Tinjauan Sistematis: Analisa Perbandingan Jenis Firewall pada Implementasi Dalam Keamanan Jaringan

*Systematic Review: Comparison Analysis of Firewall Types on Implementation in Network Security*

Moch Fajar Purnomo Alam (1611601434), Winny Purbaratri (1611601194)

*Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia*

**Abstrak**

**Tujuan –**Paper ini akan membahas metode yang digunakan paling baik untuk Implentasi Firewall dalam Keamanan Jaringan

**Desain/Metodologi/Pendekatan -** Paper ini memberikan tinjauan literatur dari jurnal

**Temuan** – Mengetahui bagaimana Implementasi Firewall dalam Keamanan Jaringan

**Originalitas/Nilai -** Penelitian ini hanya membahas tentang implementasi Firewall pada Keamanan jaringan.

**Keyword** *Firewall, topologi, cara kerja firewall, Metoda firewall*

**Tipe Paper** *Systematic Literature review*.

1. **Pendahuluan**

Masalah keamanan jaringan semakin menjadi perhatian dikarenakan semakin banyaknya alat yang bermunculan dan tehnik yang digunakan oleh seseorang secara ilegal untuk masuk kedalam sistem atau membuat lumpuh sistem yang ada secara ilegal. Selain itu adanya celah dan tidak ada sistem keamanan yang melindungi sistem menjadikan sistem rentan terhadap serangan. [2]

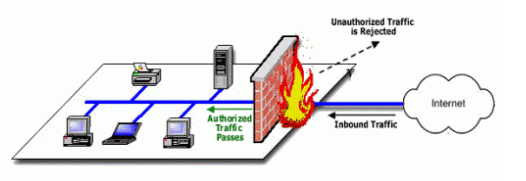
1. **Pengertian Firewall**

Firewall dalam program keamanan informasi serupa dengan firewall bangunan karena mencegah jenis informasi tertentu bergerak antara dunia luar, yang dikenal adalah jaringan yang *untrusted* (misalnya internet), dan dunia dalam, yang dikenal sebagai jaringan *trusted*. Firewall mungkin merupakan jaringan terpisah yang berisi sejumlah perangkat pendukung. Firewall dapat dikategorikan dengan mode pengolahan, era pengembangan atau struktur.[1]

Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik hardware maupun software. Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke komputer anda, dengan firewall semua itu dapat diatasi dengan mudah.

Firewall yang sederhana biasanya tidak memiliki kemampuan melakukan filtering terhadap paket berdasarkan isi dari paket tersebut. Sebagai contoh, firewall tidak memiliki kemampuan melakukan filtering terhadap e-mail bervirus yang Anda download atau terhadap halaman web yang tidak pantas untuk dibuka. Yang bisa dilakukan firewall adalah melakukan blokir terhadap alamat IP dari mail server yang mengirimkan virus atau alamat halaman web yang dilarang untuk dibuka. Dengan kata lain, firewall merupakan sistem pertahanan yang paling depan untuk jaringan Anda. [3]

