BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Jaman sekarang, jumlah pengguna internet meningkat pada setiap menitnya. Pada tahun 2017, lebih dari 50 persen atau sekitar 143 juta orang telah menggunakan internet di Indonesia, yang berasal dari populasi sekitar 262 juta orang (APJII, 2018). Pengguna dapat mengakses apapun yang diinginkan melalui fasilitas internet. Perbuatan kejahatan menjadi kesempatan bagi pelaku yang tidak bertanggung jawab untuk menyadap, ataupun mencuri informasi pribadi. Dibawah ini, beberapa sumber daya, seperti jurnal dan buku digunakan sebagai referensi penilitian.

Sharma dan Chandresh membahas mengenai firewall dan klasifikasinya. Berbagai tindakan yang tidak diinginkan, seperti berjudi, menerobos data pribadi orang lain, meretas jaringan perusahaan dan mencuri dokumen penting memberikan kerugian dalam hal moneter maupun nilai pasarnya. Maka, memberikan pengetahuan kepada pengguna komputer pribadi dan usaha mengenai pentingnya firewall, memberikan kesempatan kepada mereka untuk mencari cara untuk menghindari serangan yang tidak diinginkan (2017).

Kumar dan Gupta menjelaskan masalah keamanan jaringan yang meningkat setiap hari. Berbagai masalah yang muncul, mengharuskan ahli komputer untuk memberikan solusi. Maka, penulis jurnal ini menerapkan firewall dan IDS dengan menggunakan pfSense. Menurutnya, tidak ada jaringan yang

sepenuhnya aman, karena serangan semakin kompleks, dan sistem kemanan juga masih sedang dikembangkan. Suatu organisasi tidak dapat sepenuhnya bergantung pada firewall karena belum ada sistem perlindungan yang dapat menolak semua kejahatan internet. Jika keamanan jaringan dilanggar, maka itu harus dilaporkan kepada administrator sehingga tindakan yang diperlukan dapat diambil (2018).

Sylvester, Asante, & Twum melakukan penelitian terhadap University of Mines and Technology untuk mempelajari pola perilaku pengguna jaringan dalam pemakaian internet dan meningkatkan kontrol akses jaringan dengan menggunakan perangkat lunak pfSense. Hasilnya menunjukkan bahwa bandwith terbatas, kecepatan LAN yang ditingkatkan dari 45 MB menjadi setidaknya 80 MB menjadi lebih aman. Paket perangkat lunak yang diinstal juga harus ditingkatkan secara berkala (2016).

Nugraha, Gunawan, & Siregar merancang dan implementasi pfSense untuk mengatasi celah pada jaringan internet karena kemudahan konfigurasi dan kemudahan akses yang disediakan. Maka, sistem captive portal dibuat agar mewajibkan setiap pengguna komputer untuk melakukan login terlebih dahulu sebelum mengakses internet. Secure Sockets Layer (SSL) dan HyperText Transfer Protocol (HTTP) pada Captive Portal juga di-implementasi untuk melindungi data pengguna dari pihak luar. Kemudian pemakaian bandwith oleh pengguna internet diatur dengan manjemen bandwith yang dimiliki oleh pfSense (2015).

Beberapa referensi dari buku juga digunakan untuk memahami lebih dalam mengenai pfSense, seperti “Mastering pfSense” (Zientara, 2016) dan “pfSense: The Definitive Guide Version 2.1” (Buechler & Pingle, 2013). Semua

referensi ini digunakan karena bab kedua meninjau literatur saat ini pada bidang yang relevan, yaitu “Perancangan Keamanan Jaringan Menggunakan Firewall pfSense”.

2.2 Landasan Teori

2.2.1 Internet

Internet merupakan singkatan dari kata “interconnection networking”. Maksud dari kata ini adalah menggunakan media elektronik untuk melayani masyarakat pengguna jaringan komunikasi, yang dimana saling terhubung dengan menggunakan standar sistem global Transmission Control Protocol/Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran paket.

Minat pengguna internet semakin besar karena dampak positif yang diterima oleh pengguna komputer. Berbagai macam informasi semakin mudah didapatkan dari mesin pencari, seperti Google, tanpa harus ke perpustakaan untuk mencari informasi satu-per-satu dari buku, sehingga lebih efisien dan efektif bagi pembaca. Selain itu, dalam sektor ekonomi, transaksi jual-beli juga mengalami perkembangan melalui “e-commerce”, sebagai tempat transaksi secara online.

Manfaat dari internet dapat dirasakan oleh banyak pihak, namun tidak bisa dilupakan adanya tata tertib internet yang harus dipatuhi. Isu moral, seperti pelanggaran hak cipta, pencurian identitas, pernyataan kebencian (hate speech), dan pornografi telah diatur dalam undang-undang, untuk melindungi pengguna internet dan mensejahterahkan masyarakat agar terhindar dari pengguna internet yang tidak bertanggung jawab (Sukaridhoto, 2014).

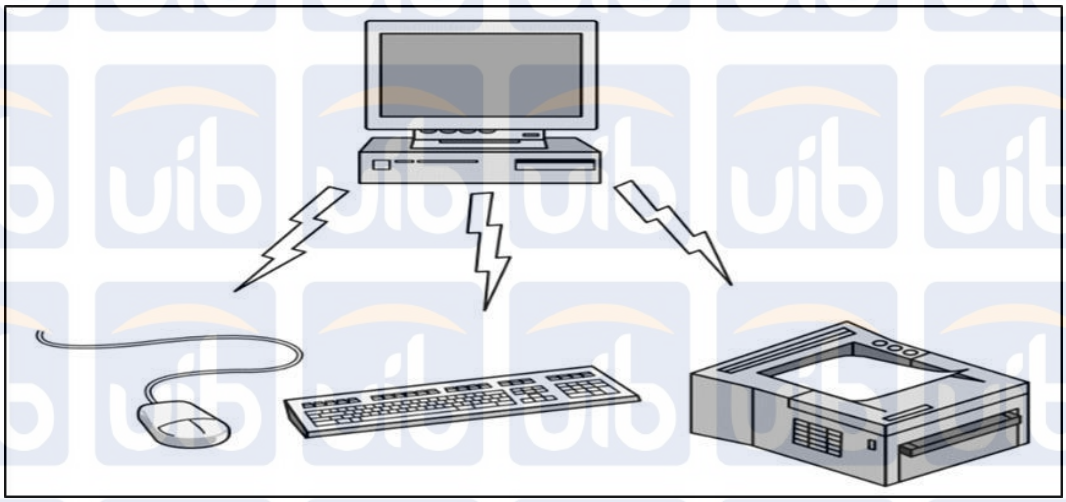
2.2.2 Jaringan Komputer

Gabungan sejumlah komputer yang biasanya terdiri dari dua atau lebih dari perangkat komputer disebut sebagai "jaringan komputer", ini juga termasuk perangkat lainnya, seperti printer, hub, dan sebagainya. Semua perangkat yang telah dihubungkan akan saling berinteraksi melalui media perantara berupa media kabel ataupun media tanpa kabel (nirkabel) untuk bertukar data berupa teks, gambar, audio, dan video. Manfaat jaringan komputer dapat dirasakan oleh pengguna individu maupun perusahaan. Semua ini terjadi karena bertujuan agar pengirim (transmitter) dapat mengirim data dengan cepat dan efisien kepada penerima (receiver).

