OPTIMASI KEAMANAN *VIRTUAL PRIVATE NETWORK* UNTUK KOMUNIKASI DATA DI PUSAT INFORMASI PENGEMBANGAN PEMUKIMAN DAN BANGUNAN (PIP2B)

Diana¹, Javier Rezon Gumiri², Ali Wandra³

^{1,2,3} Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Bengkulu Jl. Bali Kota Bengkulu, telp (0736) 22765/fax (0736) 26161

> ¹diana@umb.ac.id ²javierrezon1@gmail.com ³aliwandra@gmail.com

Abstrak: Keamanan, kemudahan dan kecepatan transfer (pertukaran data) adalah salah satu aspek yang penting dari suatu jaringan komunikasi, terutama untuk perusahaan-perusahaan skala menengah ke atas., sehingga jatuhnya informasi yang bersifat rahasia diambil dan dimanfaatkan oleh-oleh orang yang tidak bertanggung jawab akan menyebabkan kerugian yang besar, untuk mengatasi permasalahan ini perlu *Virtual Private Network* dan mengoptimalkan keamanan nya menggunakan metode *Port Knocking* dengan menutup semua port yang terbuka dan hanya mengijinkan koneksi yang telah melakukan tahap "*knocking*" terhadap port tertentu diperbolehkan melalukan koneksi server tersebut agar komunikasi data antara pihak Pusat Informasi Pengembangan Pemukiman dan Bangunan dengan Mitra kerjanya lebih mudah dan aman dalam menyelesaikan pekerjaannya, Hasil pengujaian dengan adanya jaringan ini di sana ada service atau layanan-layanan yang ada bisa berjalan sesuai harapan tanpa terhambat waktu dan tempat dan metode port knocking keamanan lebih optimal karena memerlukan pengetukan port dan protocol terlebih dahulu, jadi untuk hak akses ke server lebih aman tidak sembarang orang dapat mengakses jika tidak ada izin.

Kata Kunci: keamanan, Virtual Private Network, Port Knocking,

Abstract: Security, ease and speed of transfer (data exchange) is one of the important aspects of a communication network, especially for medium and high-scale companies, so that confidential information is taken and used by irresponsible people. causes great losses, to overcome this problem it is necessary to use a Virtual Private Network and optimize its security using the Port Knocking method by closing all open ports and only allowing connections that have done a "knocking" stage for certain ports to be allowed to do the server connection so that data communication between the Settlement and **Building Development Information Center with** its partners is easier and safer in completing the work, the results of testing with this network are there services or services that can run as expected without being hampered by time and place and the port knocking method security is more optimal because it requires tapping on the port and protocol first, so for safer access rights to the

server, not just anyone can access it if there is no permission.

*Keywords: security, Virtu*al Private Network, Port Knocking,

I. PENDAHULUAN

Pusat Informasi Pengembangan Pemukiman dan Bangunan (PIP2B) Bengkulu ` adalah suatu lembaga publik inovatif yang mendukung pembangunan dan menyediakan akses dan layanan informasi teknologi, konsultasi dan advokasi, serta meningkatkan kapasitas dan kompetensi pelaku penyelenggaraan pembangunan di bidang ke Cipta Karyaan. Berkaitan dengan hal tersebut, di PIP2B Kota Bengkulu belum adanya suatu jaringan private yang dapat diakses oleh pihak perusahaan, sehingga masih ditemukan kendala-kendala apabila pihak perusahaan dan mitra kerja di PIP2B dalam menyelesaikan suatu pekerjaannya apabila dikerjakan dengan jarak jauh tanpa harus berada di lingkungan PIP2B dan semua data di input dan diakses melalui jaringan public (internet), Terdapat banyak user yang dapat dengan mudah mengakses jaringan lokal maupun internet, hal ini menjadi suatu masalah bagi administrator jaringan dalam mengelola user-user tersebut. Terutama pengelolaan terhadap user siapa saja yang boleh mengakses dan tidak terhadap jaringan tersebut.

Masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data) adalah salah satu aspek yang penting dari suatu jaringan komunikasi. terutama untuk perusahaanperusahaan skala menengah ke atas. Teknologi internet dahulu digunakan oleh perusahaan atau instansi pemerintah maupun badan sebagai sebuah komunikasi jaringan yang terbuka yang penggunanya dapat mengakses, berbagi dan menambah informasi. sehingga jatuhnya informasi yang bersifat rahasia diambil dan dimanfaatkan oleh-oleh orang yang tidak bertanggung jawab akan menyebabkan kerugian yang besar, untuk mengatasi permasalahan ini perlu Virtual Private Network (VPN) dan mengoptimalkan keamanan nya menggunakan metode Port Knocking dengan menutup semua port yang terbuka dan hanya mengijinkan koneksi yang telah melakukan tahap "knocking" terhadap port tertentu untuk diperbolehkan melalukan koneksi VPN server tersebut dan agar komunikasi data antara pihak PIP2B dengan Mitra kerjanya lebih mudah dan aman dalam menyelesaikan pekerjaannya

Pada penelitian terdahulu *Virtual Private Network* adalah salah satu fasilitas yang ada pada

server ClearOS yang memungkinkan para pekerja IT dapat mengakses jaringan internal kantor menggunakan koneksi jaringan pribadi dari luar dan Proxy Server dengan Metode Access Control List merupakan salah satu teknik selektivitas permintaan sambungan dalam komunikasi data untuk mengijinkan atau sebaliknya, sejumlah paket data dari suatu host komputer menuju ke tujuan tertentu dengan judul Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International[1]. Virtual Private Network mempunyai beberapa penerapannya termasuk jaringan Open vpn, jaringan ini merupakan teknologi yang digunakan untuk membangun jaringan vpn yang relative mudah dan murah serta konfigurasinya sangat mudah untuk server dan client. Open vpn juga memberikan keamanan dalam mentransfer data antar kantor cabang. Mengoptimalisasikan kinerja jaringan akan membantu keamanan, kecepatan dan penghematan bandwitch dalam suatu perusahaan dengan judul Perancangan Virtual Private Network Dan Optimalisasi Interkoneksi Mengunakan Teknologi Open vpn Pada PT. Tirta Musi Palembang [2].

