BAB 3
ANALISIS DAN PERANCANGAN SISTEM

3.1. Analisis Sistem

Analisis ini merupakan suatu tindakan untuk mengetahui lebih jauh tentang obyek yang akan diteliti. Bab ini akan menguraikan proses analisis perancangan dan implementasi *Unified Threat Management (UTM) Firewall* berbasisa *Linux* ini sebagai sistem keamanan jaringan di DPRD Provinsi Jawa Barat. Sebelum dilakukan perancangan dan pembangunan sistem, terlebih dahulu dilaksanakan analisis kebutuhan pokok sistem yang akan dibangun.

Analisis sistem merupakan suatu tahapan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem. Selain itu, bertujuan untuk mendapatkan pemahaman secara keseluruhan tentang sistem yang akan dibangun berdasarkan masukan dari pihak-pihak luar dan juga pengalaman analisis yang berkepentingan dengan sistem tersebut.

3.1.1. Analisis Masalah

Penelitian dalam tugas akhir ini adalah menganalisis data sistem yang berjalan, data ancaman serangan yang terjadi di DPRD Provinsi Jawa Barat dengan seluruh sistem jaringan yang ada imbasnya dan data perencanaan terhadap sistem yang akan dibangun. Terdapat berbagai masalah yang dirasakan oleh DPRD Provinsi Jawa Barat, diantaranya adalah ancaman serangan, sistem keamanan jaringan dan penanganan terhadap suatu ancaman serangan. Sehingga penelitian ini ditujukan untuk menangani permasalahan yang dihadapi DPRD Provinsi Jawa Barat.

3.1.1.1. Permasalahan Yang dihadapi

Pada permasalahan yang terjadinya pada sistem keamanan jaringan komputer DPRD Provinsi Jawa Barat diantaranya pada tahun 2009 terjadi beberapa kali penyerangan *deface* tarhadap halaman *Home* dan Fraksi dalam

kurun waktu yang berdekatan. Selanjutnya pada tahun 2010 terjadi ancaman serangan deface pada bagian modul agenda dan ditahun yang sama terjadi juga terjadi penyerangan *PHP Injection* dan *SQL Injection* dimana pengeksekusian *query illegal* dengan *drop database*. Kemudian pada tahun 2011 terjadi ancaman serangan *spam* dan *malware* pada *mail server*. Pada tahun antara 2012 – 2014 terjadi lagi penyerangan *deface* terhadap *web server*. Kemudian yang terakhir pada tahun 2015 terjadi sebuah penyerangan *spoofing* untuk pengakses terhadap *Database Server*. Dari pada itu sistem *control monitoring* masih belum terpusat sehingga penanggung jawab IT membutuhkan waktu yang lebih dalam maintenance dan mengevaluasi keamanan jaringan komputer.

1. *Deface* dan *DDOS*

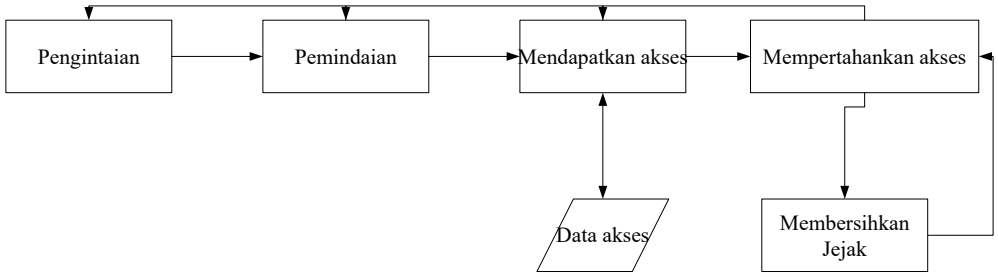
Pada tabel 3.1 ini adalah data – data ancaman *deface* terhadap *web server* DPRD Provinsi jawa yang menyababkan berubahnya *content* pada situs **drpd.jabarprov.go.id**

Tabel 3. 1 Data ancaman

Tahun	Bulan	Waktu	Penyerangan	Keteranga
2009	Januari	*Tue Jan* 20 12:20:03 UTC 2009	*Deface, DDOS*	Taget situs DPRD
	Febuari	*Mon Feb* 16 01:20:43 UTC 2009	*Deface, DDOS*	Taget situs DPRD
	April	*Tue Apr* 14 01:20:52 UTC 2009	*Deface, DDOS*	*Down* situs DPRD
	Agustus	*Sat Aug* 22 14:20:22 UTC 2009	*Deface, DDOS*	Taget situs DPRD

Tujuan utama dari penyerangan teknik *deface* pada situs **dprd.jabarprov.go.id** adalah merubah halaman *website* dengan menambahkan gambar, tulisan pada informasi agenda modul, fraksi dan *home page* pada situs DPRD Provinsi Jawa Barat tanpa sepengetahuan adminnya. Hal ini terjadi dikarenakan belum optimalnya sistem keamanan jaringan komputer dalam melindungi sebuah *server* termasuk *web server*.

Adapun tahapan ancaman penyerang bisa melakukan penyerangan terhadap suatu system melalui beberapa tahap sebagai berikut:



Gambar 3. 1 Tahapan suatu ancaman

Adapun deskripsi dari gambar 3.1 adalah sebagai berikut:

1. Tahap pengintaian

   Pada tahap ini penyerang akan mengumpukan informasi sebanyakbanyaknya tentang target yang akan diserang.
2. Pemindaian

   Setelah penyerang mendapatkan informasi target dari serangannya, maka tahap selanjutnya adalah mencari celah untuk masuk ke dalam sistem.
3. Mendapatkan akses

   Pada tahap ini terjadi proses untuk melakukan ekploitasi terhadap kesalahan implementasi dan kerentanan dari sistem komputer maupun jaringan.
4. Mempertahankan akses

   Pada tahap ini terjadi proses penguasaan terhadap sistem, dan biasanya disertai dengan proses untuk mempertahankan akses tersebut dengan cara memasang *backdoor*, *rootkit*, atau *trojan*.
5. Membersihkan jejak

   Pada tahap ini penyerang akan membersihkan jejak dengan cara memanipulasi atau menghapus bukti yang terdapat pada catatan atau *log system* atau *Instruction Prevention System*

Kerentanan pada *Web*site **http://dprd.jabarprov.go.id** disebabkan beberapa hal, yaitu kerentanan dari program *Web server* (*IIS* atau *Apache*), kerentanan dari sistem operasi yang digunakan, dan kerentanan dari kode program yang digunakan untuk membangun halaman *web*. Apabila kerentanan sudah diketahui, maka *penyerang* akan mengexploitasi kerentanan tersebut untuk mendapatkan hak akses sebagai *root* atau *administrator* dari sistem.

2. *SQL Injection* dan *PHP Injection*

Pada tabel 3.2 adalah penyerangan *PHP Injectian* dan *SQL Injection* diketahui dan berhasil direkam pada *system log.* Hal tersebut terjadi disebabkan karena staff IT DPRD Provinsi Jawa Barat belum melakukan *upgrade* pada bahasa pemograman *PHP* yang saat itu versi 5.0 dimana sudah diketahui kelemahan pada versi tersebut. Akibat dari penyerangan tersebut adalah terjadinya pengeksekusian *query drop* pada *database server* dimana *database server* tersebut juga mempunyai sistem keamanan yang optimal.

Tabel 3. 2 Data acamanan *SQL Injection*

Tahun	Bulan	Waktu	Penyerangan	Keterangan
2009	Febuari	*Wed Feb* 18 09:20:35 UTC 2009	*Sql Injection*	Celah pada *form* situs DPRD
2010	Juni	1. *Thu Jun* 22 15:20:00 UTC 2. *Tue Jun* 24 15:42:03 UTC 2010	*PHP Injection* dan *Sql Injection*	*bug* pada situs DPRD
2011	April	*Mon Apr* 10 15:20:03 UTC 2011	*PHP Injection*	*bug* pada situs DPRD
	Mei	*Sun May* 11 11:20:03 UTC 2011	*SQL Injection*	*Database Server*
	Oktober	*Sun Oct* 16 15:20:03 UTC 2011	*Php Injection*	*bug* pada situs DPRD
	November	*Sun Nov* 20 15:20:03 UTC 2011	*SQL Injection*	*Database Server*

2012	Juni	*Sat Jun* 16 18:20:03 UTC 2012	*SQL Injection*	*Database Server*

3. *Virus*

Data – data yang berhasil direkam terkait penyeberan virus komputer yang biasanya terjadi di komputer *client* pada jaringan DPRD Provinsi Jawa Barat terdapat pada penjelasan tabel 3.3 berikut ini.

Tabel 3. 3 Data Ancaman *Virus*

No	Nama Virus	*Type*
1	*Autoexe.bat*	*Direct action virus*
2	*Recycle Bin*	*Virus*
3	*Exploria.bat*	*Virus*
4	*Reva.vbs*	*Virus*
5	*Trojan*	*Virus*
6	*Discusx.vbs*	*Virus*
7	*Trile*	*Worm*
8	*Sality.exe*	*Virus*
9	*Win32*	*Virus*
10	*Autorun.gen*	*Virus*
11	*PSWBugbear.B*	*Worm*
12	*Lovgate.F*	*Worm*
13	*Trile.C*	*Worm*
15	*Sobig.D*	*Worm*
16	*Relax*	*Virus*
17	*Melissa.A*	*Virus*
18	*Bablas*	*Virus*
19	*O97M/Y2K*	*Virus*
20	*Virus Bagle.BC*	*Virus*
21	*Backdoor Alnica*	*Virus*
22	*Virus: Trojan.Lodear*	*Virus*

23	*W32.Beagle.CO@mm*	*Virus*
24	*Backdoor.Zagaban*	*Virus*
25	W32/Netsky-P	*Virus*
26	W32/Mytob-GH	*Virus*
27	W32/Mytob-EX	*Virus*
28	W32/Mytob-AS, Mytob-BE, Mytob-C, and Mytob-ER	*Virus*
29	Zafi-D	*Virus*
30	W32/Netsky-D	*Virus*
31	Storm Worm	*Virus*
32	Blaster	*Virus*
33	Nachi	*Virus*

Pada tabel 3.3 yang diambil dari salah satu *client* staff bagian umum dan administrasi terdapat sebuah komputer *client* yang terinfeksi salah satu *virus* dengan menggunakan antivirus *AVG, Avira* dan *Smadav*.

4. *Spam*

Dalam beberapa kejadian email *spam* tersebut berisi sebuah *malware* dengan menggunakan konten *advertising*. Mengirim *email* menggunakan alamat *email* sangat dimungkinkan karena protokol SMTP (*Simple Mail Transfer Protocol*) yang digunakan dalam pertukaran email tidak pernah memverifikasi alamat *email* dengan alamat *IP Address* dimana user bebas mengirim *email* dari manapun dengan menggunakan alamat email siapapun. Berikut ini data – data ancaman spam yang dijelaskan pada tabel 3.4.

Tabel 3. 4 Data Ancaman *Mail Spam*

Tahun	Bulan	Waktu	Penyerangan
2009	Juni	*Wed Jun* 18 09:20:35 UTC 2009	*Mail Server*
	November	*Wed Nov* 18 09:20:35 UTC 2009	*Mail Server*
2010	Junuari	1. *Thu Jun* 22 15:20:00 UTC 2. *Tue Jun* 24 15:42:03 UTC 2010	*Mail Server*
	Mei	*Mon May* 17 13:50:52 UTC 2010	*Mail Server*
2011	April	*Mon Apr* 10 15:20:03 UTC 2011	*Mail Server*
	Mei	*Sun May* 11 11:20:03 UTC 2011	*Mail Server*
	Oktober	*Sun Oct* 16 15:20:03 UTC 2011	*Mail Server*
	November	*Sun Nov* 20 15:20:03 UTC 2011	*Mail Server*
2012	Mei	*Sat Jun* 16 18:20:03 UTC 2012	*Mail Server*
	Desember	*Wed Des* 12 12:20:13 UTC 2012	*Mail Server*
2013	Januari	*Thu Jan* 19 11:20:23 UTC 2013	*Mail Server*
	Juli	*sun Jul* 15 15:20:03 UTC 2013	*Mail Server*
	September	*Sat Sep* 22 15:20:03 UTC 2013	*Mail Server*
	Desember	*Thu Des* 20 15:20:03 UTC 2013	*Mail Server*
2015	September	*Mon Sept* 21 17:20:03 UTC 2015	*Mail Server*

Adapun data *email spam* yang diambil dari *mail server* yang termuat pada penjelasan tabel 3.5 berikut ini.

Tabel 3. 5 Data *Spam Mail*

No	Keyword Spam	Keterangan
1	*Event*	*Spam*
2	*Discount* Produk	*Spam*
3	Promo	*Spam* iklan baris
4	Kesempatan Kerja	*Spam* surat elektronik
5	Kesempatan Kuliah Luar Negeri	*Spam web*
6	*Spam blog*	*Spam blog*

7	*Flash Sell*	*Spam* jejaring sosial
8	Iklan Jasa	*Spam web*
9	Konsultasi	*Spam messangger*
10	*Junk mail*	*Spam wiki*
11	*Non commercial spam*	*Spam newgroup*
12	*Virus spam*	*Spam blog*

Bentuk *spam* yang terjadi di mail server DPRD Provinsi Jawa Barat adalah *spam* surat elektronik, *spam* pesan instan, *spam newsgroup*, *spam* mesin pencari informasi *Web* (*Web* search engine *spam*), *spam* blog, *spam* wiki, *spam* iklan baris daring, *spam* jejaring sosial.

5. *Malware*

Aksi yang dilakukan *malware* pada jaringn DPRD Provinsi Jawa barat disebut *Direct Action*. Pada tabel 3.6 ini adalah data – data virus yang terjadi pada jaringan komputer *client* di DPRD Provinsi Jawa Barat.

Tabel 3. 6 Data Ancaman *Malware*

No	Type Malware	Keterangan
1	*Virus*	*Win32/sality* *Win32/virut* *Win32/alman* *Trojan.Loader*
2	*Worm*	*ADMw0rm* *Win32/autoit*
3	*Troujan House*	*Win-trojan/SubSeven* *Win-trojan/Back Orifice* *Win-trojan/Ecokys* *Win32/sirefef*
5	*Keyloger*	*Keyloger*
6	*Adware*	*Win32/adware. registrycleanfix* *Win32/adware.mycentria* *Win32/adware.threatnuker*

7	*Wabbit*	*Wabbit*
8	*Spyware*	*Spyaxe*
9	*Backdoor*	*Menyerupai Troujan dan Worm*
10	*Rookit dan Exploit*	*DDos dan Spoofing*

6. *Spoofing*

Pada beriktu ini merupakan data - data penyerangan *spoofing* dengan jenis *identity Spoofing*. Penyebab penyerangan tersebut berawal dari pegawai DPRD yang lalai dalam menggunakan jaringan komputer, sehingga disalah gunakan oleh user tertentu dengan tujuan perubahan *configuration* pada jaringan tersebut serta akses ke beberapa *server*. Pada penjelasan tabel 3.7 ini terdapat beberapa data informasi penyerangan dengan *type spoofing* dan *exploit*

Tabel 3. 7 Data Ancaman *Spoofing* dan *Eksploitas*

Tahun	**Bulan**	**Waktu**	**Penyerangan**
2010	Agustus	Wed Aug 11 17:20:03 UTC 2010	*Spoofing Exploit*
	November	sun Nov 21 16:23:03 UTC 2010	*Spoofing Exploit*
2012	Janari	sun Jan 15 12:20:03 UTC 2012	*Spoofing Exploit*
	Maret	sun Mar 11 12:20:03 UTC 2012	*Spoofing Exploit*
	Oktober	wed Oct 17 15:20:03 UTC 2012	*Spoofing Exploit*
2013	Maret	Fri Mar 10 15:20:03 UTC 2013	*Spoofing Exploit*
	April	sun Apr 16 15:20:03 UTC 2013	*Spoofing Exploit*

Penyerangan dengan tipe *spoofing* jelas mempunyai target yaitu *server* maupun *management jaringan* yang dimana terdapat informasi yang menguntungkan pihak penyerang. Peranan orang dalam dalam sebuah instansi sangatlah penting terhadap penyerangan ini. Ini yang terjadi pada jaringan komputer DPRD provinsi jawa barat dimana ada keterlibatan pihak dalam terhadap penyerangan ini. Pada tabel 3.8 berikut ini adalah target utama dari penyerangan ini.

Tabel 3. 8 Data Ancaman *Spoofing*

No	Target Spoofing	Keterangan
1	*Database Server*	mengakses *database* anggaran keuangan
2	*Router Mikrotik*	Perubahan pada konfigurasi *Bandwidth*

Pada kasus *spoofing* pada jaringan DPRD Provinsi Jawa Barat melibatkan orang dalam yang mempunyai kepentingan pada tindakan ini seperti keinginan mengakses server untuk melihat dan mengambil data tesebut.

7. *Content Filtering*

Beberapa data kategori *content* berikut yang masuk kedalam *content filtering* adalah pada tabel 3.9 berikut ini.

Tabel 3. 9 *Content Filtering*

No	Content	Keterangan
1	Pornografi	Tindakan yang dilakukan dengan *Drop Action*
2	Perjudian	Tindakan yang dilakukan *Drop Action*
3	Narkoba	Tindakan yang dilakukan *Drop*

		Action
4	Kekersan	Tindakan yang dilakukan *Drop Action*
5	Rasisme	Tindakan yang dilakukan *Drop Action*
6	*Malware*	Tindakan yang dilakukan *Drop Action*
7	*Spyware*	Tindakan yang dilakukan *Drop Action*
8	*Phising*	*Drop Action*

8. *Centre control management*

Dalam menangi permasalahan maupun melakukan perubahan pada sistem jaringan komputer dibutuhkanya sistem *Centralized controlling* atau kontrol terpusat terhadap sistem jaringan sangat Hal ini dikarena dengan adanya Sistem Kontrol terpusat ini bagian Penanggung Jawab IT bisa lebih menyederhanakan prosedur dalam hal monitoring dan maintenance terhadap perubahan dan keamanan jaringan.

3.1.1.2. Pemecahan Masalah yang diusulkan

Dari permasalahan – permasalaan yang sudah dijelaskan sebelumnya, maka salah satu solusi sistem teknologi yang bisa mengatasi malasah tersebut adalah dengan menggunakan sistem keamanan jaringan *Unified Threat Management (UTM) Firewall* berbasis *Linux.* Pada sistem keamanan *Firewall* sebelumnya akan dengan cepat menjadi usang di dalam era *Internet* saat ini di mana banyak aplikasi mengirim atau menerima yang menyebabkan lalu lintas data lebih sibuk dari *Port* yang biasanya diperbolehkan oleh t*raditional Firewall* [1].

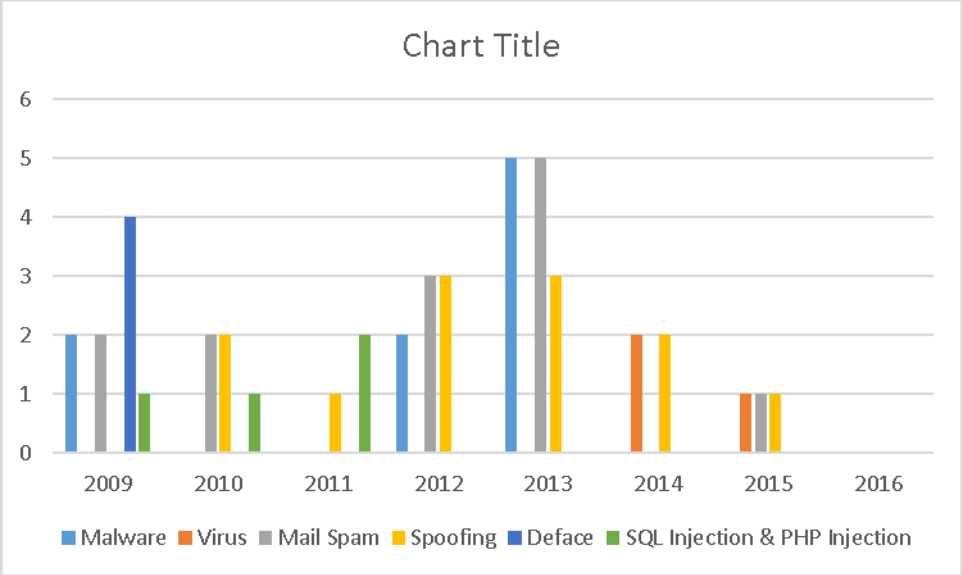
Sistem keamanan jaringan *Unified Threat Management* (UTM) *Firewall* berbasis *Linux* ini mempunyai keunggulan dimana tidak hanya bisa melakukan satu fungsi keamanan saja tetapi memiliki lebih dari satu fungsi keamanan

jaringan yang lainya dan sesuai dengan permasalahan keamanan jaringan yang terjadi pada DPRD Provinsi Jawa Barat dimana terjadi ancaman serangan dengan berbagai macam type ancaman serangan seperti *deface*, *PHP Injection, Sql Injection, spam*, *malware* dan *spoofing* serta membutuhkan sistem keamana jaringan yang terpisah dari router mikrotik yang saat ini difungsikan salah satunya sebagai sistem keamanan jaringan sehingga membebankan kinerja pada router mikrotik tersebut.

Unified Threat Management (UTM) *Firewall* adalah Sistem keamanan jaringan yang sebelumya pengembangan dari sistem keamanan *traditional Firewall* dimana berfungsi hanya bisa melakukan perizinan lalu lintas sebuah *packet data* yang dianggap aman dan mencegah lalu lintas jaringan yang dianggap tidak aman. Sistem keamanan tersebut *Unified Threat Management* (UTM) *Firewall* merupakah sebuah *modern Firewall* yang didalamnya berfungsi tidak hanya membuka dan menutup lalu lintas terhadap keamanan *packet data* tetapi mempunyai fungsi lain didalamnya sebagai *Instruction Detection / Prevention System*, *Anti-spam, Web content filter*, *Anti-virus* dan *Virtual Private Network* (*VPN*) dengan *management control monitoring centralize system* atau sistem manajemen kontrol monitoring terpusat [1].

3.1.1.3. Grafik ancaman serangan

Gambar 3.2 adalah data grafik ancaman yang telah terjadi di sistem jaringan DPRD Provinsi jawa barat dari tahun 2009 sampai 2010



Gambar 3. 2Grafik Ancaman

Pada gambar grafik ancaman tersebut, ancaman *mail spam* tertinggi terjadi pada tahun 2013 dimana ancaman *deface* juga tertinggi pada tahun 2013 tersebut. *mail server* dari tahun 2009 sampai 2015 selalu terjadi ancaman.

3.1.1.4. Perbandingan penangan ancaman serangan

Adapun perbandingan antara tujuan ancamanan serangan dan penanganan ancamanan serangan adalah pada tabel 3.10 berikut ini.

Tabel 3. 10 Perbandingan Ancaman

No	Ancaman Serangan	Tujuan Serangan	Penangan Ancaman Serangan
1	*Deface*	Merubah dan mengganti content *Web*site	*Firewall, Upgrade Source Code Website*
2	SQL Injection	Mendapatkan data dari *Database Server*	*Web Aplikasi Firewall*
3	*Virus*	Mendapatkan dan mengirimkan informasi ke sekelompok indivu dari sistem yang	*Anti Virus*

		sudah terinfeksi	
4	*Spam*	*Phising*	*IPS, Firewall*
5	*Malware*	Mencari kelemahan sistem	*IPS, Firewall, Conten Filtering*
6	*Spoofing*	Mendapatkan hak akses ke jaringan	*Firewall, VPN*

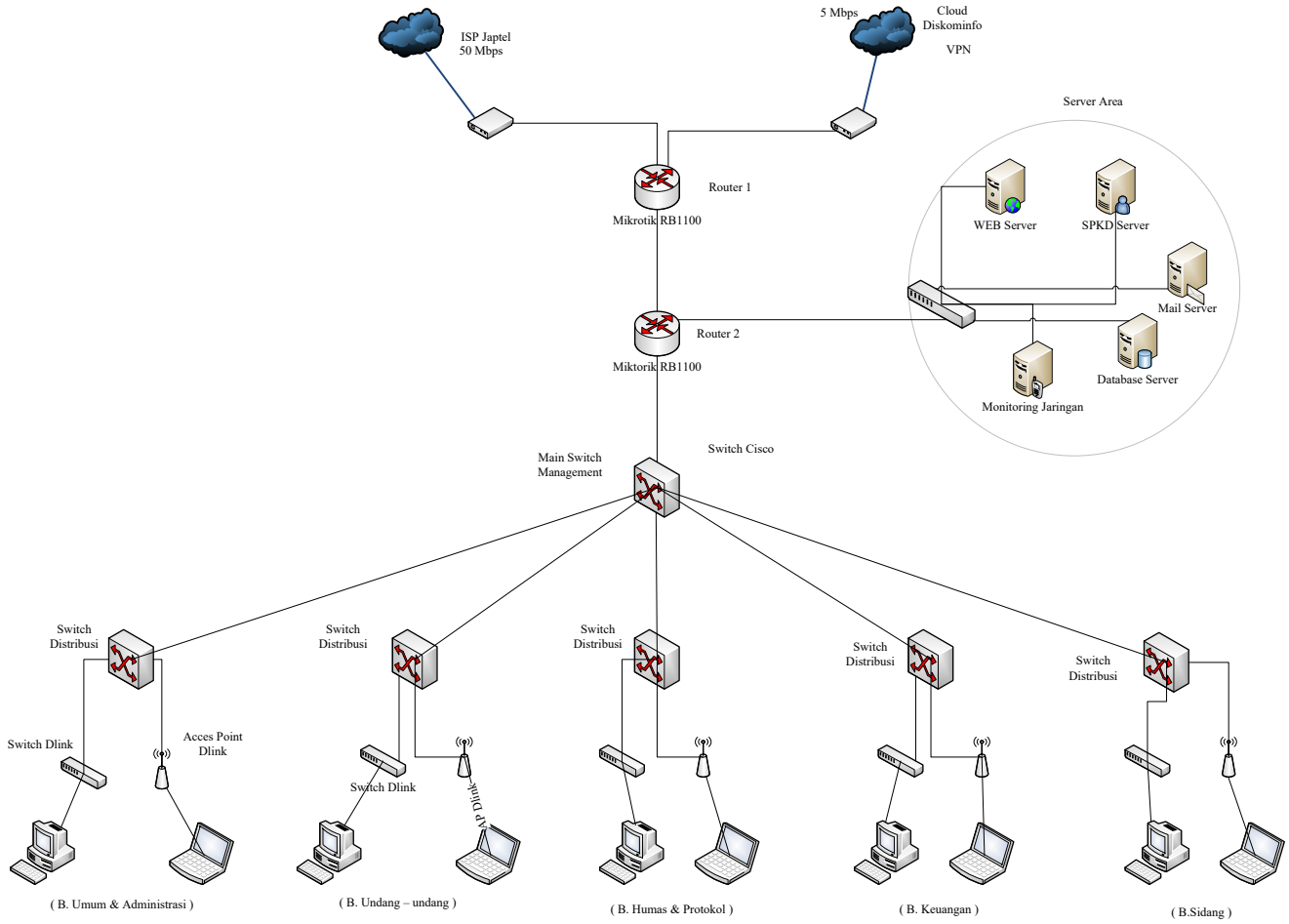
3.1.2. Sistem yang berjalan

Analisis sistem berjalanan dilakukan untuk mengetahui berapa banyak *user* yang terlibat dalam jaringan komputer, bagaimana skema jaringan komputer yang diterapkan, bagaimana penerapan sistem keamanan jaringan yang berjalan, bagaimana spesifikasi *hardware* untuk terhadap keamanan jaringan yang berjalan dan apa saja data yang tersebar ke unit- unit kerja.