1. **Cara Kerja Firewall**
2. Firewall pada dasarnya merupakan penghalang antara komputer Anda (atau jaringan) dan Internet (luar dunia). Firewall bisa hanya dibandingkan dengan seorang penjaga keamanan yang berdiri di pintu masuk rumah Anda dan menyaring pengunjung yang datang ke tempat AndaDia mungkin mengizinkan beberapa pengunjung untuk masuk sementara menyangkal orang lain yang ia tersangka penyusup yang. Demikian pula firewall adalah sebuah program perangkat lunak atau perangkat keras yang menyaring informasi (paket) yang datang melalui internet ke komputer pribadi Anda atau jaringan komputer.
3. Firewall dapat memutuskan untuk mengizinkan atau memblokir lalu lintas jaringan antara perangkat berdasarkan aturan yang pra-dikonfigurasi atau ditentukan oleh administrator firewall. Kebanyakan personal firewall seperti firewall Windows beroperasi pada seperangkat aturan pra-konfigurasi yang paling cocok dalam keadaan normal sehingga pengguna tidak perlu khawatir banyak tentang konfigurasi firewall.
4. Firewall pribadi adalah mudah untuk menginstal dan menggunakan dan karenanya disukai oleh pengguna-akhir untuk digunakan pada komputer pribadi mereka. Namun jaringan besar dan perusahaan-perusahaan lebih memilih orang-orang firewall yang memiliki banyak pilihan untuk mengkonfigurasi sehingga untuk memenuhi kebutuhan khusus mereka. Sebagai contoh, perusahaan mungkin membuat aturan firewall yang berbeda untuk server FTP, Telnet server dan server Web. Selain itu perusahaan bahkan dapat mengontrol bagaimana karyawan dapat terhubung ke Internet dengan memblokir akses ke situs web tertentu atau membatasi transfer file ke jaringan lain. Jadi selain keamanan, firewall dapat memberikan perusahaan kontrol luar biasa atas bagaimana orang menggunakan jaringan.
5. **Illustrasi Cara Kerja Firewall**



Gambar 1. Cara Kerja Firewall

Firewall menggunakan satu atau lebih metode berikut untuk mengatur lalu lintas masuk dan keluar dalam sebuah jaringan:

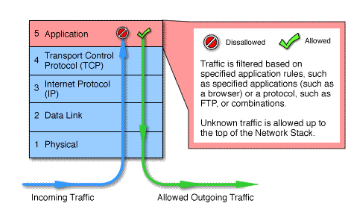
* **Packet Filtering:** Pada metode ini paket (potongan kecil data) dianalisa dan dibandingkan dengan filter**.** Filter paket memiliki seperangkat aturan yang datang dengan tindakan menerima dan menolak yang pra-dikonfigurasi atau dapat dikonfigurasi secara manual oleh administrator firewall.. Jika paket berhasil membuatnya melalui filter ini maka itu diperbolehkan untuk mencapai tujuan, kalau tidak akan dibuang.
* **Stateful Inspeksi:** Ini adalah metode baru yang tidak menganalisa isi dari paket. Sebaliknya ia membandingkan aspek kunci tertentu setiap paket database sumber terpercaya.. Kedua paket yang masuk dan keluar dibandingkan terhadap database ini dan jika perbandingan menghasilkan pertandingan yang wajar, maka paket yang diizinkan untuk melakukan perjalanan lebih lanjut. Jika tidak, mereka akan dibuang.[5]

1. **Jenis Firewall**
2. **Packet Filtering Router :**
3. Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.
4. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak.
5. Penyaringan packet ini di konfigurasikan untuk menyaring paket yang akan di transfer secara dua arah (baik dari dan ke jaringan lokal).
6. Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protocol transport yang di gunakan (UDP, TCP), serta nomor port yang digunakan.
7. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, relatif lebih cepat.

Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi, serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

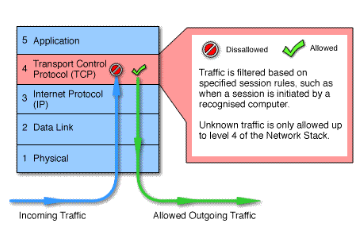
* IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
* Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
* Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protocol TCP dan memiliki offset = 1 pada IP fragment (bagian IP)

1. **Application / Proxy Firewall**: Firewall jenis ini yang sering kita  sebut proxy, dimana proxy  mampu membaca isi paket data yang berisi content yang akan dikirim /diterima user,firewall bisa mengidentifikasi paket yang berisi pecahan file dengan extensi tertentu dan content dengan kandungan text tertentu.makanya firewall jenis ini digunakan untuk memfilter content yang akan diterima user . seperti memblock download  file executable untuk menghindari penyebaran malware,memblock situs tertentu misalnya memblock situs yang mengandung kalimat porno dan social media.