Tujuan dari penelitian ini adalah untuk mengoptimalkan koneksi VPN keamanan menggunakan Metode Port knocking agar tidak sembarang orang bisa akses VPN Pusat Informasi Pengembangan Pemukiman dan Bangunan (PIP2B) Kota Bengkulu untuk komunikasi data, sehingga dapat memudahkan pekerjaan pihak perusahaan dan mitra kerjanya tanpa terhambat waktu, tempat dan terjamin keamanan datanya.

II. LANDASAN TEORI

A. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web) penelitian dengan judul Jaringan Komputer Dan Pengertiannya, Jaringan memungkinkan manajemen sumber daya lebih efisien, misalnya, banyak pengguna dapat saling berbagi printer tunggal dengan kualitas tinggi, dibandingkan memakai printer kualitas rendah di masing-masing meja kerja dengan judul Memilih Topologi Jaringan Dan Hardware Dalam Desain Sebuah Jaringan Komputer, Dalam pengukuran kinerja koneksi jaringan komputer ini menggunakan metode QoS (Quality of Service) untuk mengetahui jumlah bandwidth, throughput, delay dan packet loss berdasarkan standar THIPON menggunakan metode action research, dengan tahapan penelitian melakukan diagnosing, action planning, action taking, evaluating dan learning perangkat jaringan komputer yang ada di SMK Teknologi Bistek Palembang agar dapat mengetahui kelemahan dari setiap node dan jaringan yang ada di SMK Teknologi Bistek Palembang [3]-[4]-[5].

B. Intranet

Intranet merupakan sebuah jaringan komputer berbasis protokol TCP/IP seperti internet, hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet (WARNET) pun dapat dikategorikan intranet dan sistem ini akan menampilkan informasi mengenai hal-hal sesuai dengan apa yang dikehendaki oleh pembuat dengan judul Rancang Bangun Sistem Informasi Permintaan Atk Berbasis Intranet (Studi Kasus:

Kejaksaan Negeri Rangkasbitung) [6]. Dalam segi penggunaan, geografis maupun implementasinya, Intranet bekerja secara luas dan maksimal seperti halnya internet. Namun demikian Intranet sangat terbatas dalam hal privilege dan hak akses para pemakainya dengan judul Komputerisasi Pengolahan Data Penerimaan Peserta Didik Baru Di SMK Negeri 3 Pati Berbasis Intranet [7]. intranet sangat terbatas dalam hal privilege dan hak akses para pemakainya dengan judul Pengembangan Web Intranet Fisika Untuk Meningkatkan Penguasaan Konsep Dan Kemampuan Pemecahan Masalah Siswa SMK [8]. Intranet didefinisikan sebagai LAN (Local Area Network)/WAN (Wide Area Network) perusahaan yang menggunakan teknologi internet dan terlindungi oleh firewall perusahaan dengan judul Analisis dan perancangan sistem informasi dengan intranet: studi kasus persediaan material PT Balfour Beatty Sakti Indonesia [9].

C. Protokol

Protokol mendefinisikan apa yang dikomunikasikan, bagaimana dan kapan terjadinya komunikasi. Di mana program tersebut dapat membantu para pengguna komputer di dalam sebuah jaringan yang terkoneksi atau badan-badan hukum dalam pekerjaan sehingga dapat menghemat waktu, uang, dan tenaga dengan judul Pengembangan Aplikasi Pertukaran Pesan Berbasis Teks Melalui Jaringan Lokal (LAN) Menggunakan Microsoft Visual C++ 6.0 [10]. Dalam suatu jaringan komputer, terjadi sebuah proses komunikasi antar entiti atau perangkat yang berlainan sistemnya. Entiti atau perangkat ini adalah segala sesuatu yang mampu menerima dan mengirim. Untuk berkomunikasi mengirim dan menerima antara dua entity dibutuhkan pengertian di antara kedua belah pihak dengan Judul Rancang

Bangun Jaringan Komputer Dan Internet di Sekolah[11]. Protokol berfungsi untuk menghubungkan terminal pengirim dan penerima sehingga dalam berkomunikasi dan bertukar informasi dapat berjalan dengan baik dan benar penelitian dengan judul Sistem Telemetri Pemantauan Suhu Lingkungan menggunakan jaringan Mikrokontroler dan Jaringan WIFI [12].

D. Internet

Internet adalah suatu jaringan komputer yang sangat besar, terdiri dari jutaan perangkat komputer yang terhubung melalui suatu protocol tertentu untuk penukaran informasi antar komputer tersebut, Melalui internet orang dapat melakukan komunikasi dengan seseorang bahkan dengan beberapa komunitas sekaligus penelitian dengan judul Peranan Internet Terhadap Generasi Muda Di Desa Tounelet Kecamatan Langowan Barat [13]. Popularitas internet telah membuka banyak peluang ragam iklan yang dapat ditawarkan kepada publik antara lain: melalui Situs Jejaring Sosial (SJS), website, e-mail, video, widget, game, pop-up, instant messaging, dan lain-lain, Kehadiran internet memberikan revolusi fenomena dalam sejarah teknologi komunikasi masal penelitian dengan judul Internet Advertising Sebagai Media Komunikasi Pemasaran Interaktif [14]. Pada awalnya Internet atau WEB hanya dipergunakan untuk kepentingan Militer yaitu suatu tekhnologi yang dipergunakan untuk mengirimkan pesan melalui satelit, akan tetapi lama kelamaan teknologi tersebut akhirnya meluas, dan bahkan Internet pada saat ini sudah sama populernya dengan Telephone penelitian dengan judul Sistem Penjualan Berbasis Web (E-Commerce) Pada Tata Distro Kabupaten Pacitan [15].

