OPTIMASI KEAMANAN JARINGAN HOSTPOT MENGGUNAKAN PFSENSE PADA STMIK PROFESIONAL MAKASSAR

Yahya Matori
Program Studi Teknik Komputer, STMIK Profesional
yoyosonor@gmail.com

Abstrak

Dalam jurnal ini di kembangkan metode keamanan captive portal mikrotik dengan menggunakan pfsensei sebagai model keamanan yang diterapkan pada stmik professional Makassar. untuk meningkatkan keamanan apada jaringan kampus stmik professional sendiri ,dengan ditingkatkannya keamanan pada sisi router di area kampus stmik profesioanal maka keamanan data lebih terjamin. Peralatan yang di butuhkan untuk membangun system ini tidak terlalu banyak hanya dengan modal satu personal computer dan Iso file pfsensei yang di download pada situs resminya.dengan begitu dari segi biaya sangat minim untuk membangun system keamanan seperti yang di sebutkan.diatas

Kata Kunci:*Pfsense,CaptivePortal,Stmikprofesional*

A. PENDAHULUAN

Dalam membangun kebutuhan terhadap akses internet yang aman di kalangan mahasiswa perlu kiranya untuk menambah serta memperbaharui fasilitas yang terkait dengan internet, untuk itu kebutuhan internet yang semakin meningkat dan tingginya permintaan akan akses yang stabil serta cepat di butuhkan sebuah router yang handal guna memfasilitasi kendala yang ada, dengan dukungan alat yang mampu untuk menangani semua itu, sebuah router yang handal serta gratis dapat di gunakan di berbagai jenis computer yg terdapat di lingkungan kita. Router yang mempunyai fasilitas serta tingkat keamanan yang tidak dapat di ragukan lagi di kelasnya .pfSense adalah FreeBSD berbasis sistem operasi, diturunkan dari m0n0wall, OS yang menggunakan penyaring paket OpenBSD pf. pfSense dirancang untuk digunakan sebagai firewall dan router. Selain menjadi kuat, fleksibel firewall dan routing platform, ini meliputi daftar panjang fitur terkait dan sistem paket yang memungkinkan upgrade lebih lanjut tanpa menambah gembung dan potensi kerentanan keamanan ke basis distribusi.

PFSENSE

pfSense adalah proyek yang populer dengan lebih dari 1 juta download sejak awal, dan terbukti dalam instalasi yang tak terhitung mulai dari jaringan rumah kecil melindungi PC dan Xbox untuk perusahaan besar, universitas dan organisasi-organisasi lain melindungi ribuan perangkat jaringan.

Proyek ini dimulai pada tahun 2004 sebagai pencabangan dari proyek monowall, tetapi fokus terhadap instalasi PC lengkap daripada perangkat keras yang tertanam fokus m0n0wall.pfSense juga menawarkan gambar tertanam untuk instalasi berbasis Compact Flash

Fasilitas pfSense

1. Firewall
2. Negara Tabel
3. Network Address Translation (NAT)
4. Redundansi
5. Load Balancing

Fungsi Firewall pada Pfsense

Menyaring oleh IP sumber dan tujuan, IP protokol, port sumber dan tujuan untuk TCP dan UDP lalu lintas, membatasi koneksi simultan pada per-aturan

PfSense menggunakan p0f, sebuah OS pasif maju / fingerprinting jaringan utilitas untuk memungkinkan penyaringan Sistem Operasi berdasarkan sambungannya memungkinkan mesin FreeBSD dan Linux ke Internet, tapi memblok mesin Windows. pfSense dapat melakukannya dengan pasif mendeteksi Sistem Operasi yang digunakan.