3.1.2.1. Analisis Skema Jaringan Komputer yang berjalan

Saat ini DPRD Provinsi Jawa Barat telah menerapkan jaringan komputer Local *Area Network* (LAN) dengan topologi *extended star* dan bertipe *client – server* dimana *client* berperan sebagai perangkat yang menerima yang akan menampilkan dan menjalankan aplikasi dan *server* sebagai perangkat yang menyediakan dan bertindak sebagai pengelola aplikasi, data, dan keamanannya. Pada keberjalanannya sistem keamanan jaringan yang dilakukan oleh staff IT untuk penanganan dan pencegahan terhadap ancaman serangan dilakukan dengan melalui cara yaitu melalui sistem keamanan *Firewall* pada *Mikrotik Router OS.*

Gambar 3.3 berikut adalah skema jaringan komputer *Local Area Network* (LAN) yang berada di DPRD Provinsi Jawa Barat:

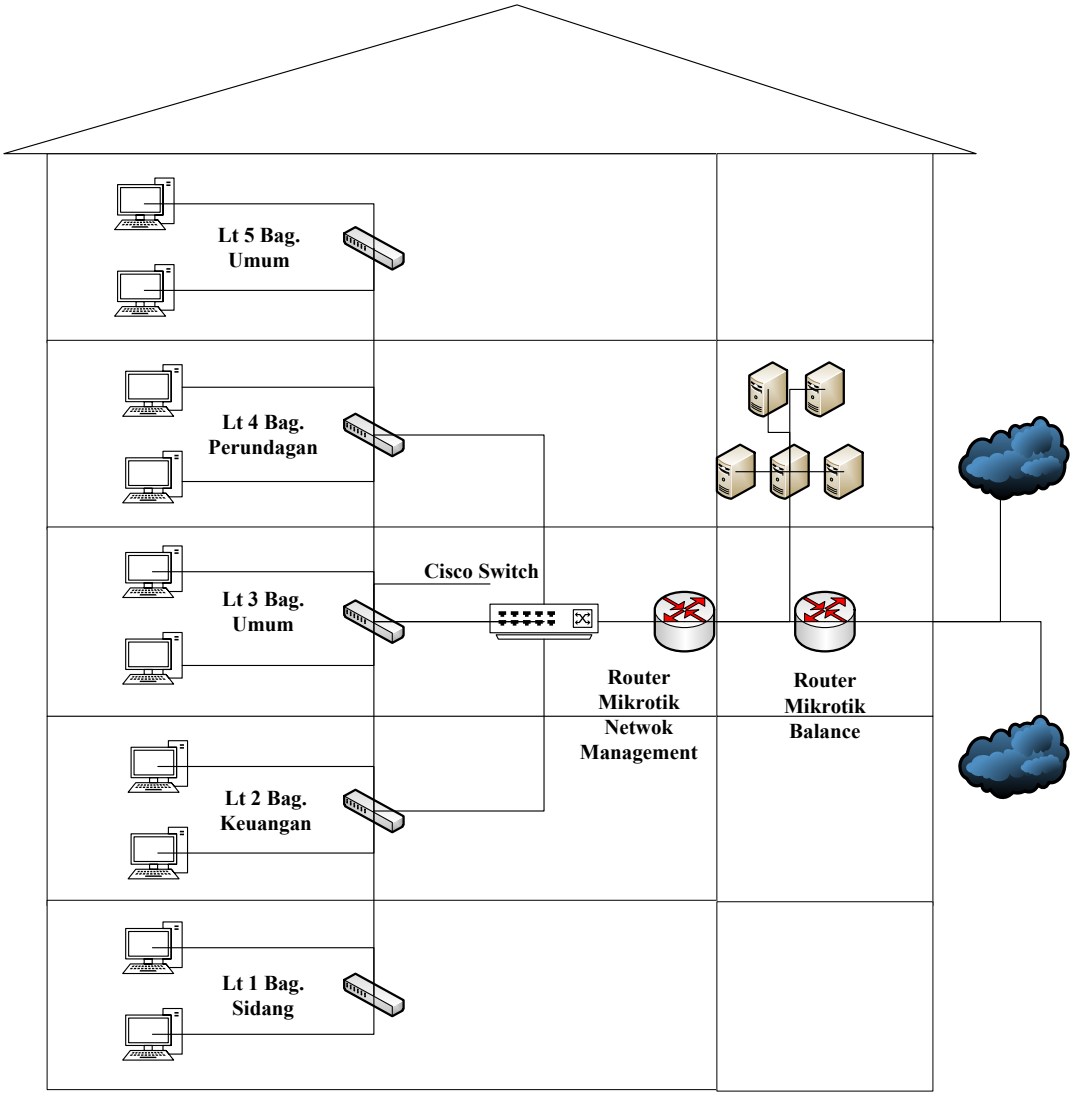


Gambar 3. 3 Topologi Jaringan

Keterangan :

1. *Router* pertama berfungsi sebagai *firewall* dan *load balancing*
2. *Router* kedua berfungsi sebagai *management network*
3. *Switch cisco catalys* berfungsi sebagai *management vlan*
4. *Packet data* yang masuk dari luar jaringan (*internet*) melewati *router* yang berfungsi sebagai firewall untuk filtering
5. *Packet data* dari jaringan local ke jaringan luar (internet) harus melewati router yang berfungsi sebagai firewall untuk filtering.

Adapun design sistem jaringan komputer DPRD Provinsi Jawa Barat yang diterapkan dengan insfrastruktur gedung itu sendiri, terdapat pada gambar 3.4 berikut ini.



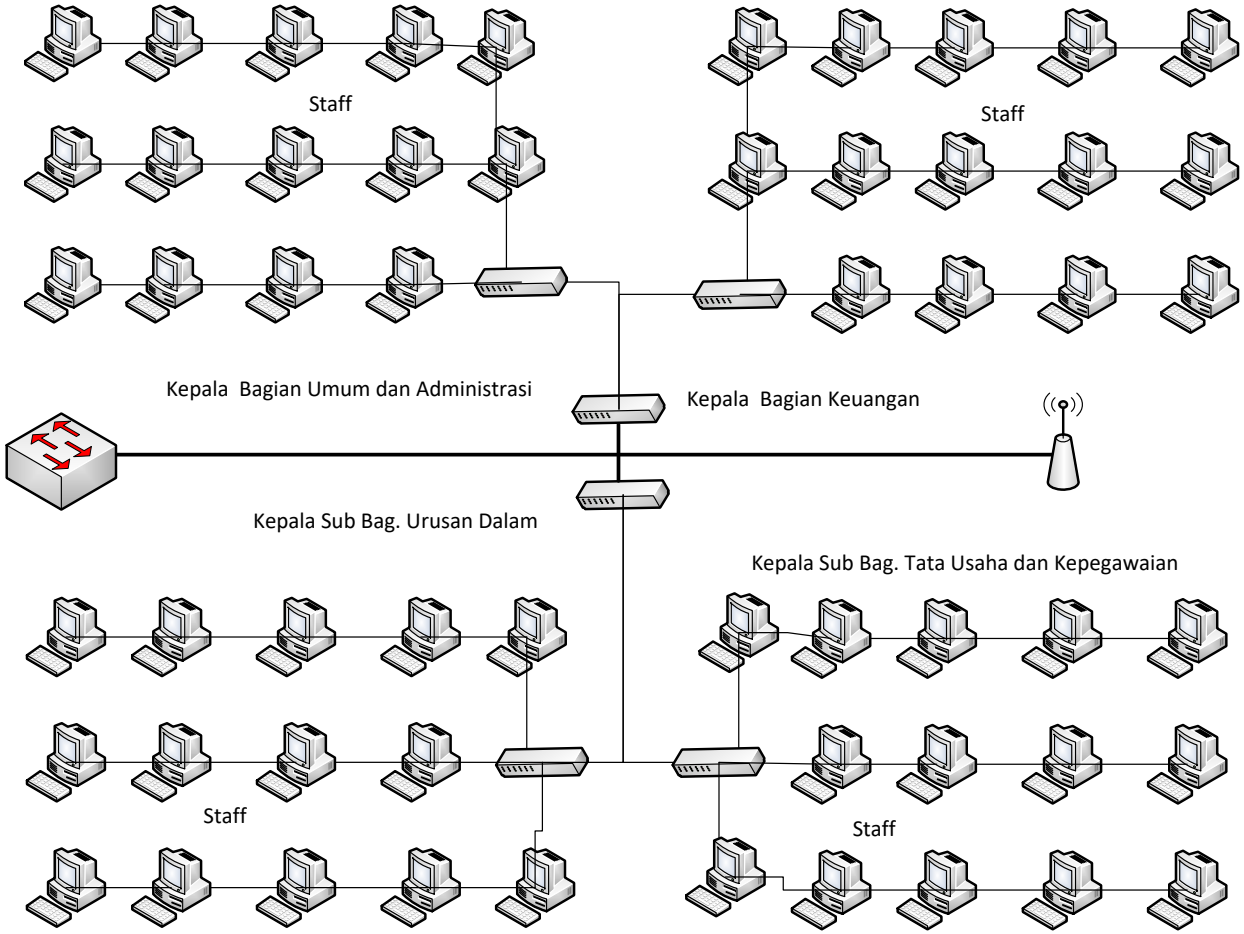
Gambar *3. 4* Insfrastruktur dan Jaringan DPRD

Keterangan :

1. Jumlah lantai dalam gedung insfrastruktur DPRD Provinsi Jawa Barat adalah 5 Lantai
2. *Ruangan Server – server* yang dimiliki oleh sistem jaringan ini terdapat pada lantai 3 disamping Bagian Umum dan administrasi
3. *Vlan* digunakan untuk mempermudah dalam membedakan setiap beda bagian staff

A. Topology Bagian Umum dan Administrasi

Pada gambar Berikut 3.5 ini adalah gambaran *topology* jaringan komputer pada bagian Umum dan administrasi beserta *IP Address* yang digunakan pada bagian ini.



Gambar 3. 5 Topologi Bag. Umum dan Administrasi

Berdasarkan informasi yang didapat, maka dapat disimpulkan bahwa topologi jaringan yang terdapat di staff bagian umum dan administrasi terdiri dari dua jaringan yang di bedakan berdasarkan media nirkabel dan kabel. Adapun *IP Address* pada bagian umum dan administrasi yang sedang berjalan pada tabel 3.11 berikut ini.

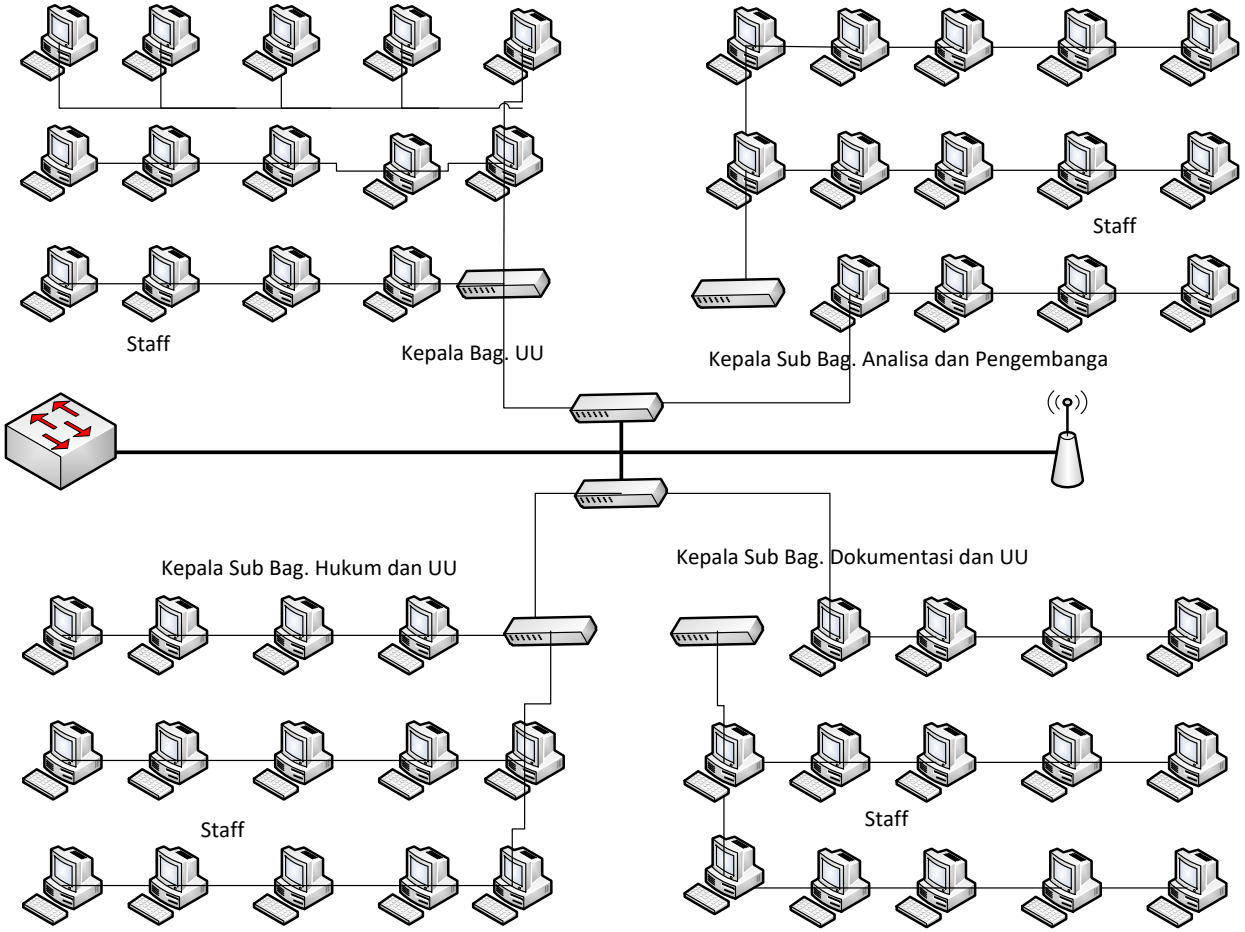
Tabel 3. 11 *IP Address* Bag. Umum dan Administrasi

No	TCP/IP		Keterangan
1	*IP Address*	: 217.10.1.0/24	*Vlan 10*
2	*Subnet*	: 255.255.255.0	
3	*Gateway*	: 200.10.1.2	
4	*DNS*	: 8.8.8.8	

Pada staff bagian umum dan administrasi mempunyai *client* tetap sebanyak 50 *user*. *User* ini termasuk kepala bagian umum dan administrasi hingga bagian staff. Pengalokasian *IP Address* pada bagian ini sebanyak 254 *IP Address*. Hal ini dikarena untuk sebagai cadangan *IP Address* terhadap user yang mempunyai gadget seperti *laptop*, tab dan *smartphone* yang terhubung kedalam jaringan DPRD Provinsi Jawa Barat.

B. Topology Bagian Undang – Undang.

Pada gambar 3.6 Berikut ini adalah gambaran topology jaringan komputer pada bagian Undang- undang beserta *IP Address* yang digunakan pada bagian ini.



Gambar 3. 6 Topologi Bag. Hukum dan Undang - Undang

Berdasarkan informasi yang didapat, maka dapat disimpulkan bahwa topologi jaringan yang terdapat di staff bagian Undang - undang terdiri dari dua jaringan yang di bedakan berdasarkan media nirkabel dan kabel. Adapun *IP Address* pada bagian umum dan administrasi yang sedang berjalan pada tabel 3.11 berikut ini.

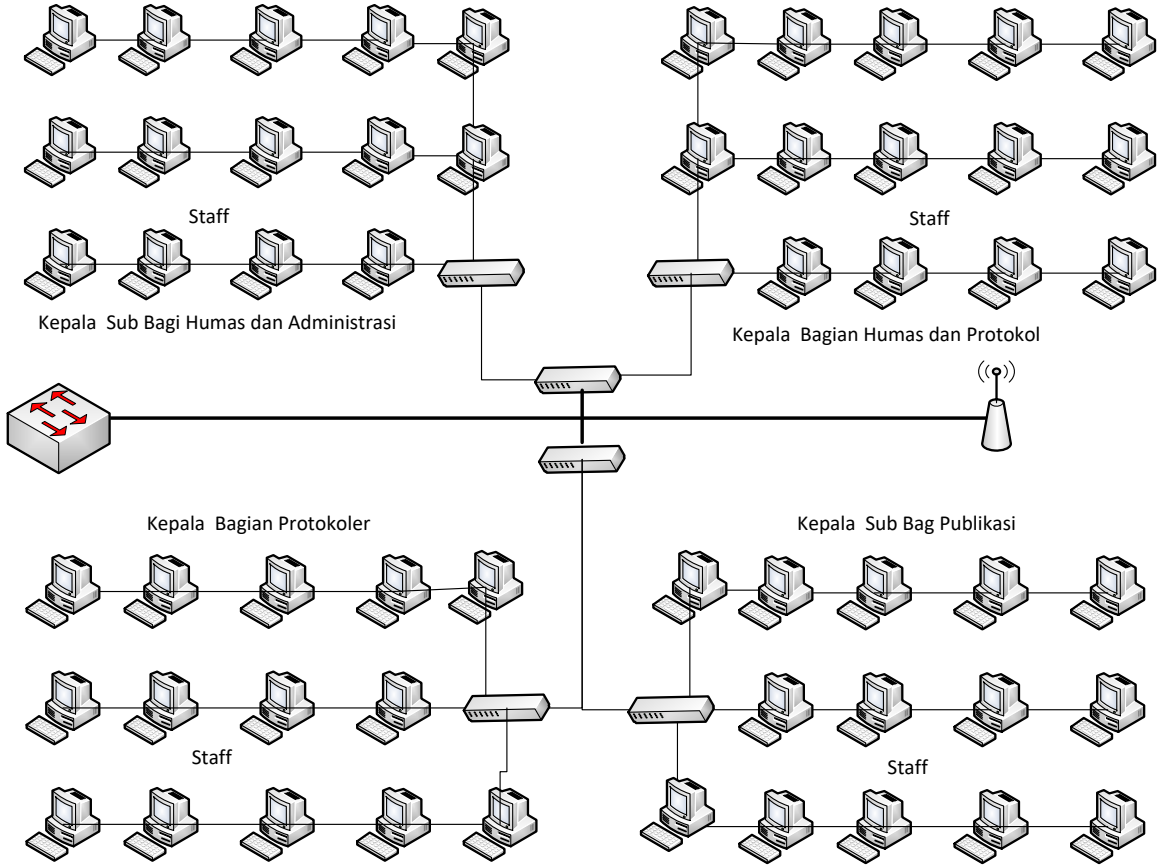
Tabel 3. 12 *IP Address* Bag. Hukum dan Undang - Undangan

No	TCP/IP		Keterangan
1	*IP Address*	: 217.10.2.0/24	*Vlan 20*
2	*Subnet*	: 255.255.255.0	
3	*Gateway*	: 200.10.1.2	
4	*DNS*	: 8.8.8.8	

Pada staff bagian Undang - undang mempunyai *client* tetap sebanyak 50 user. *User* ini termasuk kepala bagian umum dan administrasi hingga bagian staff. Pengalokasian *IP Address* pada bagian ini sebanyak 254 *IP Address.* Hal ini dikarena untuk sebagai cadangan *IP Address* terhadap user yang mempunyai gadget seperti *laptop*, tab dan *smartphone* yang terhubung kedalam jaringan DPRD.

C. Topology Bagian Humas dan Protokol

Pada gambar Berikut 3.7 ini adalah gambaran topology jaringan komputer pada bagian Humas dan Protokol beserta *IP Address* yang digunakan pada bagian ini.



Gambar 3. 7 Topologi Bag. Humas dan Protokol

Berdasarkan informasi yang didapat, maka dapat disimpulkan bahwa topologi jaringan yang terdapat di staff bagian humas dan protokoler terdiri dari dua jaringan yang di bedakan berdasarkan media nirkabel dan kabel. Adapun *IP Address* pada bagian umum dan administrasi yang sedang berjalan pada tabel 3.13 berikut ini.

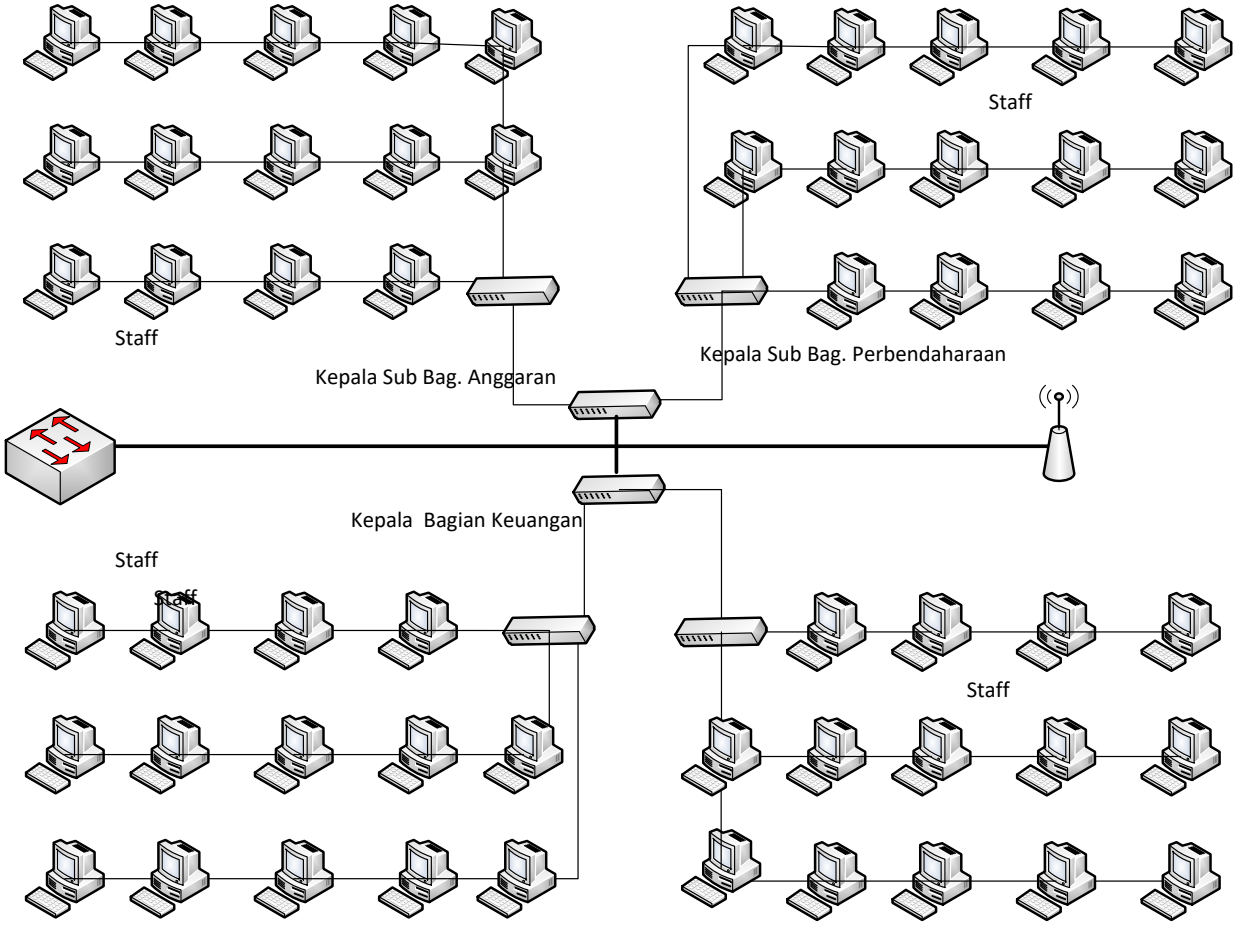
Tabel 3. 13 *IP Address* Bag. Humas dan Protokol

No	***TCP/IP***	**Keterangan**
1	*IP Address* : 217.10.3.0/24	*Vlan 30*
2	*Subnet* : 255.255.255.0	
3	*Gateway* : 200.10.1.2	
4	*DNS* : 8.8.8.8	

Pada staff bagian humas dan protokoler mempunyai *client* tetap sebanyak 50 *user*. *User* ini termasuk kepala bagian umum dan administrasi hingga bagian staff. Pengalokasian *IP Address* pada bagian ini sebanyak 254 *IP Address*. Hal ini dikarena untuk sebagai cadangan *IP Address* terhadap user yang mempunyai gadget seperti *laptop*, tab dan smartphone yang terhubung kedalam jaringan DPRD.

D. Topology Bagian Keuangan

Pada gambar 3.8 berikut ini adalah gambaran topology jaringan komputer pada bagian Keuangan beserta *IP Address* yang digunakan pada bagian ini.



Gambar 3. 8 Topologi Bag. Keuangan

Berdasarkan informasi yang didapat, maka dapat disimpulkan bahwa topologi jaringan yang terdapat di staff bagian Keuangan terdiri dari dua jaringan yang di bedakan berdasarkan media nirkabel dan kabel. Adapun *IP Address* pada bagian keuangan yang sedang berjalan pada tabel 3.14 berikut ini.

Tabel 3. 14 *IP Address* Bag. Keuangan

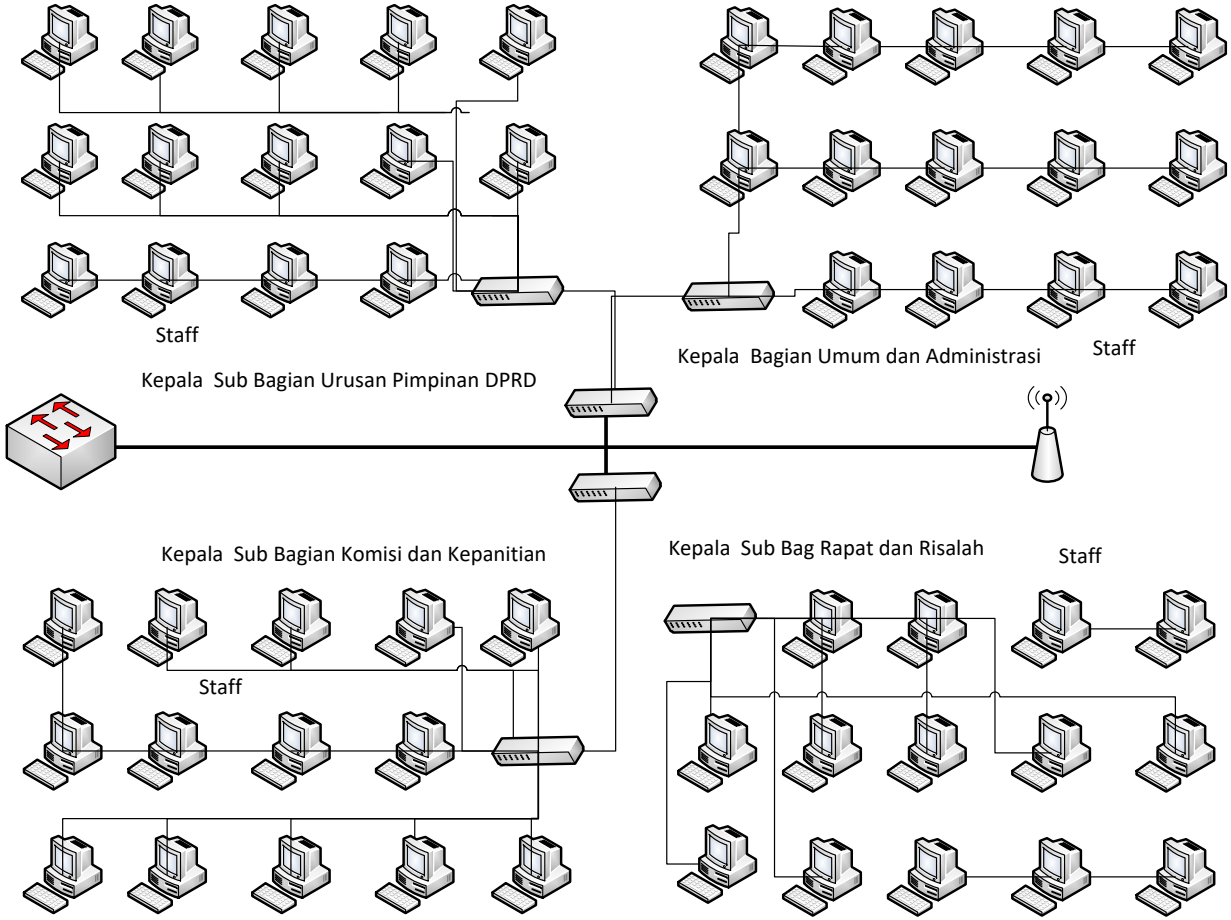
No	TCP/IP		Keterangan
1	*IP Address*	: 217.10.4.0/24	*Vlan 40*
2	*Subnet*	: 255.255.255.0	
3	*Gateway*	: 200.10.1.2	
4	*DNS*	: 8.8.8.8	

Pada staff bagian Keuangan mempunyai *client* tetap sebanyak 50 user. User ini termasuk kepala bagian Keuangan hingga bagian staff. Pengalokasian *IP Address* pada bagian ini sebanyak 254 *IP Address*. Hal ini dikarena untuk sebagai cadangan *IP Address* terhadap user yang mempunyai gadget seperti *laptop*, tab dan smartphone yang terhubung kedalam jaringan DPRD.