Model client-server digunakan oleh perusahaan sebagai jaringan komputer untuk berbagi informasi perusahaan, dan desktop karyawan dimanfaatkan sebagai klien untuk mengakses server. Sebagai individu, jaringan memberikan akses untuk mendapatkan informasi dan hiburan, beserta cara membeli dan menjual produk dan layanan. Cara yang paling sering digunakan untuk mengakses internet adalah melalui telepon ataupun penyedia kabel di rumah, namun tidak jarang sekarang yang mengakses melalui nirkabel untuk laptop dan telepon. Dengan tujuan dan manfaat yang berbeda bagi setiap penggunanya, maka jaringan dapat terbagi menjadi beberapa macam; PAN (Personal Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), dan WAN (Wide Area Network) (Wongkar, Sinsuw, & Xaverius, 2015).

2.2.3 PAN (Personal Area Network)

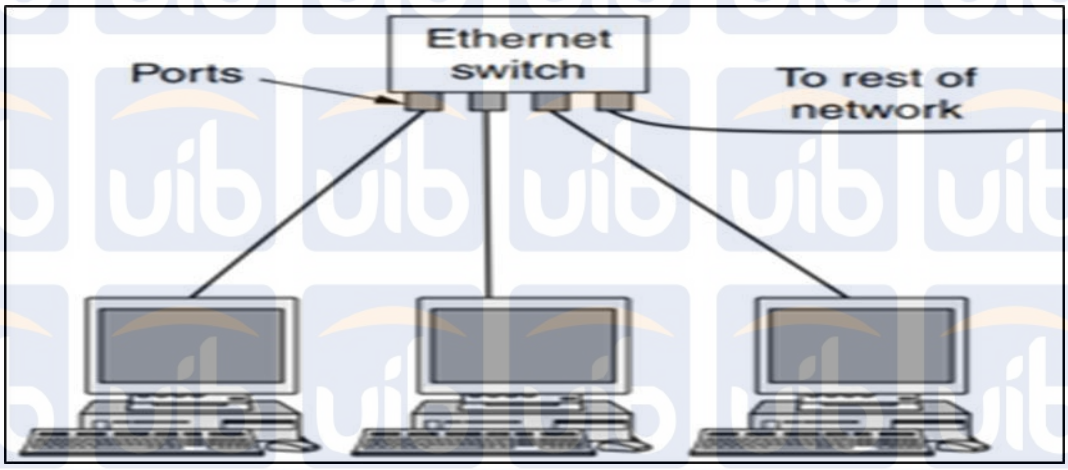
Jaringan komputer jenis PAN digunakan untuk berkomunikasi antara perangkat pribadi, yang biasanya berupa komputer, smartphone, tablet, dan lain-lain. Secara bersama beberapa perusahaan merancang jaringan nirkabel yang berjarak pendek untuk menghubungkan beberapa komponen ini tanpa kabel, yang sekarang disebut dengan "bluetooth". Jaringan ini bisa ke tingkat yang lebih besar lagi, dengan catatan salah satu perangkat harus mengambil peran sebagai router internet. Sebagai contoh, jaringan nirkabel yang menghubungkan komputer dan periferalnya. Kebanyakan dari pengguna komputer memiliki monitor, mouse, keyboard, dan printer terpasang, karena untuk mengoneksi semua peralatan komputer tersebut harus menggunakan kabel. Banyak pengguna baru yang sangat kesulitan untuk menemukan kabel yang tepat untuk dipasangkan diantara komputer dan perangkat lainnya sebagai penghubung, sehingga jaringan PAN sangat dibutuhkan bagi pengguna komputer dan elektronik untuk memenuhi kebutuhan konsumer (Wongkar, Sinsuw, & Xaverius, 2015).



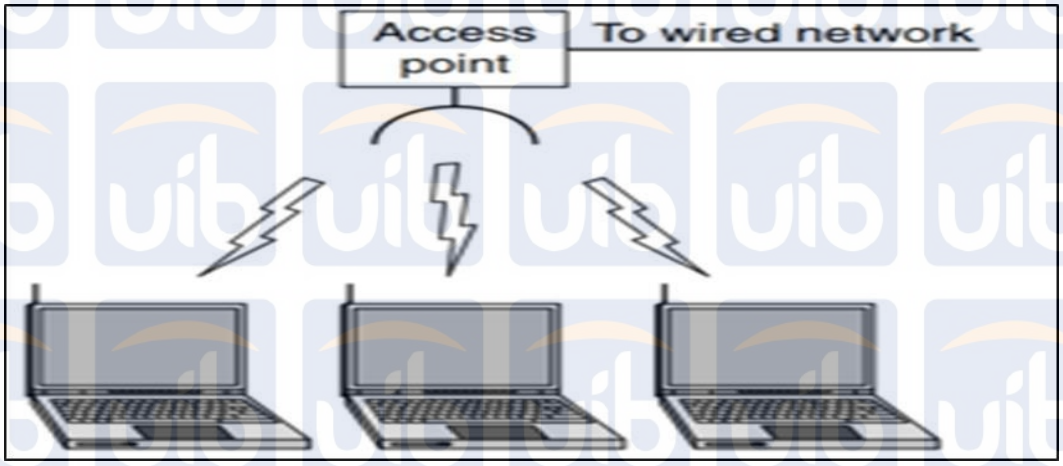
Gambar 2. 1 Konfigurasi PAN bluetooth

2.2.4 LAN (Local Area Network)

Jenis jaringan LAN merupakan yang paling sering digunakan untuk menghubungkan komputer pribadi dengan berbagai sumber, misalnya printer. Jaringan komputer ini dipasang disekitar bangunan rumah, kantor, dan pabrik. Sehingga, ketika LAN digunakan oleh perusahaan, maka akan disebut sebagai jaringan perusahaan. Dua komputer dapat dikoneksi dengan menggunakan kabel untuk mendapatkan jaringan ataupun ribuan komputer yang terhubung ke jaringan dengan menggunakan koneksi wireless. Komputer dan komponennya dapat dihubungkan dengan peralatan komputer dengan harga yang relatif murah, seperti hub, wireless access point, kabel Ethernet, dan adaptor jaringan (Wongkar, Sinsuw, & Xaverius, 2015).