1. Pilihan untuk log atau tidak sesuai aturan lalu lintas log masing-masing.
2. Sangat kebijakan rute yang fleksibel mungkin dengan memilih gateway berdasarkan per-aturan (untuk load balancing, failover, beberapa WAN, dsb)
3. Alias memungkinkan pengelompokan dan penamaan IP, jaringan dan port.Hal ini membantu menjaga ruleset firewall lebih bersih dan mudah dimengerti, khususnya di lingkungan dengan beberapa IP publik dan server banyak.
4. Transparan 2 firewall lapisan mampu - dapat menjembatani antarmuka dan filter lalu lintas di antara sistem,
5. Paket normalisasi dari dokumentasi pf adalah normalisasi paket jadi tidak ada ambiguitas dalam interpretasi oleh tujuan akhir dari paket tersebut.Direktif juga reassembles paket terfragmentasi, melindungi beberapa sistem operasi dari beberapa bentuk serangan, dan tetes paket TCP yang memiliki kombinasi bendera tidak valid. "
6. Diaktifkan di pfSense secara default
7. Dapatkah menonaktifkan jika perlu. Pilihan ini menyebabkan masalah untuk beberapa implementasi NFS, tapi aman dan harus meninggalkan diaktifkan pada instalasi paling.
8. Filter Nonaktifkan - dapat menonaktifkan firewall filter sepenuhnya jika ingin mengaktifkan pfSense menjadi router murni.

Negara tabel firewall memelihara informasi tentang koneksi jaringan terbuka.pfSense adalah firewall stateful, secara default semua peraturan yang stateful. Kebanyakan firewall tidak memiliki kemampuan untuk mengendalikan meja halus negara.pfSense memiliki banyak fitur yang memungkinkan kontrol granular tabel negara bagian, berkat kemampuan pf OpenBSD's.Ukuran tabel negara Adjustable - ada beberapa pfSense instalasi produksi dengan menggunakan beberapa ratus ribu negara.Negara standar ukuran tabel adalah 10.000, tetapi dapat ditingkatkan dengan cepat ke ukuran yang di inginkan. Setiap negara berlangsung sekitar 1 KB RAM, sehingga tetap dalam penggunaan memori pikiran ketika ukuran tabel negara

Pada basis per-aturan:

1. Batasi koneksi klien secara simultan
2. Batas negara per host
3. Batas koneksi baru per detik
4. Tentukan negara timeout
5. Tentukan tipe negara

Network Address Translation (NAT)

1. Depan Port termasuk kompor dan penggunaan beberapa IP publik
2. 1:01 NAT untuk IP individu atau seluruh subnet.
3. Outbound NAT Default pengaturan NAT semua lalu lintas keluar ke WAN IP. Dalam skenario beberapa WAN, pengaturan default outbound NAT lalu lintas ke IP dari interface WAN yang digunakan.

   Advanced NAT memungkinkan Outbound perilaku default yang akan dinonaktifkan, dan memungkinkan penciptaan NAT sangat fleksibel (atau tidak NAT) aturan.
4. NAT Refleksi - dalam beberapa konfigurasi, refleksi NAT adalah layanan mungkin sehingga dapat diakses oleh publik IP dari jaringan internal.

Keterbatasan NAT

PPTP dan GRE Batasan - Keadaan kode pelacakan di pf untuk protokol GRE hanya dapat melacak sesi tunggal per IP publik per server eksternal.Ini berarti jika menggunakan koneksi VPN PPTP, hanya satu mesin internal dapat terhubung secara bersamaan ke server PPTP di Internet.Seribu mesin dapat terhubung secara bersamaan sampai ribuan server PPTP yang berbeda, tetapi hanya satu secara bersamaan ke server tunggal.Pekerjaan hanya tersedia sekitar adalah dengan menggunakan beberapa IP publik pada firewall, satu per klien, atau menggunakan beberapa IP publik di server PPTP eksternal. Ini bukan masalah dengan jenis lain koneksi VPN. Sebuah

solusi untuk ini saat ini sedang dalam pembangunan.

