SNFT
UMSIDA 2015
SEMINAR NASIONAL
FAKULTAS TEKNIK

Universitas
Muhammadiyah
Sidoarjo

PROCEEDING

Seminar Nasional Fakultas Teknik
Universitas Muhammadiyah Sidoarjo

ISSN : 2460 - 8262

Mengembangkan Energi Terbarukan dan Mewujudkan Smart City

Diterbitkan Oleh :
Fakultas Teknik - Universitas Muhammadiyah Sidoarjo

SNFT

UMSIDA 2015

SEMINAR NASIONAL FAKULTAS TEKNIK

ISSN : 2460 - 8262

Diterbitkan Oleh :
Fakultas Teknik - Universitas Muhammadiyah Sidoarjo
Kampus II : Jl. Raya Gelam 250, Candi Sidoarjo

PROCEEDING

SEMINAR NASIONAL DAN CALL FOR PAPERS 2015

TEMA : MEGEMBANGKAN ENERGI TERBARUKAN DAN MEWUJUDKAN SMART CITY

12 SEPTEMBER 2015
AULA KAMPUS 1
UNIVERSITAS MUHAMMADIYAH SIDOARJO

PROCEEDING

SEMINAR NASIONAL DAN CALL FOR PAPERS 2015

ISSN 2460-8262

Fakultas Teknik
Universitas Muhammadiyah Sidoarjo

SEMINAR NASIONAL DAN CALL FOR PAPER 2015

FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH SIDOARJO

PENANGGUNG JAWAB

Izza Anshory, ST, MT

KETUA PELAKSANA

Eko Agus Suprayitno, S.Si, MT

PROCEEDING EDITOR

Edi Widodo, MT
Karyanik, ST, MT
Dr.Eng Rachmad Firdaus ST, MT
Sy.Syahrorini, ST,MT
Hana Catur Wahyuni, MT
Hindarto, S.Kom., MT

TIM REVIEWERS

Dr. Ir. Udi Subakti Ciptomulyono,M.Eng.Sc
Dr. M. Faisal S.Kom, MT
Dr. Ir. Lailis Syafa'ah, MT
Dr. Wibowo M.Sc

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH SIDOARJO

UCAPAN TERIMA KASIH

Rektor UMSIDA

Ricky Elson

KATA PENGANTAR KETUA PANITIA

Assalamu'alaikum Wr. Wb

Puji sykur kehadirat Allah SWT, atas berkat Rahmat dan Hidayah – Nya Seminar Nasional Fakultas Teknik – Universitas Muhammadiyah Sidoarjo (UMSIDA) dapat dilaksanakan sesuai dengan jadwal yang telah direncanakan, 12 September 2015.

Universitas Muhammadiyah Sidoarjo khususnya Fakultas Teknik, dalam prosesnya selalu berusaha untuk meningkatkan kualitas pengelolaan institusi dan atmosfer akademik. Peningkatan atmosfer akademik dapat terbentuk dengan adanya interaksi yang berkelanjutan antar civitas akademika yang ada dalam internal institusi pendidikan tinggi tersebut, maupun antar institusi pendidikan tinggi lainnya. Fakultas Teknik Universitas Muhammadiyah Sidoarjo memiliki empat program studi, yaitu Program Studi Teknik Informatika, Program Studi Teknik Industri, Program Studi Teknik Mesin, dan Program Studi Teknik Elektro.

Salah satu cara untuk meningkatkan interaksi yang berkelanjutan tersebut, adalah dengan diselenggarakannya kegiatan publikasi hasil penelitian. Publikasi penelitian dapat membentuk interkasi positif antara mahasiswa, dosen, praktisi dan masyarakat. Dengan melakukan publikasi hasil penelitian atas karya ilmiahnya, mahasiswa, dosen dan praktisi maupun peneliti selaku sumber daya manusia utama suatu pendidikan tinggi dapat mengetahui perkembangan keilmuan yang ditekuninya.

Seminar Nasional dan *Call For Paper* merupakan agenda rutin bagi Fakultas Teknik Universitas Muhammadiyah Sidoarjo, pada tahun ini, kami mengusung tema "Megembangkan Energi Terbarukan dan Mewujudkan Smart City". Diharapkan pula kegiatan ini dapat dijadikan sebagai sarana komunikasi antar peneliti, akademisi maupun praktisi, sekaligus sebagai sarana publikasi pendidikan tinggi penyelenggara (UMSIDA).

Sebagai penutup kami, atas nama panitia, mengucapkan terima kasih kepada seluruh partisipan kegiatan Seminar Nasional dan *Call for Paper* Fakultas Teknik 2015, semoga kegiatan ini dapat bermanfaat bagi diri kita, instusi pendidikan tinggi, masyarakat dan bangsa, serta perkembangan ilmu pengetahuan dan teknologi.

Wassalamu'alaikum Wr.Wb

Sidoarjo, 2 September 2015
Ketua Panitia,

Eko Agus Suprayitno, S.Si, MT.

KATA PENGANTAR DEKAN FAKULTAS TEKNIK

Assalamu' alaikum Wr. Wb

Alhamdulillah, puji syukur kepada Allah SWT, yang selalu melimpahkan rahmat dan hidayahNya pada kita semua. Selamat datang dan terima kasih atas peran serta peserta Seminar Nasional Fakultas Teknik Universitas Muhammadiyah Sidoarjo.