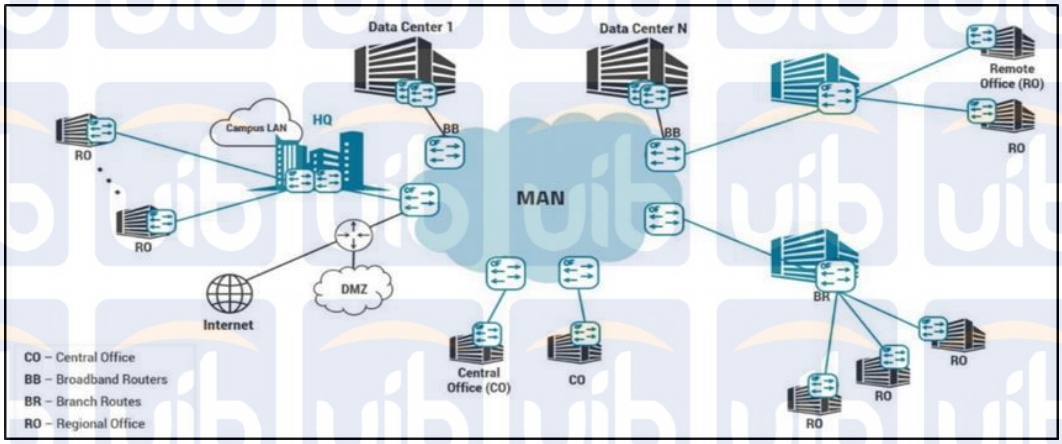
Gambar 2. 2 Jaringan yang menggunakan kabel



Gambar 2. 3 Jaringan tanpa kabel (wireless)

2.2.5 MAN (Metropolitan Area Network)

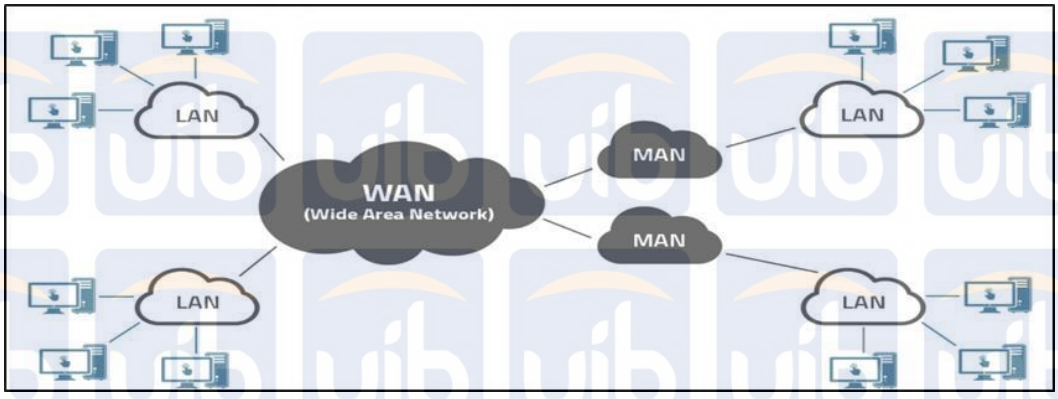
MAN merupakan jaringan yang lebih besar daripada LAN, namun lebih kecil dari WAN. Ini dikarenakan beberapa LAN digabungkan untuk membentuk suatu jaringan yang luas. MAN diciptakan untuk menghubungkan komputer dalam suatu kota, yang biasanya mencakup mulai dari beberapa mil hingga puluhan mil. Untuk dapat memahami lebih lanjut, contoh yang paling dikenal adalah jaringan televise kabel dengan sistem pemasangan antenna yang dihubungkan dengan antenna besar diatas bukit terdekat yang kemudian sinyalnya akan disalurkan ke rumah pelanggan (Wongkar, Sinsuw, & Xaverius, 2015).



Gambar 2. 4 Jaringan MAN

2.2.6 WAN (Wide Area Network)

Jaringan WAN lebih besar daripada LAN, dan MAN, karena terdiri dari beberapa gabungan jenis jaringan yang lebih kecil. Ini sebabnya, WAN mampu mencakup suatu negara ataupun benua. Sebagai contoh, kantor cabang akan didirikan di berbagai kota, yang dimana masing-masing kantor berisi komputer yang khusus untuk menjalankan suatu program atau aplikasi (Wongkar, Sinsuw, &Xaverius,2015).



Gambar 2. 5 Jaringan WAN

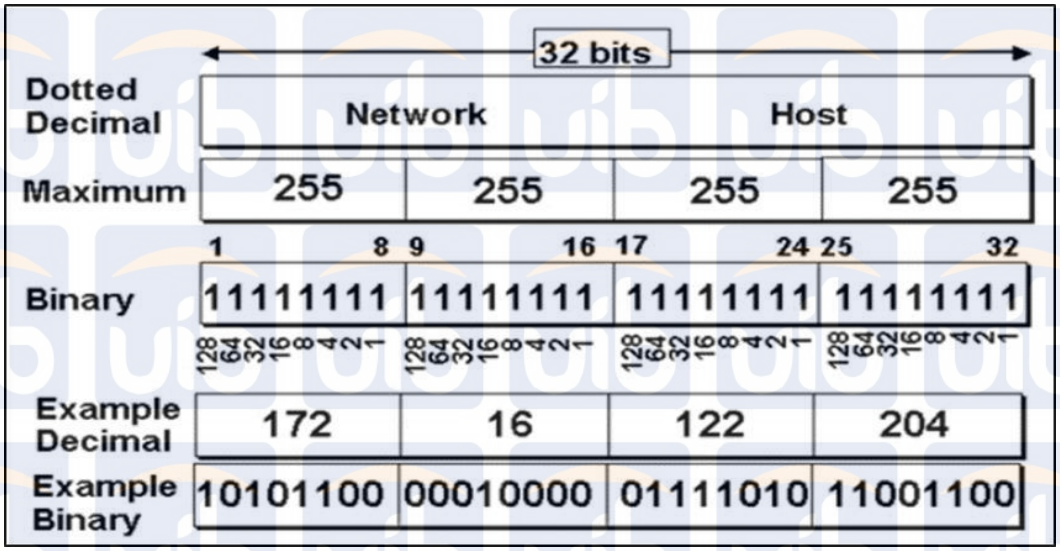
2.2.7 IP Address

IP Address merupakan singkatan dari “Internet Protocol Address”. Ini digunakan sebagai alamat lokasi jaringan dan sebagai alat identifikasi host atau antarmuka pada jaringan yang dilabelkan pada alat komputer, printer, dan router. Semua ini bertujuan untuk mengenali komputer yang mencoba mengirimkan data kepadanya.