SIP Batasan - Secara default, semua lalu lintas TCP dan UDP selain SIP dan IPsec mendapatkan sumber port ditulis ulang.Informasi lebih lanjut tentang hal ini dapat ditemukan dalam dokumentasi pelabuhan statis. Karena sumber ini port menulis ulang adalah bagaimana pf track yang IP internal membuat koneksi ke server eksternal yang diberikan, dan hampir semua lalu lintas SIP menggunakan sumber yang sama port, hanya satu perangkat SIP dapat terhubung secara bersamaan ke server tunggal di Internet. Kecuali SIP perangkat dapat beroperasi dengan port sumber penulisan ulang (paling tidak bisa), dapat tidak menggunakan beberapa ponsel dengan server di luar tunggal tanpa menggunakan IP publik yang didedikasikan per perangkat. Paket sipproxd sekarang menyediakan solusi untuk masalah ini di pfSense

NAT refleksi keterbatasan Refleksi

NAT - hanya dapat digunakan dengan kisaran port kurang dari 500 pelabuhan dan tidak dapat digunakan dengan host 1:01 NAT.

Redundansi

Dua atau lebih firewall dapat dikonfigurasi sebagai kelompok failover.Jika satu antarmuka gagal pada primer atau utama berjalan offline sepenuhnya, menjadi sekunder aktif.pfSense juga mencakup kemampuan konfigurasi sinkronisasi, sehingga dapat membuat perubahan pada konfigurasi primer dan mereka secara otomatis melakukan sinkronisasi dengan firewall sekunder.

pfsync memastikan tabel negara adalah firewall failover direplikasi ke semua dikonfigurasi firewall. Ini berarti koneksi yang ada akan dipertahankan dalam kasus kegagalan, yang penting untuk mencegah gangguan jaringan.

Keterbatasan

1. Hanya bekerja dengan IP publik statis, tidak bekerja dengan DHCP, PPPoE, PPTP, atau jenis WAN Bigpond (akan diselesaikan di masa mendatang)
2. Membutuhkan minimal tiga alamat IP publik
3. Cadangan firewall yang idle (failover aktif-pasif), tidak ada clustering aktif-aktif
4. Failover tidak instan, dibutuhkan sekitar 5 detik untuk beralih host cadangan untuk master. Selama waktu lalu lintas tidak akan berlalu, tetapi negara-negara yang ada akan menjaga konektifitas failover setelah selesai. Ini outage 5 detik selama kegagalan bahkan tidak terlihat pada kebanyakan lingkungan.

Load Balancing

Load balancing outbound digunakan dengan koneksi beberapa WAN untuk menyediakan kemampuan load balancing dan failover. Lalu lintas diarahkan ke gateway load balancing yang diinginkan atau kolam di dasar per-aturan firewall.

Inbound load balancing digunakan untuk mendistribusikan beban antara beberapa server. Ini biasanya digunakan dengan server web, server mail, dan lain-lain. Server yang gagal untuk menanggapi permintaan ping atau koneksi port TCP dikeluarkan dari kolam.

- Sama mendistribusikan beban antara semua server yang tersedia - tidak dapat mendistribusikan beban tidak merata antara server saat ini.
- Hanya memeriksa apakah server merespon koneksi port ping atau TCP. Tidak dapat memeriksa apakah server kembali konten yang valid.

Kekurangan & Kelebihan pfSense

Kelebihan

Gratis

Dapat menghubungkan beberapa koneksi WAN dan load balancing. Captive Portal yang meninggalkan administrator untuk membatasi sesi (dalam cara yang serupa dengan program yang digunakan oleh kafe internet)

stable

fitur banyak

Kekuranagan

Banyak memerlukan RAM

Captive portal

Captive portal memungkinkan user untuk memaksa otentikasi, atau redirection untuk klik melalui halaman untuk akses jaringan. Hal ini umumnya digunakan pada jaringan hot spot, namun juga banyak digunakan dalam jaringan perusahaan untuk lapisan tambahan