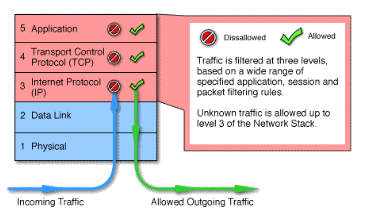
***Gambar 2. Application/Proxy Firewall***

1. **Circuit-Level Gateway Firewall** akan membaca session yang akan terjadi, dan memastikan bahwa session yanng akan terbentuk berasal dari sumber dan tujuan yang benar dan sah. hal ini untuk menghindari spoofing (pembodohan mesin) oleh hacker dan melakukan tindakan MITM (Man in the midle attack) dengan mencuri session atau membat session palsu.



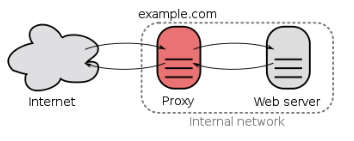
***Gambar 3.* Circuit-Level Gateway Firewall**

1. **Stateful Multilayer Gateways (Layer 4 +5 OSI  &TCP/IP)** : Ini adalah jenis firewall paling mantap karena jenis firewall ini dapat membaca ip header dan isi dari paket data , dapat menentukan sesi yang akan terjadi sah atau tidak dan secara bersamaan dapat menentukan paket yang berisi content sesuai dengan rule atau tidak,Stateful multilayer (SML) tidak menggunakan proxy sehingga kecepatan pemfilteran akan sangat luar biasa cepatnya dan lebih unggul dibanding dengan proxy.



***Gambar 4. Stateful Multilayer Gateways (Layer 4 +5 OSI  &TCP/IP)***

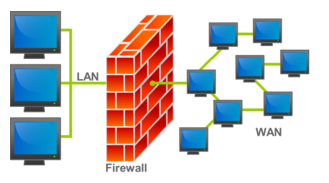
1. **Reverse-Proxy Firewalls** : Pada umumnya firewall digunakan untuk melindungi client, Reverse-Proxy Firewalls dibuat dan diirancang untuk melindungi Server , yap server diletakan di dalam jaringan internet yang liar dan berbahaya ,Reverse-Proxy reverse-proxyFirewalls akan menjadi tameng dalam menghadapi serangan dari hacker dari internet. Contoh Reverse-Proxy Firewalls adalah Cloudflare CDN (Content Delivery Network ) yang bertugas digaris depan untuk melayani permintaan pengunjung dan menangkal serangan hacker. Reverse-Proxy Firewalls akan menyembunyikan IP asli dari server sehingga hacker akan berusaha lebih keras untuk menemukan IP asli dari server yang ingin diserang. Reverse-Proxy Firewalls juga berfungsi sebagai cache untuk meringankan beban dari server. [12]



***Gambar 5. Reverse-Proxy Firewalls***

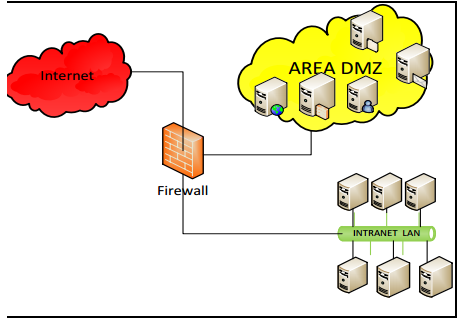
1. **Hybrid firewall** adalah salah satu jenis firewall yang menggunakan beberapa jenis elemen-elemen dari satu atau lebih tipe firewall. Sebenarnya hybrid firewall merupakan bukan sesuatu hal yang baru. Firewall yang komersial pertama adalah DEC SEAL, DEC SEAL adalah firewall berjenis hybrid dengan menggunakan proxy dari bastion hosts dan packet filtering pada gateway (gate). Sistem hybrid seringkali digunakan untuk menambahkan layanan baru secara cepat pada sistem firewall yang sudah tersedia. Kita bisa saja menambahkan sebuah *circuit gateway*atau *packet filtering*pada firewall yang berjenis *application gateway,*karna untuk itu diperlukan kode proxy yang ditulis untuk setiap service baru yang akan disediakan.