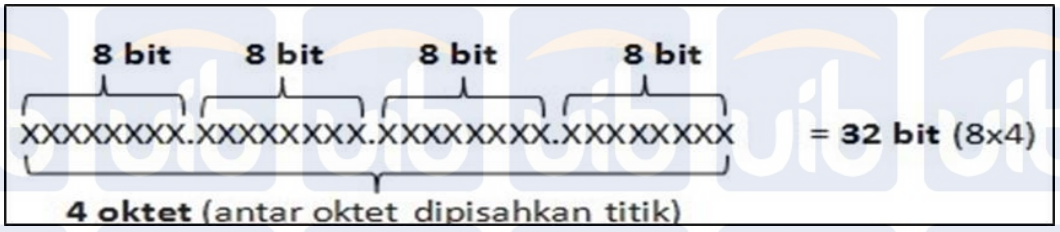
Ada 2 jenis IP Address, yaitu “IP Address Public” yang biasa digunakan pada jaringan global internet, kemudian “IP Address Private” yang biasa merupakan alamat IP untuk digunakan pada komputer dan perangkatnya dengan jaringan yang berskala lokal (LAN).

Untuk memahami lebih lanjut, disini ada beberapa alamat khusus yang baik untuk diketahui sebelumnya; Pertama adalah “Network Address”, yang akan menunjukkan alamat suatu jaringan, namun yang paling kecil menurut IP Address. Selanjutnya, “Broadcast Address”, ini digunakan dalam jaringan yang paling kecil menurut IP Address untuk mengirimkan paket ke seluruh host. Terakhir merupakan “Loopback”, yang merupakan alamat lokal yang dimiliki setiap komputer, dan bernilai 127.0.0.1.

Berdasarkan format dari IP Address versi 4 (IPv4), ini terdiri dari bilangan biner 32 bit, dan terbagi menjadi 4 kelompok. Setiap kelompok terdiri dari bilangan biner 8 bit, dan tanda pemisah tersebut disebut dengan “oktet” (Wardoyo, Ryadi, & Fahrizal, 2014).

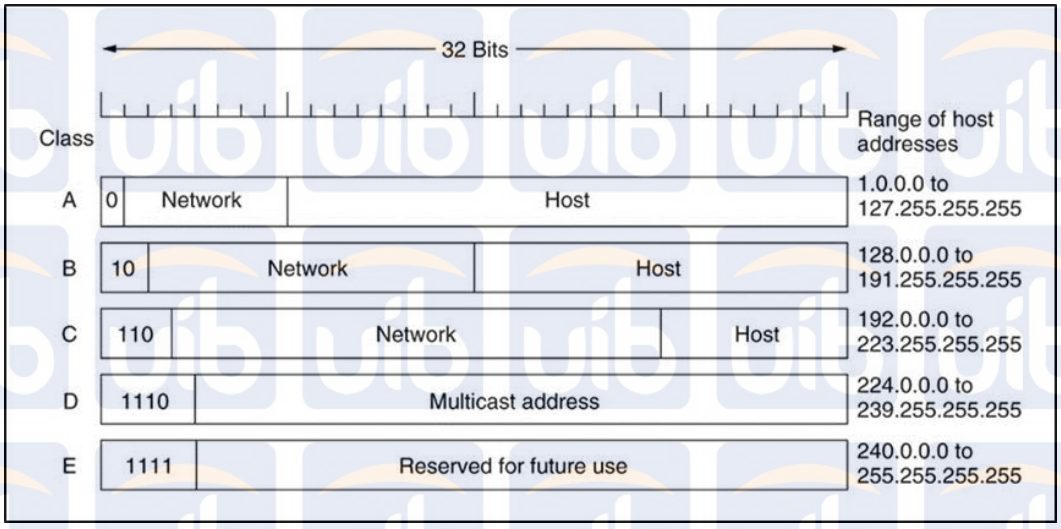


Gambar 2. 6 Format dari IP Address versi 4 (IPv4)



Gambar 2. 7 Format penulisan IP Address

Dalam IP Address, terdapat dua cara pembagian, yaitu: "Classfull Addressing", yang dibagi berrdasarkan kelas-kelas IP Address (Class A-E); dan "Classless Addressing", yang berupa pengalamatan tanpa kelas, dengan cara mengalokasikan IP Address dalam notasi "Classless Inter Domain Routing" (CIDR).



Gambar 2. 8 Berbagai macam kelas IP Address

Kelas A

Format : 0nnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 0

Panjang NetID : 8 bit

Panjang HostID : 24 Bit

Byte Pertama : 0-127

Jumlah : 126 Kelas A (0 dan 127 dicadangkan)

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214 IP Address disetiap kelas A

Deskripsi : Diberikan untuk jaringan dengan jumlah host yang besar

Kelas B

Format : 10nnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 10

Panjang NetID : 16 Bit

Panjang HostID : 16 Bit

Byte Pertama : 128-191

Jumlah : 16.384 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx

Jumlah IP : 65.532 IP Address di setiap kelas B

Deskripsi : Dialokasikan untuk jaringan besar dan sedang

Kelas C

Format : 110nnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 110

Panjang NetID : 24 Bit

Panjang HostID : 8 Bit

Byte Pertama : 192-223

Jumlah : 2.097.152 Kelas C

Range IP : 192.xxx.xxx.xxx sampai 223.255.255.xxx

Jumlah IP : 254 IP Address disetiap kelas C

Deskripsi : Diberikan untuk jaringan berukuran kecil

Kelas D

Format : 1110nnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 1110

Bit Multicast : 28 Bit

Byte Inisial : 224-247

Deskripsi : Kelas D digunakan untuk keperluan IP Multicast

Kelas E

Format : 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

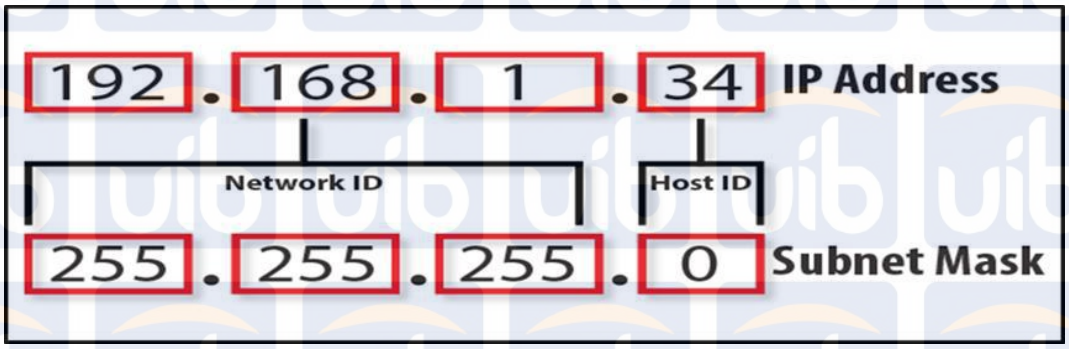
Bit Pertama : 1111

Bit Cadangan : 28 Bit

Bit Inisial : 248-255

Deskripsi : Kelas E dicadangkan untuk keperluan eksperimen

Format IP Address juga terdiri dari pembagian kelas-kelas yang berdasarkan dua hal, yaitu: “Network ID”, yang digunakan untuk menunjukkan jaringan lokasi komputer berada; dan “Host ID”, untuk menunjukkan host pada suatu jaringan, seperti workstation, server, router, host TCP/IP, dan lainnya.