E. Jaringan Virtual Private Network (VPN)

Jaringan Virtual Private Network (VPN) dengan memanfaatkan protokol EoiP, Ethernet over Internet Protokol (EoIP) merupakan protokol pada Mikrotik RouterOS yang berfungsi untuk membangun sebuah Network Tunnel antar MikroTik Router di atas sebuah koneksi TCP/IP yaitu dengan memanfaatkan koneksi internet sebagai penghubungnya penelitian dengan judul Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP[16]. Virtual Private Networkadalah teknologi jaringan yang memanfaatkan komputer media komunikasi public (open connection atau virtual circuits), seperti Internet, untuk menghubungkan beberapa jaringan local penelitian dengan judul nalisis Quality Of ServiceJaringan Virtual Private Network(VPN)di STMIK STIKOM Indonesia[17]. Aplikasi sistem informasi tersebut bisa diakses melalui internet secara private dengan teknologi VPN (Virtual Private Network). Namun dalam perkembangannya para administrator jaringan dituntut untuk bekerja dengan cepat, handal, dan profesional ketika terjadi masalah pada lalu lintas (traffic) yang disebabkan oleh penggunaan lalu secara *overloaded* lintas data dan akan mempengaruhi kecepatan koneksi antar perangkat jaringan, sehingga penggunaan internet tidak optimal dengan judul Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN) [18].

F. Komunikasi Data

Komunikasi data adalah proses pengiriman data atau informasi dari suatu sumber (disebut *source*) ke tujuan (disebut *destination*). Komunikasi data dapat dilakukan antara dua jenis komputer atau lebih yang jenisnya sama ataupun berbeda dengan judul Komunikasi Data Dan Komputer [19]. Mata pelajaran komunikasi data bertujuan memberikan pemahaman dan penguasaan pengetahuan serta keterampilan tentang ragam aplikasi komunikasi data, proses komunikasi data dalam jaringan, aspek-aspek teknologi komunikasi data dan suara, dan kebutuhan telekomunikasi dalam jaringan dengan Pengembangan E-Modul judul Berbantuan Simulasi Berorientasi Pemecahan Masalah Pada MataPelajaran Komunikasi Data (Studi Kasus: Siswa Kelas XI TKJ SMK Negeri 3 Singaraja) [20].

G. Port knocking

Metode port knocking seorang administrator dapat meningkatkan keamanan suatu server dari berbagai seranagn yang ditujukan utuk layanan server. Cara kerja dari metode ini adalah server akan menerima percobaa koneksi dari *client* menuju port yang sudah ditentukan setelah itu firewall akan mendeteksi percobaan tersebut dan mengizinkan client untuk mengakses server. Setelah client selesai mengakses server firewall akan menutup kembali akses ke server sehingga server tidak bisa diakses kembali penelitian dengan judul Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux [21]. Port Knocking adalah salah satu sistem keamanan yang dapat melakukan fungsi yaitu mem-blok akses yang tidak diinginkan. Pada prinsipnya, port knocking bekerja menutup seluruh port yang ada di server. Bila user menginginkan akses ke server, user melakukan "ketukan" untuk menggunakan layanan, kemudian bila user telah selesai melakukan akses maka port ditutup kembali dengan judul Aplikasi Pengendalian Port dengan Utilitas Port Knocking untuk Optimalisasi Sistem Keamanan Jaringan Komputer[22].

H. Firewall

Firewall adalah sistem dengan tujuan untuk melindungi. Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan menolak suatu atau semuahubungan/kegiatan dari suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya merupakan sebuah workstation, server, router, atau Local Area Network penelitian dengan judul paperblock akses browsing menggunakan mikrotik rb 751u-2hnd dengan schedule time (studi kasus: Disnakerpora Kota Bengkulu) [23]. Firewall merupakan salah satu solusi dalam mencegah serangan penyusup tersebut. Dengan mempelajari dengan seksama dan mengaturan hak akses yang dibutuhkan dalam suatu jaringan dan menggunakan software yang sesuai, maka kita dapat merancang firewall yang cocok untuk diterapkan. Firewall sendiri diterapkan untuk dapat melindungi dengan melakukan filtrasi, membatasi ataupun menolak suatu koneksi pada jaringan dengan judul Desain dan Implementasi Firewall dengan Layer 7 Filter Pada Jaringan Teknik Elektro[24].

III. METODE PENELITIAN

A. Metode Pengembangan Sistem

Network Development Life Cycle (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data, langkah-langkahnya sebagai berikut :

1. Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini

2. Simulation Prototype.

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Boson, Packet Tracert, Netsim, dan sebagainya

3. Implementation.

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya

4. Monitoring.

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*.

5. Management.

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. B. Flowchart Penerpan Port Knocking



Gambar 1. Penerapan Port Knocking

c. Tahapan-Tahapan Sistem

Berikut gambaran tahapan-tahapan proses penerapan *Port Knocking* pada sistem:

- 1. Nomor 1 proses memulai akan melakukan knocking port.
- 2. Nomor menunjukan proses mengetuk port tahap pertama.
- Nomor 3 validasi port yang akan di ketuk, apabila port yang diketuk sudah benar maka ip addressnya akan dikelompokan pada address list"knock", apabila salah akan diulang ke proses Nomor 2.
- 4. Nomor 4 menunjukan ip address yang mengetuk sesuai dengan port yang telah diatur akan dikelompokan dalam address list "knock". dalam waktu 15 detik jika tidak melakukan ketukan port selanjutnya, maka proses akan diulangi dari Nomor 2.
- 5. Nomor 5 menunjukan proses mengetuk port tahap kedua.
- Nomor 6 validasi port yang akan di ketuk, apabila port yang diketuk sudah benar maka ip addressnya akan dikelompokan pada address list"safe", apabila salah akan diulang ke proses Nomor 2.
- Nomor 7 menunjukan ip address yang mengetuk sesuai dengan port yang telah diatur akan dikelompokan dalam address list "safe". dalam waktu 30 detik jika tidak

melakukan ketukan selanjutnya, maka proses akan diulangi dari Nomor 2.