Dalam rangka memfasilitasi semua kalangan, dosen, mahasiswa, peneliti, pelaku bisnis dan masyarakat umum dalam mempublikasikan hasil penelitiannya, dan sebagai jembatan untuk melakukan *sharing* dalam rangka pengelolaan energi dan tata kota, maka Fakultas Teknik menyelenggarakan Seminar dengan tema Megembangkan Energi Terbarukan dan Mewujudkan Smart City.

Seminar ini diharapkan dapat memberikan wawasan mengenai pentingnya kreativitas teknologi dalam memajukan bangsa. Selain itu, berbagai konsep, dan hasil penelitian bidang rekayasa teknologi dibahas dalam seminar ini. Konsep dan hasil penelitian ini akan disajikan dalam presentasi dan diskusi ilmiah yang melibatkan peneliti dengan berbagai macam bentuk penelitian rekayasa teknologi.

Akhirnya, kami mewakili civitas akademik Fakultas Teknik Universitas Muhammadiyah Sidoarjo menyampaikan terimakasih kepada semua pihak, panitia seminar, peserta seminar, dan semua pihak yang telah membantu pelaksanaan seminar ini. Selamat melaksanakan seminar dan diskusi ilmiah, semoga acara ini mendapat ridlo dari Allah SWT dan bermanfaat bagi kita semua. Amin.

Wassalamu 'alaikum Wr .Wb

Sidoarjo, 2 September 2015

Dekan Fakultas Teknik

Izza Anshory, ST, MT

SUSUNAN PANITIA SEMINAR NASIONAL FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH SIDOARJO

Penanggung Jawab	: Izza Anshory, ST, MT
Ketua Pelaksana	: Eko Agus Suprayitno, S.Si, MT
Sekretaris	: Ribangun Bamban J, ST, MM
Bendahara	: Indah Sulistyowati, ST, MT
Tim Reviewer Ahli	: Dr. Ir. Udi Subakti Ciptomulyono,M.Eng.Sc Dr. M. Faisal S.Kom, MT Dr. Ir. Lailis Syafa'ah, MT Dr. Wibowo M.Sc
Sie. Pengelolaan Artikel	: Edi Widodo, MT Karyanik, ST, MT Dr.Eng Rachmad Firdaus ST, MT Sy.Syahrorini, ST,MT Hana Catur Wahyuni, MT Hindarto, S.Kom., MT
Sie. Acara	: Athika Sidhi Cahyana, MT. Wiwik Sulistyowati, MT Ali Akbar, ST, MT
Sie. Humas	: Roni Pambudi, S.Kom. Mulyadi, ST, MT Farisa Rimahirdani Tedjo Sukmono, ST, MT
Sie.Kesekretariatan	: Yulian Findawati, ST, M.MT Nidhom Masduqi, ST.
Sie Perlengkapan	: Boy Isma Putra, MM. Suharjo Ngatiran
Sie. Dokumentasi & Publikasi	: Arif Senja Fitroni, S.Kom. Arif Rahman, M.Psi Andry Rachmadany, S.Kom Mochamad Alfan Rosid, S.Kom, M.Kom

Sie. Konsumsi	: Ade Evianti, S.Kom. Asmaul Husnah,SE Yuanita,S.Kom
Sie. Transportasi	: Umar Khasan, BA (Koordinator) Supeno Taufiq
Sie. Dana Usaha	: Ir. Sumarno, MM Wiwik Sumarmi,Ir, MT Suprianto, S.Si, M.Si Jamaludin, Ir. MM

DAFTAR ACARA SEMINAR NASIONAL FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH SIDOARJO

Sabtu, 12 September 2015

Jam	**Acara**	**Keterangan**	
07.00 – 08.30	Her- Registrasi	Aula Kampus 1 UMSIDA	
08.30 – 08.45	Laporan Ketua Panitia	Aula Kampus 1 UMSIDA	
08.45 – 09.00	Sambutan dan Pembukaan oleh Rektor	Drs. Hidayatullah, M.Si	
09.00 – 11.30	Keynote Speech	Ricky Elson	Moderator : Ali Akbar, ST, MT
11.30 – 12.30	Makan Siang dan Sholat		
13.00 – 16.00	Sidang Komisi : Presentasi Lisan		
16.00 – 16.30	Pengambilan Sertifikat		

DAFTAR ISI

KATA PENGANTAR KETUA PANITIA i
KATA PENGANTAR DEKAN FAKULTAS TEKNIK ii
SUSUNAN PANITIA SEMINAR NASIONAL FAKULTAS TEKNIK iii
DAFTAR ACARA SEMINAR NASIONAL FAKULTAS TEKNIK v
DAFTAR ISI..... vi

1. SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN PROGRAM STUDI MENGGUNAKAN FUZZY INFERENCE SYSTEM DENGAN METODE MAMDANI BERBASIS WEB