Gambar 2. 9 Format IP Address

Aturan dasar dalam menentukan “Network ID” adalah 127.0.0.1 tidak dapat digunakan. Ini dikarenakan merupakan default yang sudah diatur untuk

menunjukkan dirinya sendiri (loop-back). “Host ID” juga tidak boleh diatur sebagai 1 (contohnya: 126.255.255.255), yang dapat diartikan sebagai ID broadcast, yang merupakan alamat mewakili seluruh anggota pada jaringan.

Network ID dan Host ID tidak boleh menggunakan IP Address yang sama dengan 0 (contoh, 0.0.0.0). Host ID yang menggunakan 0, dapat diartikan sebagai alamat jaringan. Alamat jaringan digunakan untuk menunjukkan suatu jaringan, dan bukan host. Maka, Host ID harus unik dalam suatu jaringan, dan dalam dua host tidak boleh memiliki Host ID yang sama (Lukman, 2016).

Seiring dengan pertumbuhan jaringan, maka jaringan akan semakin besar. Pada saat itu, pembagian jaringan akan sangat dibutuhkan, karena semakin sulit untuk dikendalikan. Pengelompokan berdasarkan host dan faktor umum kedalam jaringan yang sama sangat dibutuhkan saat perencanaan jaringan. Perancang jaringan juga harus bertanya: Apakah atas dasar jaringan tersebut harus dibagi? Ini dikarenakan, secara umum, masalah yang sering terjadi pada jaringan besar adalah penurunan kinerja, masalah keamanan, dan manajemen alamat.

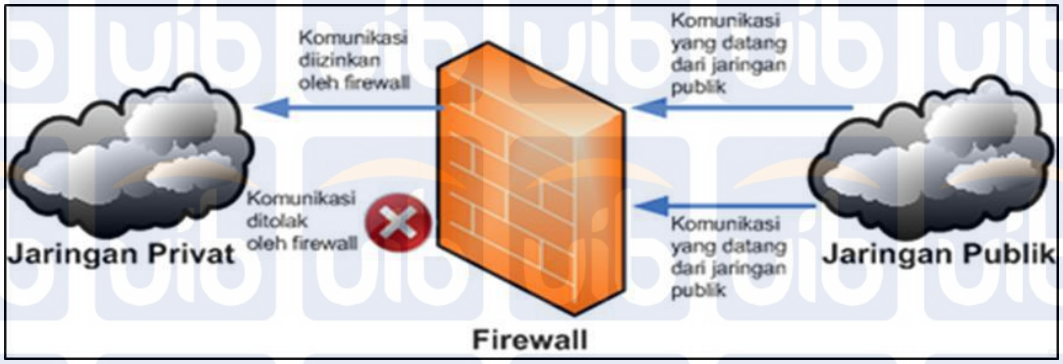
Penurunan kinerja yang dimaksudkan ini adalah beberapa host yang besar terhubung ke satu jaringan, dan ini dapat menghasilkan volume lalu lintas data yang meregangkan, atau berpengaruh pada sumber daya jaringan seperti kemampuan bandwith, dan router. Pembagian jaringan akan memberikan manfaat pada host yang perlu berkomunikasi, maka ketika dikelompokkan, ini akan mengurangi lalu lintas di seluruh antarjaringan.

Sebagai bentuk pengelolaan alamat pada jaringan yang besar, mengelompokkan host yang perlu berkomunikasi ke dalam satu kelompok akan

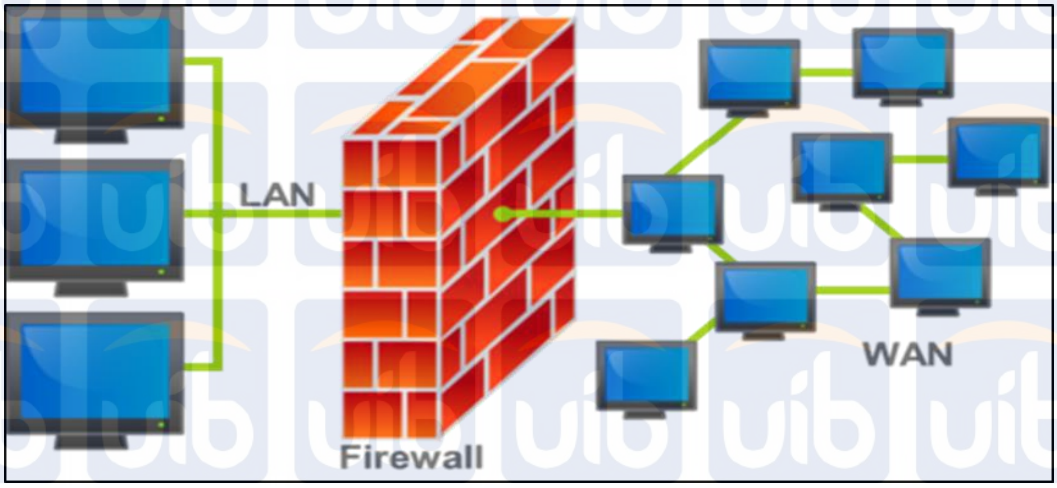
mengurangi pengeluaran yang tidak diperlukan dari semua host yang perlu mengetahui semua alamat ini. Untuk tujuan lain, host hanya perlu mengetahui alamat perangkat perantara, yang mereka kirimi paket kepada semua alamat tujuan lainnya. Perangkat perantara ini disebut sebagai “gateway” (Mulyana, 2013).

2.2.8 Firewall

Firewall dapat berarti alat jaringan yang memiliki salah satu fungsi untuk menyaring lalu lintas masuk dan keluar menggunakan perangkat keras, atau layanan yang berjalan pada komputer yang memiliki kemampuan untuk menyaring lalu lintas melalui perangkat lunak. Pada penelitian ini, penulis akan berfokus pada perangkat lunak pfSense sebagai firewall (Sylvester, Asante, & Twum 2016).



Gambar 2. 10 Ilustrasi mengenai firewal



Gambar 2. 11 Ilustrasi mengenai firewall dalam sebuah jaringan komputer

Tujuan utama dari firewall adalah membangun penghalang antara jaringan internal (yang dipercaya) dan jaringan eksternal (yang tidak dipercaya). Semua firewall jaringan memiliki kemampuan untuk melakukan filter paket. Ini merupakan kemampuan untuk memeriksa paket dan menentukan bila sesuai dengan aturan penyaringan filter paket.

Firewall pada pfSense memiliki tiga pilihan tindakan utama untuk menyaring trafik lalu lintas: “Pass” untuk menerima akses dan mengijinkan melewati firewall. “Block” adalah kondisi disaat akses diterima, namun paket langsung dibuang secara diam-diam. “Reject” juga akan menyebabkan paket akan terbuang, namun pesan port yang tidak dapat dicapai akan dikembalikan ke pengirim (untuk memberitahu bahwa firewall telah memblokir lalu lintas).