E. Topology Bagian Sidang

Pada gambar 3.9 berikut ini adalah gambaran topology jaringan komputer pada bagian sidang beserta *IP Address* yang digunakan pada bagian ini.

G;;;ambar 3. 9
Topologi Bag.
Sidang



Berdasarkan informasi yang didapat, maka dapat disimpulkan bahwa topologi jaringan yang terdapat di staff bagian Sidang terdiri dari dua jaringan yang di bedakan berdasarkan media nirkabel dan kabel. Adapun *IP Address* pada bagian umum dan administrasi yang sedang berjalan pada tabel 3.15 berikut ini.

Tabel 3. 15 *IP Address* Bag. Sidang

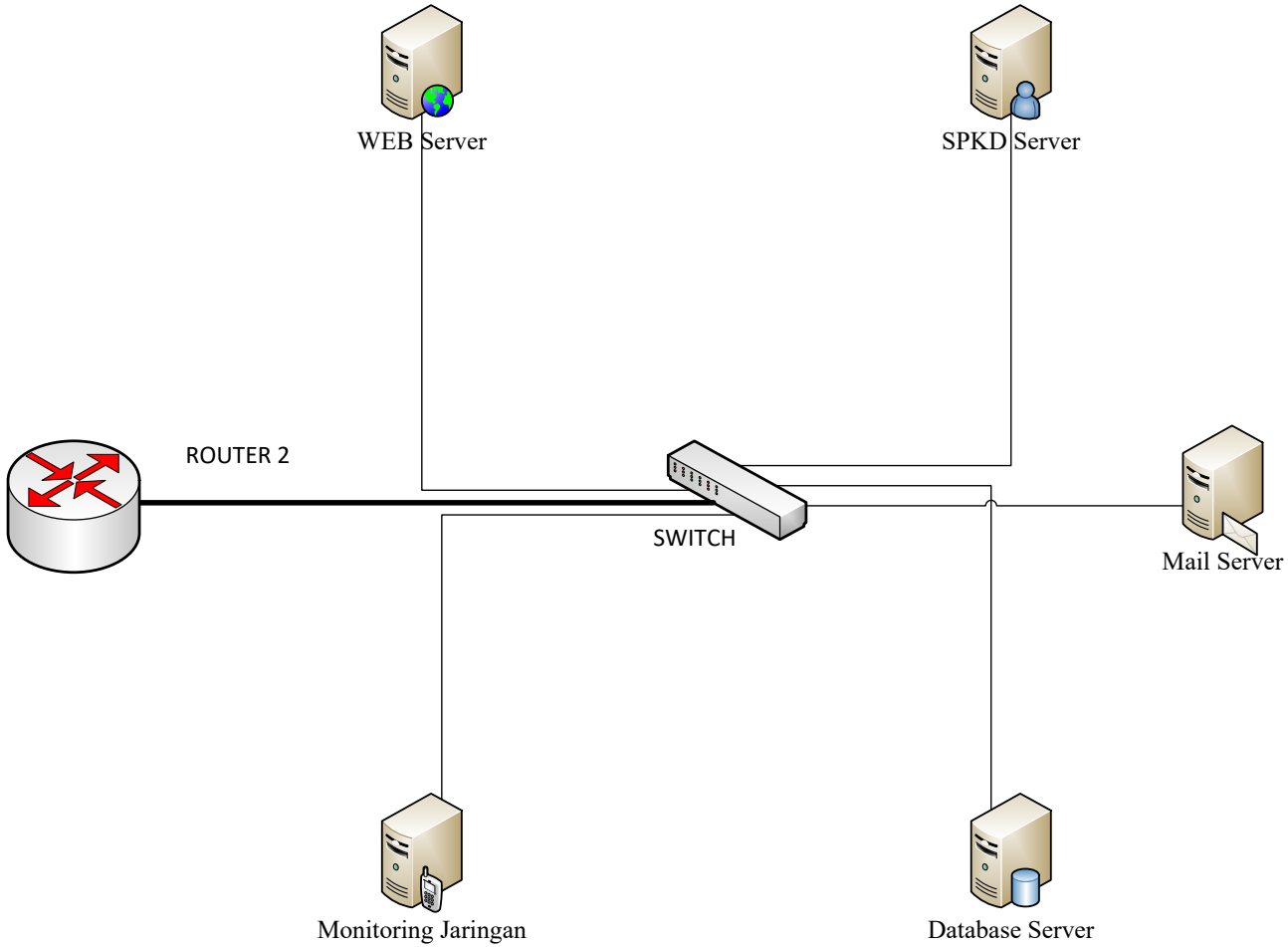
No	TCP/IP		Keterangan
1	*IP Address*	: 217.10.1.0/24	Vlan 50
2	*Subnet*	: 255.255.255.0	
3	*Gateway*	: 200.10.1.2	
4	*DNS*	: 8.8.8.8.8	

Pada staff bagian Sidang mempunyai *client* tetap sebanyak 50 user. User ini termasuk kepala bagian Sidang hingga bagian staff. Pengaloka`4sian *IP Address* pada bagian ini sebanyak 254 *IP Address*. Hal ini dikarena untuk sebagai cadangan *IP Address* terhadap user yang mempunyai ` gadget seperti *laptop*, tab dan smartphone yang terhubung kedalam jaringan DPRD.

F. Topology Bagian *Server – Server*

Pada penjelasan gambar 3.10 berikut ini adalah gambaran *topology* jaringan komputer pada bagian Ruang *server* berserta *IP Address* dan spesifikasi pada masing-masings *Server*.

.



Gambar 3. 10 Topologi Bag. *Server*

Keterangan :

1. Semua *server* pada jaringan ini berbasis *Linux*
2. Pada bagian *server* tidak menggunakan *Vlan*
3. Ruangan server hanya bisa dimasuki oleh penanggung jawab IT

Sedangkan untuk data – data *server* pada jaringan DPRD Provinsi Jawa Barat dapat dilihat pada tabel 3.16 berikut ini.

Tabel 3. 16 *IP Address* Bag. Server

No	Nama *server*	Protokol IP
1	*Web server*	*IP Address* : 200.10.3.2 *Subnetting* : 255.255.255.0 *Gateway* : 200.10.3.1 *DNS* : 8.8.8.8
2	SKPD *Server*	*IP Address* : 200.10.3.3 *Subnetting* :255.255.255.0 *Gateway* : 200.10.3.1 *DNS* : 8.8.8.8
3	Mail *server*	*IP Address* : 200.10.3.4 *Subnetting* : 255.255.255.0 *Gateway* : 200.10.3.1 *DNS* : 8.8.8.8
4	*Database server*	*IP Address* : 200.10.3.4 *Subnetting* : 255.255.255.0 *Gateway* : 200.10.3.5 *DNS* : 8.8.8.8
5	Monitoring Jaringa	*IP Address* : 200.10.3.3 *Subnetting* : 255.255.255.0 *Gateway* : 200.10.3.6 *DNS* : 8.8.8.8

Dalam sebuah sistem jaringan komputer DPRD Provinsi jawa barat ini mempunyai 5 buah seperti yaitu *Web server*, skpd *server*, *mail server*, *database*

server dan monitoring jaringan. Pengalokasian *IP Address* yang dikhususkan pada bagian *server* ini menggunakan *IP Address*. 212.121.12.0

6. *Web Server*

Fungsi utama dari *Web server* adalah untuk memindahkan berkas yang diminta oleh pengguna melalui protokol komunikasi tertentu. Oleh karena dalam satu halaman *Web* biasanya terdiri dari berbagai macam jenis berkas seperti gambar, video, teks, audio, file dan lain sebagainya, maka pemanfaatan *Web server* berfungsi juga untuk mentransfer keseluruhan aspek pemberkasan dalam halaman tersebut, termasuk teks, gambar, video, audio, file dan sebagainya pada situs dprd.jabarprov.go.id.

Adapun data – data yang kumpulkan terhadap keberjalanya sistem dijelaskan pada tabel 3.17 yaitu:

Tabel 3. 17 Data *Web Server*

No	Informasi	Keterangan
1	*Web server*	*Web Server* untuk situs **dprd.jabarprov.go.id**
2	Sistem Operasi	*Linux Redhat*

7. SKPD *Server*

Fungsi utama dari SKPD *server* adalah untuk *translate audio* hasil siding kedalam teks dokument. Adapun data – data yang kumpulkan terhadap keberjalanya sistem terdapat pada penjelasan tabe 3.18 yaitu:

Tabel 3. 18 Data SKPD *Server*

No	Informasi	Keterangan
1	*SKPD Server*	*Server* untuk *translate* hasil rapat *audio* ke dalam bentuk tulisan laporan
2	Sistem Operasi	*Linux Ubuntu*

8. Mail *server*

Fungsi utama dari *mail server* sebagai pengatur atau penerima dan penyalur respon atas email yang masuk. Adapun data – data yang kumpulkan terhadap keberjalanya sistem terdapat penjelasan pada tabel 3.19 yaitu:

Tabel 3. 19 Data *Mail Server*

No	Informasi	Keterangan
1	*Mail Server*	Sebagai email resmi dari institusi DPRD Provinsi Jawa Barat
2	Sistem Operasi	Linux Ubuntu

9. *Database server*

Fungsi utama dari *database server* sebagai penyimpanan data hasil rapat, anggaran, data administrasi. Adapun data – data yang kumpulkan terhadap keberjalanya sistem yaitu:

Tabel 3. 20 *Database Server*

No	Informasi	Keterangan
1	*Dataabase server*	Tempat pengolahan data – data seperti administrasi hingga content. *Service* yang digunakana adalah *Apache*
3	Sistem Operasi	*Linux Redhat*

10. Monitoring Jaringan

Tabel 3. 21 Data Monitoring Jaringan

No	Informasi	Keterangan
1	*Monitoring*	Ganglia
3	Sistem Operasi	*Linux Ubuntu*

3.1.2.2. Analisis Sistem keamanan yang berjalan

Saat ini sistem jaringan keamanan komputer yang diterapkan pada DPRD provinsi jawa barat adalah dengan menggunakan *Firewall* berbasis *Mikrotik OS*. Penerapan sistek keamanan jaringan *Firewall* ini di kombinasikan dengan router *mikrotik RB1100* disamping dalam manajemen sebuah jaringan. Berikut ini gambaran sistem kerja keamanan dengan *Firewall* pada DPRD jawa barat.

A. Router 1

Pada tabel 3.22 berikut ini adalah pembagian *port ethernet* dari *router mikrotik* 1 dimana terdapat empat modul *ethernet* tetapi yang digunakan hanya 3 modul *ethernet*.

Tabel 3. 22 Data *Router 1*

No	*Hardware*	*IP Address*	Keterangan
1	*Ether-1*	192.168.1.2	Modem 1
2	*Ether-2*	192.168.2.3	Modem 2
3	*Ether-3*	200.20.20.1	Router 2
4	*Ether-4*	-	-

B. Router 2

Pada tabel 3.23 berikut ini adalah pembagian *port ethernet* dari *router mikrotik* 1 dimana terdapat empat modul ethernet tetapi yang digunakan hanya 3 modul ethernet.

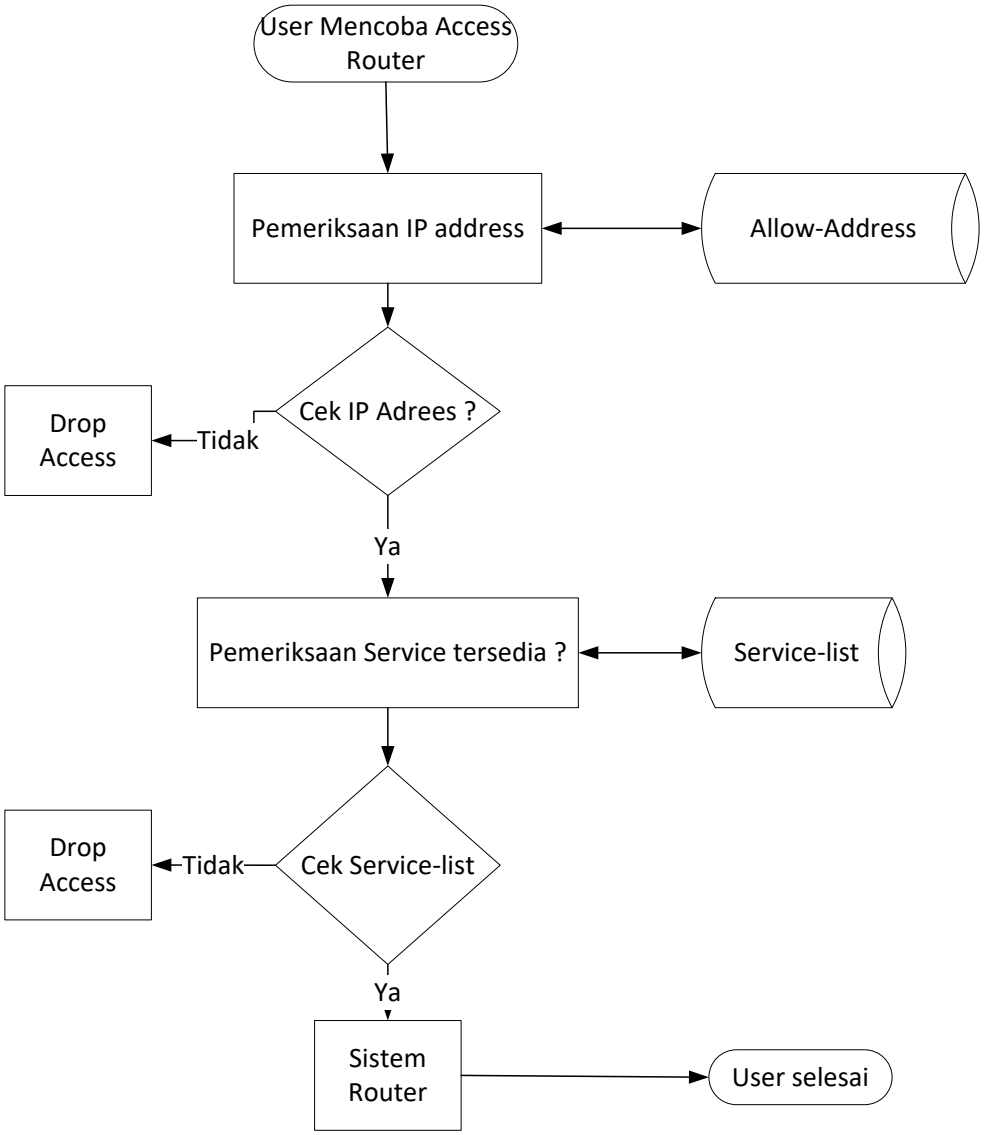
Tabel 3. 23 Data *Router 2*

No	*Hardware*	*IP Address*	Keterangan
1	*Ether-1*	*200.20.20 2*	*Router 1*
2	*Ether-2*	*200.10.4.1*	*Server*
3	*Ether-3*	*200.10.3.0*	*LAN*
4	*Ether-4*	-	-

Dalam sistem keamanan yang berjalan saat ini pada jaringan DPRD Provinsi Jawa Barat masih menggunakan *firewall* konvensional, dimana prinsip dari konvensional ini adalah membuka dan menutup terhadap port yang menjadi celah keamanan. Didalam beberapa kejadian yang dialami terhadap sistem keamanan jaringan ini, secara keseluruhan disebabkan salah satunya adalah diketahui port pada jaringan tersebut yang masih terbuka disamping penanggung jawa IT tidak menyadarinya.

C. *Port access* dan *remoting*

Pada port *access dan remoting* yang diproteksi untuk menghindari kejadian yang tidak di inginkan oleh pihak penanggung jawab IT dengan tindakan *knocking*. Dalam sesi login untuk meremote router mikrotik pihak penanggung jawab IT menggunakan tambahan rules *Firewall* yaitu protocol *ICMP* dimana protocol ini berfungsi ketika pengiriman *protocol ICMP* untuk *request port* hanya valid dalam 1 menit. Jika *IP Address* sesuai dengan *address-list* di *Firewall mikrotik* maka akan maka termasuk dalam daftar *IP Address* valid. Mikrotik hanya mengenali request dalam membuka port hanya pada *IP Address* yang terdapat di *IP Address*-list. Berikut ini port yang di tutup oleh penanggung jawab IT.



Gambar 3. 11 *Flowchartt* Alur *Access Remotting*

Pada gambar 3.12 adalah alur untuk mengakses router dengan memperhatikan port yang terdapat rule yang telah disepaki sebelumnya. Pada tabel ini adalah aturan hanya penanggung jawab IT yang bisa mengakses pada port – port tertentu.

Tabel 3. 24 Data *Port Access*

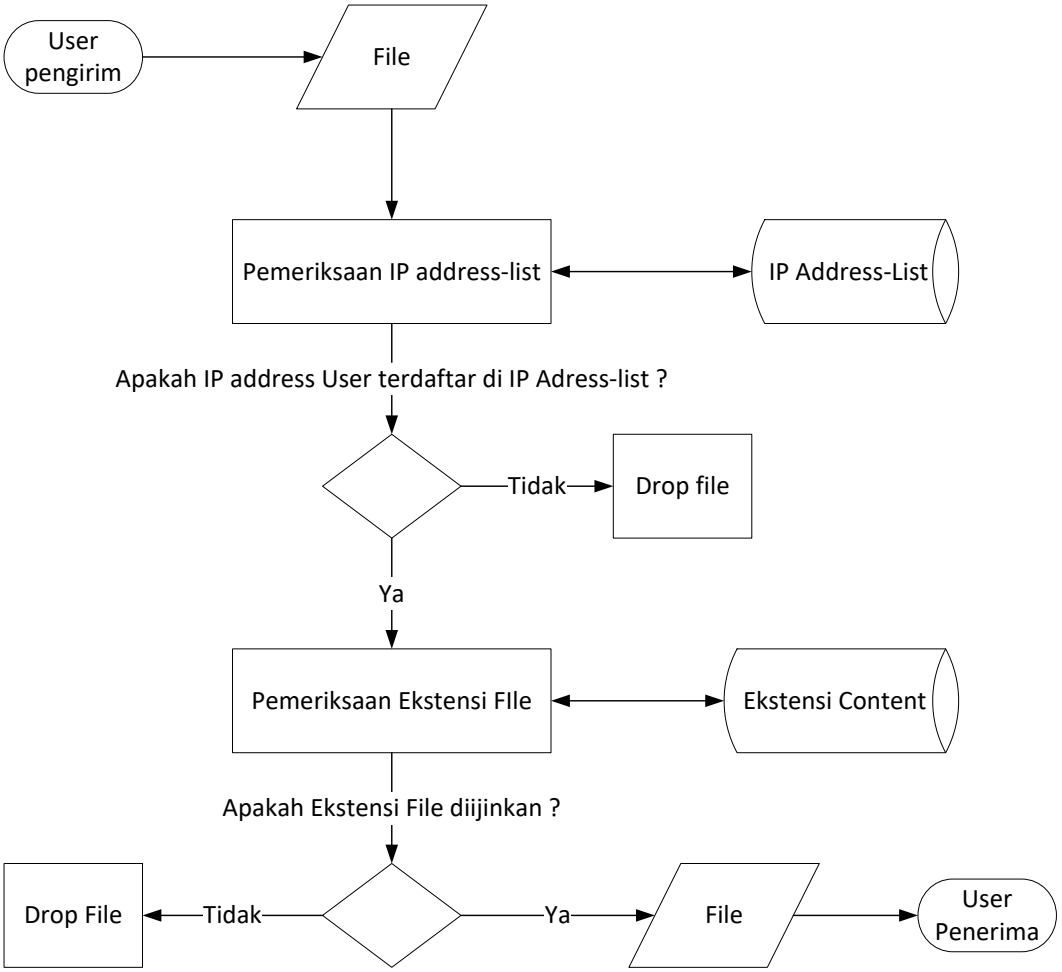
NO	Port Number	Protocol	Keterangan
1	80	*TCP*	Digunakan untuk akses via *Web*
2	22	*TCP*	Digunakan untuk akses via *SSH*

3	8291	*TCP*	Digunakan untuk akses via *Winbox*
4	23	*TCP*	Digunakan untuk akses via *Telnet*
5	8728	*TCP*	Digunakan untuk akses va *API*
6	8728	*TCP*	Diguanakan akses untuk va *Api-ssl*
7	443	*TCP*	Digunakan untuk akses via *wwe-ssl*

Dengan melakukan *chain=input* dan *action=drop* maka *router mikrotik* yang tidak mengenali suatu *IP Address* dari *IP Address-list* akan melakukan *drop*.

D. Port Transfer Data

Pada bagian *transfer file* di jaringan DPRD ini pihak penanggung jawab IT melakukan *policy control FTP* dimana hanya hanya untuk *document* saja. Berikut ini adalah *port file transfer protocol* pada *mikrotik*.



Gambar 3. 12 *Flowchart* Layanan *Transfer Data*

Keterangan :

1. Untuk melakukan *transfer file* pada jaringan, hanya bisa jika memenuhi aturan yang sudah ditetapkan seperti *port number* dan *IP Address*

Tabel 3. 25 Daftar Port Layanan Transfer Data

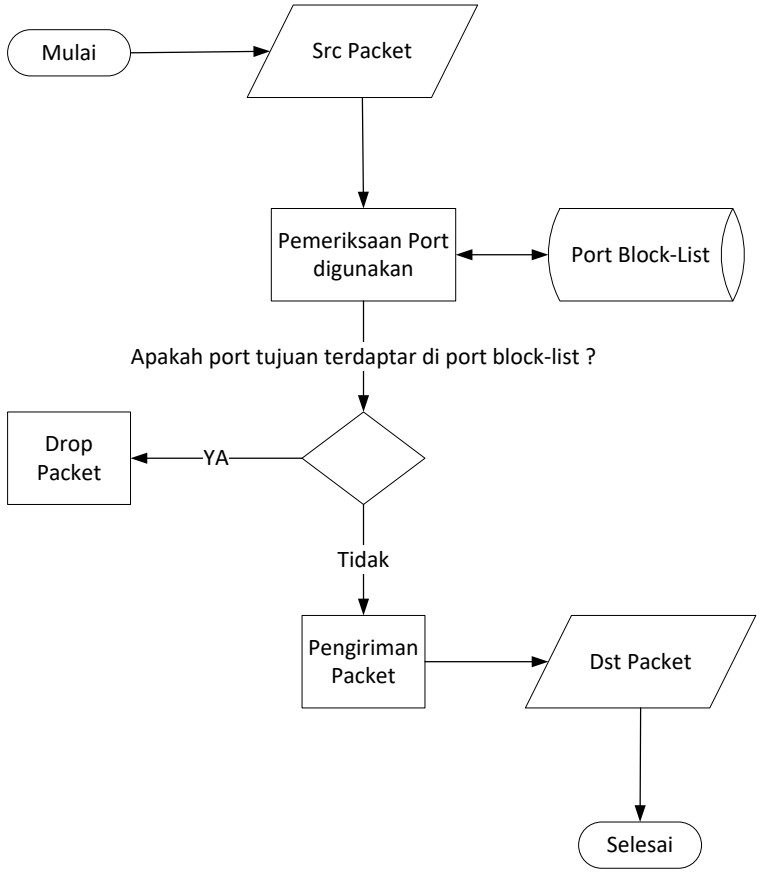
No	Port Number	Protocol	Keterangan
1	20	*TCP*	Digunakan untuk *File Transfer Protokol*
2	21	*TCP*	Dgunakan untuk *File Ttransfer Protokol*

Pada *policy control FTP* ini *file* yang diizinkan berupa *extended Microsoft office* dan *multimedia.* Penanggung jawab IT menggunakan *IP Address-*

list jika terjadinya *transfer* antar file diluar *extended Microsoft office dan multimedia*

E. *Port* celah terhadap *virus.*

Penanggung Jawab IT melakukan kebijakan aturan *filtering* terhadap *packet data* dimana ketika *packet data* tersebut masuk dalam *list-rule* maka *packet data* akan *drop action.*



Gambar 3. 13 *Flowchartt* Pemeriksaan Virus

Keterangan :

1. Untuk pemeriksaan virus sesungguhnya dengan mengetahui *port destination* dari packet yang dikirimkan tidak secara murni mendeteksi virus tersebut.

Pada tabel 3.26 adalah daftar port yang ditutup oleh pihak penanggung jawab IT DPRD Provinsi Jawa Barat.