   Muhammad Farizqo, Ade Eviyanti..... 1-10

2. SISTEM OTOMASI PENYIRAMAN PADA TANAMAN JAHE BERBASIS ARDUINO

   Mustafi Jurokhman, Syamsudduha Syahrorini..... 11-20

3. IMPLEMANTASI SENSOR PIR UNTUK PENGHEMATAN ENERGI LISTRIK PADA RUANG KELAS DI UMSIDA

   Mochammad Ilyas, Dwi Hadidjaja, Indah Sulistiyowati..... 21-27

4. DETEKSI WAJAH DENGAN PEMINDAI KINECT XBOX 360 MENGGUNAKAN MICROSOFT KINECT SDK DAN WPF C#

   Indra Prasetyanto, Cahyo Darujati, Agustinus Bimo Gumelar..... 28-32

5. RANCANG BANGUN DESAIN MOTIF BATIK MENGGUNAKAN METODE ALGORITMA GENETIKA

   Sugito Muzaqi, Cahyo Darujati, Bimo Gumelar..... 33-40

6. PENGARUH KELELAHAN KERJA DAN METODE PEMBELAJARAN TERHADAP MOTIVASI KULIAH DENGAN METODE STRUCTURAL EQUATION MODELING

   Fajar Aminulloh, Atikha Sidhi Cahyana..... 41-44

7. IMPELEMTASI MANAJEMEN KEAMANAN SISTEM INFORMASI DENGAN MODEL VIRTUAL PRIVATE NETWORK & PORT KNOCKING (Studi Kasus : STIE Perbanas Surabaya)

Hariadi Yutanto, Moch.Nurhadi 45-51

8. ANALISA PERBANDINGAN PENGELASAN MENGGUNAKAN ELEKTRODA BESI COR (CIA-1) DENGAN ELEKTRODA MILD STEEL (LB-52) YANG DICELUP OLI TERHADAP KEKUATAN TARIK MATERIAL BESI COR KELABU FC-30

Mulyadi, Syarief Hidayatullah 52-61

9. ANALISA PENJADWALAN JOB SHOP PADA MESIN PELUBANGAN TEMPAT ACESSORIES PINTU ALMARI UNTUK MEMINIMASI MAKESPAN DENGAN METODE EARLIEST DUE DATE DI PT.XHT.

Abdul Rofik, Tedjo Sukmono 62-66

10. SYSTEM AUTOMATIC PADA MESIN CRUSHER BERBASIS PLC OMRON CPM 2A

Bambang Sunardi, Izza anshory 67-74

11. PENDETEKSIAN SINYAL SUARA JANTUNG MENGGUNAKAN INSTRUMENTASI PHONOCARDIOGRAPHY

Agus Hayatal Falah, Eko Agus Suprayitno 75-81

IMPELEMTASI MANAJEMEN KEAMANAN SISTEM INFORMASI DENGAN MODEL VIRTUAL PRIVATE NETWORK & PORT KNOCKING (Studi Kasus : STIE Perbanas Surabaya)

Hariadi Yutanto[1], Moch.Nurhadi[2]
[1,2]STIE Perbanas Surabaya
[1]antok@perbanas.ac.id

ABSTRAK

Virtual Private Network (VPN) merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke public network(WAN) seolah-olah menjadi private network dan bahkan bergabung dengan *private network* itu sendiri. Dengan mengunakan teknologi ini, maka seseorang dapat mengakses sumber daya jaringan yang berada di dalam *private network*, dan mendapatkan hak akses dan pengaturan yang sama bagaikan secara fisik berada di tempat dimana private network itu berada. Penelitian ini mencoba untuk menganalisis dan merancang suatu sistem keamanan jaringan yang dapat dimanfaatkan untuk menghubungan antara jaringan komputer baik di kantor maupun diluar kantor. Metode analisis dilakukan dengan observasi terhadap jaringan yang terdapat di STIE Perbanas Surabaya serta mengidentifikasi permasalahan yang dapat dibantu dengan menggunakan teknologi jaringan. Sedangkan, metode perancangan dilakukan dengan membuat topologi jaringan serta menentukan elemen yang dibutuhkan untuk merancang teknologi VPN dengan model keamanan *portknocking*, dimana pengguna yang diijinkan dapat melakukan manipulasi *rule firewall* dengan mengirimkan ketukan(*knocking*) atau informasi kepada *firewall* sebelum melakukan akses ke jaringan lokal dengan menggunakan *user authenticate* VPN. Kemudian memberikan usulan konfigurasi sistem dan melakukan test untuk mengetahui apakah sistem yang diusulkan dapat berjalan dengan baik atau tidak. Hasilnya adalah VPN dapat digunakan untuk menghubungkan jaringan dari komputer rumah atau yang terhubung dari *public network* dengan sumber daya jaringan di komputer/server STIE Perbanas Surabaya dengan mudah dan memiliki tingkat keamanan yang tinggi.