Dalam pfSense, urutan aturan merupakan faktor yang sangat penting untuk menjalankan tugas firewall. Kebanyakan orang menulis peraturan dengan benar, namun karena urutan peraturan tersebut berada di posisi yang salah, sehingga memunculkan reaksi yang tidak diharapkan dari pfSense Tentu saja, peraturan

pfSense dicek satu-per-satu oleh sistem ini secara berurutan, dari yang pertama hingga ke yang terakhir. Sehingga, aturan pertama yang cocok dengan paket akan diterapkan, dan sisa dari peraturan dari paket tersebut tidak akan diterapkan. Pemeriksaan aturan akan berhenti setelah kecocokan aturan yang pertama terbaca, kecuali untuk floating rules.

Mulailah aturan dari yang paling spesifik, yang memiliki banyak kriteria dalam aturan untuk ditaruh pada posisi yang paling atas, kemudian dilanjutkan dengan yang general untuk mendapatkan hasil yang maksimal dari pemeriksaan firewall. Pengguna tidak mengharapkan sistem pfSense untuk mendeteksi masalah yang sangat umum, dan akhirnya berhenti pengecekan disitu. Itulah sebabnya, detail tentang aturan sangatlah penting untuk diterapkan.

Beberapa hal yang perlu diperhatikan sebagai tips. Bila koneksi tidak berjalan dengan baik, maka pastikan aturan telah terdaftar pada incoming interface, karena setiap incoming interface memiliki aturan yang terpisah. Bila peraturan diletakkan pada lokasi incoming interface yang salah, maka peraturan tersebut tidak akan pernah dicek.

Pastikan juga tidak ada aturan interface group yang cocok dengan lalu lintas (traffic). Aturan interface group diperiksa sebelum aturan interface, karena itu diharapkan agar tidak ada aturan interface group yang diatur secara general, untuk menghindari kesamaan pada lalu lintas yang akan mengakibatkan sistem tidak dapat bekerja dengan sempurna.

Pastikan juga tidak ada aturan quick floating yang cocok juga dengan lalu lintas. Aturan floating yang regular tidak akan menimbulkan masalah, namun

aturan quick floating akan menimpa aturan interfaces. Jadi, pastikan pengaturan aturan yang lebih spesifik, agar tidak sama dengan lalu lintas.

Sebagai catatan, aturan firewall berlaku untuk koneksi, dan bukan untuk paket individual. Jadi, aturan pada firewall akan dievaluasi pada saat ada koneksi baru yang telah dibuat. Bila aksi yang dibuat adalah untuk membiarkannya "pass" dari lalu lintas, dan state yang baru telah dibuat pada state table yang baru, maka aturan pada firewall tidak akan dievaluasi kembali.

Menambahkan aturan block/reject baru tidak akan memutuskan koneksi yang ada, bila sebelumnya telah membiarkan lalu lintas untuk "pass". Ini dikarenakan state yang sudah tersimpan pada state table sebelumnya, yang telah memberikan sistem untuk memberikan akses melewati lalu lintas, kecuali ditutup kembali. Bila pengaturan aturan ini mempengaruhi hasil kerja pada sistem, maka state table dapat diatur kembali untuk memperbaiki keadaan.

Secara default, interface tidak memiliki aturan, maka semua trafik akan diblokir secara default. Ini dikarenakan tidak ada aturan yang telah diatur, sehingga tindakan otomatis yang akan diambil adalah "block". Jadi, bila ingin membuat koneksi baru seperti koneksi internet wireless, pengguna komputer harus secara eksplisit menambahkan aturan laluan "pass" ke pilihan interface apa saja, agar koneksi dapat melaluinya. Secara default, semua arus lalu lintas yang tidak cocok akan diblokir, dan ini dikenal sebagai "whitelist approach". Semua lalu lintas harus diijinkan untuk "pass" secara jelas kepada koneksi yang pengguna komputer inginkan untuk melewati interface. Ini sangat berguna untuk koneksi WAN, karena dapat memilah koneksi yang diijinkan untuk memasuki

koneksi pengguna komputer. Selain itu, pengguna komputer dapat menambahkan aturan “allow to all” di akhir aturan antarmuka yang diatur. Ini bermanfaat untuk mengijinkan koneksi apa saja diluar sana yang belum diatur dalam interface rule set, yang sebagaimana dikenal sebagai “blacklist approach”. Semua lalu lintas harus di “block/reject” secara jelas, karena sisanya akan diijinkan sistem untuk “pass”, agar dapat melewati lalu lintas. Ini sangat berguna untuk LAN interfaces, karena secara umum diluar sana ada banyak aplikasi yang pengguna komputer ingin gunakan untuk membuat beberapa koneksi, seperti internet.

Ini tidak memungkinkan bagi pengguna komputer untuk mengerti semua jenis aplikasi dan memahami semua tipe koneksi. Jadi, akan lebih masuk akal bila pengguna komputer untuk “block” koneksi yang tidak diinginkan, dan berasumsi bahwa yang lain tidak akan mengganggu performa sistem, sehingga pengaturan diatur menjadi “pass”. Tidak bermasalah bila pengguna ingin memutar cara pengaturan, untuk mengunakan whitelist approach terhadap LAN interfaces, dan blacklist approach terhadap WAN interfaces. Namun, ini akan sangat menyulitkan bila menggunakan whitelist approach terhadap LAN interfaces, karena pengguna komputer harus membuat profil terhadap semua software yang dimiliki, untuk memastikan dapat bekerja dengan baik. Kelebihannya adalah bila ada malware yang mencoba untuk memasuki koneksi, maka malware tidak mampu berkomunikasi kepada koneksi yang dimiliki pengguna komputer, karena sisa semua pengaturan telah di “block” dari koneksi. Sebaliknya, sangat tidak disarankan untuk mengatur pengaturan blacklist approach terhadap WAN

interfaces, karena akan menghasilkan performa yang tidak diinginkan (Zientara, 2016).

Perlu diketahui beberapa jenis-jenis firewall, yang dibedakan berdasarkan caranya bekerja, yaitu Packet Filtering Gateway, Application Layer Gateway (Proxy Firewall), Circuit Level Gateway, dan Stateful Multilayer Firewall (SMIF) (Kumar & Gupta, 2018). Jenis firewall yang telah disebutkan akan dijelaskan secara ringkas dibawah ini.

2.2.9 Packet Filtering Gateway

Packet Filtering Gateway merupakan jenis firewall yang bertugas melakukan penyaringan terhadap paket yang datang dari luar jaringan yang dilindunginya. Penyaringan paket terjadi berdasarkan sumber IP paket, tujuan IP paket, dan atribut lainnya seperti protocol transport (UDP, TCP), serta nomor port yang digunakan. Informasi yang berasal dari paket akan dianalisa dan kemudian ditentukan aksi yang akan dilakukan terhadap paket berdasarkan program firewall yang telah diatur tersebut. Aksi keputusannya adalah untuk menerima dan diteruskan atau ditolak paketnya.