keamanan pada akses nirkabel atau internet. Teknik captive portal memaksa klien HTT Ppada jaringan untuk melihat halaman web khusus (biasanya untuk keperluan otentikasi) sebelum menggunakan internet secara normal. Sebuah portal captive ternyata browser Web keperangkat otentikasi[1]. Ini dilakukan dengan mencegat semua paket, terlepas dari alamat atauport, sampai user membuka browser dan mencoba untuk mengakses Internet. Pada waktu

itubrowser ini dialihkan ke halaman web yang mungkin memerlukan otentikasi dan/atau pembayaran, atau hanya menampilkan acceptable use policy dan meminta user untuk setuju. Captive portal digunakan di banyakWi-Fi hotspot, dan dapat digunakan untuk mengontrol akses kabel (rumah apartemen misalnya, kamar hotel, pusat bisnis,
Karena halaman login itu sendiri harus disampaikan kepada klien, baik itu halaman login yang disimpan secara lokal di gateway, atau server web hosting halaman yang harus "daftar putih" melalui taman berdinding untuk memotong proses otentikasi. Tergantung pada set fitur gateway, server web dapat beberapa daftar putih (katakanlah untuk iframe atau link alam halaman login). Selain membolehkan akses URL dari web host, beberapa gate way dapat white list port +TCP. Alamat MAC dari klien terpasang juga dapat diatur untuk melewati proses login.

Redirection By HTTP

Jika klien tidak terauthentikasi permintaan situs web, DNS dipertanyakan oleh browser dan IP yang sesuai . Browser kemudian mengirimkan permintaan HTTP ke alamat IP. Permintaan ini, akan dicegat oleh firewall (dikonfigurasi sebagai transparent proxy) dan diteruskan ke redirect server. redirect Server merespon dengan respon HTTP biasa yang berisi HTTP 302 kode status untuk mengarahkan klien ke Captive Portal.

PRedirect

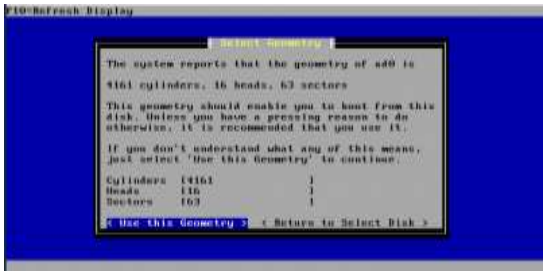
Lalu lintas Klien dapat juga diarahkan dengan menggunakan IP redirect pada tingkat 3 lapisan.

Redirection By DNS

Ketika klien meminta sebuah situs web, DNS dipertanyakan oleh browser. Firewall akan memastikan bahwahanya server DNS(s) yang disediakan oleh DHCP dapat digunakan oleh klien tidak terauthentikasi (atau, sebaliknya, akan meneruskan seluruh permintaan DNS oleh klien tidak terauthentikasi ke server DNS). Ini server DNS akan mengembalikan alamat IP dari halaman Portal Captive sebagai hasil dari semua DNS lookup. Dalam rangka untuk melakukan pengalihan oleh DNS captive portal menggunakan DNS keracunan untuk melakukan serangan Man-in-the-middle. Akibatnya, pengguna akan melihat pelanggaran sertifikat SSL ketika mencoba untuk mengunjungi halaman HTTPS. Untuk membatasi dampak keracunan DNS biasanya TTL 0 digunakan. Penggunaan nilai TTL dari 0 masih akan menimpa cacheresolver pengguna lokal yang dapat menyebabkan konflik dengan layanan sebelumnya dikonfirmasi.

Serangan terhadap Portal Captive

Captive portal telah dikenal memiliki se aturan firewall tidak aman. Kadang-kadang set aturan akan rute permintaan



DNSdari klien ke internet, atau server DNS yang disediakan akan memenuhi permintaan sewenang-wenang dns dilakukan oleh klien. Hal ini memungkinkan klien untuk mengakses internet terbuka dengan Tunneling TCP atau IP over DNS.