KEYWORD: *manajemen keamanan sistem informasi, keamanan jaringan, virtual private network (VPN), firewall, knocking, user authenticate.*

1.Pendahuluan

Teknologi informasi dan komunkasi sangat bermanfaat, berdayaguna tinggi dan mendukung semua proses bisnis khususnya perguruan tinggi. Seiring dengan berkembangnya teknologi jaringan komputer secara luas seperti koneksi internet, dapat menimbulkan masalah baru, yaitu keamanan jalur koneksi. Permasalahan keamanan merupakan hal yang paling pentingagar pengguna tetap merasa aman dalam bekerja setiap kali melakukan koneksi dengan jaringan luas[10].
Koneksi internet ataupun koneksi ke jaringan luas seringkali memunculkan masalah baru terkait dengan manajemen keamanan sistem informasi, yaitu terbukanya jalur koneksi. Hal ini yang sering dimanfaatkan oleh para *hacker* untuk mencuri data melalui jaringan. Peran seorang *network administrator* sangat diperlukan dalam mendesain sebuah jaringan yang aman dan sekaligus memberikan kemudahan bagi pengguna yang akan melakukan akses jaringan.Jalur komunikasi dan pertukaran informasi dapat berjalan lancar pada saat port telah dibuka. Namun terkadang dengan terbuka port tersebut akan membuka celah bagi orang yang tidak bertanggung jawab untuk melakukan serangan sebagai celah port yang terbuka. Didalam konfigurasi *firewall* pada umumnya akan menutup semua jalur komunikasi port yang rentan terhadap serangan dan juga port yang tidak penting dapat ditutup. Cara tersebut merupakan sistem pengamanan yang efektif yang dilakukan oleh seorang *network administrator*.

Hal ini yang melatarbelakangi mengapa perlunya manajemen keamanan sistem informasi dan juga kemudahan akses bagi admininistrator jaringan dan para pengguna yang terpercaya untuk dapat terkoneksi dengan jaringan internal melalui jaringan internet.Ada 2 tahapan yang dilakukan oleh pengguna untuk manajemen keamanan sistem informasi, yaitu denganmelakukan cara *knocking port* untuk membuka akses *port* pada *firewall*[1] dan dilanjutkan dengan *tunnel* menggunakan *virtual private network* (VPN) ke jaringan local [4]. Al-Bahadili (2010) dalam penelitiannya berusaha mengembangkan dan mengevaluasi kinerja teknik *port knocking*,yang dapat mencegah semua jenis serangan hacker dan sebagai persyaratan keamanan jaringan. dengan menggunakan tiga teknik, yaitu: *port-knocking (PK), steganography*, dan otentifikasi dua arah *(mutual authentication)*, yang disebut dengan*hybrid port-knocking* (HPK). HPK digunakan untuk otentikasi host dengan membuat layanan lokal yang terlihat dari *port scanning*. Kinerja teknik yang diusulkan dievaluasi dengan mengukur rata-rata waktu otentikasi, dibandingkan dengan rata-rata waktu untuk otentikasi yang digunakan teknik otentikasi port.

Prihanto (2013) dalam penelitiannya mengembangkan sistem keamanan *port knocking* di mikrotik menggunakan komponen bahasa pemrograman Delphi untuk melakukan *port knocking*.Hasil dari penelitian menunjukkan bahwa *tools knocking*yang dikembangkan dapat men-*generate script firewall filter rule* dalam bentuk *.rsc yang outputnya dapat diekspor kedalam mikrotik. Hasil pengujian lain yaitu dengan *toolsnmap* sebagai monitoring

menunjukkan setelah *knocking* berhasil dilakukan maka port 22, 23 dan 80 yang awalnya close menjadi open, sedangkan pengujian dengan ping testsetelah *knocking* berhasil dilakukan, maka status ping menjadi *Reply* yang sebelumnya *Request Time Out.*Munanza (2006) dalam penelitiannya *virtual private network* (VPN) server yang telah dirancang menggunakan koneksi remote pada perangkat andorid berfungsi dengan baik. Pengujian sistem VPN server untuk koneksi remote pada perangkat android ini menjamin terjaganya koneksi antara *client-sever* dari masalah *sniffing*, sehingga apabila terjadi *sniffing* maka IP yang terjadi indikasi tersebut akan terlihat jelas dan indikasi tersebut dapat dengan mudah dikenali, dan juga menjamin data atau informasi yang ada saat koneksi antar *client-server* dengan adanya IP tunelling pada sistem VPN.

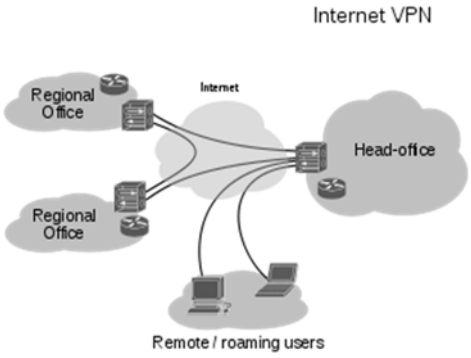
STIE Perbanas Surabaya merupakan salah satu Perguruan Tinggi Swasta (PTS) di Surabaya yang memiliki banyak proses dibidang IT yang melibatkan dosen, mahasiswa, pimpinan, prodi, dan karyawan. Kebutuhan untuk melakukan koneksi antara komputer/server yang berada di kantor dengan komputer di rumah civitas merupakan hal yang sangat diperlukan, mengingat banyaknya aktifitas yang harus dikerjakan. Oleh karena itu, diperlukan sebuah penelitian yang mampu memberi solusi atas permasalahan "**Bagaimana membuat manajemen keamanan sistem informasi dari akases internetmenujukomputer/server STIE Perbanas Surabaya dengan mudah dan memiliki tingkat keamanan tinggi**"**.**