Kita juga dapat memberikan autentifikasi pengguna yang lebih ketat pada *Steatful packet filter* dengan menambahkan proxy pada tiap service. Apapun basis teknologi yang digunakan sebuah firewall pada umumnya berlaku sebagai gateway yang terkontrol diantara dua atau lebih network dimana setiap trafik harus melewatinya. Sebuah firewall menjalankan security dan meninggalakan jejak yang dapat ditelusuri. [13]



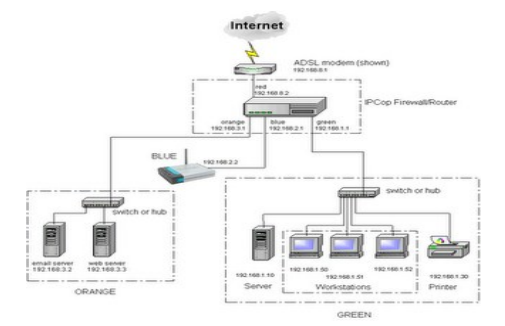
***Gambar 6. Hybrid firewall***

1. **Topologi Firewall**
2. Firewall DMZ atau jaringan perimeter adalah jaringan security boundary yang terletak diantara suatu jaringan privat LAN dan jaringan publik (internet). DMZ didefinisikan sebagai sebuah host komputer atau jaringan kecil yang dimasukkan kedalam sebuah zona netral diantara sebuah jaringan perusahaan privat dan jaringan publik. DMZ menghalangi user dari luar mengakses secara langsung sebuah server yang berisi data-data perusahaan. [6]



***Gambar 7. Firewall DMZ***

1. IPCop adalah suatu distribusi open source Linux yang menyediakan fitur simple-to-manage firewall appliance berbasis perangkat keras PC. IPCop juga merupakan suatu stateful firewall dibuat berdasarkan pada Linux netfilter framework.[7]



***Gambar 8. Firewall IPCop***

**2.Objectivitas**

Artikel yang berkaitan dengan pertanyaan penelitian:

1. Jenis Firewall apa yang sering digunakan dalam Implementasi Keamanan Jaringan?
2. **Metodologi**
3. Kriteria Kelayakan:

Kriteria berikut menggunakan: Artikel yang ditulis di Jurnal Nasional dan Jurnal Internasional.

1. Sumber Informasi

Penelitian ini diterapkan pada GOOGLE Search, GOOGLE Scholars, Emerald Insight dan IEEE Xplore. Artikelnya juga telah dibaca untuk memastikan apakah jurnal yang tampil pada mesin pencari telah sesuai dengan tema yang ingin ditampilkan.

1. Study Selection

Pilihan penelitian diorganisir dengan menggunakan empat fase:

1. Publikasi penelitian yang berkaitan dengan Implementasi Firewall untuk Keamanan Jaringan. Fase dicari menggunakan string (“Implementasi Firewall untuk Keamanan Jaringan”)
2. Eksplorasi Judul, abstrak, identifikasi kata kunci dan seleksi berdasarkan kriteria kelayakan
3. Artikel lengkap dan parsial yang belum pernah ada Dieliminasi dibaca untuk mengidentifikasi apakah itu terkait dengan kriteria kelayakan
4. Memilih Jurnal untuk mengidentifikasi apakah jurnal yang didapat sudah memenuhi kelayakan kriteria.
5. Proses Pengumpulan Data

Sebuah evaluasi mengungkapkan mesin pencari Google Search, Google Scholars, Emerald Insight dan IEEE Explore adalah sumber terbaik untuk tujuan topik pada jurnal sistematik literatur ini; Setelah pencarian awal itu diikuti 4 langkah:

