    - Apakah daya tambahan, daya cadangan, AC, dan / atau koneksi jaringan dibutuhkan pada lokasi fisik?
- Personil
    - Siapa yang akan bertanggung jawab untuk mengelola firewall?
    - Apakah sistem administrator membutuhkan pelatihan sebelum firewall ini digunakan?
- Kebutuhan Masa Depan
    - Apakah firewall memenuhi kebutuhan masa depan organisasi?

Konfigurasi Firewall

Tahap konfigurasi melibatkan semua aspek konfigurasi platform firewall. Ini termasuk instalasi perangkat keras dan perangkat lunak, mengkonfigurasi kebijakan, mengkonfigurasi logging dan alert, serta mengintegrasikan firewall ke dalam arsitektur jaringan.

Instalasi Hardware dan Software

a. Setelah firewall dipilih dan tersedia, perangkat keras, sistem operasi dan software firewall harus diinstall.
b. Sebelum software diinstall dan setelah sistem operasi diinstall, sistem operasi perlu diperkuat dengan menginstall patch yang terbaru. Kemudian install software firewall.
c. Berikutnya, sistem firewall perlu dipatch atau diupdate jika vendor menyediakan patch atau pun update dari software firewall tersebut. Hal ini dilakukan baik terhadap firewall jenis hardware maupun firewall berbasis software.
d. Selama proses instalasi dan konfigurasi, hanya administrator yang diijinkan untk mengelola firewall. Semua layanan manajemen untuk firewall, seperti SNMP harus dinonaktifkan secara permanen kecuali diperlukan.
e. Jika firewall memiliki fitur management user, sebaiknya dibuatkan beberapa account untuk personel-personil yang bertanggungjawab mengelola firewall.
f. Firewall jaringan harus ditempatkan di ruangan yang memenuhi persyaratan yang direkomendasikan. Ruangan yang digunakan secara fisik harus aman untuk mencegah personil yang tidak memiliki hak untuk mengakses firewall.

g. Sebaiknya jam internal firewall harus konsisten dengan semua sistem lainnya yang digunakan oleh sebuah organisasi. Hal tersebut dapat dilakukan dengan memanfaatkan sistem NTP server untuk melakukan sinkronisasi dengan sumber waktu otoritatif. Hal ini diperuntukan untuk membandingkan log dari beberapa sistem ketika menganalisis masalah.

Kebijakan Konfigurasi

Setelah perangkat keras dan perangkat lunak yang telah terinstal, administrator dapat membuat kebijakan firewall. Beberapa firewall menerapkan kebijakan melalui aturan eksplisit; beberapa firewall memerlukan mengkonfigurasi pengaturan firewall yang kemudian membuat aturan internal, beberapa firewall membuat kebijakan dan aturan secara otomatis dan ada pula yang menggunakan kombinasi dari ketiga jenis konfigurasi. Hasil akhirnya adalah seperangkat aturan yang disebut ruleset yang menggambarkan bagaimana firewall bertindak. Beberapa vendor memiliki batasan atau saran pada urutan aturan dalam sebuah ruleset. Sementara itu adalah umum untuk memikirkan aturan firewall yang mempengaruhi lalu lintas yang muncul pada antarmuka internal atau eksternal. Untuk membuat ruleset, pertama kali harus ditentukan apa jenis lalu lintas (protokol, alamat sumber dan tujuan, dll) yang dibutuhkan oleh aplikasi disetujui untuk organisasi.

Minimal, aturan yang seharusnya didefinisikan adalah :

- Port filtering harus diaktifkan di tepi luar jaringan dan di dalam jaringan juga jika diperlukan.
- Penyaringan konten harus dilakukan sedekat mungkin dengan penerima konten.

Jika menerapkan beberapa firewall perlu memiliki aturan yang sama, aturan-aturan tersebut seharusnya disinkronisasi antar firewall. Hal tersebut biasanya tergantung fitur yang dimiliki oleh firewall.

Konfigurasi sistem pencatatan dan alert

Langkah selanjutnya dalam proses konfigurasi adalah untuk mengatur sistem pencatatan dan alert. Logging adalah langkah penting dalam mencegah dan pemulihan dari kegagalan serta memastikan bahwa konfigurasi keamanan yang tepat diatur pada firewall. Logging yang tepat juga dapat memberikan informasi penting untuk merespon insiden keamanan. Bila mungkin, firewall harus dikonfigurasi baik untuk menyimpan log secara lokal maupun secara terpusat. Keterbatasan sumber daya, kemampuan firewall logging, dan situasi lain dapat mengganggu kemampuan untuk menyimpan log baik lokal maupun terpusat.