2.ISI

2.1 Virtual Private Network (VPN)

Virtual private network (VPN) atau saluran komunikasi khusus yang efisien menggunakan jaringan internet.VPN digunakan bagi yang membutuhkan ruang sendiri di internet (Madjid, 2006).Sebagai contoh suatu komunitas yang memerlukan keamanan jaringan di internet dapat melakukan pertukatan informasi dalam lingkungannya sendiri.VPN berjalan pada topologi yang membuat suatu terowongan khusus.Fungsi VPN adalah memberikan koneksi yang aman antara user yang terhubung melalui internet dengan jaringan internal.Umumnya VPN diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan semacam ini memiliki kantor cabang yang cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan LAN.VPN dapat menjadi pilihan yang cukup tepat.Tentu saja VPN bisa diimplementasikan oleh pengguna rumah atau oleh siapa pun yang membutuhkannya. Secara garis besar cara kerja VPN adalah sebagai berikut:

a. VPN mendukung banyak protocol jaringan seperti PPTP, L2TP, IPsec dan SOCK, dimana protocol-protocol tersebut membantu kerja VPN untuk proses authentifikasi.
b. VPN klien dilakukan oleh user terpercaya yang telah diberi akses oleh administrator jaringan.
c. Jaringan VPN juga terenkripsi yang dapat meningkatkan keamanan.



Gambar 1.Koneksi Melalui Virtual Private Network

2.2 Firewall

Firewall adalah sebuah sistem keamanan yang dirancang untuk mencegah akses atau serangan dari dalam maupun ke luar jaringan. Firewall dapat diimplementasikan dalam hardware dan software, atau kombinasi keduanya. Implementasi *firewall* umumnya digunakan untuk mengontrol akses pengguna yang mengakses jaringan pribadi yang terhubung ke Internet, khususnya intranet. Semua lalu lintas aktivitas yang masuk atau keluar melalui jaringan intranet melewati firewall akan dikontrol bagi user yang tidak memenuhi kriteria keamanan tertentu secara otomatis akan terblokir [2].
Fungsi *firewall* sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *firewall* mengatur, memfilter dan ,mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan private yang di lindungi, beberapa kriteria yang dilakukan *firewall* antara lain :

a. Alamat IP dari komputer asal
b. Port TCP/UDP komputer asalke tujuan
c. Alamat IP dari komputer tujuan
d. Port TCP/UDP tujuan data pada komputer tujuan

e. Informasi header yang disimpan dalam paket data

Secara spesifik fungsi *firewall* adalah melakukan authentifikasi terhadap akases jaringan,Gambar 2 merupakan gambar implementasi *firewall*

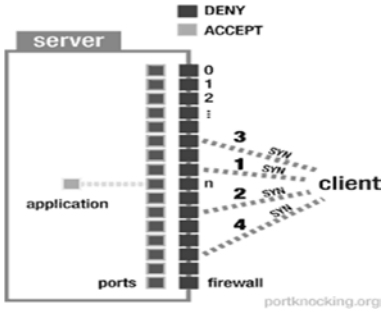
Gambar 2. Firewall

Cara kerja *firewall* pada umumnya dalam melindungi jaringan komputer internal, antara lain :

a. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
b. Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
c. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan. Misalnya firewall yang terintegrasi pada suatu antivirus akan menyaring dan mencegah file yang sudah terjangkit virus yang mencoba memasuki jaringan internal.
d. Melaporkan semua aktivitas jaringan dan kegiatan firewall.

2.3.Manajemen Keamanan Menggunakan Technologi Knocking Port

Knocking port adalah sebuah teknik atau metode membuka port secara eksternal melalui *firewall* dengan cara melakukan usaha koneksi pada suatu port yang tertutup dengan urutan upaya koneksi yang telah ditentukan [3]. Dengan kata lain*portknocking* adalah sebuah metode untuk membangun sebuah komunikasi *host-to-host* dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. *Knocking port* diimplementasikan dengan mengkonfigurasi Sebuah program kecil yang disebut daemon guna memonitor log *firewall* untuk permintaan koneksi dan menentukan apakah klien terdaftar pada alamat IP yang disetujui dan telah melakukan urutan ketukan yang benar. Jika jawabannya adalah ya, *firewall*akan membuka port yang terkait secara dinamis. Tujuan utama dari *knocking port* adalah mencegah penyerang dari pemindai sistem seperti remote akses SSH dengan melakukan port scanning [5]. Jika penyerang mengirimkan urutan ketukan yang salah, *port* yang dilindungi tidak akan muncul atau terbuka seperti pada Gambar3 berikut.