Tabel 3. 26 Data *Port Number* yang ditutup

No	Port Number	Protocol
1	135-139	*TCP*
2	445	*TCP, UDP*
3	593	*TCP*
4	1024-1030	*TCP*
5	1080	*TCP*
6	1214	*TCP*
7	1363	*TCP*
8	1364	*TCP*
9	1373	*TCP*
10	1377	*TCP*
	1433-1434	*TCP*
11	2745	*TCP*
12	2283	*TCP*
13	2535	*TCP*
14	2745	*TCP*
15	3127	*TCP*
16	3410	*TCP*
17	4444	*TCP, UDP*
18	5554	*TCP*
19	8866	*TCP*
20	9898	*TCP*
21	10000	*TCP*
22	10080	*TCP*
23	12345	*TCP*
24	17300	*TCP*
25	27374	*TCP*
26	65506	*TCP*

F. Port Anti-Spam

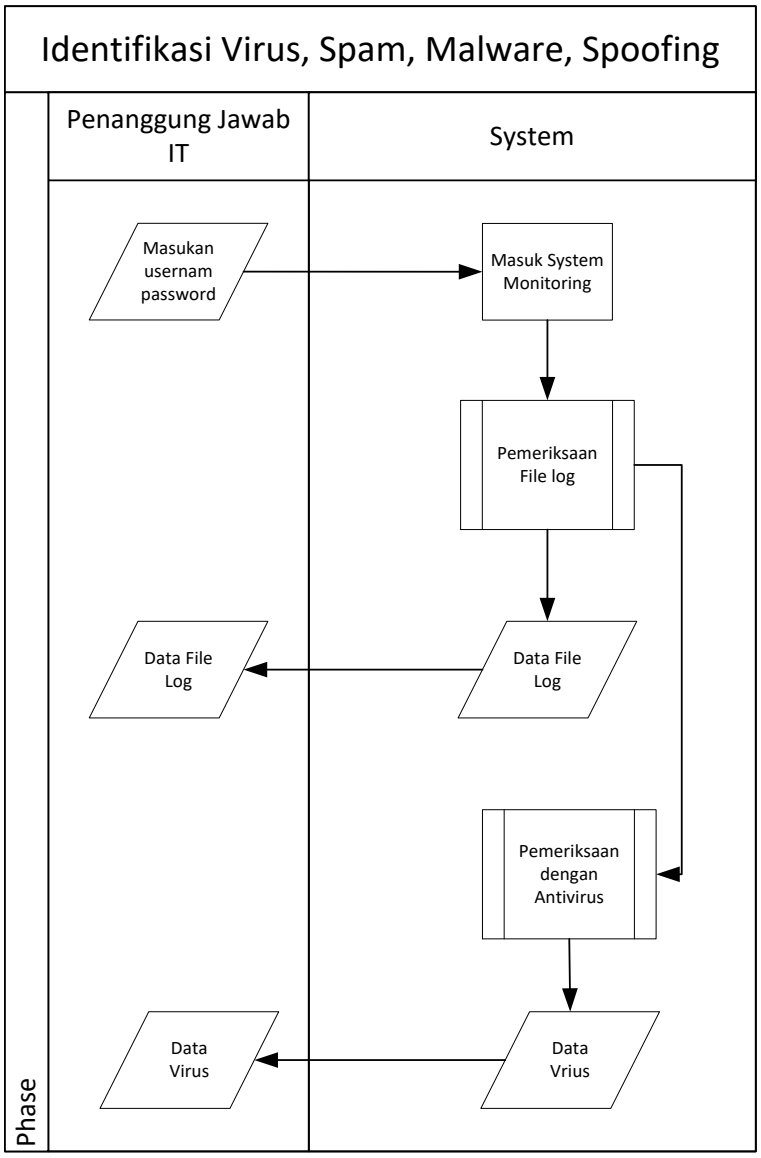
Port yang tertera pada penejelasan tabel 3.27 merupakan daftar *port* yang ditutup oleh penanggung jawa IT untuk pencegahan terdapat *spam.*

Tabel 3. 27 Data Port *Anti-Spam* yang di tutup

NO	Port Number	Protocol	Keterangan
1	135-139	*TCP*	Koneksi terhadap RPC
2	445	*TCP*	Layanan *sharing file*
3	593	*TCP*	*RPC over HTTP endpoint mapper Remote Procedure Call*
4	4444	*TCP*	Layanan *sharing file*
5	5554	*TCP*	Layanan *sharing file*
6	9996	*TCP*	Layanan *sharing file*
7	995-999	*UDP*	*POP3 over SSL Exchange Server, IMAP over SSL Exchange Server*
8	53	*TCP*	Layanan *sharing file*

G. Identifikasi *Virus, Malware, Spam, Spoofing*

Untuk megidentifikasi terdap *Virus, Malware, Spam* dan *Spoofing* oleh penanggung jawab IT, maka yang dilakukan sesuai gambar 3.14 dimana penanggung jawa IT menggunakan *file log* dan *anti-virus.*



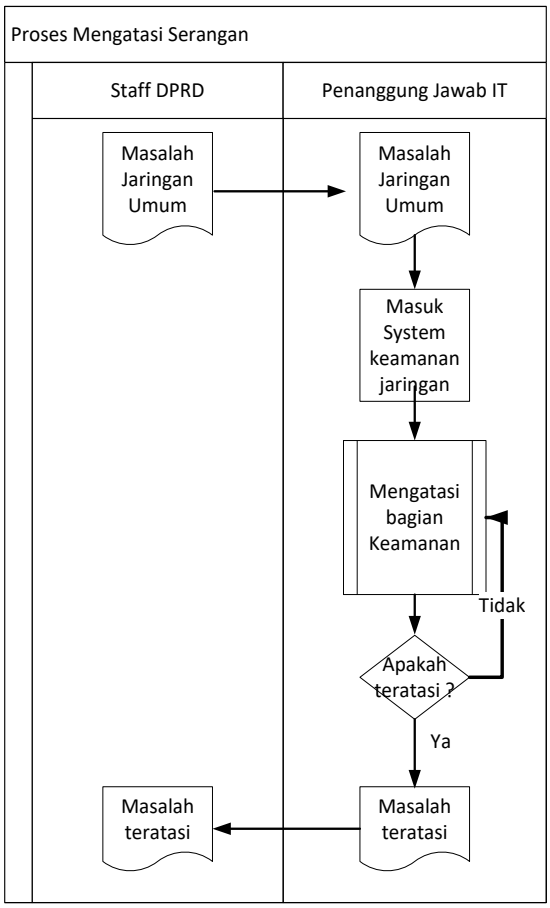
Gambar 3. 14 *Flowchart* identifikasi

3.1.2.3. Analisis procedure penangan keamanan jaringan

Pada tahapan analisis procedure penangan sistem keamanan jaringan yang berjalan di DPRD Provinsi jawa barat dibagi menjadi dua yaitu user dan penanggung jawa IT. Pada dasarnya penanganan oleh user ini hanya sebatas pengetahui umum saja seperti mendapatkan informasi telah terjadi perubahan pada *Web*site DPRD provinsi jawa barat dan mendapatkan infomasi pada ancaman serangan virus pada komputer *client* dengan notifikasi dari antivirus

tersebut. Untuk penangan keamanan jaringan secara teknisnya, masih dibawah pengawasan Penanggung jawab IT.

1. **User**

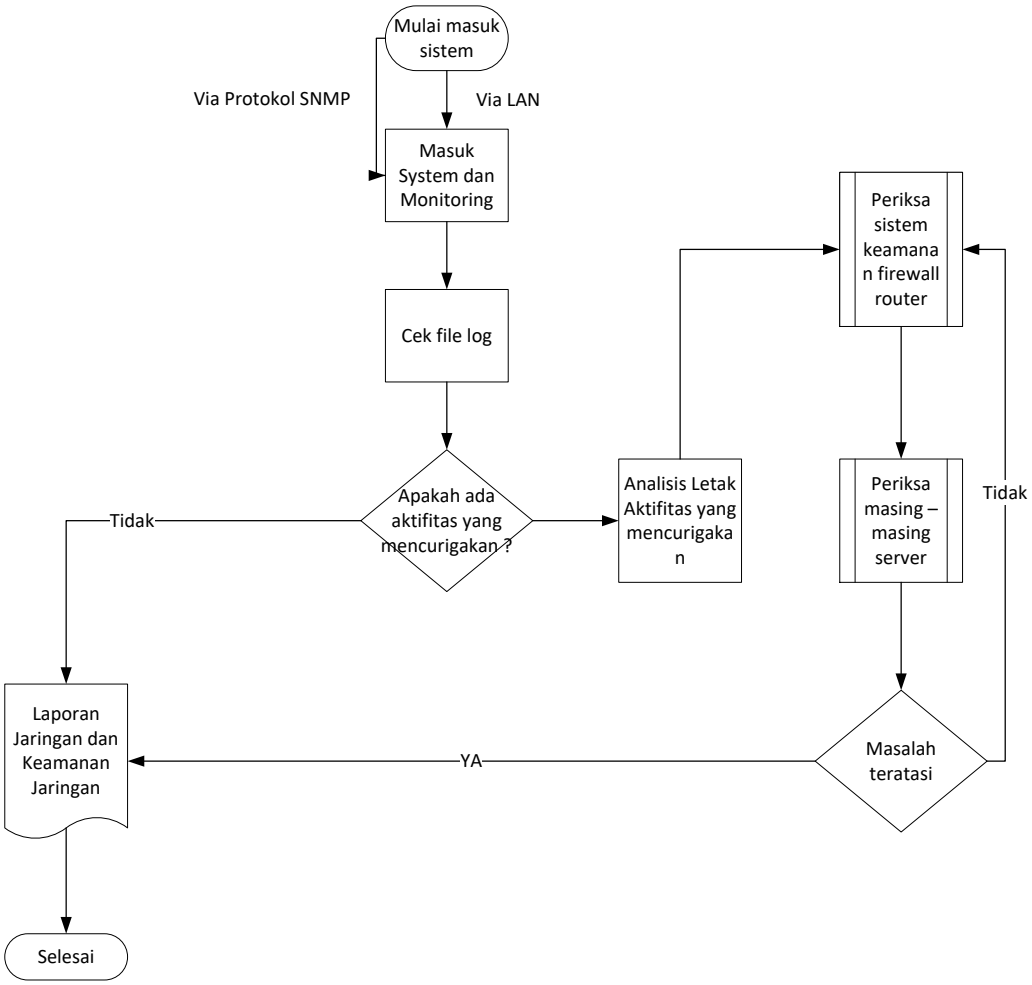


Gambar 3. 15 Flowmap penangan keamanan jaringan user

Keterangan :

Pada gambar 3.15 tersebut beberapa staff melakukan laporan terhadap masalah yang terjadi kepada penanggung jawab IT.

2. Penanggung Jawab IT



Gambar 3. 16 *Flowchart* penangan Jaringan Komputer Penanggung Jawa IT

Keterangan :

1. Dalam monitoring jaringan, penanggung jawa IT dalam melakukan tindakan memonitoring ataupun menangani sebuah permasalahan dapat melalui jaringan *Local Area Nework* (LAN) secara langsung ataupun melalui remote dengan memfaatkan protocol snmp pada router mikrotik.
2. Penanggung jawa IT akan mengecek terhadap *file log system* untuk mengetahui terhadap aktifitas apa saja yang telah terjadi pada jaringan tersebut.

3. Ketika tdak ada aktifitas yang mencurigakan, maka penanggung jawa IT keluar dari sistem jaringan komputer dan membuat laporan mingguan terhadap performa jaringan tersebut.
4. Ketika penanggung jawa IT mengetahui ada sebuah aktifitas mencurigakan melaui *system log file* atau sistem monitoring jaringan, maka penanggung jawa IT akan mengalisa pada bagian tertentu yang dicurigai.
5. Penanggung jawa IT biasanya melakukan pengecekan terhadap masing – masing *server* dan router. setelah mengetahui dan mengatasi terhadap aktifitas yang mencurigan yang bisa menimbulkan ancaman, maka penanggung jawa IT akan membuat laporan untuk mengevalui sistem yang ada.

3.1.2.4. Analisis Perangkat Keras Jaringan

Pada tahapan ini dilakukan tindakan analisis perangkat keras jaringan yang terhubung pada pada *local area network* (LAN) antara lain *PC client, Server, Router Mikrotik* dan perangkat keras pendukung lainya.

a. Spesifikasi PC *client*

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa pc *client* yang jaringan DPRD Provinsi Jawa Barat.

Tabel 3. 28 Data Spesifikasi *Client*

No	***Hardware***	**Keterangan**
1	*Processor*	*Intel Core 2 Duo E7500 Processor (2.93Ghz, 1,066 FSB, 3MBL2 Cache)*
2	*Memori*	*2GB DDR3 1066MHz SDRAM*
3	*Hard Drive Type*	*500GB SATA*
4	*Graphics*	*Integrated Intel Graphics Media Accelerator X4500*
5	*Audio*	*Terintegrasi*
6	*Jaringan*	*Gigabit Ethernet*
7	*Kecepatan*	*10 / 100 / 1000 Mbps*

	Jaringan	
8	*Tipe Keyboard*	*Optional*
9	*Input Device Type*	*Optional*
10	*Slot Provided*	*PCIe x16 (1), PCIe x1 (3), Mini-PCIe (1)*
11	*I/O Port*	*6 x USB 2.0, eSATA, LAN, Audio, 1 Serial, 2 PS/2 for Keyboard and Mouse*
12	*Optical Drive Type*	*16X Max DVD-RW Drive*
13	Sistem Operasi	*Windows 7*

b. PC *Server*

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa *PC server* yang jaringan DPRD Provinsi Jawa Barat.

Tabel 3. 29 Data Spesifikasi *PC Server*

No	***Hardware***	Keterangan
1	*Processor*	*XEON E3-1225 V3*
2	*RAM*	*16 GB UDIMM, 1600 MT/s, Low Volt, Single Rank, x4 Data Width*
3	*RAID controller*	*Not RAID controller*
6	*Processor Onboard*	*Intel(R) Xeon(R) Processor E3-1225 v3 3.2GHz 8M Cache,4C/4T,turbo,84W - TPM*
7	*Power Supply Type*	*Single Power Supply, 290W*
8	*Processor Type*	*Intel Xeon*
9	*Networking*	*Integrated Intel 82579 Gigabit Ethernet LAN*
11	*Optical*	*DVD+/-RW,SATA*
12	*Hard Drive*	*1 TB 7.2K Entry SATA 3.5in Cabled Hard Drive*
13	*I/O Ports*	*Free Mouse dan Keyboard*

c. Mikrotik

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa router *mikrotik* pada jaringan DPRD Provinsi Jawa Barat yang berfungsi terhadap manejaman jaringan.

Tabel 3. 30 Data Spesifikasi *Mikrotik*

No	***Hardware***	**RB1100AHx2**
1	*CPU speed*	1066MHz
2	*Current Monitor*	Tidak ada
3	*CPU*	P2020
4	*RAM*	2GB
5	*Architecture*	PPC
6	*LAN ports*	13
7	*Gigabit*	Ada
8	*MiniPCI*	0
9	*Integrated Wireless*	0
10	*Memory Cards*	1
11	*Memory card type*	microSD
12	*Power Jack*	110/220V
13	*802.3af support*	Tidak ada
14	*PoE*	12-24V
15	*Voltage Monitor*	Ada
16	*PCB temperature monitor*	Ada
17	*CPU temperature monitor*	Ada
18	*Dimensions*	*1U case: 44 x 176 x 442 mm, 1200g. Board only: 365g*
19	*Operating System*	*RouterOS*
20	*Temperature range*	*-30°C to +65°C*
21	*RouterOS License*	*Level 6*

d. Perangkat Keras Pendukung Jaringan

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa PC *client* yang jaringan DPRD Provinsi Jawa Barat yang dijelaskan pada tabel 3.31.

Tabel 3. 31 Data Perangkat Keras Pendukung

No	Nama Perangkat Keras	Kategori
1	*ISP Provider*	*ISP*
2	*Belden 6e*	*Cable*
3	*cisco catalyst 2950-24 specification*	*Switch*
4	Perangkat pendukung	*Switch*
5	Perangkat pendukung	*Acces Point*

3.1.2.5. Analisis Perangkat Lunak

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa analisis perangkat lunak yang jaringan *DPRD Provinsi Jawa Barat* yang dijelaskan pada tabel 3.32

Tabel 3. 32 Data Perangkat Lunak

No.	Nama Perangkat Lunak	Kategori
1	*Window 7*	*PC Client*
2	*Router OS*	*Mikrotik RB1100*
3	*Redhat*	*Server Database*
4	*Linux Ubuntu*	*Web Server*, Mail *Server*, SPKD *server*
5	*Phpmyadmin*	*Database Server*

3.1.2.6. Analisis Data User

Berdasarkan data dan informasi yang didapat berikut ini adalah data - data terhadapa user yang jaringan *DPRD Provinsi Jawa Barat*

Tabel 3. 33 Data *User*

No	Nama User	Jumlah	Keterangan
1	Staff IT	3	Masuk kedalam kategori kelompok ahli
2	Staff Bagian Persidangan	50	-
3	Staff Undang – undangan	50	-
4	Staff Humas dan Protol	50	-
5	Staff Umum dan Administrasi	50	-
6	Staff Keuangan	50	-
7	Kelompok Jabatan Funsional	10	b. Dokter Gigi 2 c. Analisis kepegawian 5 d. Dokter Poliklinik 3

3.1.2.7. Analisis *IP*

1. Public

IP Public ini digunakan sebagai *web server* pada situs DPRD Provinsi Jawa Barat dengan data sesaui tabel 3.49 berikut ini.

Tabel 3. 34 Data IP Public

No	TCP/IP	Keterangan
1	*IP Address*	49.236.219.106
2	*Gateway*	49.236.219.1
3	*Subnet*	255.0.0.0
4	*DNS*	8.8.8.8

2. IP Address Private

IP Private merupakan *IP Address* yang digunakan pada jaringan DPRD Provinsi Jawa barat dengan menggunakan *class C.*

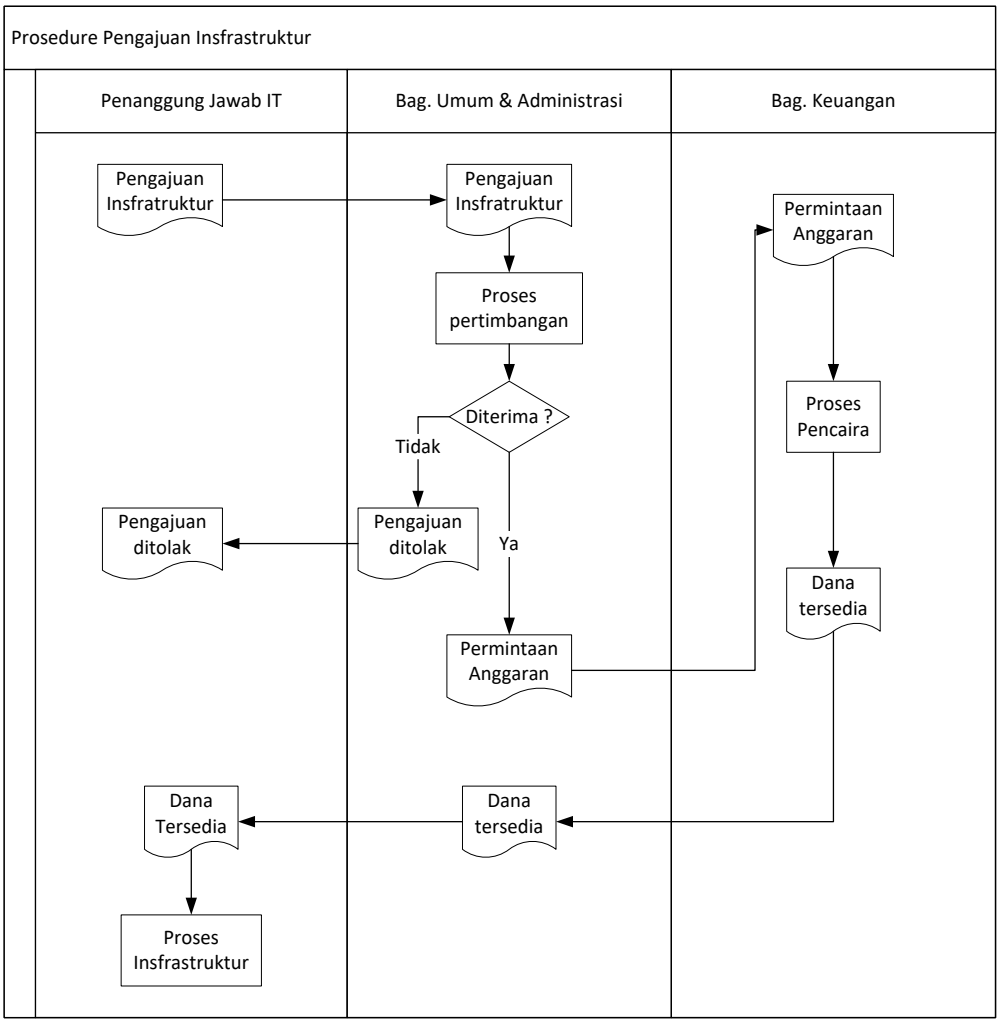
Tabel 3. 35 Data IP Private

NO	TCP/IP	Keterangan	
1	*IP Addresss*	217.10.1.0/24	*Vlan* 10
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
2	*IP Addresss*	217.10.2.0/24	*Vlan* 20
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
3	*IP Addresss*	217.10.3.0/24	*Vlan* 30
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
4	*IP Addresss*	217.10.4.0/24	*Vlan* 40
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
5	*IP Addresss*	217.10.5.0/24	*Vlan* 50
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
6	*IP Addresss*	217.10.6.0/24	*Vlan* 60
	Subnet	255.255.255.0	
	Gateway	200.10.1.2	
	DNS	8.8.8.8.8	
7	*IP R1 E1 buat modem 1*	*IP Addresss* Subnet Gateway DNS	192.168.1.2
8	*IP R1 E2 buat modem 2*	*IP Addresss* *Subnet*	192.168.2.1

		Gateway *DNS*	
9	*IP R1 E3 buat router 2*	*IP Addresss* *Subnet* *Gateway* *DNS*	192.168.2.1
10	*IP R2 E2*	*IP Addresss* *Subnet* *Gateway* *DNS*	*Trank vlan*
11	*Switch Cisco*	*Eth 1 trunk*	192.168.2.1
12	*IP R2 E3*	*IP Addresss* *Subnet* *Gateway* *DNS*	200.10.3.1/24 255.255.255.0 200.10.1.2 8.8.8.8.8
13	*Server*	*IP Addresss* *Subnet* *Gateway* *DNS*	200.10.3.2/24 255.255.255.0 200.10.1.2 8.8.8.8.8
14	*Modem 1*		192.168.1.1
14	*Modem 2*		192.168.3.1

3.1.2.8. Flowmap Birokrasi DPRD Provinsi Jawa Barat

Pada gambar 3.17 merupakan alur birokrasi dalam pengadaan insfrastruktur pada lembaga DPRD Jawa Barat. Melibat tiga bagian yaitu Penanggung Jawab IT, Bag. Umum dan Administrasi dan Bagian Keuangan.



Gambar 3. 17 flowmap Birokrasi DPRD

Keterangan:

1. Setiap melakukan pengajuan penambahan insfrastruktur IT oleh penanggung jawa ke pihak DPRD Jabar, maka mekanismenya melalui staff umum dan staff keuangan
2. Persetujuan insfrastruktur berada pada pihak Bagaian Administrasi dan Umum
3. Bagian Keuangan hanya melakukan rekomendasi dari Bagian Umum dan administrasi

3.1.3. Analisis Kebutuhan Sistem

Pada tahapan ini merupakan analisis kebutuhan terhadap sistem yang akan dibangun. Analisis kebutuhan sistem ini dibagi menjadi dua, yaitu analisis kebutuhan perangkat keras dan analisis kebutuhan perangkat lunak.

3.1.3.1. Analisis kebutuhan perangkat keras

Analisis kebutuhan perangkat keras ini digunakan sebagai *server Unified Threat Management* (UTM) *Firewall* berbasis *Linux* pada sistem jaringan komputer DPRD Provinsi jawa barat. Berikut ini daftar kebutuhan perangkat keras terhadap sistem keamanan jaringan *Unified Threat Management* (UTM) *Firewall* berbasis *Linux*.

Tabel 3. 36 Analisis Kebutuhan Perangkat Keras

No	Perangkat Keras	Nama Perangkat Keras
1	*Processor*	*Minimum Dua core 2.0 GHz*
2	*Motherboard*	*MSI*
3	*RAM*	*4 GB*
4	*Hard Disk*	*Minimum 8 GB*
5	*Monitor*	*17 inchi*
6	*Mouse*	*Standar*
7	*Keyboard*	*Standar*
8	*Network Card*	*Support for full virtualization and paravirtualization*
9	*Cable*	*Belden cat6e*
10	*Switch*	*Standar*
11	*Modem*	*standar*

3.1.3.2. Analisis kebutuhan perangkat lunak

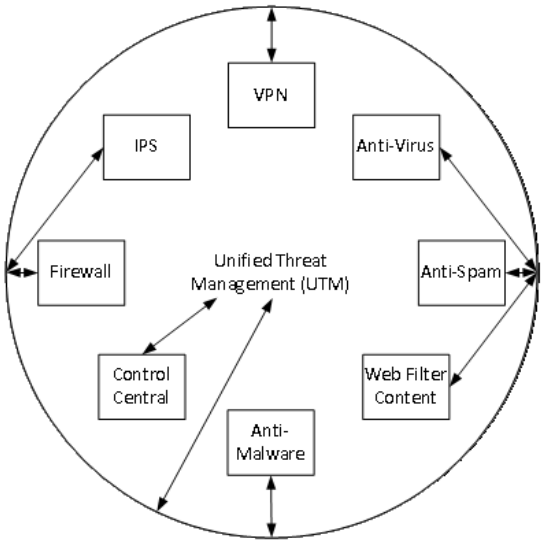
Analisis kebutuhan perangkat lunak ini digunakan sebagai *server Unified Threat Management* (UTM) *Firewall* berbasis *Linux* pada sistem jaringan komputer DPRD Provinsi jawa barat. Berikut ini daftar kebutuhan perangkat

lunak terhadap sistem keamanan jaringan *Unified Threat Management* (UTM) *Firewall* berbasis *Linux*.

Tabel 3. 37 Analisis Kebutuan Perangkat Lunak

No	Typer Perangkat Lunak	Nama Perangkat lunak
1	Sistem operasi	*Endian Firewall UTM Linux-based Operating System* *Windows 7*
2	*Web Server*	*Apache*
3	*Web* Browser	*Google Chrome*
4	*VPN client*	*OpenVPN*

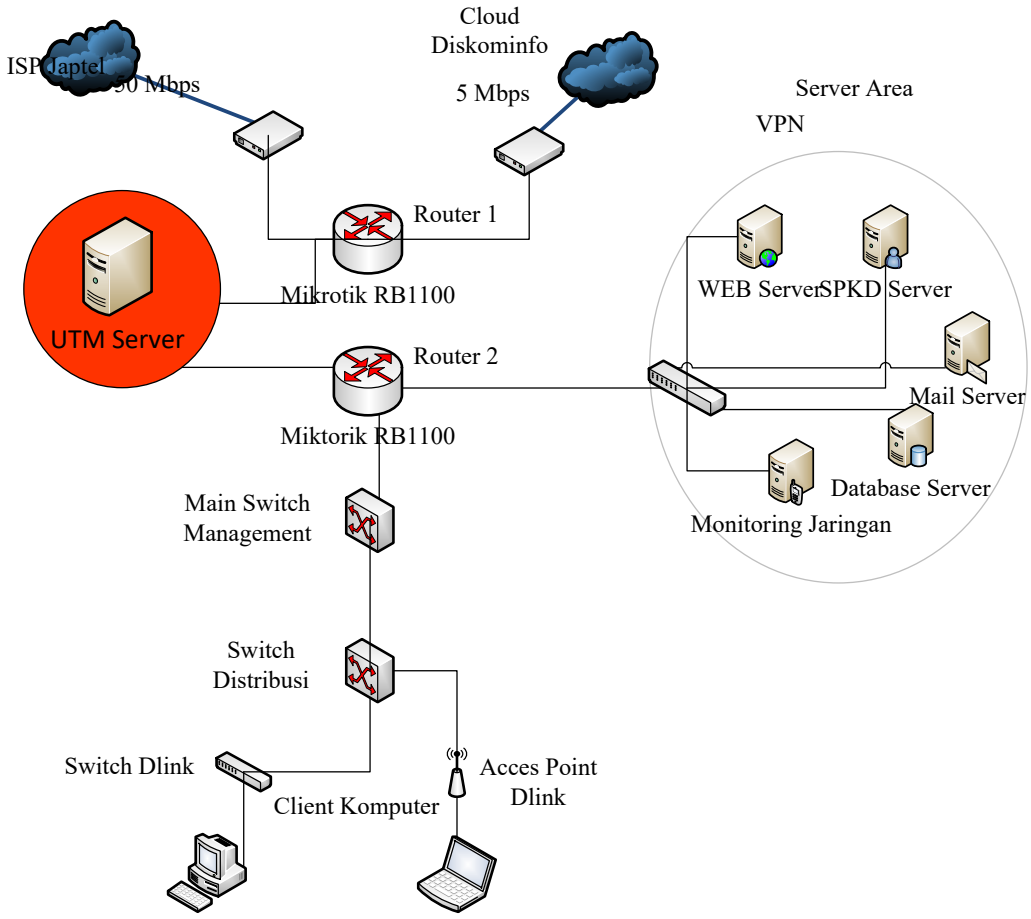
3.1.3.3. Analisis Teknologi *UTM Firewall*



Gambar 3. 18 Analisis Teknologi *UTM Firewall*

Keterangan :

Pada Gambar 3.18 dan gambar 3.19 di atas bahwa *Firewall, Control, Anti-Malware, Web Filter Content, Anti-Spam, Anti-Virus, VPN* dan *IPS* terhubun pada satu sistem control terpusat.