1. Seleksi Query dan mesin pencari, pencarian awal Implementasi Firewall dalam Keamanan Jaringan yang sesuai pada ***Google Search*** sebanyak 13 (tiga belas) buah Jurnal yang memiliki standar Jurnal Nasional. ***Emerlad Insight*** sebanyak 2 (dua) buah Jurnal yang terbit pada tahun 1998 dan tahun 2013. ***Google Scholars*** sebanyak 7 (tujuh) buah Jurnal yang terbit dari tahun 2014 sampai tahun 2017. ***IEEE Explore*** sebanyak 15 (lima belas) buah jurnal yang terbit dari tahun 2012 sampai tahun 2017.
2. Pencarian Jurnal disempurnakan dengan manual karena tidak semua artikel terkait dengan Implementasi Firewall pada keamanan Jaringan.
3. Ekstensi dan verifikasi, dimana setiap artikel itu di periksa judul, abstrak dan isi jurnal yang ada disesuaikan dengan kriteria kelayakan.
4. Klasifikasi publikasi yang relevan, klasifikasi publikasi itu berbasis bidang keamanan jaringan, metode yang digunakan pada Firewall.
5. **Hasil**

Pencarian pada topik Implemetasi Firewall dalam keamanan Jaringan yang sesuai dengan kriteria kelayakan akan ditampilkan pada Tabel 1. Publikasi Jurnal Implementasi Firewall Dalam Keamanan Jaringan. Jurnal yang direview sebanyak 37 (tiga puluh tujuh) buah Jurnal dari Jurnal skala Nasional dan Jurnal yang terindeks Internasional.

Tabel 1. Publikasi Jurnal Implementasi Firewall Dalam Keamanan Jaringan.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No | Penulis | Tahun | Penerbit | Judul | Abstraksi | Masalah | Kelemahan | Kelebihan | Metodologi | Hasil |
| 1 | Hannes Holm and Mathias Ekstedt | Vol. 21 No. 4, 2013 pp. 250-265 | @Emerald Group Publishing Limited | *Estimates on the effectiveness of web application firewalls against targeted attacks* | *untuk mengestimasi efektifitas Web Application Firewall (WAFs) untuk mencegah serangan injeksi* | *apakah ada operator berpengalaman yang memantau WAF; apakah Alat kotak hitam otomatis telah digunakan saat menyetel WAF; apakah tuning individu WAF adalah profesional yang berpengalaman; dan apakah upaya signifikan telah dilakukan untuk menyetel WAF* |  |  | *Perkiraan efektivitas WAF dengan menggunakan metode klasik Cookies.* | *Hasilnya menunjukkan bahwa tingkat pencegahan rata-rata WAF adalah 80 persen jika semua tindakan telah dipekerjakan. Jika tidak ada tindakan yang dilakukan maka tingkat pencegahan rata-rata adalah 25 persen.* |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |  |  |  |
| 27 |  |  |  |  |  |  |  |  |  |  |
| 28 |  |  |  |  |  |  |  |  |  |  |
| 29 |  |  |  |  |  |  |  |  |  |  |
| 30 |  |  |  |  |  |  |  |  |  |  |
| 31 |  |  |  |  |  |  |  |  |  |  |
| 32 |  |  |  |  |  |  |  |  |  |  |
| 33 |  |  |  |  |  |  |  |  |  |  |
| 34 |  |  |  |  |  |  |  |  |  |  |
| 35 |  |  |  |  |  |  |  |  |  |  |
| 36 |  |  |  |  |  |  |  |  |  |  |
| 37 |  |  |  |  |  |  |  |  |  |  |