Gambar3.*Knocking* Port

2.4 Basis Data

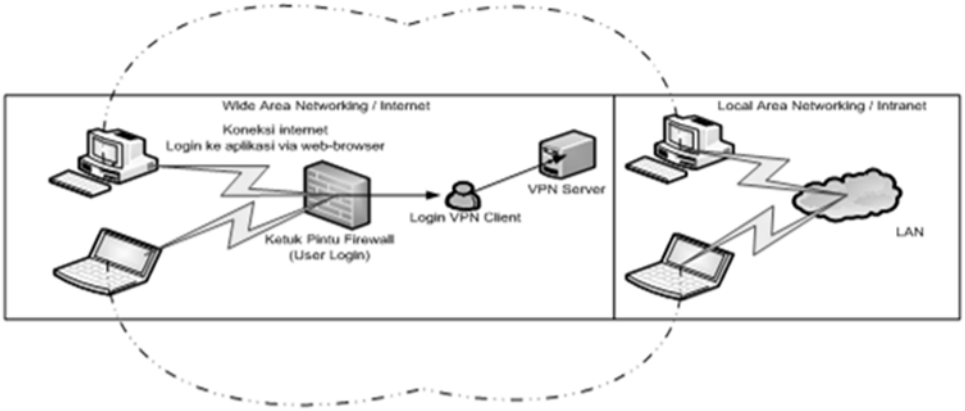
Database adalah suatu kumpulan atau susunan data operasional lengkap dari suatu organisasi yang diorganisir atau dikelola dan disimpan secara terintegritasi dengan menggunakan metode tertentu menggunakan komputer sehingga mampu menyediakan informasi yang optimal yang diperlukan pemakainya. Sedangkan sistem basis data adalah suatu sistem penyusunan dan mengelola *record-record* menggunakan komputer untuk menyimpan atau merekam serta memelihara data operasional lengkap sebuah organisasi atau perusahaan sehingga mampu menyediakan informasi yang optimal yang diperlukan pemakai untuk proses pengambilan keputusan.Menurut Marlinda (2004)pengertian Basis Data adalah: “Kumpulan file yang mempunyai kaitan antara satu file dengan file lain sehingga membentuk satu bangunan data untuk menginformasikan suatu perusahaan instansi, dalam batasan tertentu”. Kesimpulan di atas adalah basis data merupakan suatu kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan dalam sebuah komputer dan digunakan perangkat lunak untuk memanipulasinya.

2.5 Bahasa Pemrograman PHP

PHP merupakan salah satu bahasa scripting yang terpasang pada HTML.Sebagian besar sintaks mirip dengan bahasa C, Java dan Perl, ditambah beberapa fungsi PHP yang spesifik.Tujuan utama bahasa ini adalah untuk memungkinkan perancang web menulis halaman web dinamik dengan cepat.PHP ditulis dan diperkenalkan pertama kali sekitar tahun 1994 oleh Rasmus Lerdorf melalui situsnya untuk mengetahui siapa saja yang telah mengakses ringkasan *online*-nya.PHP merupakan bahasa berbentuk skrip yang ditempatkan dalam server dan diproses di server PHP merupakan bahasa berbentuk skrip yang ditempatkan dalam server dan diproses di server. Hasilnya akan dikirimkan ke client, tempat pemakai menggunakan browser. PHP dikenal sebagai sebuah bahasa scripting, yang menyatu dengan tag-tag HTML, dieksekusi di server, dan digunakan untuk membuat halaman web yang dinamis seperti halnya Active Server Pages (ASP) atau Java Server Pages (JSP). PHP merupakan sebuah software open source. Secara khusus, PHP dirancang untuk membentuk web dinamis. Artinya, ia dapat membentuk suatu tampilan berdasarkan permintaan terkini. Pada prinsipnya, PHP mempunyai fungsi yang sama dengan skrip-skrip seperti ASP (Active Server Page), Cold Fusion, maupun Perl.

2.6. Overview Sistem

Tahapan yang dilakukan oleh pengguna sivitas STIE Perbanas yang akan melakukan koneksi akses ke jaringan lokal STIE Perbanas Surabaya, yaitu diawali dengan melakukan login akses melalui internet melalui browser internet explorer. Setelah login berhasil dilanjutkan dengan melakukan login VPN client.Jika sukses maka Laptop/PC pengguna sivitas dapat terkoneksi ke dalam jaringan lokal STIE Perbanas Surabaya.



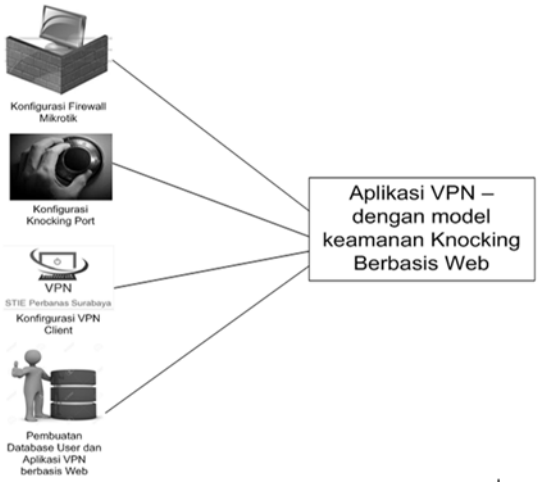
Gambar 4. Overview Model

2.7. Tahapan Implementasi

Tahapan rancanganmodel keamanan VPN dan *portknocking* ini dibagi menjadi 4 tahap besar, yaitu sebagai berikut :

1. Proses setting *Firewall* di mikrotik.
2. Proses pembuatan *knockingport client* di windows.
3. Proses pembuatan VPN *client*di windows.
4. Proses pembuatan *database user* dan sistem aplikasi VPN &*knocking* berbasis web.