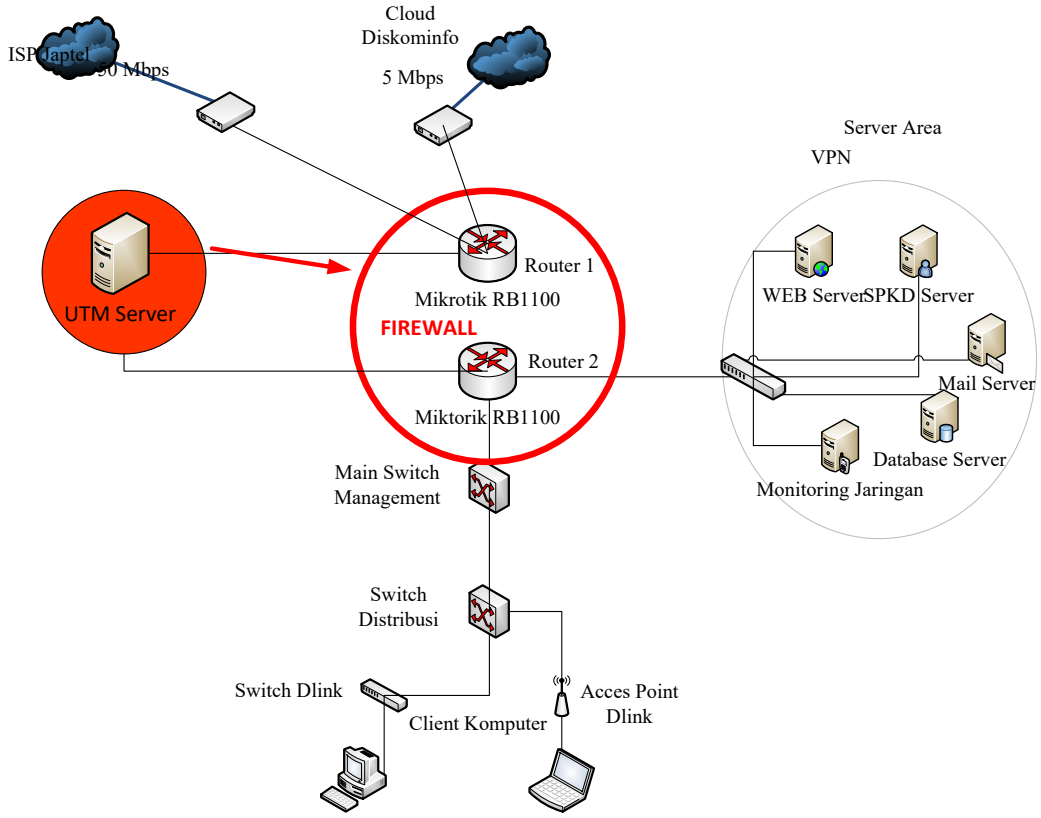
Gambar 3. 19 Konsep *UTM Firewall*

Keterangan:

1. Penempatan Server *UTM firewall* berada diantar router 1 dan router 2
2. Router 1 tetap difungsikan sebgai *load balancing*
3. *Router 2* tetap digunakan sebagai *network management*
4. setiap *packet data* yang masuk dan keluar jaringan akan melewati *UTM firewall server* untuk melakukan *filtering* terhadap packet data

4. *Firewall*

Pada gambar 3.20 Penggunaan *UTM firewall* berbasis *Linux* Server sebagai *Firewall* bertugas untuk pengamanan router mikrotik



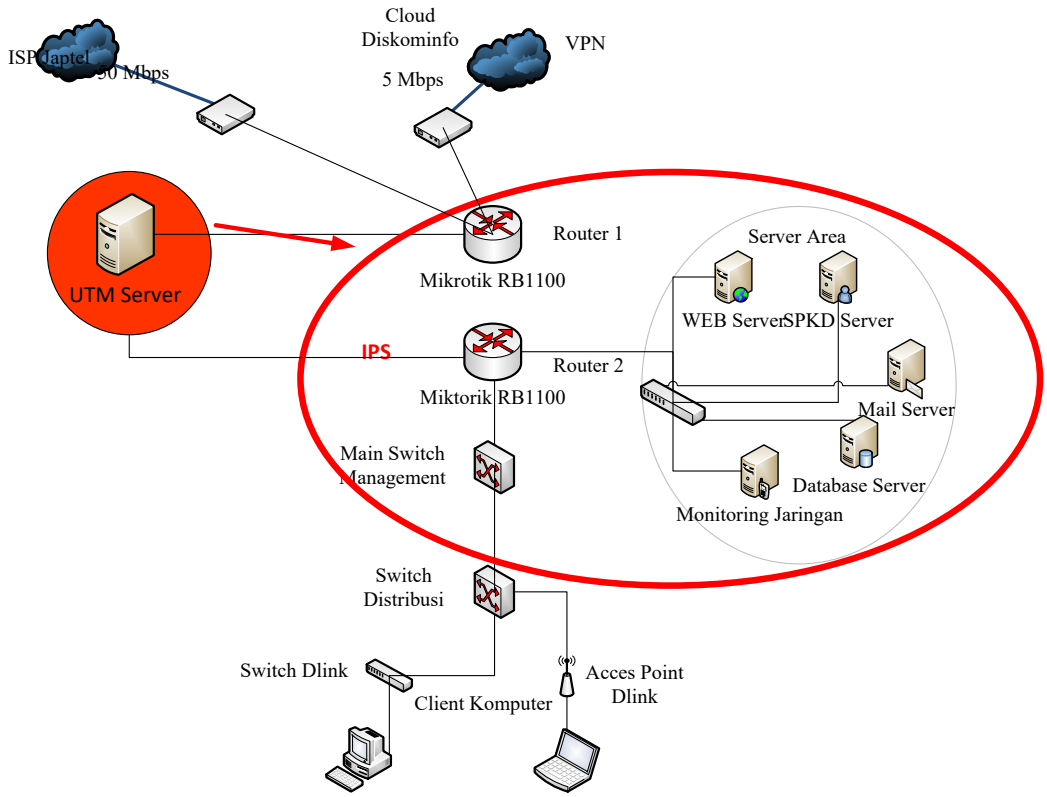
Gambar 3. 20 Konsep Firewall

Keterangan:

1. *UTM firewall* difungsikan sebagai firewall untuk *handle* fungsi firewall pada router 1 dikarenakan tidak ada perubahan pada insfrastruktur IT yang ada, hanya penamban insfrastruktur IT.
2. Fungsi utama dari *UTM firewall* ini untuk filtering *packet data* yang dating dari router 1 dan router 2 kedalam server *UTM Firewall*

5. *IPS*

Pada gambar 3.21 *UTM firewall* berbasis *Linux* Server sebagai *IPS* dengan fungsi untuk mendeteksi packet yang menurigakan dalam jaringan internal DPRD Provinsi Jawa Barat.



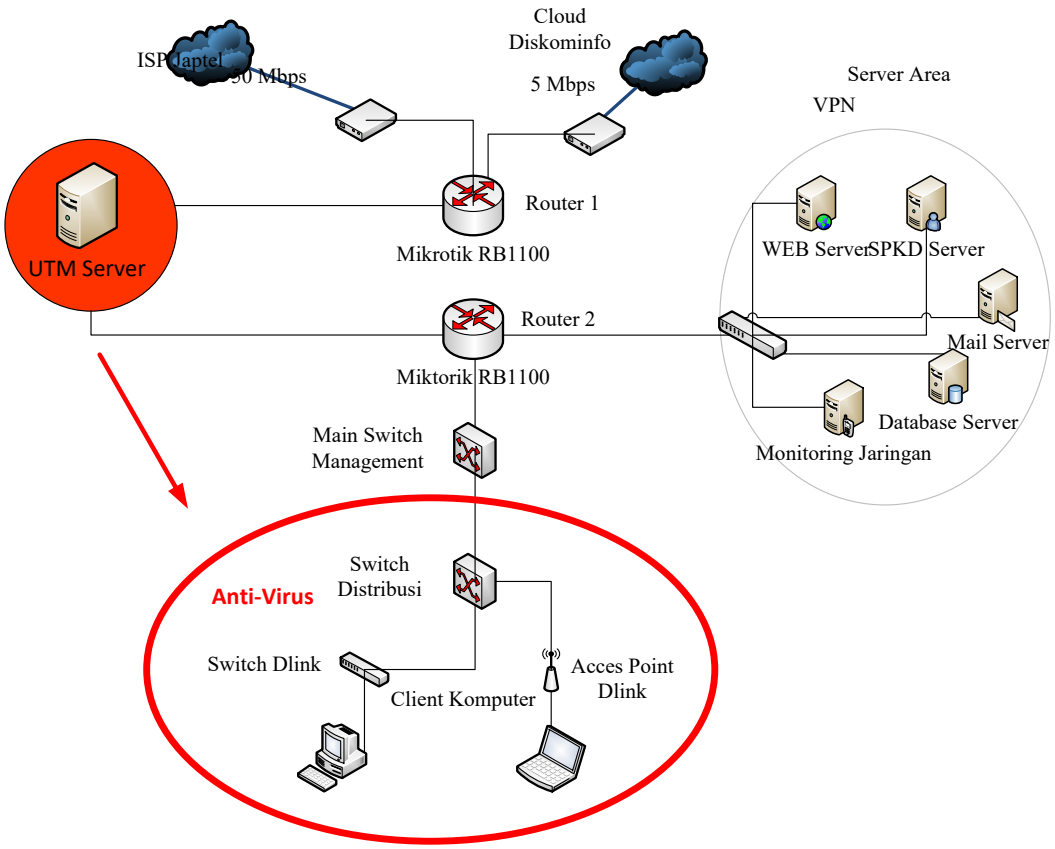
Gambar 3. 21 Konsep *IPS*

Keterangan:

1. *UTM firewall server* di fungiskan sebagai *Intrusion Prevent System* dimana untuk mendeteksi aktifitas mencurigakan pada router dan *server.*
2. *UTM firewall* berfungsi sebagai *IPS* ini bertindak mencocokan lalu lintas packet data pada jaringan DPRD Jabar sesuai *rule-list* yang terdapat pada *IPS*
3. *IPS* untuk menterminasi serangan yang dicurigai melalui penggunaan *packet TCP, RST* atau pesan *ICMP Unreachable*. *IPS* mengkonfigurasi secara otomatis *firewall* untuk *drop traffic* berdasar yang dideteksi oleh *IPS*. Untuk kemudian melakukan prevention terhadap koneksi tertentu.

6. Anti-Virus

Pada gambar 3.22 berikut ini *UTM firewall* berbasis *Linux* Server berfungsi sebagai Anti-Virus untuk melindungi komputer *client* pada jaringan initernal.



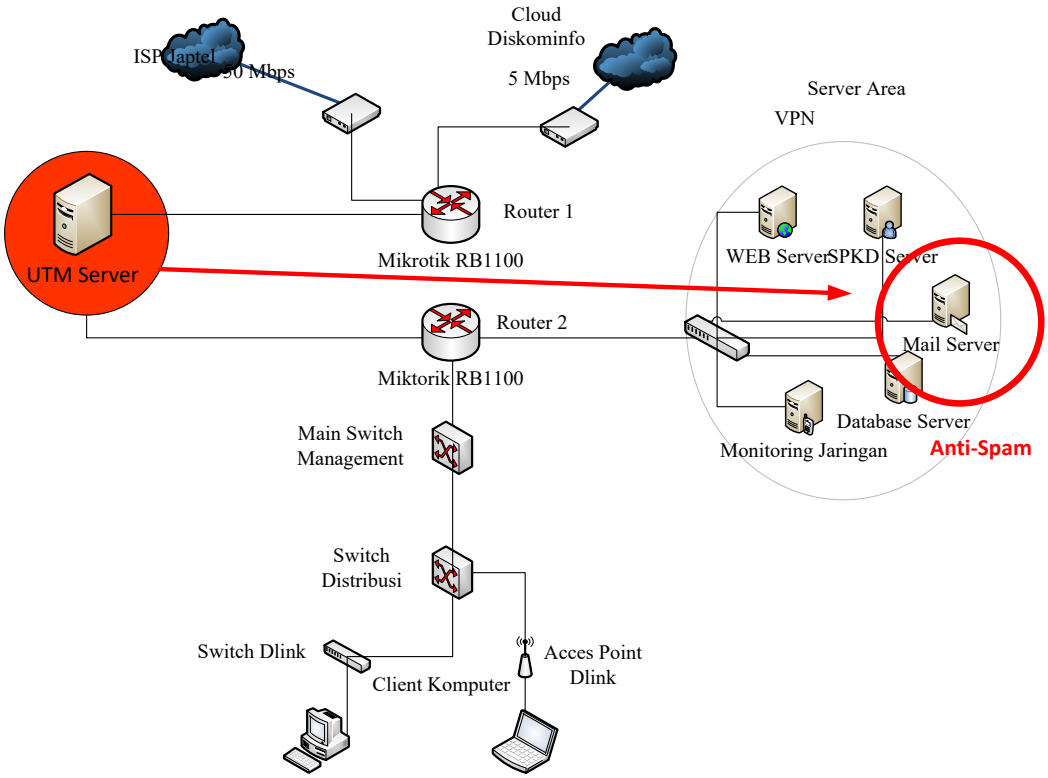
Gambar 3. 22 Konsep Anti-Virus

Keterangan:

1. *UTM firewall* sebagai Anti-virus di fungsikan untuk melindungi *client* yang berada ada jaringan DPRD Jabar.
2. *UTM firewall* sebagai anti-virus yang berperan untuk mengatasi terdapat serangan *DDOS.*
3. *File archieve* yang berlalu lintas pada jaringan ini selalu di scanning oleh anti-virus

7. Anti-Spam

Pada gambar 3.22 berikut ini *UTM firewall* berbasis *Linux Server* berfungsi sebagai *Anti-Spam* yang bertugas untuk memproteksi *Mail Server* dari *spam*



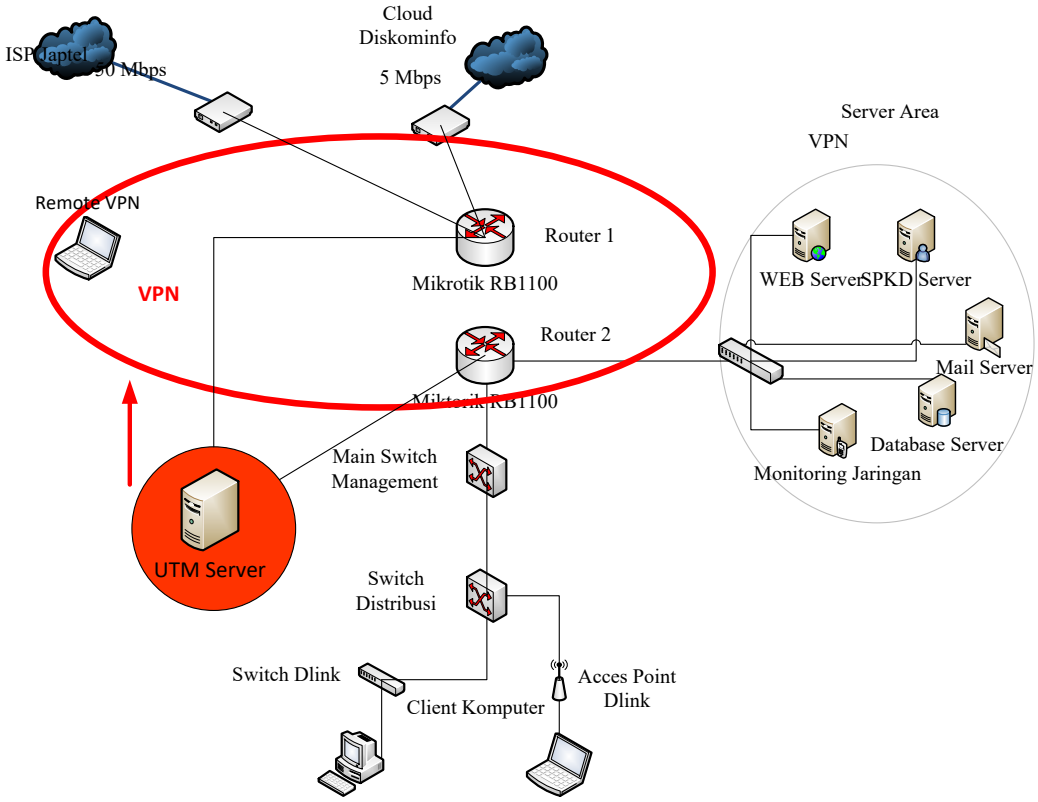
Gambar 3. 23 Konsep Anti-*Spam*

Keterangan:

1. *UTM firewall* difungsikan sebagai *Anti-Spam* untuk memproteksi terdapat *mail server.*
2. Email yang masuk dari internet akan melewati *UTM firewall* untuk melakukan *filtering* sesuai aturan.
3. Email yang terditeksi spam akan disimpan pada server *UTM firewall* ini.
4. Untuk email yang keluar juga dilakukan filtering

8. VPN

Pada gambar 3.24 di bawah *UTM firewall* berbasis *Linux* Server sebagai VPN dimana penanggung jawab IT bisa melakukan remotting dari luar jarinngan



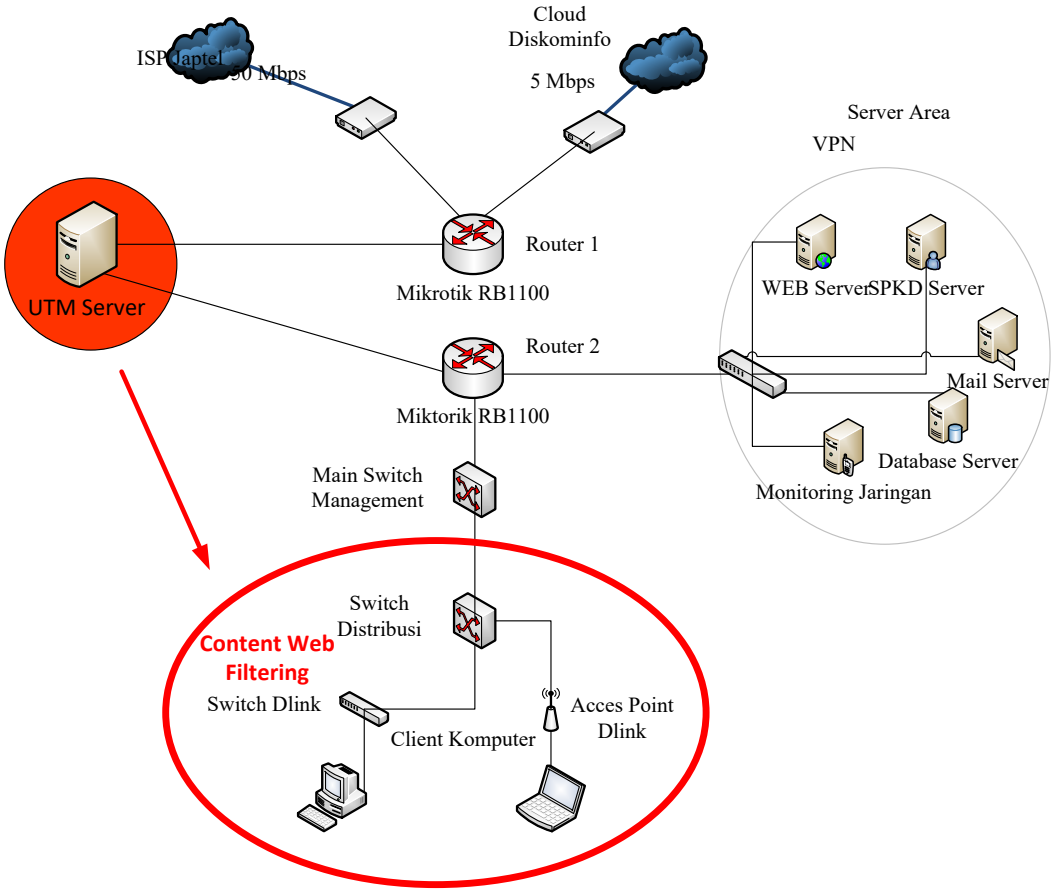
Gambar 3. 24 Konsep *VPN*

Keterangan:

1. *UTM firewall* yang di fungsikan sebagai *VPN server* dimana untuk memdahakn penanggung jawa IT dalam monitoring jaringan ketika tidak berada ditempat.
2. *VPN* ini hanya berlaku untuk penanggung jawab IT saja

9. Web Content Filter

Pada gambar 3.25 berikut ini *UTM firewall* berbasis *Linux* Server sebgai Content Web Filtering dimana penyaringan terhadap content tertentu



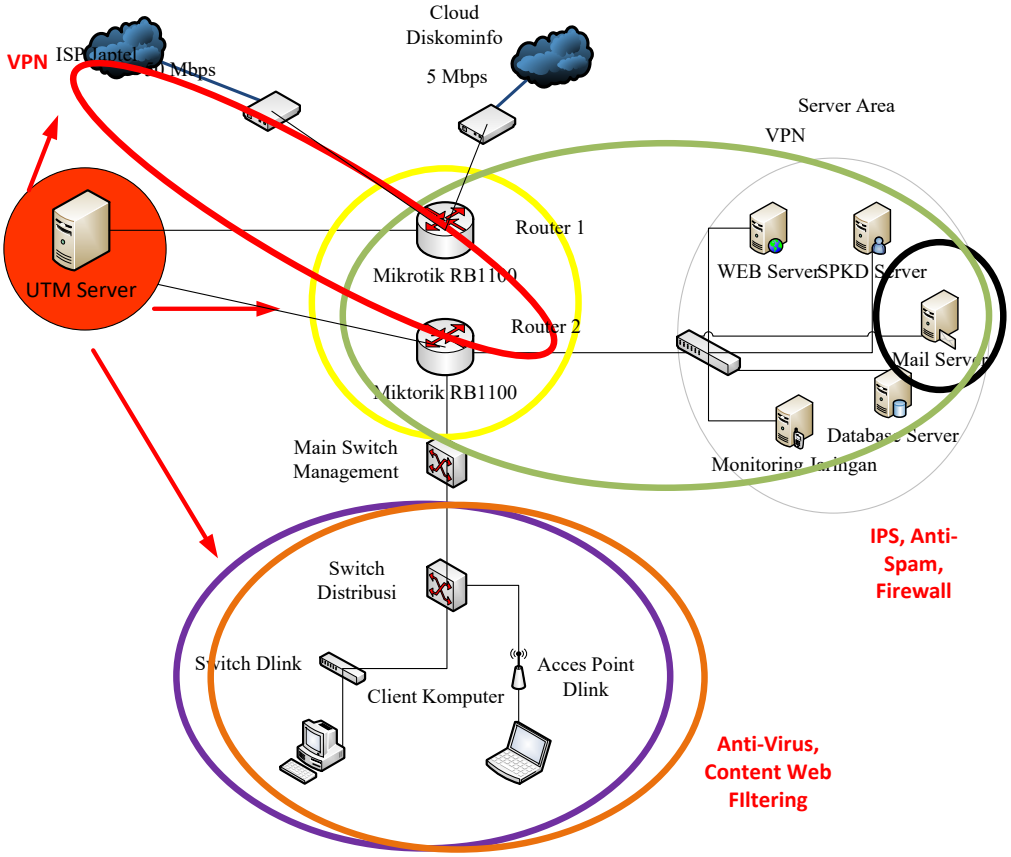
Gambar 3. 25 Konsep Web Content Filter

Keterangan:

1. *UTM Firewall*l difungsikan sebagai *web content filtering* dimana untuk melakukan filtering terdapat packet data dari dalam jaringan yaitu *client* pada jaringan DPRD Jabar.
2. Untuk semua *client* dalam mereqest packet data harus sesuai aturan pada UTM Server

10. Control Application

Pada gambar 3.26 berikut ini *UTM firewall* berbasis *Linux* Server sebgai Control Application terpusat untuk mengatur semua security



Gambar 3.26 Analisis *Control Application*

Keterangan:

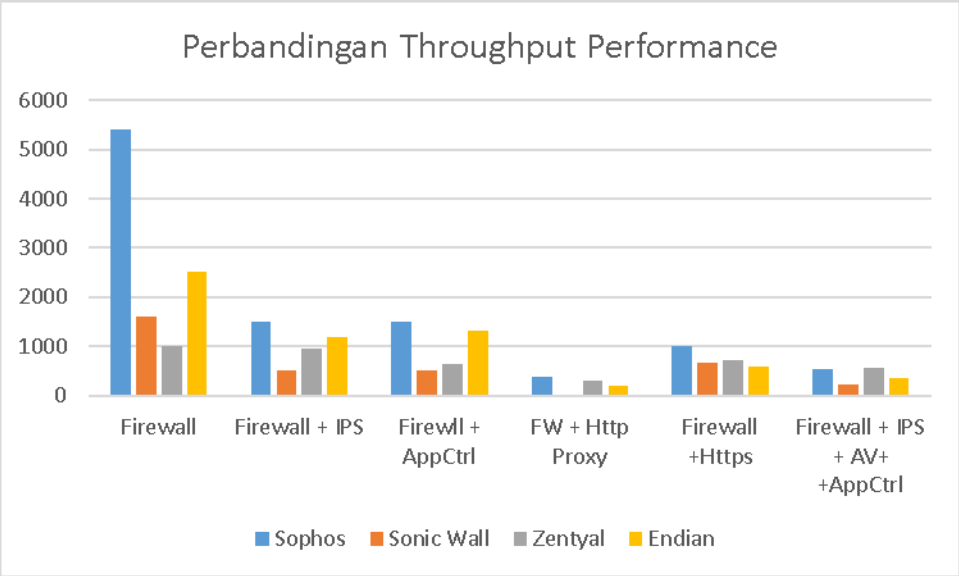
1. Semua system keamana pada UTM server dapat dimonitoring pada system terpusat yaitu pada UTM Server
2. Pada UMT Firewall ini, selalu melakukan history pada log file untuk tahap evaluasi
3. Warna merah tanda *VPN*
4. Warna orange tanda *content filtering*
5. Warna biru tanda *anti-virus*
6. Warna hitam tanda *anti-spam*
7. Warna hijau tanda *IPS*
8. Warna kuning tanda *firewall*

3.1.3.4. Perbandingan *Unified Threat Management Firewall Security*

Pengetesan ini dilakukan untuk membandingkan kinerja dari Unified Threat Management itu sendiri.

A. Throughput Test Performance

Pada gambar 3.27 berikut ini adalah hasil pengetesan *performance throughput* untuk membandingkan kinerja

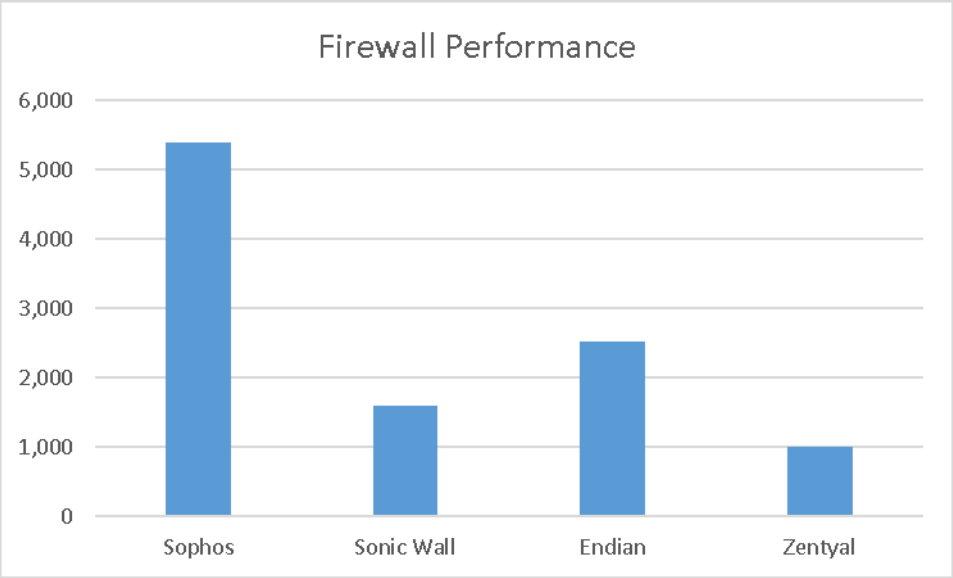


Gambar 3. 27Grafic Perbandingan *Throughput Test Performance*

Pada grafik diatas menunkukan bahwa performa dari *endian Firewall* itu sendiri cukup bagus sebagai sistem *Firewall*

B. Firewall Test Performance

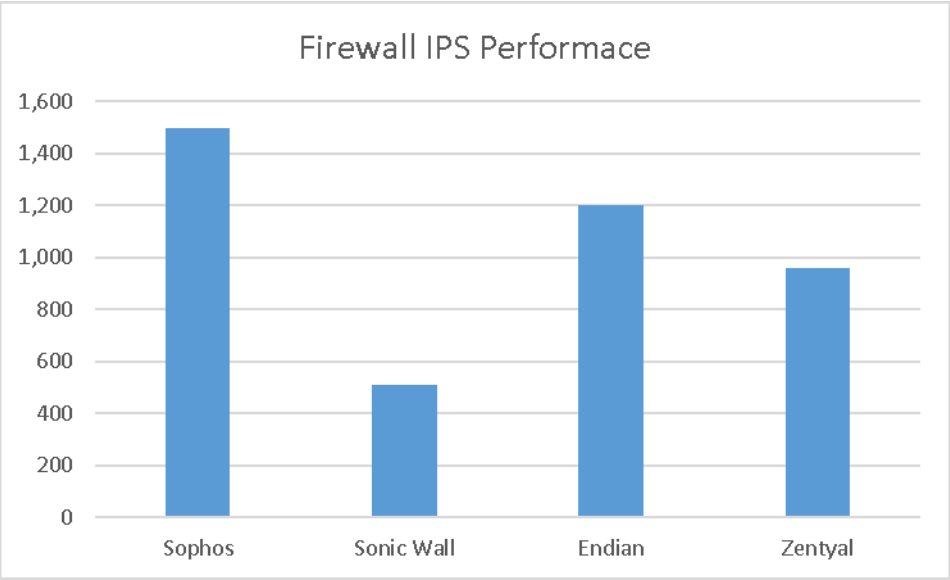
Pada gambar 3.28 adalah perbandingan performa *Firewall* dari berbasis *base* sistem operasi.