- Nomor 8 menunjukan proses mengetuk protocol Icmp. Dan akan dikelompokan dalam address list "ping". dalam waktu 3 menit.
- 9. Nomor 9 validasi port yang akan di ketuk, apabila port yang diketuk sudah benar maka sudah dapat mengakses VPN server apabila salah akan diulang ke proses Nomor 2.
- Nomor 10 ip address yang telah berada pada address list "ping" yang telah melakukan ketukan protocol "icmp" akan diperkenankan untuk mengakses VPN server.
- 11. Nomor 11 selesai.

IV. HASIL DAN PEMBAHASAAN

A. Hasil

a. Instalasi Mikrotik RouterBoard 750

RB750 adalah produk routerboard yang sangat mungil dan diperuntukkan bagi penggunaan SOHO. Memiliki 5 buah port ethernet 10/100, dengan prosesor baru Atheros 400MHz. Sudah termasuk dengan lisensi level 4 dan adaptor 12V.



Gambar 2. Mikrotik RouterBoard 750

b. Konfigurasi Mikro Router Board 750

Proses konfigurasi Mikrotik bertujuan agar Mikrotik dapat digunakan untuk menghubungkan Mitra ke VPN PPTP di PIP2B sesuai pada rancangan jaringan yang telah di buat.

1. Menambahkan IP address pada LAN (Local area Network) untuk jaringan lokal.

	- Loved Area Committee States	Nel2009		
Terral effects official	V Local And Committee Properties	Personal Support Andrea (1922) 2/10 Lobertum		
Sharings adversiond sharing	Manufra (Shara	latend		
uneup	Connectures Conne	The care per D settings many rel adjusted all P rose reliver's capacity. The resolution Distances, processed to advect advections. In the appropriate P of Prop.		
	Lo Company of L	Colline or Falters approximite		
	The convertor set for University term	a tes Pa Dinorg IF added		
	W. Classific Microsoft Renveaks	Waldwest 297,160,20, 01		
	R Stat Paint Schedule	miltred mark 200 - 200 - 200 - 2		
	R. 2 Plan and Phone Downsy by Missouri Hermatian Rev. 1. Internet Produced Design 617 (PDP)	100 and prevent 200, 100 - 00 - 1		
	Contract Protocol Contract of Contract	(1) this are really one as sold to a substrate all.		
and the second second second	M + Link Later Tracksp-Soccess Responder	🗰 Liter Bay Tolkinerg Diel are per adde cones.		
CT Digitalities and and	Include and Includ	realized bitst service: FSC - 108 - 81 - 1		
Laste My Well Tachsonger	Theory Ben Topportunite Castrol Photosoft Parents Photosoft (Paramitade	Allowed William and		
Hart Property Versel	An all a design provide provide that provide community and the	Control and Control Control -		

Gambar 3. Tampilan IP Address LAN

2. Jalankan aplikasi winbox lalu connect untuk masuk kedalam Mikrotik.





 Menambahkan IP address pada mikrotik interface 2 agar mikrotik dapat memberikan jalur koneksi ke jaringan lokal

A Gast Sat									
an interfactory									
25 Bullet									
*E ***									
ID Settle									
* S Math									
10-10 E	40.9	1				P			
M755	Accounting	Terration of the local division of the local	-	-		and a second second			1010
at Realing	Academies	-	190,160,38,120	4	08.	•	<1111 (CI 1 7)		
all System	Dist	Metsore.		×.	Cevel	Addres .	Halmosh.	Interface	
Contract .	DHCP Dert	Padan.	at sol	14	Auto	1 10	100.00.01 100.000.00.0		
all Films	DOCT Finish			-					
- Log	DACE Lands				Deabler				
A Natio	DME				Same				
of Fach	Finned				Cost				
M New Swarid	Manager				Dames .				
NAME OF THE	Pres.								
C Partice	NewHeat	Invalled				1			
Natio Capool II	Pathere	-							
and Married	Pres	_							
. T.d.	Baster								
	Tanki .					7.888			
	1000								

Gambar 5. Tampilan Penambahan IP Address Lokal

 Membuat DHCP Client agar jaringan lokal otomatis terhubung dengan jaringan publik / ISP (Internet Service Provider).

Autor Autor					
5.40 9.00 4.00 4.00 5.400			1. Second		- 1800 - 2 - 1
Borner File Cop Baster File Baster File Baster File Baster Baster Baster File File Baster File Baster File Baster File Baster File Baster File File File File File File File File	Intel ² Ease Star Star Star Star Star Star Star Star Star	 et gan san san san san san san san san san san san san san san	all all all all all all all all all all	j ber	
Fash Res: Tanada Anadiki 111 Parkes Mara Tanada Renad Est		 International States and	200 200 200 200 200 200 200 200 200 200	i ini	

Gambar 6. Tampilan DHCP Client dan IP dari ISP

 Menambahkan DNS dan mencentang "Allow Remote Request" agar client dapat merequest DNS dari Mikrotik.



Gambar 7. Tampilan DNS

6. Menambahkan NAT (*Network Address Translation*) yang bertujuan untuk menerjemahkan IP Address Private dari jaringan local ke IP public.

All Darit Lat we benchman 25 Bookge with Press 25 Press 26 Press 27 Bookge	Parentiales fail a	Margan Barrier Prov. Co (200) (197) (10) Roser Augo (10) Addams (1 104	rementario Antoneo (Ant. Laure Provinsia) Locale - antoneo de Carreno en Antoneo (France, San Prant, San Part, San San Jac, San J	inter 14 Annuel 14 Annuel 14
10. P [*]	0400	BHIT Puterin		100
MPLD.	decouding	farmer Address	of Extra system (Statemen)	100
nadra	Addresses	Dum	•	Easter
Clamate	Cast O Tilesa	Ter, Address		Pasta
d'anne	DesCP Hater	Unt Address	*	I Distant
6.64	DHEP Darrent	120110		
Refl.o	248	Pressie -		
Tiefe *	Termine	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	5	Lowy
t Hen-Tanimal	Philipped	Tra Pass		Parate
A A A A A A A A A A A A A A A A A A A	(Past)	1 10 Per		Final Coardees
Patron	Haighburn	In Interface		Frend Ad Doarders
Place Departs of	Packed.	Out Interface	rial 8	
1.4		Particul Mark		
		Communitation.	1	
	110-01	An and a second second	1	
	Sector.	finant fam	1	
	(interact	total table	1	
	Secto	Exemption Type:		