Keempat tahapan perancangan model keamanan digambarkan pada flowcart gambar 5. Tahap pertama adalah proses melakukan konfigurasi pada *firewall* di mikrotik untuk melakukan blok akses *input* dari internet dan menentukan protocol dan port yang akan digunakan sebagai kunci dari user membuka akses *firewall* melalui *port knocking* berikut adalah konfigurasi *firewall* di mikrotik

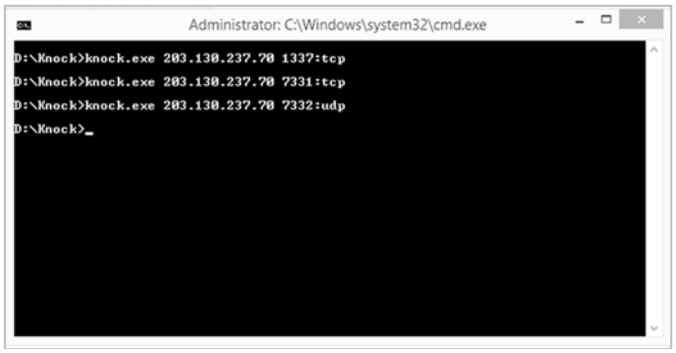


Gambar 5.Tahapan Perancangan Model Keamanan

Tahap kedua adalah membuat script berbasis DOS dengan menggunakan aplikasi *knockingclient*.Setiap user yang akan terkoneksi ke jaringan VPN harus menjalankan *script* tersebut untuk membuka *portfirewall* di mikrotik yang telah di setting pada tahap pertama.

```
[EDP@Cloud Core Router STIE Perbanas Surabaya] /ip firewall filter> add chain=input protocol=tcp dst-port=1337 action=add-src-t
o-address-list address-list=knock
[EDP@Cloud Core Router STIE Perbanas Surabaya] /ip firewall filter> add chain=input protocol=tcp dst-port=7331 src-address-list
=knock action=add-src-to-address-list address-list=safe
[EDP@Cloud Core Router STIE Perbanas Surabaya] /ip firewall filter> add chain=input protocol=udp dst-port=7332 src-address-list
=safe action=add-src-to-address-list address-list=open
[EDP@Cloud Core Router STIE Perbanas Surabaya] /ip firewall filter> add chain=input protocol=tcp dst-port=1723 action=drop
```