Contohnya adalah tujuan dari paket adalah ke server yang menggunakan IP 192.168.2.1 dengan port 80, dan kebetulan paket tersebut juga menggunakan port 80, maka firewall akan mengijinkan paket yang bertujuan ke web server yang menggunakan port 80, dan menolak paket yang bertujuan berbeda, seperti ke port 23. Berdasarkan dari arsitektur TCP/IP, firewall ini akan bekerja pada “Internet

Layer", dan biasanya merupakan bagian dari sebuah router firewall (Sharma & Chandresh, 2017).

2.2.10 Application Layer Gateway (Proxy Firewall)

Jenis firewall ini bekerja tidak hanya berdasarkan sumber, tujuan dan atribut paket, namun juga termasuk dari isi (content) paket tersebut. Mekanismenya adalah paket tidak akan secara langsung sampai ke tujuan server, melainkan hanya akan sampai ke firewall saja. Kemudian, firewall akan membuka koneksi baru ke server tujuan setelah paket tersebut telah diperiksa sesuai dengan peraturan yang berlaku. Jenis firewall ini berfokus pada suatu layanan jaringan tertentu, sehingga perlu untuk memeriksa muatan, menyediakan autentikasi, dan menjamin bahwa hanya services tertentu yang diijinkan untuk digunakan.

Contohnya adalah proxy HTTP dapat menjamin bahwa hanya trafik HTTP yang memiliki ijin akses untuk diperbolehkan lewat. Sebuah koneksi akan mengakses URL pada web server http://server.com/ikom/, maka firewall akan mengecek bila koneksi dan direktori /ikom/ diijinkan untuk mengakses melalui koneksi yang dibuka untuk dibuhungkan ke server tujuan. Berdasarkan dari arsitektur TCP/IP, maka firewall jenis ini akan bekerja pada "Application Layer" (Sharma & Chandresh, 2017).

2.2.11 Circuit Level Gateway

Jenis firewall ini bekerja pada bagian "Transport Layer" model referensi TCP/IP. Firewall akan mengawasi hubungan awal TCP, yang biasa disebut

sebagai “TCP Handshaking” sebagai proses menentukan interaksi hubungan tersebut diijinkan atau sebaliknya. Bentuk firewall jenis ini hampir sama dengan Application Layer Gateway, yang membedakan adalah bagian yang disaring terdapat pada lapisan Transport Layer (Sharma & Chandresh, 2017).

2.2.12 Stateful Multilayer Inspection Firewall (SMIF)

Jenis firewall ini merupakan penggabungan dari ketiga firewall yang sudah dibahas sebelumnya; Packet Filtering Gateway, Application Layer Gateway (Proxy Firewall), dan Circuit Level Gateway. Jenis firewall ini bekerja pada “Application Layer, Transport Layer, dan Internet Layer”. Penggabungan dari beberapa sistem firewall menjadi satu, menghasilkan jenis firewall yang paling aman untuk memberikan perlindungan pada sistem dengan memberikan banyak manfaat dari gabungan keunggulan yang ditawarkan dari setiap jenis firewall.

Jenis firewall ini melakukan penyaringan terhadap lalu lintas berdasarkan karakteristik paket, seperti yang dilakukan oleh firewall jenis Packet Filtering Gateway. Sistem ini akan melakukan pengecekan terhadap sesi koneksi, untuk menentukan bila koneksi tersebut dapat diijinkan mendapatkan akses untuk sampai ke tujuan. Selain itu juga melakukan inspeksi terhadap data yang datang dari “Application Layer” dengan menggunakan layanan tertentu. Berbeda dari Application Layer Gateway (Proxy Firewall), dan Circuit Level Gateway, jenis Stateful Multilayer Inspection Firewall (SMIF) umumnya didesain lebih transparan, seperti Packet Filtering Gateway. Stateful Multilayer Inspection Firewall (SMIF) juga lebih kompleks dibandingkan jenis firewall yang lain karena

penggabungan beberapa jenis firewall, sehingga firewall ini hanya tersedia pada beberapa firewall kelas atas, seperti Cisco PIX (Sharma & Chandresh, 2017).

2.2.13 pfSense

pfSense disediakan dalam bentuk perangkat lunak (software) yang mendukung fungsi dasar komputer (operating system) yang berbasis FreeBSD. Orientasi utama dari pfSense adalah sebagai firewall, dan router. Selain itu, pfSense juga memberikan fitur lain, yang diantaranya sebagai berikut: Firewall, Router, Virtual Private Network (VPN), Network Address Translation (NAT), Multi-WAN, PPPoE Server, Internet Filter, Server Load Balancing, Captive Portal, Dynamic DNS, Reporting and Monitoring, DHCP Server and Relay, dan lain-lain.

pfSense dirancang untuk diinstal pada Personal Computer (PC), namun juga memberikan solusi sebagai perangkat keras (hardware) tertanam. pfSense mudah dipasang dan dirawat dengan menawarkan antarmuka pengguna (user interface) berbasis web yang sangat berguna, dan berbagai fitur. Hal ini memungkinkan pfSense untuk menawarkan lebih banyak fleksibilitas. Namun, banyak dari fitur yang bermanfaat hanya sering ditemukan di router komersial yang mahal (Buechler & Pingle, 2013).

pfSense merupakan pilihan yang tepat untuk digunakan dibandingkan perangkat lunak maupun perangkat keras lainnya. Produk ini disediakan secara gratis dan open source, selain itu juga cepat dan mampu menawarkan banyak fitur kepada masyarakat luas. Pengguna dapat mengontrol perangkatnya dan

disesuaikan dengan sistem yang dimiliki berdasarkan komponen-komponen yang diinginkan (Nugraha, Gunawan, & Siregar 2015).

Membeli perlengkapan perangkat keras seperti router atau yang biasa dipanggil dengan wireless router akan sangat mahal, bila tidak mengerti cara memanfaatkan dan membeli sesuai dengan yang dibutuhkan. Ada beberapa alasan mengapa tidak membeli "wireless router" sebagai pertimbangan. Sejumlah insinyur di beberapa perusahaan harus mendesain perangkat keras yang spesial, termasuk perangkat lunak dan user interface yang mampu melaksanakan segala kebutuhan perusahaan. Memeriksa dan membuatnya berfungsi sesuai level yang diinginkan pengguna, dan harus sering terus menerus memperbarui (up to date) keamanan terbaru. Terkadang juga harus berhadapan dengan router yang bermasalah.