Gambar 3. 28 Grafik Perbandingan *Firewall Performance*

C. Firewall Intrusion Prevent System (IPS) Test Performance

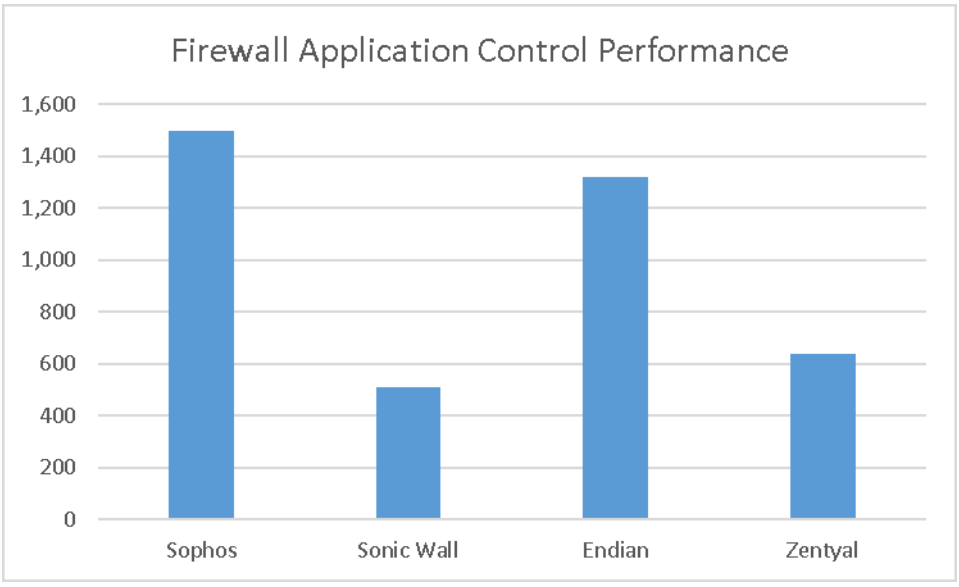
Pada gambar 3.29 merupakan perbandingan kinerja *IPS* pada sistem *Firewall* ini.



Gambar 3. 29 Grafik Perbandingan *IPS Test Performance*

D. Firewall Application Control Test Performance

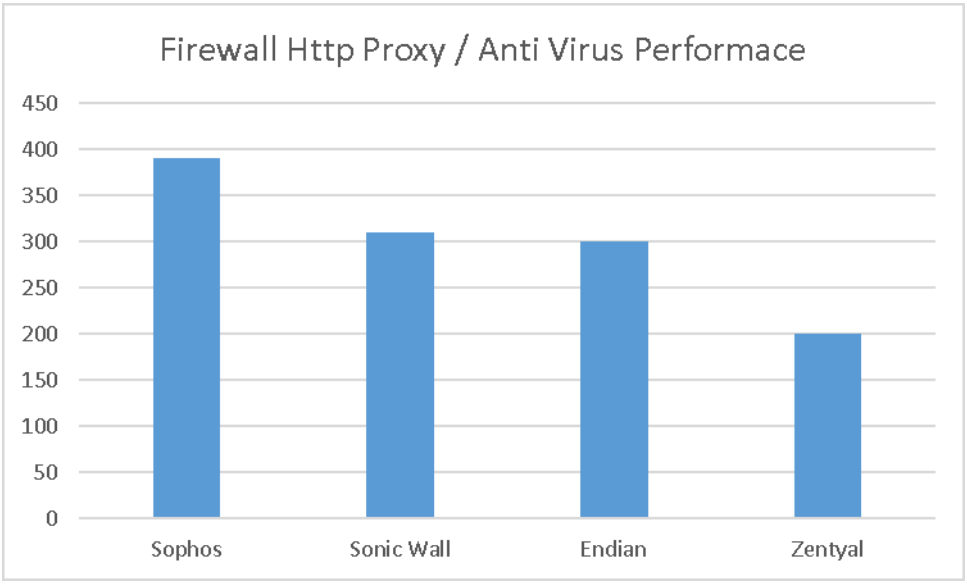
Pada tindakan ini merupakan perbandingan *Performance* kinerja *firewall* dengan application control.



Gambar 3. 30 Grafik Perbandingan *Firewall Apllication Control Performance*

E. Firewall Http Proxy Anti Virus Performance

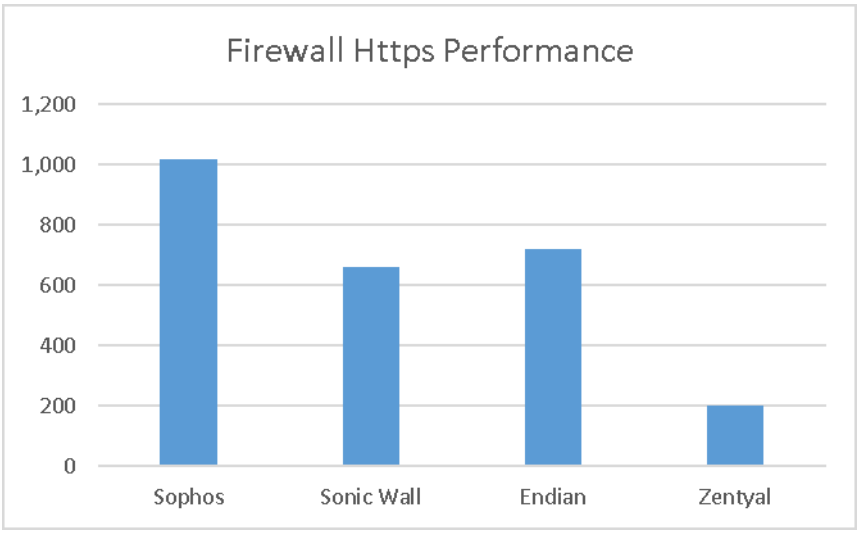
Pada tindakan ini merupakan perbandingan Performance kinerja *firewall* dengan *HTTP, Proxy* dan *anti virus.*



Gambar 3. 31 Grafik Perbandingan *Proxy Anti Virus Performance*

F. Firewall Https Performance

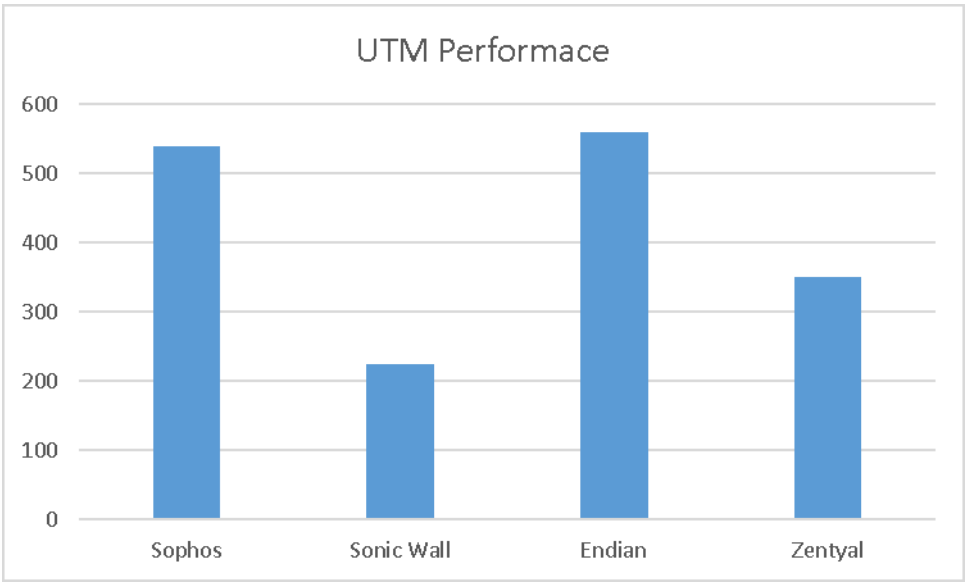
Pada tindakan ini merupakan perbandingan *Performance* kinerja firewall dengan *HTTPS.*



Gambar 3. 32Grafik Perbandingan *HTTPS Performance*

G. UTM firewall berbasis *Linux Performance*

Pada tindakan ini merupakan perbandingan *Performance* kinerja *UTM firewall* pada sistem operasi berbasis *Linux*.



Gambar 3. 33 Grafik perbandingan *UTM firewall Performance*

H. Feature Endian Firewall

Endian *Firewall* sendiri memiliki beberapa *feature* yang tertara pada tabel 3.38 berikut ini

Tabel 3. 38 *Feature Endian Firewall*

No	*Feature*	Spesifikasi *Feature*
1	*Web Interface*	*a. Simple status monitoring Systems dan Services* *b. Alerts* *c. Graphs Penggunaan* *d. Policies dan reports.*
2	*Content Filtering*	*1. content filtering* *2. filtering URLs* *3. filtering Files Patterns* *4. content filtering Keywords* *5. content filtering IP Addresses dan Ports* *6. content filtering Browsers* *7. policy management Users* *8. Block HTTP and HTTPS*
3	*Security dan intrusion Prevent*	*a. Antivirus* *b. protection Malwares* *c. Intrusion Prevention System (IPS)* *d. IP* Tabel *rules* *e. Block traffic* *f. Protection Port Scanning* *g. Auto update URL Block List.*
4	*Police Management*	*a. Content Filter Rules* *b. Policy User Management*
5	*Bandwitdh Management*	*a. Allocation Bandwith*
6	*Network Management*	*a. DHCP* *b. PPoE ISP connections* *c. Forward DNS* *d. Port Mapping with IP Address*

		e. VoIP Server Torrent event detection
7	*Remote Connectivity*	*a. VPN Server, Site to site VPN Client*

3.2. Perancangan Sistem

Perancangan sistem adalah suatu proses yang menggambarkan bagaimana suatu sistem untuk memenuhi kebutuhan pada fase analisis. Adapun tahapan yang dilakukan dalam perancangan sistem ini membahas mengenai tujuan perancangan sistem, rancangan sistem keamanan unified threat managenebt yang diterapkan pada topologi jaringan komputer di DPRD Provinsi Jawa barat.

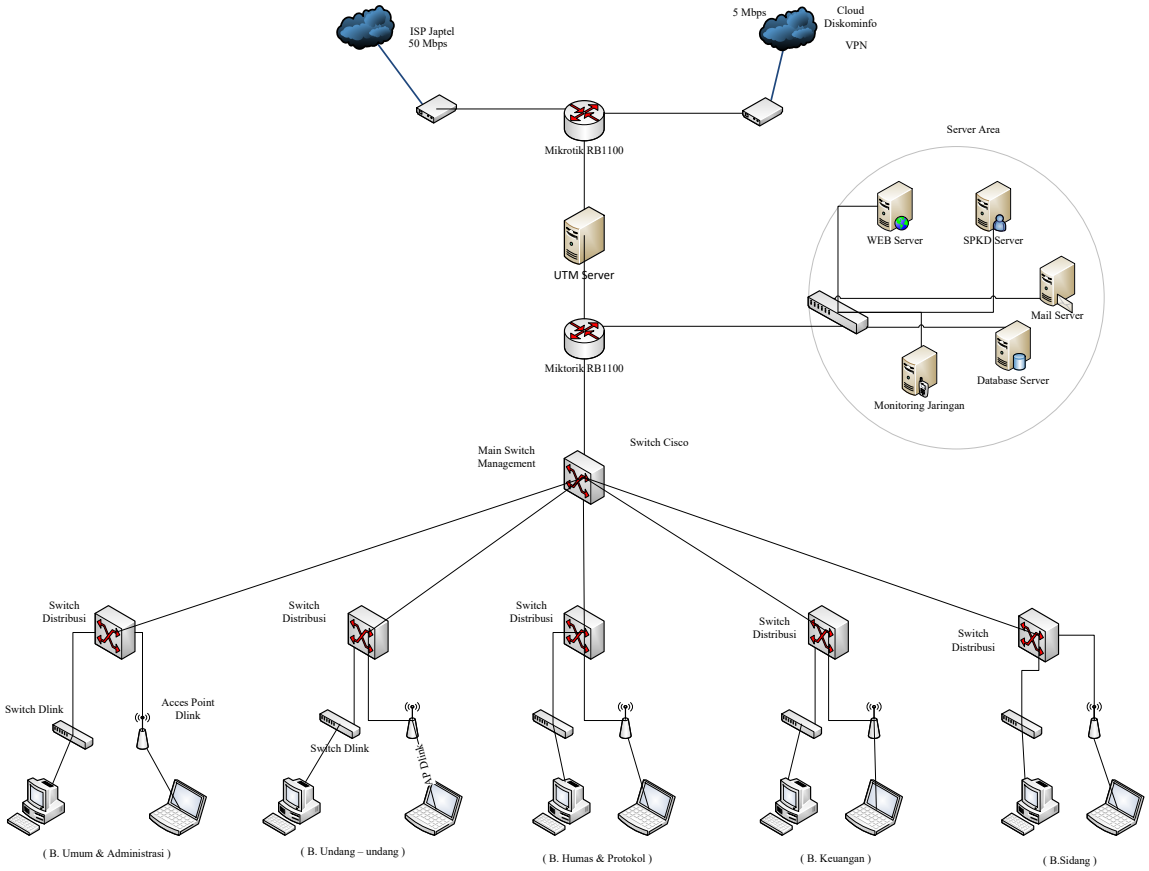
3.2.1. Tujuan perancangan sistem

Perancangan sistem merupakan tindak lanjut dari tahap analisa yang bertujuan untukmemberikan gambaran sistem keamanan jaringan yang akan dibangun. Dengan kata lain perancangan sistem didefinisikan sebagai penggambaran sketsa dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan memiliki fungsi. Selain itu, perancangan sistem bertujuan untuk mengarahkan sistem yang terinci, yaitu pembuatan perancangan yang jelas dan lengkap yang akan digunakan untuk pembuatan simulasi. Hasil analisis ini, kemudian dapat diterapkan di jaringan local area network DPRD Provinsi jawa barat dengan menggunakan Endian *Firewall* sebagai base operation system untuk keamanan jaringan *Unified Threat Management*. Hal tersebut ditujukan untuk membuat solusi untuk permasalahan yang muncul di sistem keamanan jaringan DPRD Provinsi Jawa barat.

3.2.2. Gambaran Sistem yang dibangun

Gambaran sistem keamanan jaringan ini yang akan digunakan di DPRD Provinsi Jawa Barat. Berdasarkan uraian masalah-masalah yang telah dipaparkan sebelumnya, tujuan dari gambaran sistem yang dibangun adalah untuk membuat solusi dari permasalahan yang sering timbul di DPRD Provinsi Jawa Barat. Berikut ini adalah gambaran sistem secara global yang akan dibangun:

3.2.3. Perancangan Topologi Sistem Keamanan Jaringan *UTM Firewall*



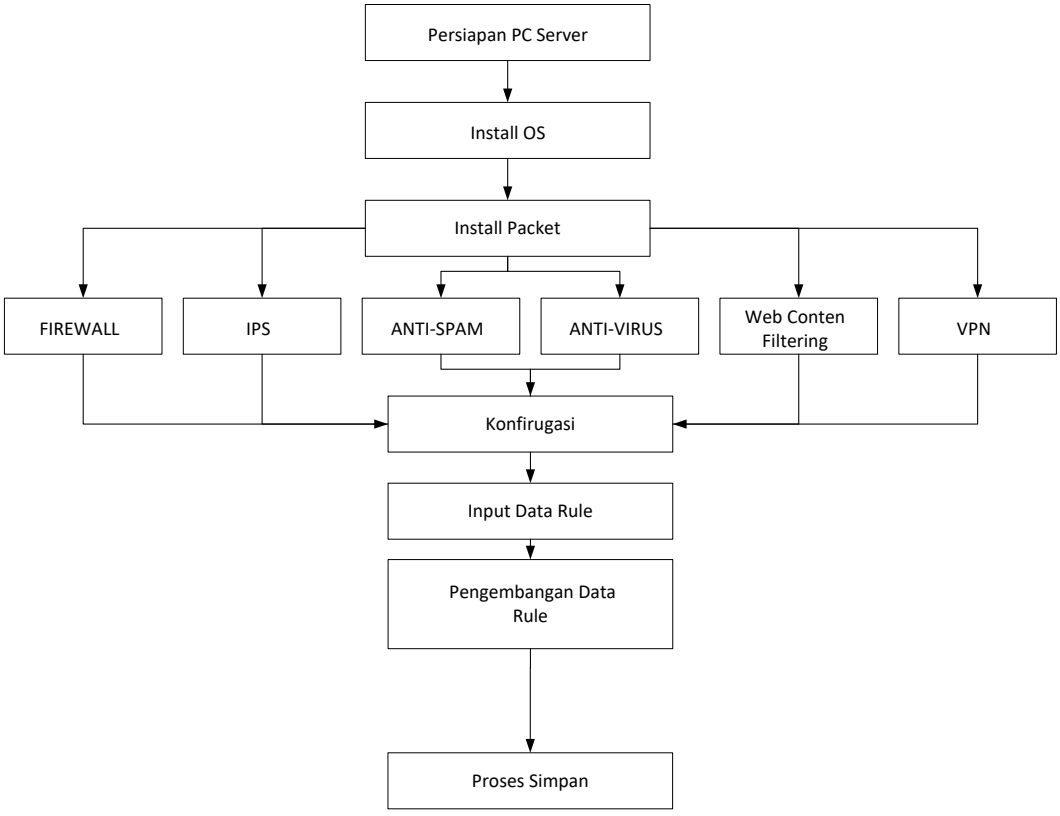
Gambar 3. 34 *Topologi UTM Firewall*

Keterangan Topology *UTM Firewall*:

1. *UTM firewall* ditempatkan diantara *Mikrotik* 1 (penghubung ke *modem ADSL*) dan *Mikrotik* 2 (penghubung ke jaringan internal
2. Pada *UTM firewall* menggunakan modul 2 *Lan Card*
3. Lalu lintas *packet data* yang masuk dan keluar akan melewati *UTM Firewall*

3.2.4. Uraian Procedure sistem yang dirancang

Berdasarkan hasil analasis metode penelitian, berikut ini adalah tahapan – tahapan dalam implementasi server Unified Threat Management (UTM) Firewall pada gambar 3.35

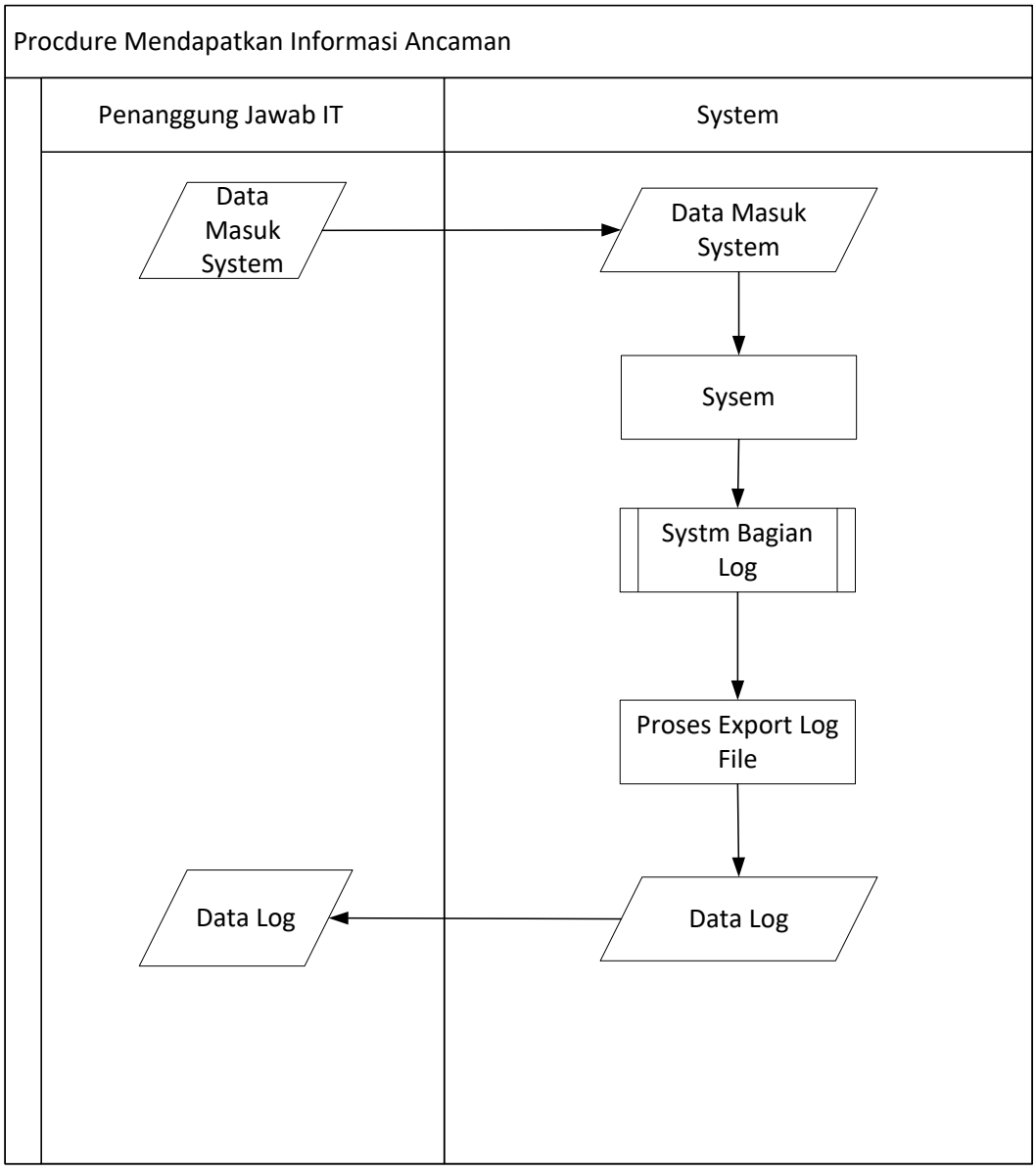


Gambar 3. 35 Procedure tahapan sistem yang dirancang

Pada setiap tahapan dilakukan secara berurutan. Urutan setelah tahapan installasi packet yaitu *firewall, IPS, Anti-Spam, Anti-virus, web content filtering dan VPN.* Selanjutnya dilakukan kebijakan seperti hak akses.

3.2.4.1. Uraian Prosedur Mendapatkan Informasi Ancaman serangan

Berdasarkan hasil analisis sistem yang berjalan pada jaringan DPRD Provinsi Jawa Barat, gambar 3.36 merupakan *flowchart* dimana Penanggung Jawab IT mendapatkan data ancaman dari sistem.

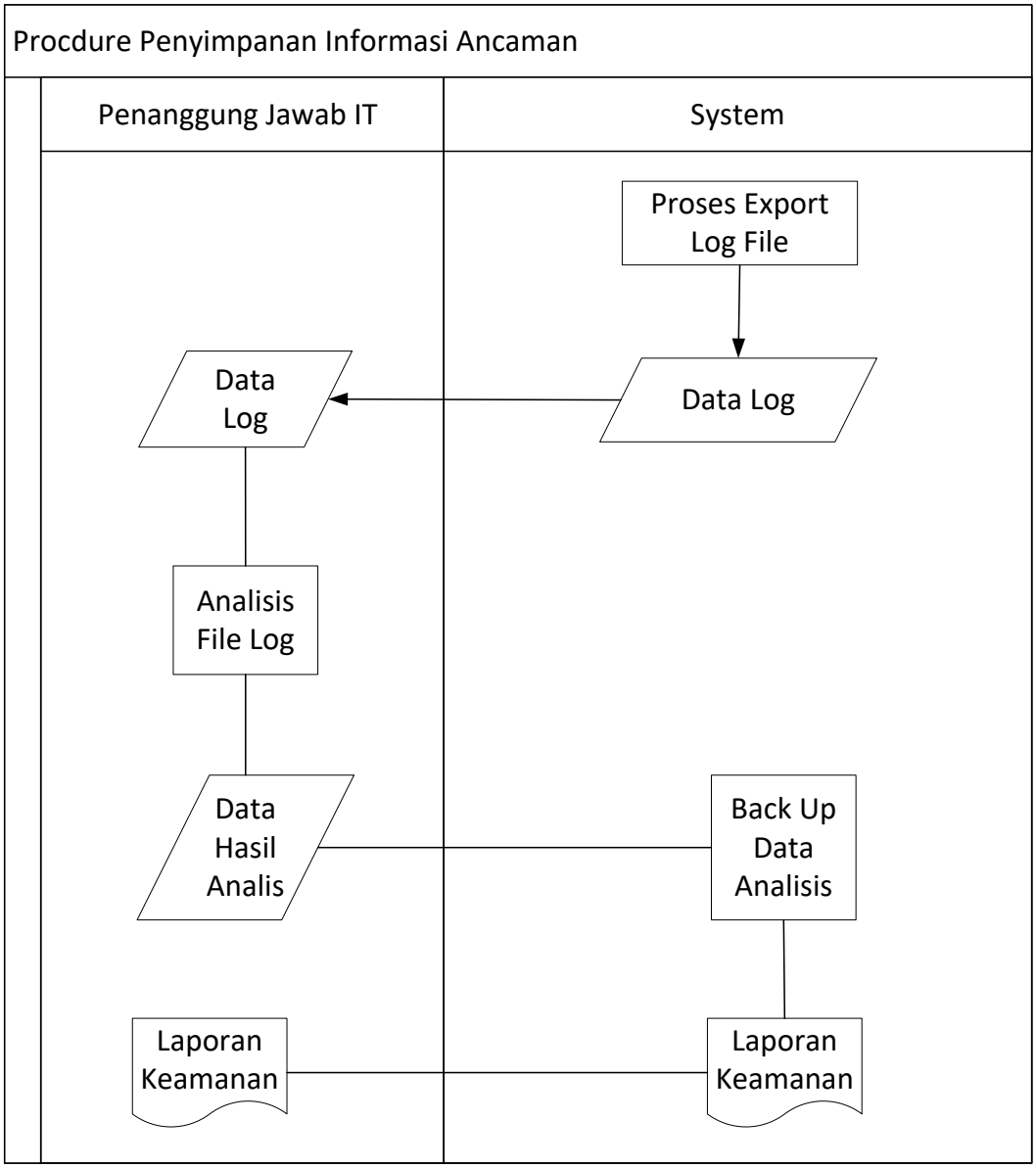


Gambar 3. 36 Procedure Mendapatkan Informasi Ancaman serangan

Pada tahapan ini data acuan untuk perancangan sistem dengan menggunakan *data log* yang sudah ada dalam penerapan UTM Server

3.2.4.2. Uraian Prosedur Penyimpanan Informasi Ancaman serangan

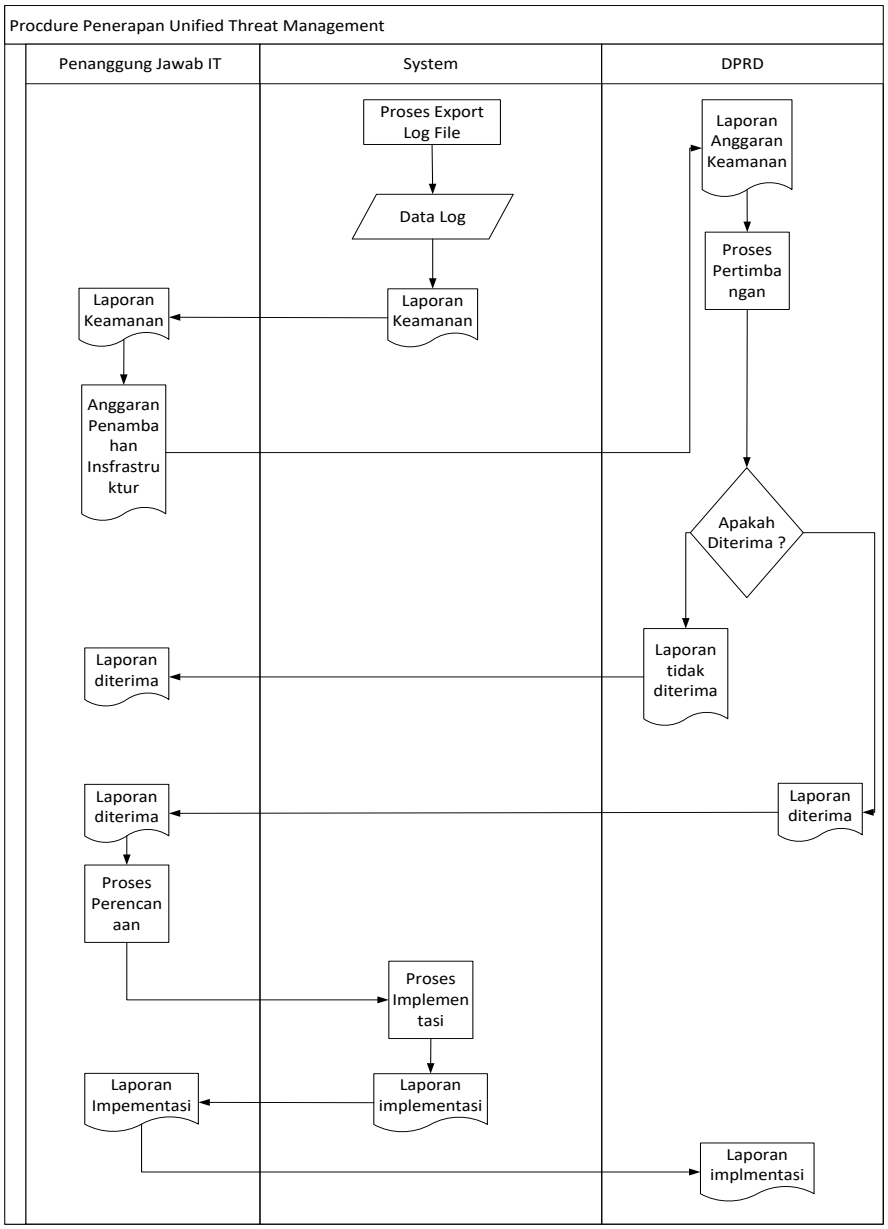
Berdasarkan hasil analisis pada sistem berjalan, gambar 3.37 merupakan *flowchart* dimana Penanggung Jawab IT melakukan peroses analysis terhadap *data log* dan melakukan penyimpanan informasi ancaman yang bertujuan di jadikan acuan dalam melakukan kebijakan keamanan.