Instalasi Pfsense

Untuk memulai instalasi pf sense di perlukan perangkat computer yang mempunyai spek sebagai berikut :

- Intel(R) Pentium(R) 4

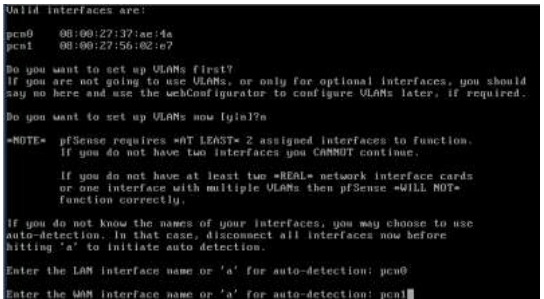
- CPU 3.00GHz

- Memory 2GB

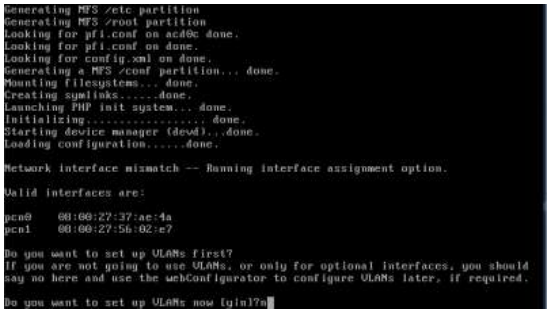
- LAN card 1 (D-LINK)

- LAN card 2 (LNK/ACT)

1. Siapkan Iso Pfsense dapat di download di alamat berikut : http://www.pfsense.org/index.php:
2. Verifikasi kebutuhan VLAN atau tidak
3. Menentukan interface yang akan di jadikan WAN dan LAN