Produk "wireless router" dirancang demi kebanyakan orang. Agar pengguna tidak mengeluh karena terlalu rumit, maka fitur yang disediakan juga sangat sedikit. Sehingga ini sangat mudah digunakan bagi pemula.

pfSense sangat cocok untuk berbagai jaringan, mulai dari yang kecil hingga yang besar. Maka, untuk menambahkan sistem pfSense ke jaringan, pengguna perlu mempertimbangkan bagaimana akan digunakan ke jaringan. Untuk memulai dengan pfSense, maka pengguna memerlukan komputer lama dan setidaknya yang terdapat dua kartu jaringan.

Bermacam manfaat dari fitur pfSense dapat digunakan oleh pengguna, dan uniknya adalah pfSense dapat diatur khusus sebagi firewall saja, atau menjalankan tugas ganda, sebagai firewall dan router. Selain itu juga dapat memilih untuk

memiliki lebih dari dua antarmuka dalam sistem pfSense (dikenal sebagai optional interfaces). Agar dapat bertindak sebagai firewall, maka sistem pfSense membutuhkan setidaknya dua antarmuka: antarmuka WAN (untuk terhubung ke jaringan luar), dan antarmuka LAN (untuk terhubung ke jaringan lokal).

Dalam pengaturan jaringan yang lebih kompleks, sistem pfSense Anda mungkin harus bertukar routing information dengan router lain di jaringan. Ada dua jenis protokol untuk bertukar informasi tersebut: “distance vector protocols”, memperoleh information routing dengan cara bertukar informasi dengan router tetangga; router menggunakan “link-state protocols” untuk membangun peta jaringan agar dapat menghitung jalur terpendek ke router lain, dengan cara setiap router menghitung jarak secara independen. pfSense mampu menjalankan kedua jenis protokol. Paket yang tersedia untuk distance vector protocols adalah RIP dan RIPv2 sebagai contoh, dan link-state protocols adalah Border Gateway Protocol (BGP) sebagai contoh.

Kegunaan umum lainnya adalah mengatur pfSense sebagai router. Di lingkungan rumah atau small office/home office (SOHO), fungsi firewall dan router sering digunakan oleh perangkat yang sama.

Pada jaringan menengah ke besar, router adalah perangkat yang terpisah dari firewall. Pada jaringan yang lebih besar dan memiliki beberapa segmen jaringan, maka pfSense dapat digunakan untuk menghubungkan beberapa jaringan ini. Dalam lingkungan tipe perusahaan, ini sering digunakan bersama, yang memungkinkan satu Network Interface Card (NIC) untuk beroperasi di beberapa broadcast domain melalui penandaan 802.1q. VLAN sering digunakan pada

konfigurasi router on a stick, di mana router memiliki koneksi fisik tunggal ke switch, dengan antarmuka Ethernet tunggal dibagi menjadi beberapa VLAN, dan penerusan paket router diantara VLAN. Salah satu keuntungan dari pengaturan ini adalah ini hanya membutuhkan satu port, dan, sebagai hasilnya, itu memungkinkan kita untuk menggunakan pfSense dengan sistem, ketika menambahkan NIC lain akan menjadi rumit atau bahkan tidak mungkin: misalnya, laptop.

Dalam kebanyakan kasus, dimana pfSense digunakan sebagai router pada jaringan berukuran menengah dan besar, ia akan digunakan untuk menghubungkan berbagai segmen LAN, namun juga bisa digunakan sebagai router WAN. Dalam hal ini, fungsi pfSense adalah menyediakan koneksi WAN pribadi ke pengguna akhir.

Kemungkinan penggunaan lain dari pfSense adalah sebagai switch. Jika memiliki beberapa antarmuka pada sistem pfSense dan menghubungkan mereka, maka pfSense dapat berfungsi sebagai switch. Ini kurang umum terjadi karena beberapa alasan.

Menggunakan pfSense sebagai switch, umumnya tidak dapat menghasilkan hasil yang baik tanpa biaya banyak uang (cost-effective). Pengguna komputer dapat membeli switch Ethernet lima-port dengan harga kurang dari apa yang diperlukan untuk membeli perangkat keras untuk sistem pfSense Membeli switch yang tersedia secara komersial juga akan menghemat uang dalam jangka panjang, karena ini memungkinkan konsumsi energi listrik yang jauh lebih sedikit

dibandingkan dengan berbagai jenis komputer yang digunakan untuk menjalankan pfSense

Switch yang tersedia secara komersial juga memungkinkan untuk mengungguli pfSense, karena pfSense akan memproses semua paket yang lewat di antara port, sementara switch Ethernet akan menanganinya dengan perangkat keras yang dibuat khusus untuk mengirimkan data antara port dengan cepat. Meskipun Anda dapat menonaktifkan penyaringan sepenuhnya di pfSense, namun tetap akan dibatasi oleh kecepatan bus tempat kartu jaringan Anda berada, diantaranya adalah PCI, PCI-X, atau PCI Express (PCI-e).

Ada juga biaya administrasi menggunakan pfSense sebagai switch. Switch sederhana dirancang untuk plug-and-play, dan pengaturan switch ini semudah mencolokkan kabel Ethernet dan kabel listrik. Switch yang terkelola biasanya memungkinkan untuk mengkonfigurasi pengaturan di konsol dan / atau melalui antarmuka web, tetapi dalam banyak kasus, konfigurasi hanya diperlukan jika Anda ingin mengubah pengoperasian switch. Jika menggunakan pfSense sebagai switch, beberapa konfigurasi akan diperlukan.

Kemungkinan lain menggunakan pfSense adalah sebagai wireless router / access point. Sebagian besar jaringan moderen menggabungkan beberapa jenis konektivitas nirkabel. Menghubungkan ke jaringan nirkabel tidak hanya lebih mudah, tetapi dalam beberapa kasus, menjalankan kabel Ethernet bukanlah pilihan yang realistis. Dengan pfSense, maka dapat menambahkan kemampuan jaringan nirkabel ke sistem dengan menambahkan wireless network card, asalkan kartu jaringan (network card) didukung oleh FreeBSD.

Umumnya, menggunakan pfSense sebagai wireless router / access point bukanlah pilihan terbaik. Solusinya adalah membeli wireless router, kemudian mengaturnya khusus bertindak sebagai access point, menghubungkan ke port LAN sistem pfSense, dan biarkan pfSense bertindak sebagai server Dynamic Host Configuration Protocol (DHCP).

Biasanya, sebuah router akan berfungsi dengan baik sebagai wireless access point dan mampu mendukung standar jaringan nirkabel terbaru dibandingkan pfSense Kemungkinan lain adalah untuk membeli khusus wireless access point. Ini umumnya murah dan beberapa memiliki fitur seperti tersedia beberapa SSID, yang memungkinkan Anda untuk mengatur beberapa jaringan nirkabel (misalnya, guest network terpisah yang terisolasi dari jaringan lokal lainnya). Menggunakan pfSense sebagai router, dan dikombinasi dengan wireless access point yang dibeli, memungkinkan memberikan pilihan yang lebih baik (Zientara, 2016).