Gambar 8. Tampilan NAT Rule

c. Konfigurasi VPN PPTP Router Server

Selanjutnya untuk membuat PPTP server dengan menggunakan aplikasi winbox. Dalam membuat PPTP server ada beberapa tahapan yang di-*setting* :

1. Mengaktifkan fitur PPTP server bertujuan agar bisa membuat profile PPTP untuk Mitra.



Gambar 9. Tampilan Mengaktifkan PPTP Server

 Membuat user VPN Mitra bertujuan untuk membuat User dan password Mitra pada saat ingin terhubung ke dalam VPN Server

Name:	ali102		OK
Password:	ali102	-	Cancel
Service:	pptp	₹	Apply
Caller ID:		-	Disable
Profile:	default-encryption	Ŧ	Comment
Local Address:	10.10.10.1	-	Сору
Remote Address:	10.10.10.2	-	Remove

Gambar 10. Tampilan Membuat User Dan Password VPN Mitra

 Membuat user VPN remote acces bertujuan untuk membuat user dan password Mitra pada saat ingin terhubung ke dalam VPN Server ketika tidak berada di bawah router Mitra.

Name:	ali 103		OK
Password:	ali 103	-	Cancel
Service:	pptp	*	Apply
Caller ID:		-	Disable
Profile:	default		Comment
Local Address:	10.10.10.1	-	Copy
Remote Address:	10.10.10.3	-	Remove
Routes:	L	-	
Limit Bytes In:	E	-	
Limit Bytes Out:	0	-	
ant Logged Out	Aug/04/2018 17:	27:49	

Gambar 11. Tampilan Membuat User Dan Password Remote Acces

 Membuat IP address komputer server, bertujuan untuk dijadikan sebagai IP komputer server PIP2B.



Gambar 12. Tampilan IP address server

 Membuat IP route, bertujuan sebagai jalur koneksi antara server dan mitra agar bisa terhubung.



Gambar 13. Tampilan IP Route

d. Konfigurasi VPN PPTP Router Mitra

Selanjutnya untuk membuat PPTP Mitra. Dalam membuat PPTP Mitra ada beberapa tahapan yang di-*setting* :

 Membuat PPTP Client dengan memasukan user dan password yang telah di buat di PPTP Server.

111										Weters (VPN PIP22 10	2		
inter	lace	PPPu	E Serv	H1 (Sécréfi	Polie:	Active (Connections L	21P Seciela	General DialOut Sta	us Traffic		DK.
+ •	-		×	0	7	PPP Sca	me	PPTP Server	SSTP Se	Connect To:	36.37.75.96		Cancel
	Name	N DD	00 10	Ty		6	L2M	tų Tx	.014	Ure	9002		Apply
		34136	ab re	a re	ri, Palit					Password	ma		Disable
										Puble	default-encryption	1	Connent
										Keepalive Timeout	60	•	Сору
											Dial On Demand		Remove
											Add Default Route		Torch
										Default Route Distance:	0		
										- Allow			
										✓ pap	✓ chap		
										🗹 mochap1	🗹 mochap2		

Gambar 14. Tampilan PPTP Client

 Membuat IP route, Membuat IP route bertujuan untuk jalur koneksi antara Mitra dan Server agar bisa terhubung

A Duck Set		Pogetia	12 K
· Interfaces		Rodes Radopt Rules MIT	
Lindge			4.4
11 FFF		Ter Addam Colores	Tataon Bodro Hat Dat Come
= Seith		245 0.000 1921681321 machate mini	Same linear transmission
*2 Mesh		1 S21611 S28 10 72111 avaatude	1 107100.001
9.P	180	States I and the second states and the secon	0 1021001270年
MPLS	Accounting	Valuantinguage.	
Rowing 1	Addenso	Town (12) that 1 plan	
@ System 1	Cloud	Dewid Anlaki	OK.
0.000	EHOP Ciwe	Dist Widdees: 112 1081 0/30	Carcel
File	DeeCP Fining	Editivar 1010101 # avenchable	4 App
Log	THOP Server	a sample in the second second	
# Radio	EN5	Dick Lating	• Diale
a Tack	Ferred	Ten lavat	¥ Corner
at Non Terranal	Holps	Annual II	Citer
MatuROUTER	Fax		heave
Patton	Negłowi	Scope 20	
MathSigned	Packing	Target Secon 10	
\rm Hanul	Pail	Fix.leg.that	
E Eni	Flowles.	Pet Source	
	1145		

Gambar 15. .Tampilan IP Route

e. Konfigurasi Port Knocking

Selanjutnya tahap konfigurasi port knocking pada VPN Server untuk mem-filter Mitra yang mengakses VPN Server PIP2B. Berikut adalah langkah-langkah dalam konfigurasi port knocking pada Mikrotik:

 Membuat rule 1 pada firewall, yang bertujuan jika ada koneksi dari luar ke dalam mengetuk port 1122 dengan protocol tcp maka tersebut akan dimasukan kedalam kelompok addresslist "knock" selama 15 detik.