Tabel 1. Cara Kerja Firewall

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Jenis Firewall | | | | | |
| No | Indikator | Packet Filtering Router | Application /Proxy Firewall | JCircuit-Level Gateway Firewall | Stateful Multilayer Gateways (Layer 4 +5 OSI  &TCP/IP) | Reverse-Proxy Firewalls | Hybrid firewall |
| 1 | Membaca Packet IP | √ | √ | √ | √ | √ | √ |
| 2 | UDP & TCP | √ | √ | √ | √ | √ | √ |
| 3 | Mampu membaca isi paket data |  | √ | √ | √ | √ | √ |
| 4 | Dapat membaca Session |  |  | √ | √ | √ | √ |
| 5 | Membaca Paket data sesuai dengan Rule yang ditentukan |  |  |  | √ | √ | √ |
| 6 | Dapat menyembunyikan IP asli dari server |  |  |  |  | √ | √ |
| 7 | Dapat berkerja dengan lebih dari satu jenis firewall |  |  |  |  |  | √ |

Tabel 2. Publikasi Jurnal Implementasi Firewall Dalam Keamanan Jaringan.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Jenis Firewall | | | | | |
| No | Indikator | Packet Filtering Router | Application /Proxy Firewall | JCircuit-Level Gateway Firewall | Stateful Multilayer Gateways (Layer 4 +5 OSI  &TCP/IP) | Reverse-Proxy Firewalls | Hybrid firewall |
| 1 | Kemudahan pemakaian | √ | √ |  |  |  |  |
| 2 | effective |  |  |  |  |  |  |
| 3 | Effisien |  |  |  |  |  |  |
| 4 | Log Activity |  |  |  |  |  |  |
| 5 | Cost |  |  |  |  |  |  |
| 6 | Ketahanan terhadap serangan |  |  |  |  |  |  |
| 7 | Hak Akses (policy) |  |  |  |  |  |  |
| 8 | Windows OS |  |  |  |  |  |  |
| 9 | Linux OS |  |  |  |  |  |  |
| 10 | Implementasi pada topology |  |  |  |  |  |  |

1. **Kesimpulan**

**Daftar Pustaka**

1. Whitman, E.W & Mattord, HJ (2011).Principles Of Information Security, USA:Cengage Learning Customer.
2. Sondakh, G et al.(2014). Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat, E-Journal Teknik Elektro dan Komputer.
3. Basten, M.V,(2017)OPTIMALISASI FIREWALL PADA JARINGAN SKALA LUAS. Diambil 27 September 2017, dari <http://www.unsri.ac.id/upload/arsip/Optimalisasi%20Firewall%20Pada%20Jaringan%20Skala%20Luas.pdf>
4. Asir, N(2013,Mei) Pengertian dan Cara Kerja Firewall. Diambil 27 September 2017, dari <https://holishasir72.wordpress.com/2013/05/30/pengertian-dan-cara-kerja-firewall/>
5. Ikhwan,S & Elfitri,I(2014,September).ANALISA DELAY YANG TERJADI PADA PENERAPAN DEMILITARIZED ZONE (DMZ) TERHADAP SERVER UNIVERSITAS ANDALAS, Vol: 3 No. 2 September 2014 ISSN: 2302 – 2949-118
6. Arifin,V & Fitriana,I(2012,Desember),Analisis Efektifitas Bandwidth Menggunakan Ipcop (Studi Kasus : Balai Besar Teknologi Energi),SETRUM – Volume 1, No. 2, Desember 2012 ISSN : 2301-465239
7. Ordinary, A (2016). Pengertian firewall ,jenis dan fungsinya, Diambil 5 oktober 2017, dari <https://www.tembolok.id/pengertian-firewall-jenis-dan-fungsi-nya/>
8. Rakhman,A (2013). Hybrid Firewalls. Diambil 5 Oktober 2017, dari <http://nuarafandi.blogspot.co.id/2013/07/hybrid-firewalls.html>
9. Khasanah, ST (2016, Desember), KEAMANAN JARINGAN DENGAN PACKET FILTERING FIREWALL(STUDI KASUS: PT. SUKSES BERKAT MANDIRI JAKARTA). Vol. IV, No.2