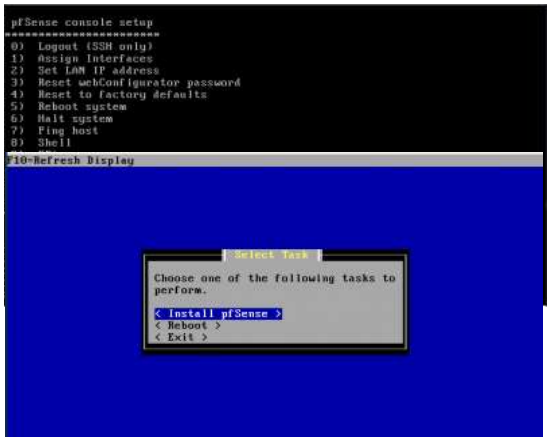
4. Opsi pemilihan Layana yang akan



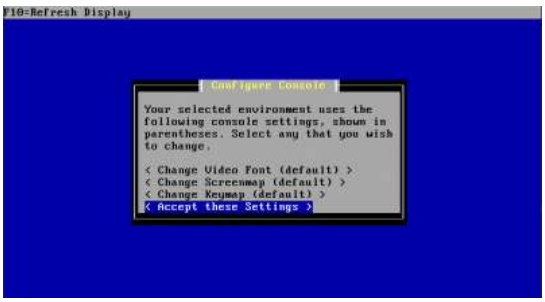
dipakai

5. Konfigurasi conslose setelah selesai settingan menu diatas

6. Proses Instalasi PfSensei
7. Opsi Pemilihan Ruang Harddisk yang akan dipakai

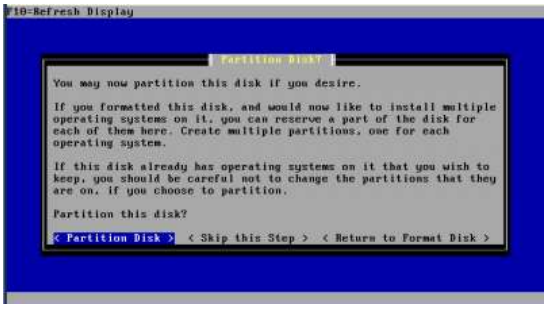


9. select geometri

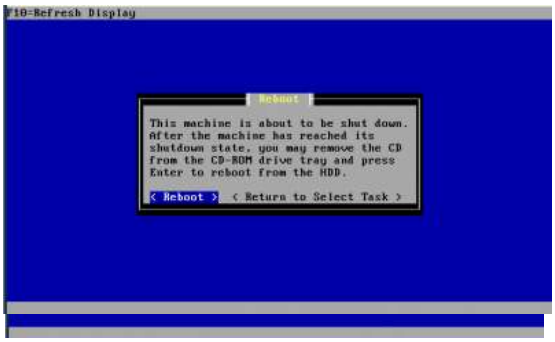


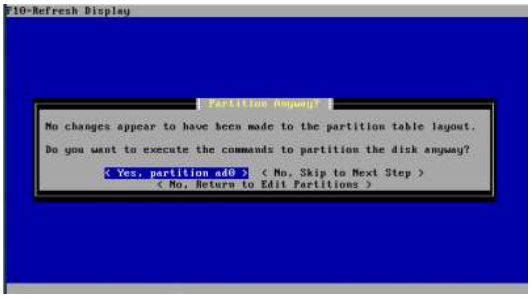
10. Proses Pemformatan disk

11.partition disk



12. Edit Partition





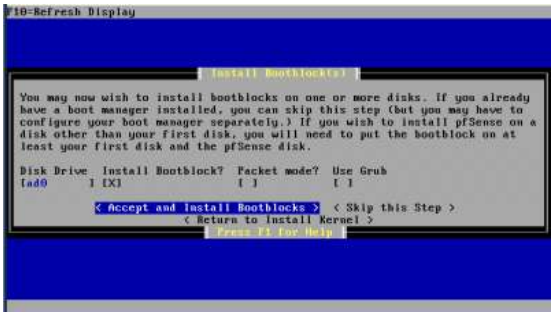
13.Informationmengenai Harddisk

15.select partition

17. informasi bahwa harrdisk telah di partisi

16. install kernel

18. install bootblock



19. bootblock sukses diinstall

20. pfsensei sukses diinstall

Captive portal pfsense

Captive portal pada pfsense akan meminta user dan password pada halaman HTMLnya dimana user akan di redirect pada sebuah page ,untuk mengaktifkan captive portal login terlebih dahulu pada pfsensei,klik menu layanan captive portal lalu tentukan LAN interface yang di gunakan untuk mengaksesnya.

Langkah selanjutnya adalah upload file HTML/PHP yang akan di gunakan untuk client yang akan login pada portal tersebut

E. KESIMPULAN

Dari Pembahasan Diatas yang telah penulis paparkan, maka dapat di simpulkan

1. Dengan mengimplementasikan Pfsense maka akan bertambah kemanan dari segi firewall dimana semakin berkembangnya teknologi maka Administrator harus mampu menggunakan pfsense sebagai bagian dari firewall tersebut
2. Penggunaan Captive portal untuk memanage client yang akan di paksa untuk masuk dan mengotorisasi dirinya sendiri sebeleum

menggunakan jaringan local maupun jarinagan public/internet

3. Proses sinkronisasi antara pfsense dengan captive portal merupakan paduan yang memungkinkan administrator meningkatkan dari segi keamanan Sistem tersebut

DAFTAR PUSTAKA

[1] www.**pfsense**.org
diakses 9 januari 2013 15.00 WIB

[2] www.**pfsense**.org/downloads
diakses 2 januari 2013 10.00 WIB
en.wikipedia.org/wiki/**PfSense**
diakses 9 januari 2013 15.00 WIB

[3] http://forum.pfsense.org/index.php
diakses 9 januari 2013 15.00 WIB