Seneral Advanced Extra Action Statistics		OK.
Chain: nov	Ŧ	Cancel
Stc. Address	•	Apply
Dst. Address:	•	Disable
Protocol: 🗌 🔓 (top)	¥ .	Comment
Src. Part		Сору
Dot. Port 🗌 1122	`	Remove
Any Port	+	Reset Counters
In Interface:	•	Reset All Counter
Out Interface:	•	-

Gambar 16. Tampilan Firewall General rule 1

iewall Rule (1122>		
General Adv	anced Extra Action Statistica		0K
Action	add ins to address list		Cancel
	🗆 Log		Apply
Log Prefix		• [Disable
Address List	knock.	× (Comment
Timeout:	00.00.15		Сору
			Remove

Gambar 17. Tampilan Firewall action rule 1

2. Membuat rule 2 pada firewall, yang bertujuan jika ada koneksi dari luar ke dalam yang berada pada kelompok address list "knock" mengetuk port 1233 dengan protocol tcp maka ip tersebut akan dimasukan kedalam kelompok addresslist "safe" selama 30 detik

Firmwall Rule <123	3		
General Advance	ed Extra Action Statistics		ОК
(Thain input	¥ C	ancel
Src. Ad	atest	•	φply
Dst. Ad	kest.	- Di	isable
Pro	tocol 🗍 6 (top)	T Co	mment
Sic	Port	•	Copy
Det	Port 1233	▲ Re	move
Any	Port	· Reset	Counters
In Inte	face.	Reset A	di Counters

Gambar 18. Tampilan Firewall General rule 2

General	Advanced	Extra	Action	Statistics		
5	Stc. Address I	list: [knock		Ŧ	}
۵)st. Address I	_ist [•

Gambar 19. Tampilan advanced rule 2

ieneral Adv	ranced Extra Action Statistics		OK
Action	add sec to address list	Ŧ	Cancel
	🗌 Log		Apply
Log Prefix:		•	Disable
ddress List:	safe	Ŧ	Comment
Timeout:	00:00:30	Ŧ	Сору

Gambar 20. Tampilan Action Rule 2

3. Membuat rule 3 pada firewall, yang bertujuan jika ada koneksi dari luar ke dalam yang berada pada kelompok address list "safe" melakukan ping maka ip tersebut akan dimasukan kedalam kelompok address-list "ping" selama 3 menit.

General Advanced Extra Action Statistics		OK.
Chain: Input	¥	Cancel
Src. Address	-	Apply
Dst. Address	•	Disable
Protocol: 1 (icmp)	1	Comment
Site Port:		Сору
Dut. Poet.	w	Remove
Any Post	*	Reset Counters
In Interface: 01 WAN	¥ *	Reset All Counters

Gambar 21. Tampilan Firewall General

General Advanced	Extra	Action	Statistics		
Src. Address L	ist 🗖	safe		Ŧ	ŀ

Gambar 22. Tampilan Firewall advanced

eneral Adv	ranced Extra Action Statistics		OK.
Action	add src to address bit	*	Cancel
	🗌 Log		Apply
Log Prefix		•	Disable
Address List	ping		Comment
Timeout	00:03:00		Сору

Gambar 23. Tampilan Firewall Action

4. Membuat rule 4 pada firewall, yang bertujuan jika ada koneksi dari luar ke dalam yang berada pada kelompok address list "ping" mengetuk protocol "icmp" maka ip tersebut akan di izinkan untuk mengakses vpn server.



Gambar 24. Tampilan Firewall General

General Advanced Extra Action Statistics		
Src. Address List 🖾 ping		T
Gambar 25. Tampilan Fi	irewall advanced	
Seneral Advanced Extra Action Statistics		OK
Action accept	Ŧ	Cancel
Li Log		Apply

Gambar 26. Tampilan Firewall Action

5. Membuat rule 5 pada firewall, yang bertujuan jika ada koneksi dari luar ke dalam yang tidak berada pada kelompok address list "ping" maka ip tersebut tidak akan di izinkan mengakses vpn server.

iesal Advanced Extra Action Statistics		0K.
Chain: input	*	Cancel
Sic. Address:		Apply
Dst. Address:		Disable
Protocol 6 (top)	¥ .	Comment
Src. Port	•	Copy
Dist. Port: 1723		Remove
Any Port	•	Reset Counters
In Interface: 01 WAN	* *	Reset All Counters

Gambar 27. Tampilan Firewall General

General	Advanced	Extra	Action	Statistics	
5	Src. Address I	List 🗓	ping		Ŧ
(Dat. Address I	List			-

Gambar 28. Tampilan Firewall Advanced

Seneral Advanced Extra Action Statistics		0K.
Action: dop		Cancel
Log		Apply
Log Prefix	•	Disable

Gambar 29. Tampilan Firewall Action

f. Konfigurasi VPN Mitra Remote Acces

Penggunaan VPN untuk Mitra adalah menghubungkn Mitra dengan network VPN Server seolah-olah berada dalam satu jaringan local. Dalam mengkoneksikan Mitra dengan VPN server dibutuhkan beberapa tahapan settingan pada Komputer Mitra. Berikut adalah settingansettingan untuk koneksi VPN user ke menggunakan Microsoft Windows .

1. Buat koneksi baru dengan cara masuk ke control panel kemudian klik *windows network and internet* lalu klik *set up a new connection or network*.



Gambar 30. Tampilan Control Panel > Network And Internet

 Menambahkan koneksi baru "Connect to a workplace" yg bertujuan membuat koneksi jaringan baru.



Gambar 31. Tampilan Set Up A Connection Or Network

 Lalu klik "use my internet connection (VPN)" yang bertujuan untuk memilih koneksi VPN yang akan di buat.



Gambar 32. Tampilan Connect To A Workplace

4. Selanjutnya masukan user dan password VPN yang telah dibuat.

Type your user n	ame and password	
User neme:	30103	
Passwords		
	IIII Show characters	
Decesie (actional)	Remember this persword	
Demain (optional)		

Gambar 33. Tampilan user dan password

5. Koneksi VPN yang telah di buat telah tersedia.



Gambar 34. Tampilan Koneksi VPN Yang Telah Dibuat

g. Monitoring

Pada tahap ini akan dilakukan monitoring terhadap system VPN yang telah dibuat yaitu dengan melakukan analisa system VPN. Pengujian dilakukan dengan cara melalukan pengujian login, dan *file sharing*.