Gambar 3. 37 Procedure Penyimpanan Ancaman Serangan

3.2.5. Uraian Procedure Penerapan *Unified Threat Management Firewall*

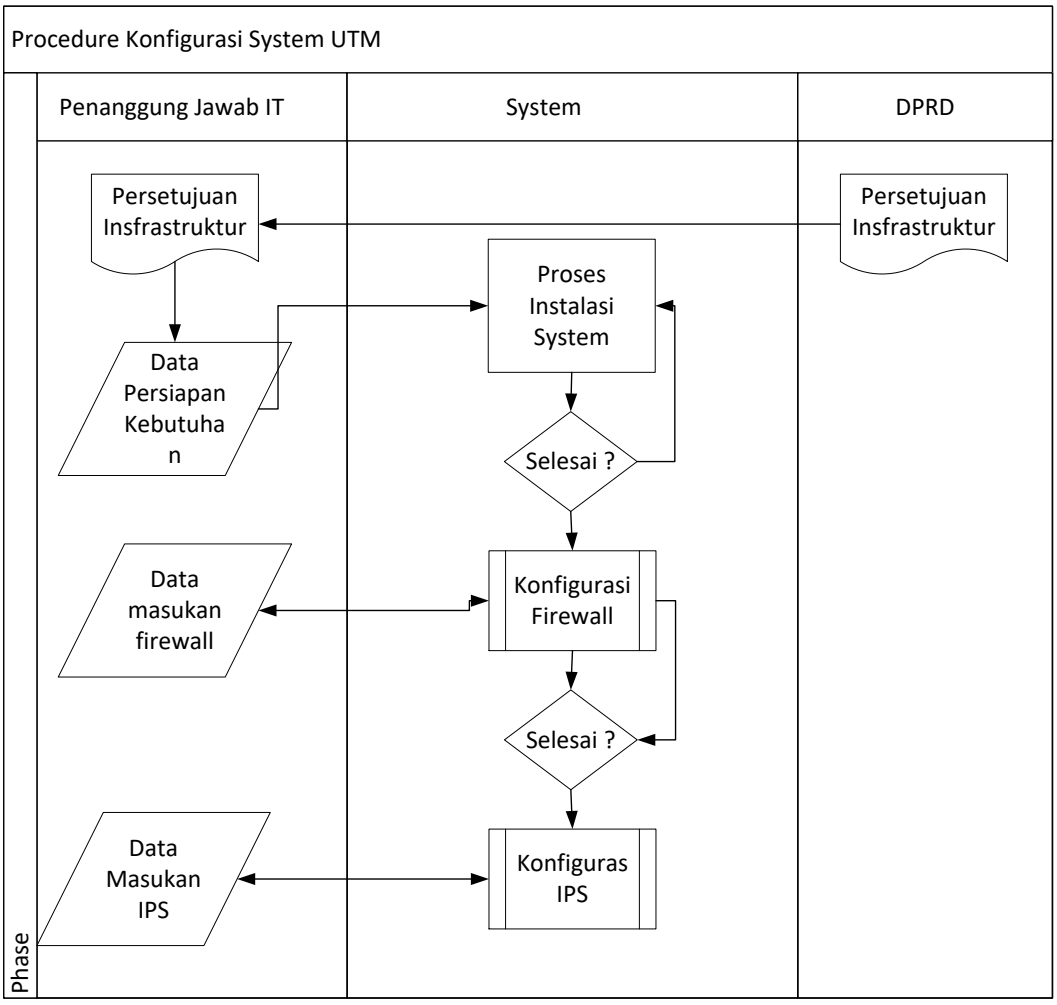
Berdasarkan hasil analisis pada sistem berjalan birokrasi, gambar 3.38 merupakan *flowmap* dimana Penanggung jawab IT dalam menerapkan *UTM firewall* harus melalui persetujuan DRPD yaitu staff Bag. Administrasi dan melaporkan hasil dari penambahan insfrastruktur tersebut.



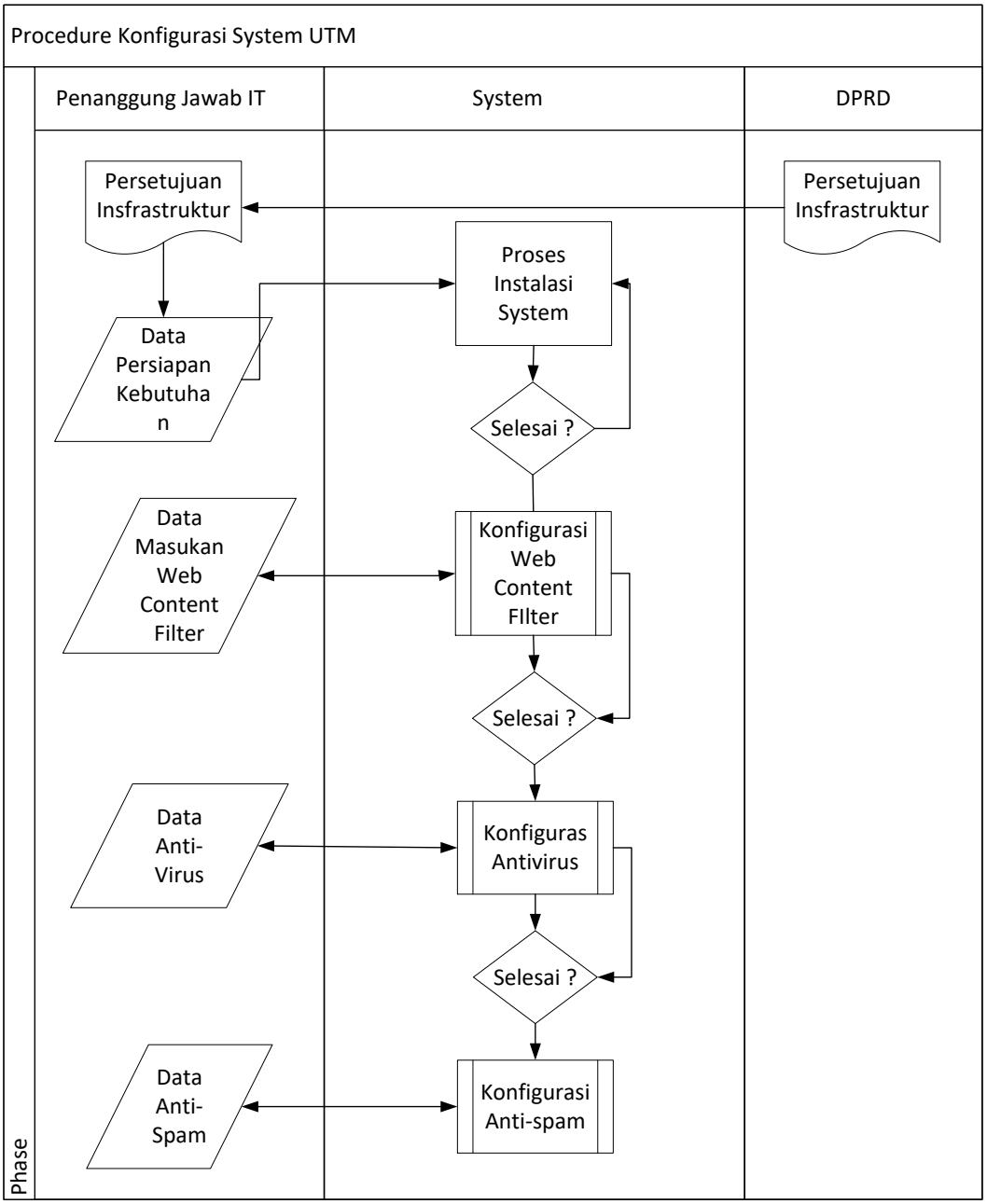
Gambar 3. 38 Procedure Penerapan *UTM Firewall*

3.2.5. Uraian Procedure Pengaturan *Unified Threat Management Firewall*

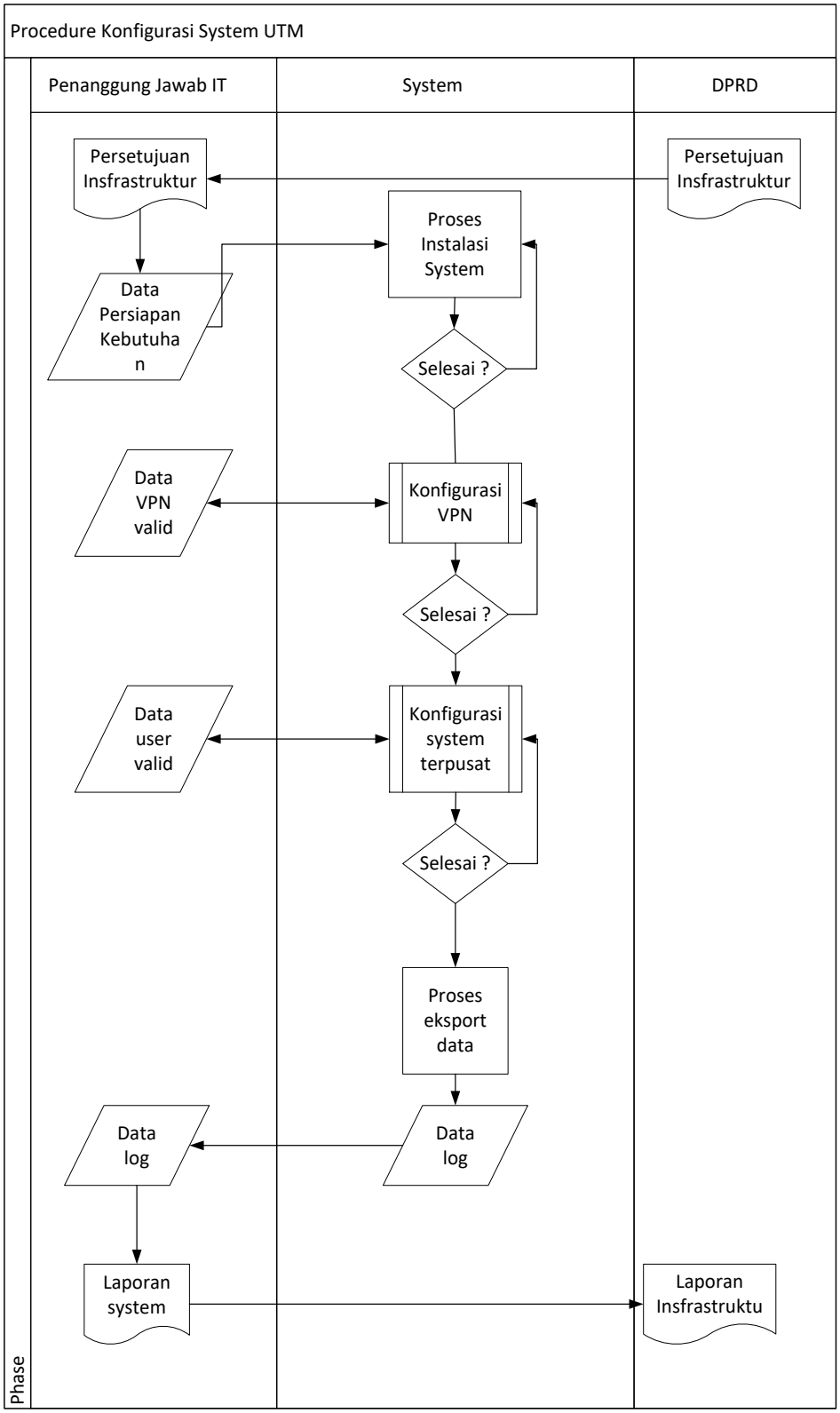
Berdasarkan hasil analisis terhadap sistem yang dirancang berikut ini pada gambar 3.39, gambar 3.40 dan gambar 3.41 merupakan tahapan – tahapan dalam pengaturan sistem keamanan *unified threat managemet (UTM) firewall*



Gambar 3. 39 Procedure Konfigurasi *UTM firewall* (1)



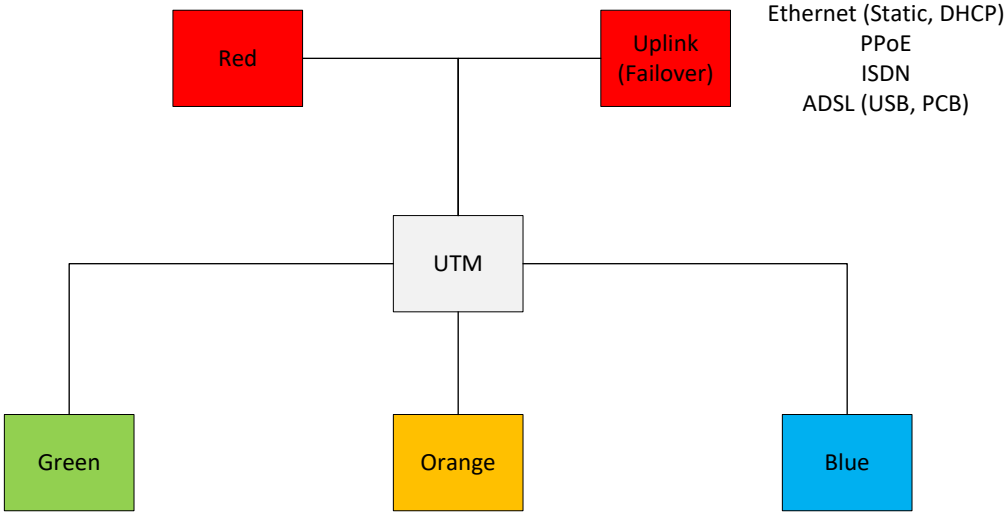
Gambar 3. 40 Procedure Konfigurasi *UTM firewall* (2)



Gambar 3. 41 Procedure Konfigurasi *UTM firewall* (3)

3.2.5.1. *Rule Network*

Tipe konfigurasi dasar yang digunakan adalah *RED/GREEN*, dimana *firewall* melindungi internal *network (GREEN)* dari *internet.* Jika untuk mengkonfigurasi wireless access point, dapat menghubungkannya ke *interface BLUE* dan mengkonfigurasi *Firewall* untuk membatasi akses di *LAN* tersebut. Jika untuk mengkonfigurasi beberapa *server* yang diperbolehkan diakses *via internet*, dapat diletakkan di *untrusted DMZ* pada *interface ORANGE*. *Interface RED* dapat dihubungkan dengan *modem* atau *NIC*, terdapat delapan Tipe *Konfigurasi Network.*



Gambar 3. 42 *Network Zone*

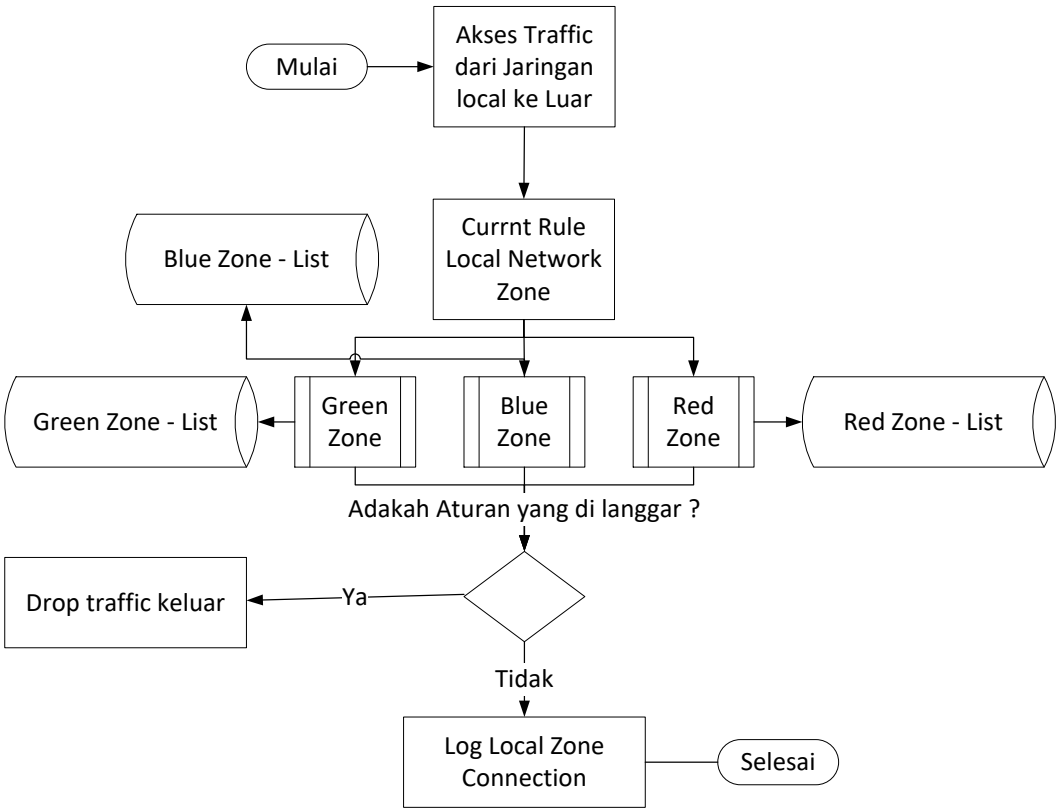
Tabel 3. 39 Data IP Address Zone

Zone	**Keterangan**	***IP Address***
Red	*Internet (WAN)*	192.168.1.0
Green	*Local Area Network (LAN)*	200.10.3.0
Orange	*DMZ (Least Protection)*	-
Bleu	*WIFI (Wireless / Hotspot)*	-

Keterangan :

1. Zona yang digunakapan hanya *Red Zone* dan *Green Zone*
2. Untuk *Red Zone* berada pada *Network 192.168.1.0*
3. Untuk *Green Zone* berada pada *Network* 200.10.3.0

Adapan *flowchart* yang tertera pada gambar 3.42 merupakan gambaran bagaimana cara kerja dari sebuah *Rule Local Network* sehingga bertujuan untuk pembagian akses terhadap jaringan secara jelas.

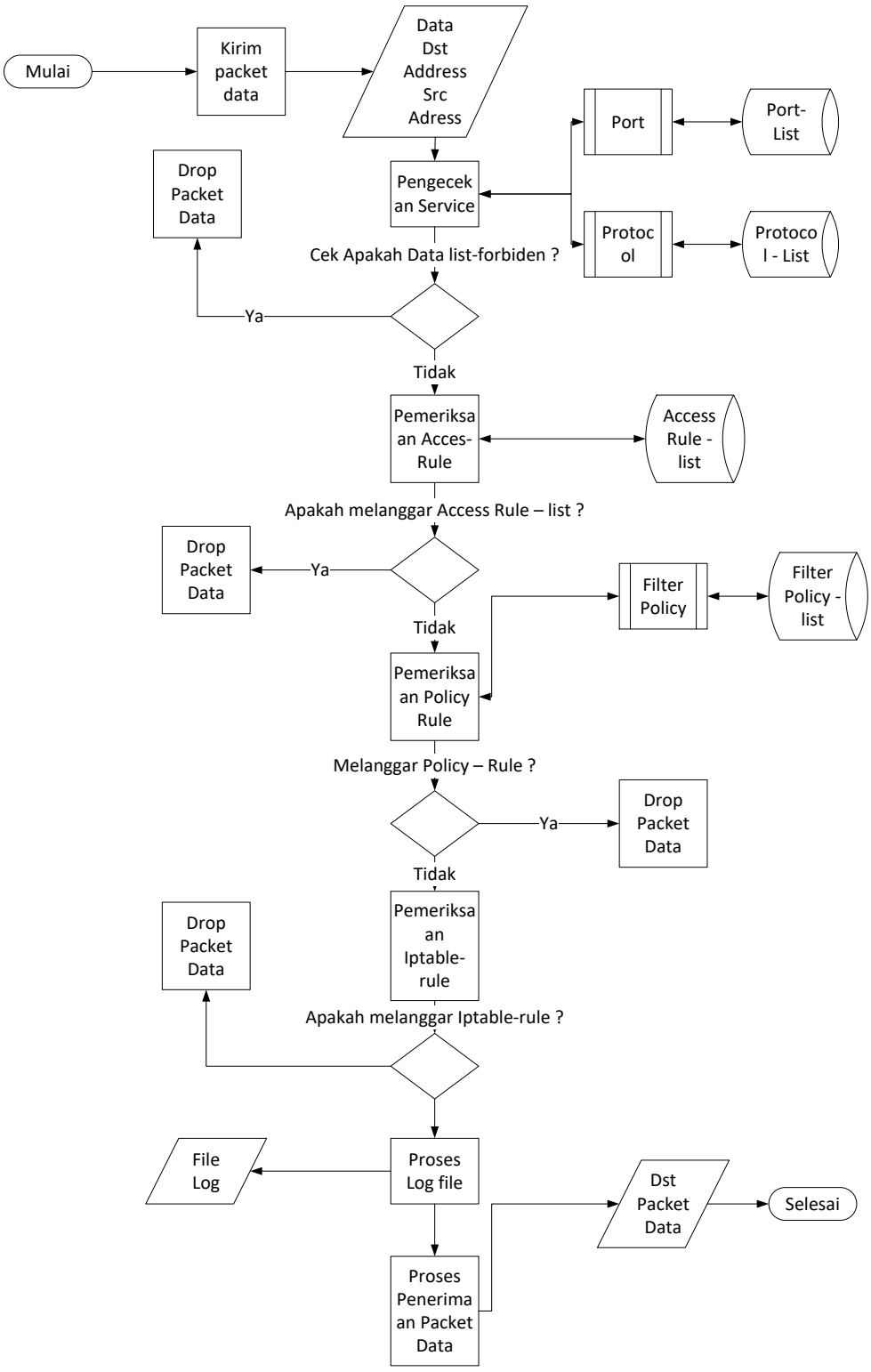


Gambar 3. 43 *Flowchart* Zone

3.2.5.2. *Firewall*

Berdasarkan hasil analisis dari sistem keamanan yang sedang berjalan, pada gambar 3.43 merupakan *flowchart* cara kerja dari sebuah *firewall* yang

memiliki aturan – aturan yang sesuai dengan analisis terhadapa masalah pada bagian *firewall* sistem yang berjalan.