Tentukan log apa dan berapa lama log dipelihara, harus dilakukan berdasarkan kasus per kasus. Selain mengkonfigurasi logging, real-time alert juga harus dibentuk untuk memberitahu administrator ketika peristiwa penting terjadi pada firewall. Pemberitahuan dilakukan ketika:

- Modifikasi atau penghentian aturan firewall
- Sistem reboot, kekurangan disk, dan peristiwa operasional lainnya

Pengujian

Firewall baru harus diuji dan dievaluasi sebelum di pasang ke jaringan produksi untuk memastikan bahwa mereka bekerja dengan benar. Pengujian harus dilakukan pada jaringan uji tanpa konektivitas ke jaringan produksi. Aspek – aspek yang perlu dievaluasi meliputi:

- Konektivitas, pengguna dapat membentuk dan memelihara koneksi melalui firewall. Ruleset, Lalu Lintas yang secara khusus diizinkan oleh kebijakan keamanan diperbolehkan. Semua lalu lintas yang tidak diperbolehkan oleh kebijakan keamanan diblokir. Verifikasi ruleset harus mencakup baik meninjau secara manual dan menguji apakah aturan bekerja seperti yang diharapkan. Kompatibilitas Aplikasi, penerapan firewall tidak mengganggu penggunaan aplikasi perangkat lunak yang ada.
- Manajemen, Administrator dapat mengkonfigurasi dan mengelola solusi efektif dan aman.
  Logging sesuai dengan kebijakan organisasi dan strategi.
- Kinerja, memberikan kinerja yang memadai selama pemakaian normal dan puncak. Dalam banyak kasus, cara terbaik untuk menguji kinerja di bawah beban dari implementasi prototipe adalah dengan menggunakan generator lalu lintas simulasi pada jaringan uji coba untuk meniru karakteristik aktual dari lalu lintas yang diharapkan semaksimal mungkin. Simulasi beban yang disebabkan oleh serangan DoS juga dapat membantu dalam menilai kinerja firewall. Pengujian harus menggabungkan berbagai aplikasi yang akan melintasi firewall, terutama yang kemungkinan besar akan terpengaruh oleh masalah jaringan throughput atau latency.
- Keamanan, implementasi firewall itu sendiri mungkin berisi kerentanan dan kelemahan yang penyerang bisa mengeksploitasi. Organisasi dengan kebutuhan keamanan yang tinggi mungkin ingin melakukan penilaian kerentanan terhadap komponen firewall.

Deployment

Sebelum memasangkan firewall pada jaringan, administrator harus memberitahu pengguna atau pemilik sistem yang berpotensi terkena dampak dari pemasangan firewall yang direncanakan, dan memerintahkan mereka yang untuk memberitahu jika mereka menemui masalah. Setiap perubahan yang diperlukan untuk peralatan lainnya juga harus dikoordinasikan sebagai bagian dari kegiatan pemasangan firewall. Kebijakan keamanan yang diungkapkan oleh konfigurasi firewall harus ditambahkan dengan kebijakan keamanan secara keseluruhan

organisasi, dan perubahan yang berkelanjutan untuk konfigurasinya harus diintegrasikan dengan proses manajemen organisasi konfigurasi.

- Jika terdiri dari beberapa firewall yang diimplementasikan, termasuk firewall pribadi atau di beberapa kantor cabang, pendekatan bertahap harus dipertimbangkan. Prototipe juga akan sangat membantu, terutama untuk mengidentifikasi dan menyelesaikan masalah kebijakan yang saling bertentangan. Ini akan memberikan administrator kesempatan untuk mengevaluasi dampak solusi firewall dan menyelesaikan masalah sebelum dipasang dibeberapa lokasi.
- Firewall biasanya bertindak pula sebagai router, firewall harus diintegrasikan ke dalam struktur jaringan routing. Hal ini sering berarti mengganti router yang berada pada tempat yang sama dalam topologi jaringan sebagai mana firewall sedang ditempatkan, tetapi juga dapat berarti mengubah tabel routing untuk router lain dalam jaringan organisasi untuk menangani penambahan ini router baru.

Pengelolaan

Fase terakhir dari perencanaan dan implementasi firewall adalah pengelolaan dan hal ini bersifat jangka panjang. Beberapa tindakan perawatan adalah:

- instalasi patch untuk perangkat firewall.
- Melakukan pembaharuan terhadap kebijakan untuk menghadapi jenis ancaman yang baru teridentifikasi.
- Memantau kinerja firewall dan log untuk memastikan bahwa pengguna mematuhi kebijakan keamanan.
- Melakukan pengujian periodik untuk memverifikasi bahwa aturan firewall berfungsi seperti yang diharapkan.
- Menyimpan log