B. Pembahasaan

Setelah semua yang diperlukan untuk membangun *system* VPN selesai, maka ada beberapa *scenario* yang akan dilakukan untuk melakukan peengujian terhadap jaringan VPN. Pada pengujian ini akan dilakukan *scenario* pertama pengujian yang terdiri atas dua pengujian diantaranya:

Tabel 1. Pengujian	Login Da	ata Benar
--------------------	----------	-----------

Kasus dan hasil uji (Data Benar)		
Data Masukan	Menggunakan ketukan	
Yang diharapkan Pengamatan	Ketukan ,user dan password (remoteaccess) yang dimasukan benar sehingga dapat terhubung VPN Ketukan,user dan password yang dimasukan diterima dan terhubung ke VPN dan File sharing bias di akses	
Kesimpulan	Di terima	

 Pengujian data benar dilakukan dengan cara masuk "command prompt" lakukan Ketukan pertama knock 36.37.75.86 1122:tcp. Akan muncul koneksi yang mengetuk di jendela "Firewall" dan di kelompokan ke dalam address list "knock" dengan waktu 15 detik.



Gambar 35. Tampilan Ketukan Pertama

 Pengetukan ke dua dilakukan dengan cara knock 36.37.75.86 1122:tcp dalam waktu 15 detik dan Akan muncul koneksi yang mengetuk di jendela "Firewall" dan di kelompokan ke dalam address list "safe"

dengan waktu 30 detik. Jika tidak berhasil maka akan mengulang pada pengetukan pertama.



Gambar 36. Tampilan Ketukan Ke Dua

3. Setelah itu mengetukan protocol "icmp" dalam waktu 30 detik dan Akan muncul koneksi yang mengetuk di jendela "Firewall" dan di kelompokan ke dalam address list "ping" dengan waktu 3 menit. Jika tidak berhasil maka akan mengulang pada pengetukan pertama.

Naem © STAFF D © sale P © teng	Auditory Tammad Considers Tame 142 (46) 100.0726 July 2212 (101 (001 A)) July 2212 (101 (001 A)) 36 (44.50 M) 000 (001 L) July 277 (201 (101 A)) July 2212 (101 (101 A)) 36 (44.50 M) 000 (001 L) July 277 (201 (101 A)) July 201 (101 A))		-	
	M Command Prompt Recomments Understand Activities All Programs and Activities All Programs and Activities All Programs and Activities All Programs and Activities Activities and Activities Activit	1	an [(0)]	
3 40000	C:\Usurev\UJ>ping 36.12.79.96 Pinying 36.37.79.46 with 32 bytes of data: Public from 55.17.75.86 bytes 31 time=63m TIL-56 mapin from 55.17.75.86 bytes-12 time=63m TIL-56 mapin from 55.17.75.86 bytes-12 time=63m TIL-56 bytes/from 53.17.75.86 bytes-12 time=30m TIL-56 bytes/from 53.17.75.86 bytes-12 time=30m TIL-56			
	Hoply from 34.32-25.46. Bytes-32 fine damn Histor Huply Com 34.32-25.46. Bytes-32 fine damn Histor Ping statistics for 36.37.75.46. Pankator Bonto 7 9. A Possilved 3.4.57. Lost v.H. (BK Inco).			

Gambar 37. Tampilan Koneksi Protocol "Icmp"



Gambar 38. Tampilan Koneksi Mitra Yang Terhubung

 Ketika pengetukan telah dilakukan. Komputer yang berada di bawah router sudah langsung terhubung otomatis kedalam VPN.



Gambar 39. Tampilan Login VPN Remote Acces

 Untuk remote access harus melakukan login manual user dan password kedalam koneksi VPN yang telah di buat



Gambar 40. Tampilan koneksi yang terhubung

 Dan dapat dilihat sekarang Mitra sudah terkoneksi ke VPN PIP2B

and Hanks	View your basic network info	emation and set up connections	• • •	
verden rebrette adapter settings advanced sharing	1.FC (This compated)	Multyle networks letternet	Seafulling	
	Partic retaint	Access System Connectional 🖉 🕫 23	Currently connected to: Network 2 Internet science FIP2B 2	1
	Network 2	Access type: Internet	betarrett access	J

Gambar 41. Tampilan Komputer Server PIP2B

 Dan sekarang data komputer server PIP2B sudah bisa akses dan *Sharing* data sudah bisa dilakukan

Denanties Methods and Shaine Center View jame	te subden	No. 12
Download:	pengujian Dran	
Decements Documents Munic Photoes	Usen2 Dian	

Gambar 42. Tampilan Komputer Server PIP2B

Tabel 2. Pengujian Login Data Salah				
Kasus dan Hasil Uji (Data salah)				
Data Masukan	Tanpa ketukan			
Yang di harapkan	Setelah kelik tombol connect maka akan muncul pesan "error 800: The remote connection was not made because attempted VPN tunnels failed"			
Pengamatan	Muncul pesan bahwa koneksi error			
Kesimpulan	Tidak diterima			

 Pengujian data salah dilakukan dengan cara melakukan login ke VPN tanpa melakukan pengetukan terlebih dahulu dan menunjukan status koneksi VPN komputer mitra "disconected" tidak terhubung kedalam VPN.



Gambar 43. Tampilan Status VPN Komputer Mitra



Gambar 44. Tampilan Login User Dan Password Remote Acces

 Pada *remote acces* setelah langsung melakukan login tanpa mengetuk muncul pesan koneksi ke vpn eror dan tidak bisa terkoneksi ke jaringan VPN.



Gambar 45. Tampilan Koneksi VPN Eror

V. KESIMPULAN

Berdasarkan hasil Pengujian: 1) VPN Server PIP2B bisa diakses oleh Mitra Kerjanya dan remote acces selama Server memberikan hak akses "autentikasi" untuk masuk kedalam , 2) Dengan adanya metode port knocking keamanan lebih optimal karena memerlukan pengetukan port dan protocol terlebih dahulu, jadi untuk hak akses ke VPN Server lebih aman dan tidak sembarang orang yang bisa akses jika tidak mendapatkan hak akses "autentikasi" tersebut, 3) Dengan adanya jaringan VPN di PIP2B, service atau layananlayanan yang ada di PIP2B bisa berjalan sesuai harapan tanpa terhambat waktu dan tempat.