Gambar 6.*Firewall*Mikrotik



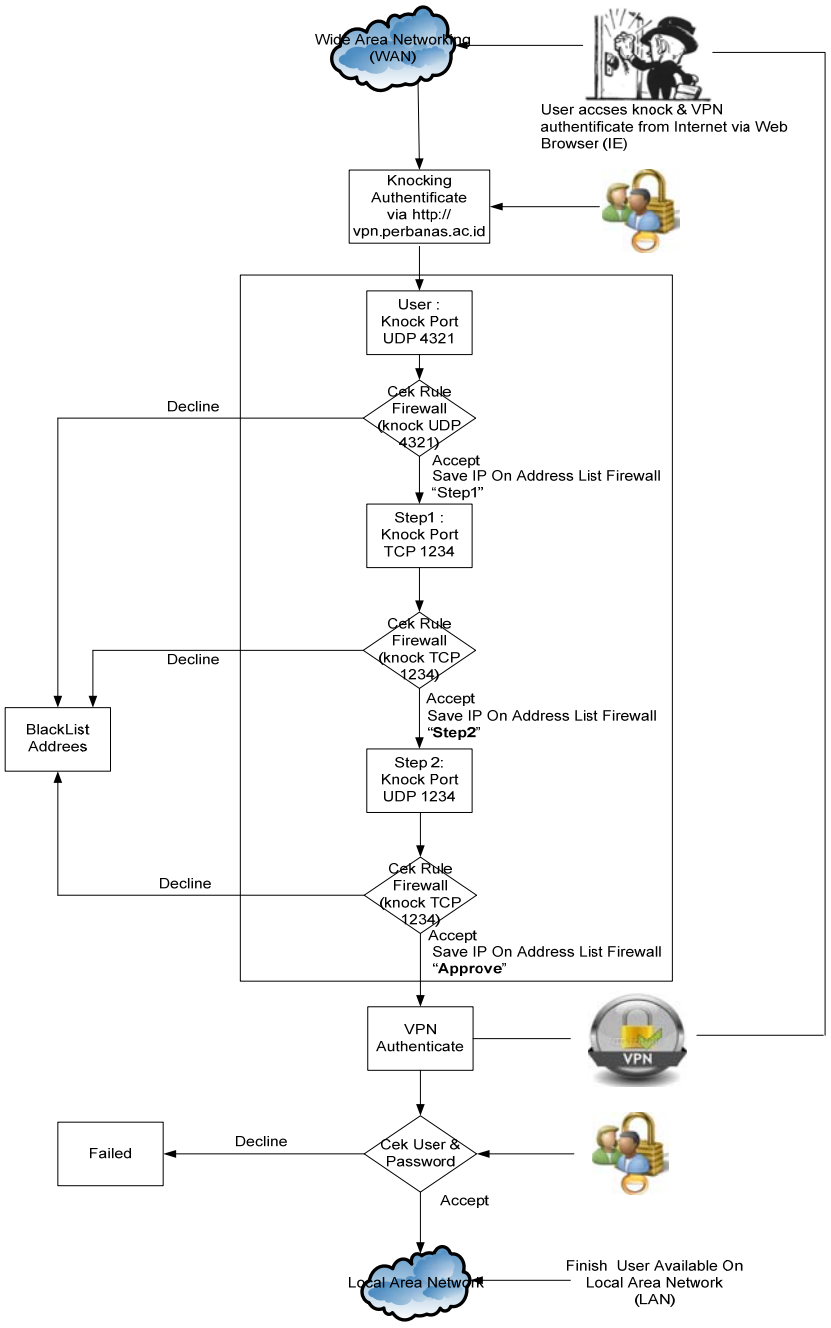
Gambar 7.*KnockingPort Client*

Tahap ketiga adalah pembuatan aplikasi *vpn client*berbasis windows melalui *Connection Manager Administration Kit*, user yang telah berhasil melakukan port *knocking*akan login pada aplikasi *vpn client* di STIE Perbanas Surabaya.

Gambar 8.VPN Client

Tahap keempat adalah melakukan desain sistem aplikasi berbasis web sebagai portal login untuk akses *knocking* port client dan vpn secara bersamaan dan otomatis untuk melakukan login pada *vpn client*menggunakan bahasa pemrograman PHP dan database mysql.

2.8 Alur ProsesKoneksi VPN



Dari penelitian yang dilakukan terhadap implementasi keamanan sistem informasi berbasis VPN dan *knocking*, ada beberapa point penting yang perlu di perhatikan, diantaranya sebagai berikut :

a. Kemudahan (*user friendly*)
   - Bagi dosen dan karyawan yang akan melakukan koneksi VPN ke STIE Perbanas Surabaya dapat melakukan akses via web di alamat https://vpn.perbanas.ac.id
   - Jaringan VPN dapat menjadi sarana akses sumber daya jaringan lokal yang tidak bergantung pada kondisi lokasi akses.

b. Keamanan (Security)

- Data yang ditransmisikan melalui jalur koneksi VPN akan dienkripsi sehingga tranfer data lebih aman
- Tingkat keamanan data untuk setiap user dosen dan karyawan yang terkoneksi terjamin dan lebih efektif, dengan menggunakan dua kali autentifikasi.

c. Kenyamanan (Simplify)
   - User tidak perlu melakukan *knockingport* pada *firewall* dan setting VPN clientdi windows, setiap user secara otomatis ketika sukses login pada web portal dan VPN client.

3. Penutup

Kesimpulan dan saran untuk pengembangan dari penilitian ini adalah

a. Sistem aplikasi keamanan manajemen informasi berbasis web yang dibuat hanya dapat berjalan di sistem operasi windows dan menggunakan browser internet explorer. Untuk pengembangan kedepan dapat dilakukan pengembangan lebih luas lagi untuk semua sistem operasi selain windows dan browser internet explorer.
b. User login pada portal https://vpn.perbanas.ac.id dengan VPN Client belum terintegrasi.
c. Port *knocking* pada *firewall*mikrotik masih bersifat statis untuk semua user.

4. Daftar Pustaka

[1] Al-Bahadili, H., Hadi, A.H. 2010. *Network Scurity Using Hybsrid Port Knocking*.International Journal of Computer Science and Network Security. Vol. 10 No. 8, August 2010. http://paper.ijcsns.org/07_book/201008/20100802.pdfdiakses tanggal 7 Maret 2015

[2] Dwiyono, A. 2008. Pengenalan *Firewall* dan IP Tables pada Jaringan Komputer. *Skripsi*. Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

[3] Estep, T.M. 2009. *Port knocking and Other Uses of 'Recent Match'*.http://www.shorewall.net/PortKnocking.html , diakses tanggal 10 Maret 2015

[4] Harrison, J. 2003. *VPN Technologies – A Compariosn*. Data Connetion Ltd. Enfield, UK. ftp://193.226.5.150/pub/users/dadarlat/retele_master/mpls-vpn/MPLS_VPN/vpntechwp.pdf. diakses tanggal2 Maret 2015

[5] Haryanto, E. 2013. Meningkatkan Keamanan Port Ssh Dengan Metode Port Knocking Menggunakan Shorewall Pada Sistem Operasi Linux. *Skripsi*. Amikom Yogyakarta

[6] Madjid, N. 2006. Perbandingan SSL (Secure SocketLayer) dan IPSec (Internet Protocol Security) pada VPN (Virtual Private Network).*Skripsi*. Teknik Informatika. ITB . Bandung

[7] Marlinda, L. 2004. *Sistem Basis Data*.Yogyakarta: Andi Offset

[8] Munanza, D. 2012. Perancangan Virtual Private Network (VPN) Server Untuk Koneksi Remote Pada Perangkat Android.http://news.palcomtech.com/wp-content/uploads/2014/09/Jurnal-_Dian_Dicky_Nicco_PerancanganVirtualPrivateNetwork.pdf. diakses tanggal 10 Maret 2015

[9] Prihanto, A. 2013. Implementasi Port Knocking Di mikrotik dengan menggunakan komponen Delphi TCP Client.*Prosiding Seminar Teknik Elektro Dan Pendidikan Teknik Elektro (STE 2013)*. Universitas Negeri Surabaya

[10] Setiawan, D. 2006. *Sistem Keamanan Komputer*. Elex Media Komputindo. Jakarta