Referensi

- T. M. Eka Wida Fridayanthie1, "Rancang Bangun Sistem Informasi Permintaan Atk Berbasis Intranet (Studi Kasus: Kejaksaan Negeri Rangkasbitung)," J. Tek. Komput. Amik Bsi, vol. 1, no. 1, pp. 55–66, 2015.
- [2] T. Openvpn, P. Pt, T. Musi, S. Sarial, A. Wijaya, and E. P. Agustini, "Perancangan Virtual Private Network Dan Optimalisasi Interkoneksi Mengunakan."
- [3] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, vol. Vol.1, pp. 1– 10, 2014.
- [4] A. Supriyadi and D. Gartina, "Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer," *Inform. Pertan.*, vol. 16, no. 2, pp. 1037– 1053, 2007.
- [5] A. Putri, Fatoni, and I. Solikin, "Analisa Kinerja Koneksi Jaringan Komputer Pada Smk Teknologi Bistek Palembang," Univ. Bina Darma, no. 12, pp. 1–11, 2016.

- [6] T. M. Eka Wida Fridayanthie1, "Rancang Bangun Sistem Informasi Permintaan Atk Berbasis Intranet (Studi Kasus: Kejaksaan Negeri Rangkasbitung)," J. KHATULISTIWA Inform., vol. 20, no. 1, pp. 1–8, 2016.
- [7] R. N. Hidayatiur, "Komputerisasi Pengolahan Data Penerimaan Peserta Didik Baru Di Smk Negeri 3 Pati Berbasis Intranet," J. Speed – Sentra Penelit. Eng. dan Edukasi, vol. 5, no. Laporan TA 2013, pp. 01–07, 2013.
- [8] A. Doyan, "Pengembangan Web Intranet Fisika Untuk Meningkatkan Penguasaan Konsep Dan Kemampuan Pemecahan Masalah Siswa Smk," *Indones. J. Phys. Educ.*, vol. 10, no. 2, pp. 117–127, 2014, doi: 10.15294/jpfi.v10i2.3447.
- [9] S. Darudiato and K. Punta, "Analisis Dan Perancangan Sistem Informasi Dengan Intranet: Studi Kasus Persediaan Material Pt Balfour Beatty Sakti Indonesia," *CommIT (Communication Inf. Technol. J.*, vol. 1, no. 1, p. 95, 2007, doi: 10.21512/commit.v1i1.471.
- [10] D. Wahyuni and S. Hadi, "Pengembangan Aplikasi Pertukaran Pesan Berbasis Teks Melalui Jaringan Lokal (LAN) Menggunakan Microsoft Visual C ++ 6 . 0," vol. 07, 2008.
- [11] T. Tristono1) and Santi Dwi Nurhumam2), "Dalam suatu jaringan komputer, terjadi sebuah proses komunikasi antar entiti atau perangkat yang berlainan sistemnya. Entiti atau perangkat ini adalah segala sesuatu yang mampu menerima dan mengirim. Untuk berkomunikasi mengirim dan menerima antara dua en," vol. 14, pp. 42– 49, 2013.
- [12] Munarso and Suryono, "Menggunakan Mikrokontroler Dan Jaringan Wifi," *Youngster Physic J.*, vol. 3, no. 3, pp. 249–256, 2014.
- [13] M. Sumolang, "Peranan Internet Terhadap Generasi Muda Di Desa Tounelet Kecamatan Langowan Barat," J. TEKNOIF, vol. 3, no. 2, p. 19, 2013, doi: 2338-2724.
- [14] E. Hariningsih, "Internet Advertising Sebagai Media Komunikasi Pemasaran Interaktif," *Jbma*, vol. I, no. 2, pp. 12–16, 2013.
- [15] M. Ahmia and H. Belbachir, "p, q-Analogue of a linear transformation preserving log-convexity," *Indian J. Pure Appl. Math.*, vol. 49, no. 3, pp. 549–557, 2018, doi: 10.1007/s13226-018-0284-5.
- [16] H. Kuswanto, "Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP," *Paradigma*, vol. 19, no. 1, pp. 46–51, 2017.
- [17] I. K. S. Satwika, "Analisis Quality of Service Jaringan Virtual Private Network (Vpn) Di Stmik Stikom

Indonesia," J. Ilm. Inform., vol. 7, no. 01, p. 60, 2019, doi: 10.33884/jif.v7i01.1016.

- [18] N. Lizarti, "Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN) Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN) Wirta Agustin," no. June 2015, 2018.
- [19] W. Stallings, "Komunikasi Data dan Komputer Dasardasar komunikasi data," no. April, p. 444, 2001.
- [20] K. A. P., D. K. A. S. S. M. S., and G. S. S. S. T. M. C., "Pengembangan E-Modul Berbantuan Simulasi Berorientasi Pemecahan Masalah Pada Mata Pelajaran Komunikasi Data (Studi Kasus: Siswa Kelas XI TKJ SMK Negeri 3 Singaraja)," *Kumpul. Artik. Mhs. Pendidik. Tek. Inform.*, vol. 6, no. 1, p. 40, 2017, doi: 10.23887/karmapati.v6i1.9267.
- [21] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," J. Teknol. Inf. Indones., vol. 2, no. 2, pp. 18–24, 2019, doi: 10.30869/jtii.v2i2.312.
- [22] S. Teknologi, A. Pengendalian, U. Port, O. S. Keaman, and R. Muzawi, "SATIN – Sains dan Teknologi Informasi Aplikasi Pengendalian Port dengan Utilitas Port Knocking untuk," no. January, 2018.
- [23] Muntahanah, Y. Darnita, and R. Toyib, "Paper Block Akses Browsing Menggunakan Mikrotik Rb 751U-2Hnd Dengan Schedule Time (Studi Kasus: Disnakerpora Kota Bengkulu)," J. Sist., vol. 7, no. 2, pp. 64–77, 2018.
- [24] D. Adhi Laksono, "Desain dan Implementasi Firewall dengan Layer 7 Filter Pada Jaringan Teknik Elektro," *Semin. TA*, vol. 2, no. Jaringan Komputer, pp. 1–7, 2012.