Gambar 3. 44 *Flowchart Firewall*

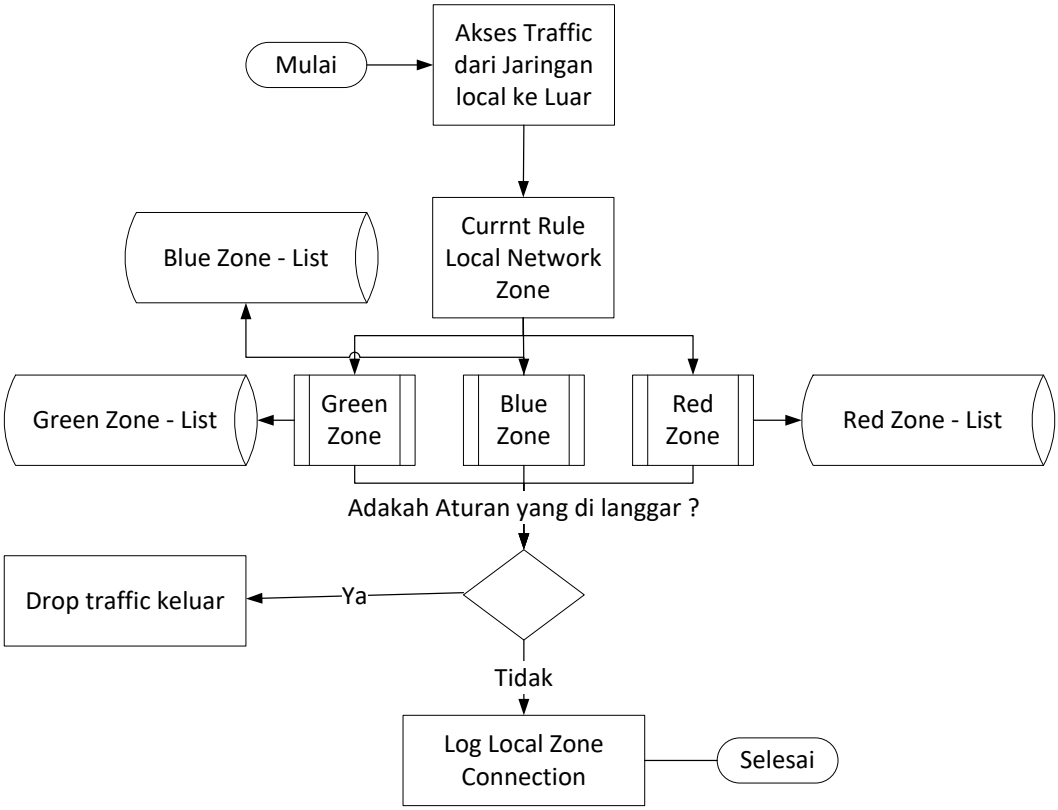
Adapun Aturan – aturan yang diterapakan sesuai dengan permasalahan dijabarkan pada tabel 3.40 terhadap *Protocol* dan *internet service.*

Tabel *3. 40 Data Rule Firewall*

No	Protokol	Source	Destination	Remark
1	*TCP*	*Green*	*80(HTTP)*	*Allow HTTP*
2	*TCP*	*Green*	*443(HTTPS)*	*Allow HTTPS*
3	*TCP*	*Green*	*21(FTP)*	*Allow FTP*
4	*TCP*	*Green*	*25(SMTP)*	*Allow SMTP*
5	*TCP*	*Green*	*110(POP3)*	*Allow POP3*
6	*TCP*	*Green*	*143(IMAP)*	*Allow IMAP*
7	*TCP*	*Green*	*53(DOMAIN)*	*Allow DOMAIN*
8	*UDP*	*Green*	*53(DOMAIN)*	*Allow DOMAIN*
9	*TCP*	*Blue*	*53(DOMAIN)*	*Allow DOMAIN*
10	*UDP*	*Blue*	*53(DOMAIN)*	*Allow DOMAIN*
11	*TCP*	*Orange*	*53(DOMAIN)*	*Allow DOMAIN*
12	*UDP*	*Orange*	*53(DOMAIN)*	*Allow DOMAIN*

A. Zona Internal Traffic

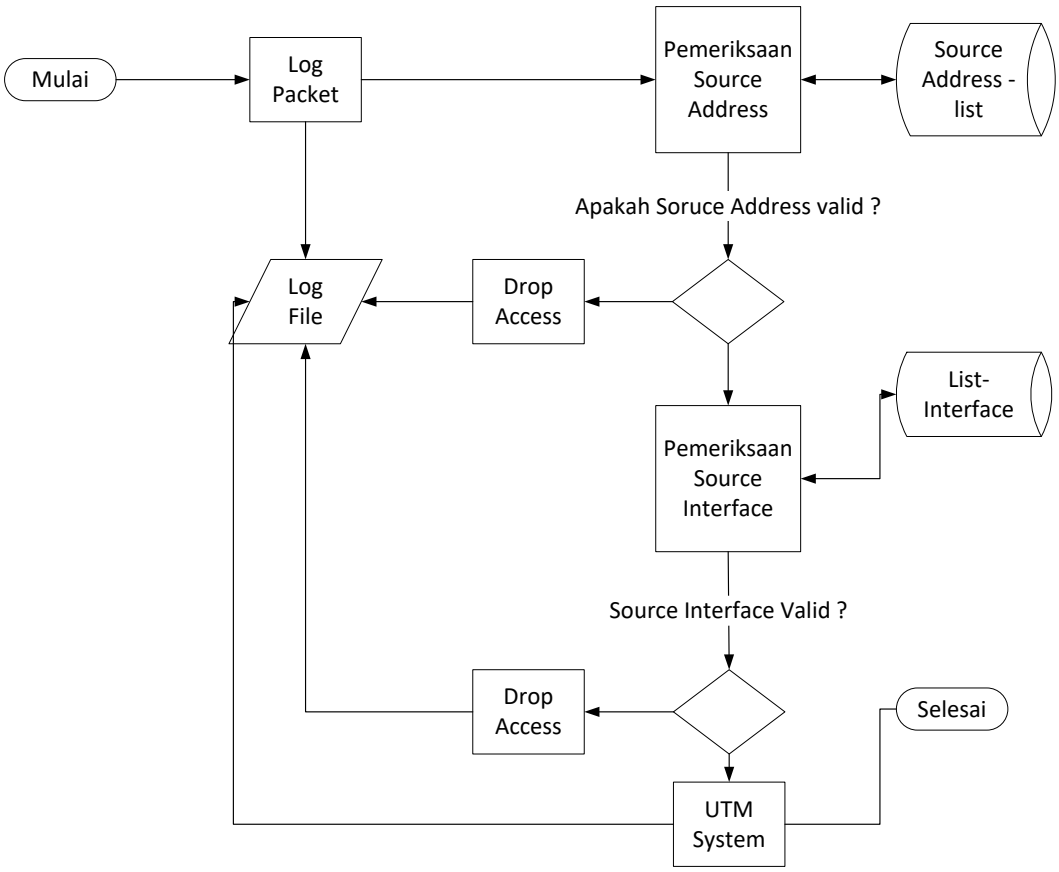
Pada bagian ini yaitu aturan yang berlaku untuk lalu lintas pada jaringan internal, sehingga semua *traffic packet data* sesuai dengan *zone network.*



Gambar 3. 45Zona Internal Traffic

B. System Access

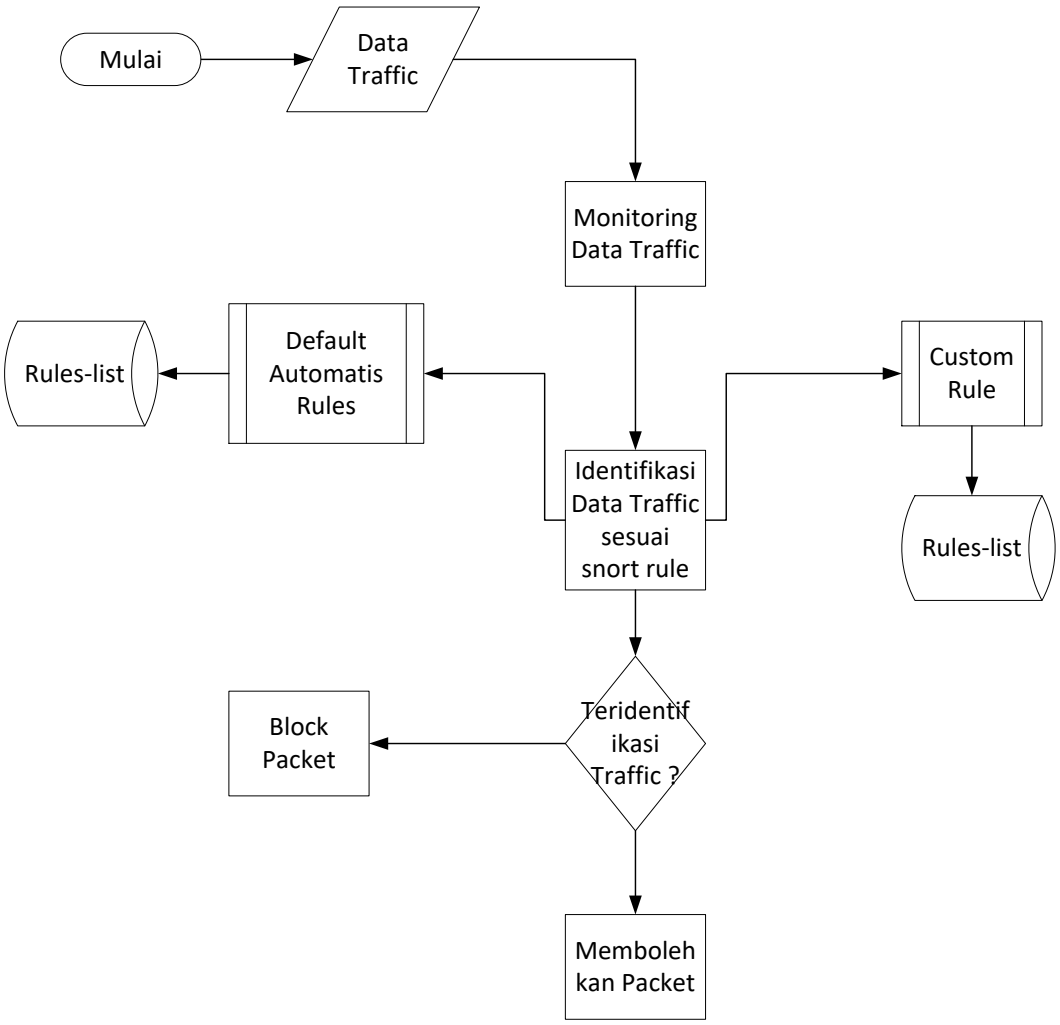
Pada gambar 3.45 merupakan gambaran akses yang valid terhadap sistem keamanan *UTM Firewall.*



Gambar 3. 46 System Access

3.2.5.3. *Intrusion Prevent System (IPS)*

Berdasarkan hasil analisis permasalaan pada sistem keamanan yang berjalan dimana belum memiliki sistem deteksi pada jaringan internal DPRD Provinsi Jawa Barat, maka pada gambar 3.46 merupakan *flowchart* cara kerja *IPS* yang bertujuan untuk mendeteksi sebuah ancaman.



Gambar 3. 47 *flowchartt IPS*

Adapun aturan – aturan yang diterpakan pada *IPS* ini, dijabarkan pada tabel 3.48 dengan mengacu pada *router, server –server* dan komputer *client*

Tabel *3.48 IPS Rule*

No	Kategori	Keterangan
1	*app-detect.rules*	Kategori ini aturan yang mencari, dan kontrol, lalu lintas dari aplikasi tertentu yang menghasilkan aktivitas jaringan. Kategori ini akan digunakan untuk mengontrol berbagai aspek bagaimana aplikasi berperilaku.
2	*server-mail*	Kategori ini berisi aturan yang mendeteksi kerentanan dalam mail server.
3	*sql*	Kategori ini berisi aturan yang mendeteksi injeksi sql atau adanya kerentanan lainnya terhadap sql seperti server.

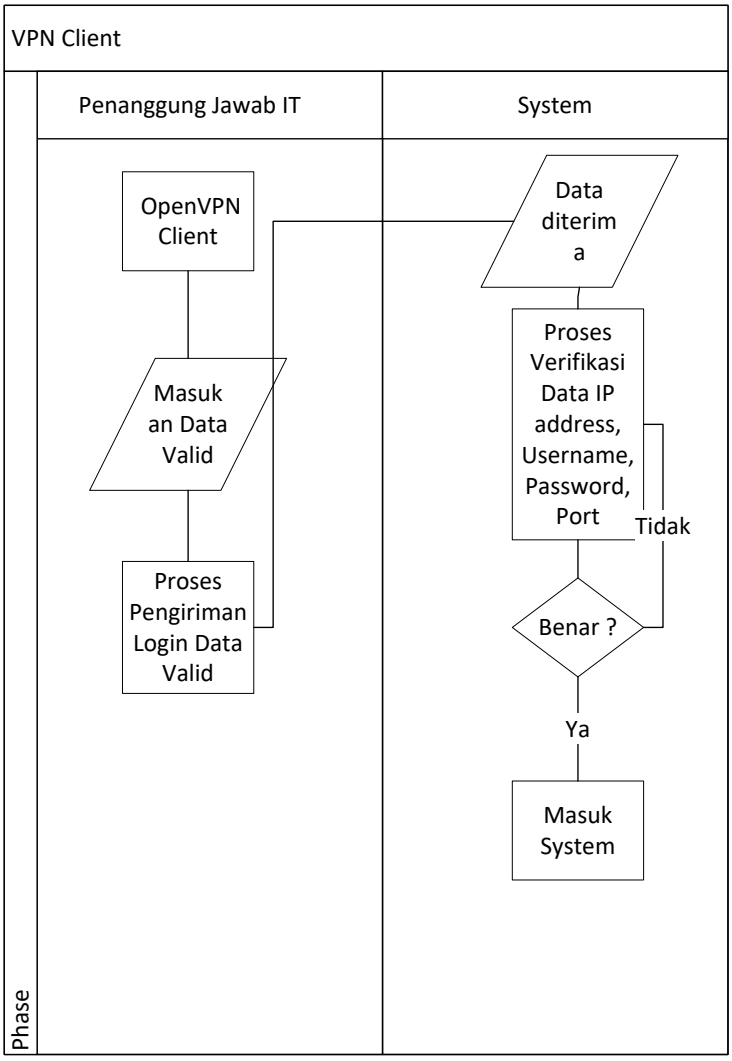
4	*server-apache*	kategori dengan kerentanan di atau serangan terhadap Apache Web Server.
5	*protocol-telnet*	Kategori ini adalah untuk aturan yang mungkin menunjukkan adanya protokol telnet atau kerentanan dalam protokol telnet pada jaringan.
6	*x11*	Kategori ini berisi aturan yang mendeteksi penggunaan x11 atau adanya kerentanan lainnya terhadap x11 seperti server.
7	*server-other*	Kategori ini berisi aturan yang mendeteksi kerentanan di atau serangan terhadap server yang tidak rinci dalam daftar di atas
8	*server-webapp*	Kategori ini berkaitan dengan kerentanan di atau serangan terhadap aplikasi berbasis web pada server.
9	*blacklist.rules*	Kategori ini berisi aturan URI, USER-AGEN, DNS, dan alamat IP yang telah ditentukan untuk menjadi indikator aktivitas berbahaya. Aturan-aturan ini didasarkan pada aktivitas dari kotak pasir Talos virus, daftar publik URL berbahaya, dan sumber data lainnya.
11	*browser-chrome.rules*	Kategori ini deteksi untuk kerentanan hadir dalam browser Chrome
12	*browser-firefox.rules*	Kategori ini deteksi untuk kerentanan hadir dalam browser Firefox
16	*browser-plugins*	Kategori ini deteksi untuk kerentanan dalam browser yang berhubungan dengan plugin untuk browser
17	*content-replace*	Kategori ini aturan apa pun yang memanfaatkan "menggantikan" fungsi dalam Snort.
18	*deleted*	Aturan tidak pernah benar-benar dihapus dari ruleset, mereka pindah ke sini.
19	*exploit*	Kategori ini mencari eksploitasi terhadap perangkat lunak dalam bentuk generik.
20	*exploit-kit*	Kategori ini berisi aturan yang secara khusus dirancang untuk mendeteksi mengeksploitasi aktivitas kit.
21	*file-execu*tabel	Kategori ini berisi aturan untuk kerentanan yang ditemukan atau disampaikan melalui file executabel, terlepas dari platform.
22	*file-flash*	Kategori ini berisi aturan untuk kerentanan yang ditemukan atau disampaikan melalui file flash. Baik dikompresi atau dikompresi, terlepas dari metode

		pengiriman platform yang diserang.
23	*file-image*	Kategori ini berisi aturan untuk kerentanan yang ditemukan di dalam file gambar.
25	*file-identify*	Kategori ini adalah untuk mengidentifikasi file melalui ekstensi file, konten dalam file (file sihir), atau kepala yang ditemukan di lalu lintas.
26	*file-java*	Kategori ini berisi aturan untuk kerentanan dalam hadir dari file Java
28	*file-office*	Kategori ini berisi aturan untuk kerentanan dalam hadir dari file Microsoft Office
31	*indicator-compromise*	Kategori ini berisi aturan yang jelas yang akan digunakan hanya untuk mendeteksi sistem dikompromikan positif, positif palsu dapat terjadi.
32	*indicator-obfuscation*	Kategori ini berisi aturan yang jelas digunakan hanya untuk mendeteksi konten dikaburkan. Seperti aturan JavaScript dikodekan.
35	*malware-backdoor*	Kategori ini berisi aturan untuk mendeteksi lalu lintas ditakdirkan untuk mendengarkan saluran perintah backdoor diketahui.
37	*malware-cnc*	Kategori ini berbahaya komando dan kontrol aktivitas diketahui untuk lalu lintas botnet diidentifikasi
38	*malware-tools*	ini berisi aturan yang berhubungan dengan alat-alat yang dapat dianggap berbahaya
39	*malware-other*	Kategori ini berisi aturan yang malware terkait, tapi tidak cocok dengan salah satu dari yang lain 'malware' kategori

3.2.5.4. *VPN*

A. Client

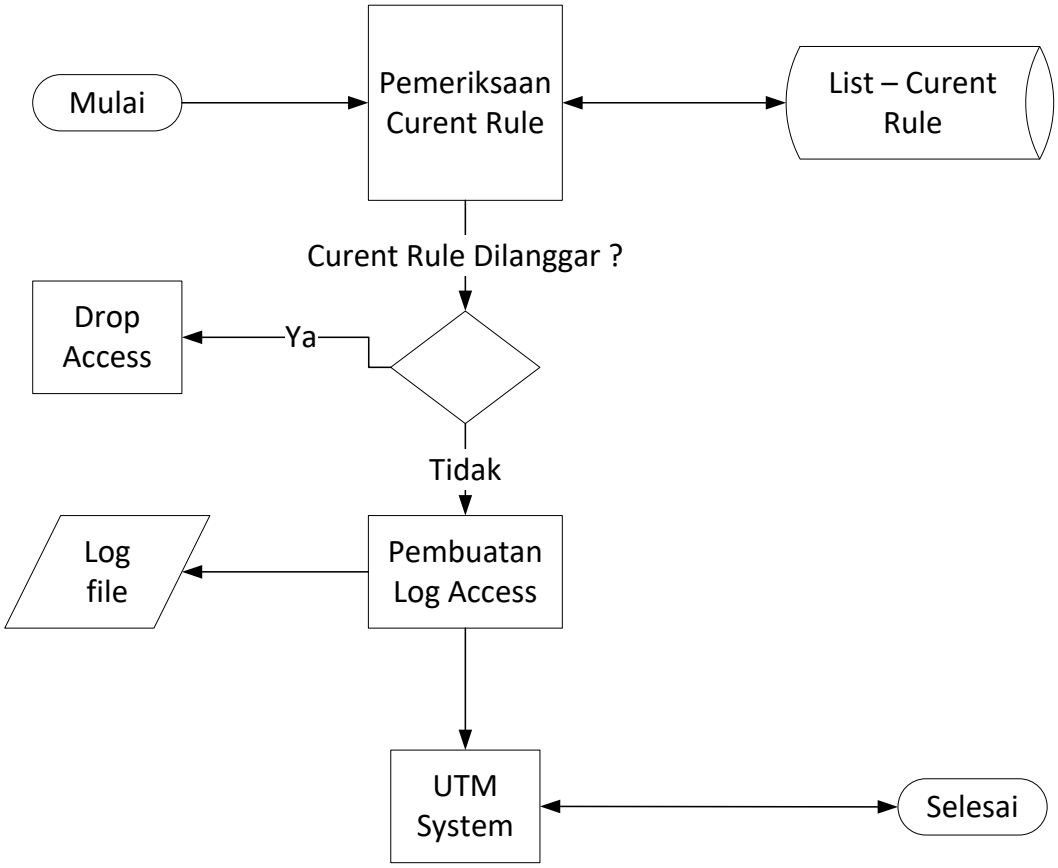
VPN Client ini bertujuan untuk mengkases server *UTM firewall* dari luar jaringan oleh penanggung jawab IT yang digambarkan pada pada gambar 3.47



Gambar 3. 48 *VPN Client*

B. *VPN Server*

Adapun gambaran pada cara kerja *VPN Server* tertera pada gambar 3.48 dengan aturan – aturan yang digunakan pada keterangan.



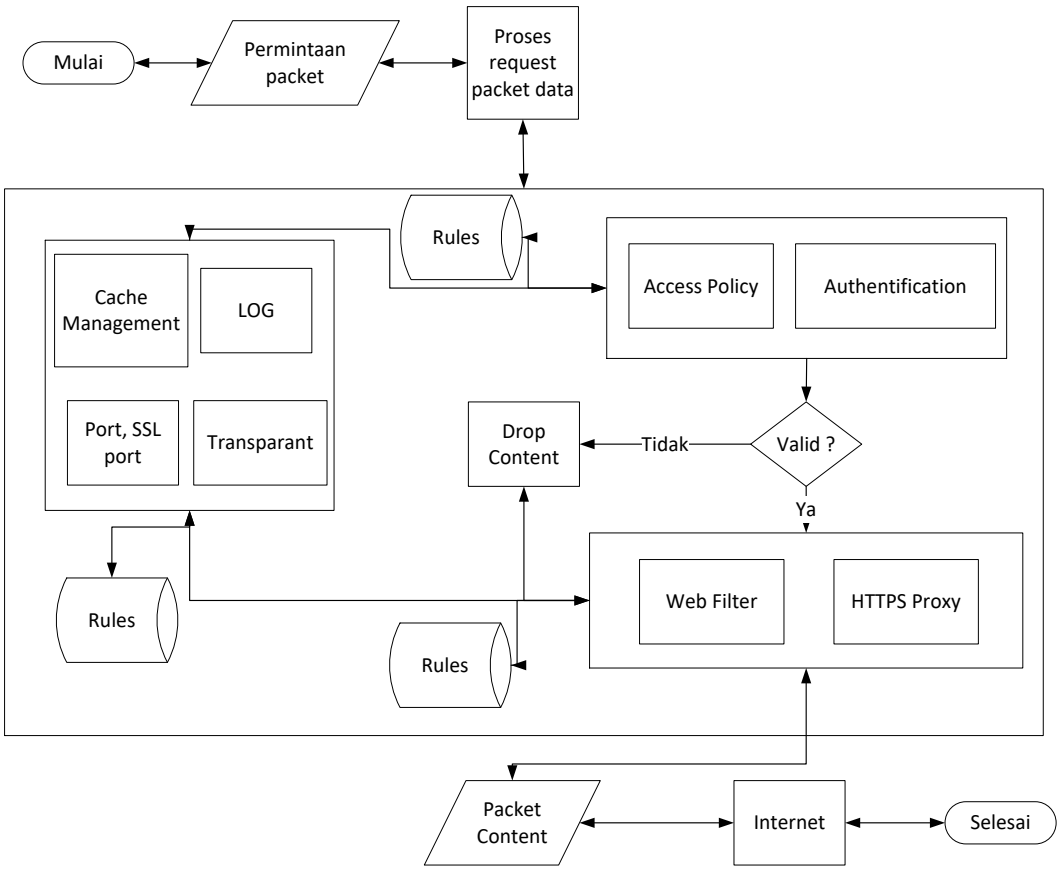
Gambar 3. 49VPN Server

Keterangan :

1. Nama akses adalaha Remote A
2. Tipe koneksi *L2TP PSK*
3. *IP Address* 192.168.0.0

3.2.5.4. *Content Web Filtering*

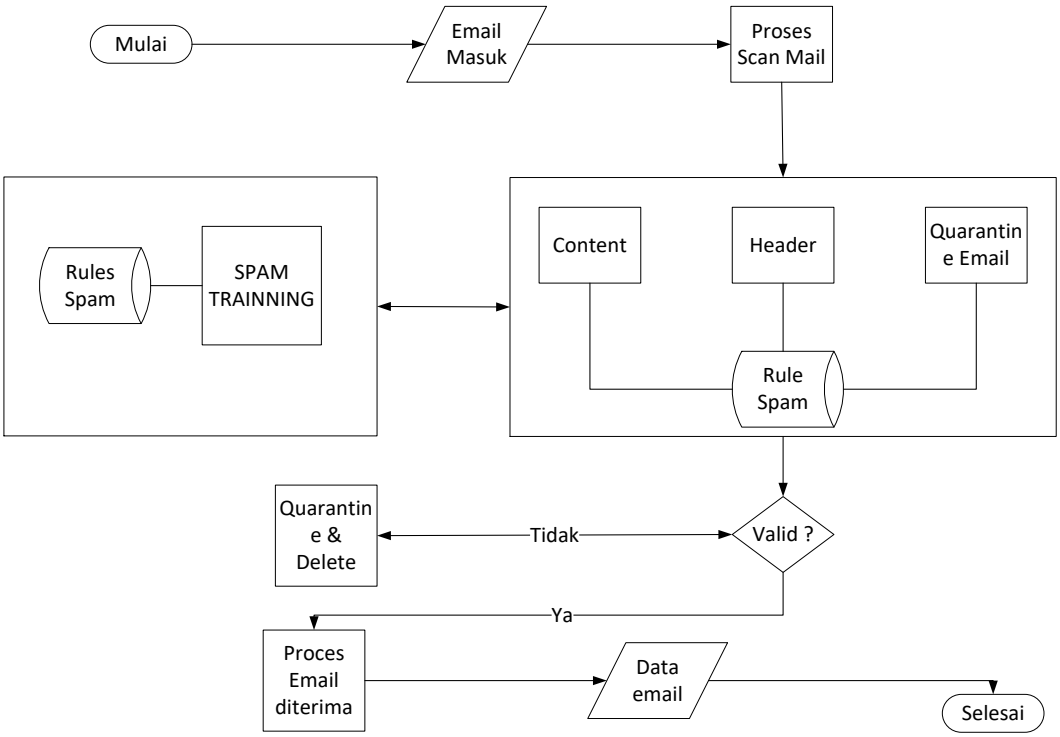
Berdasarkan hasil analisis terhadap ancaman dengan kategori fishing dimana memamfaatkan content sebagai celah masuk ke dalam jaringan internal DPRD Provinsi Jawa Barat, berikut ini pada gambar 3.49 merupakan cara kerja dari *content web filtering* ini.



Gambar 3. 50 *Content Web filtering*

3.2.5.6. Anti-Spam

Berdasarkan hasil analisis terhadap ancaman spam pada *mail server*, berikut gambaran sistem yang tertera pada gambar 3.50

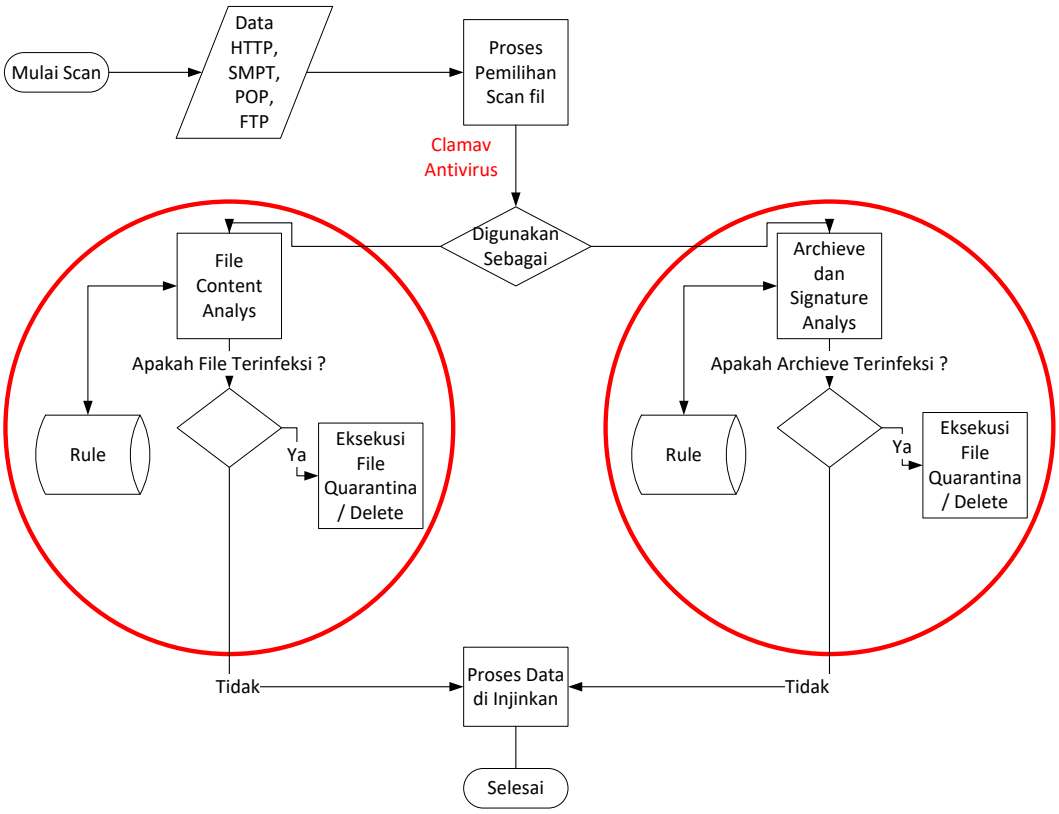


Gambar 3. 51 Procedure Anti-Spam

Adapun aturan dari *spam* ini adalah sesuai dengan permasalahan yang pernah terjadi dengan menggunakan beberapa *keyword* dan *IP Address.*

3.2.5.7. Anti-virus

Berdasarkan hasil analisis terhadap adanya ancaman serangan *virus, malware, keyloger* pada jaringan DPRD Jabar, Berikut ini pada gambar 3.51 merupakan cara kerja antivirus yang diterapkan pada server *UTM Firewall.*



Gambar 3. 52 Procedure Anti-Virus

Adapun untuk database virus menggunakan database dari clamav antivirus dengan alamat website **clamav.net/download/database**

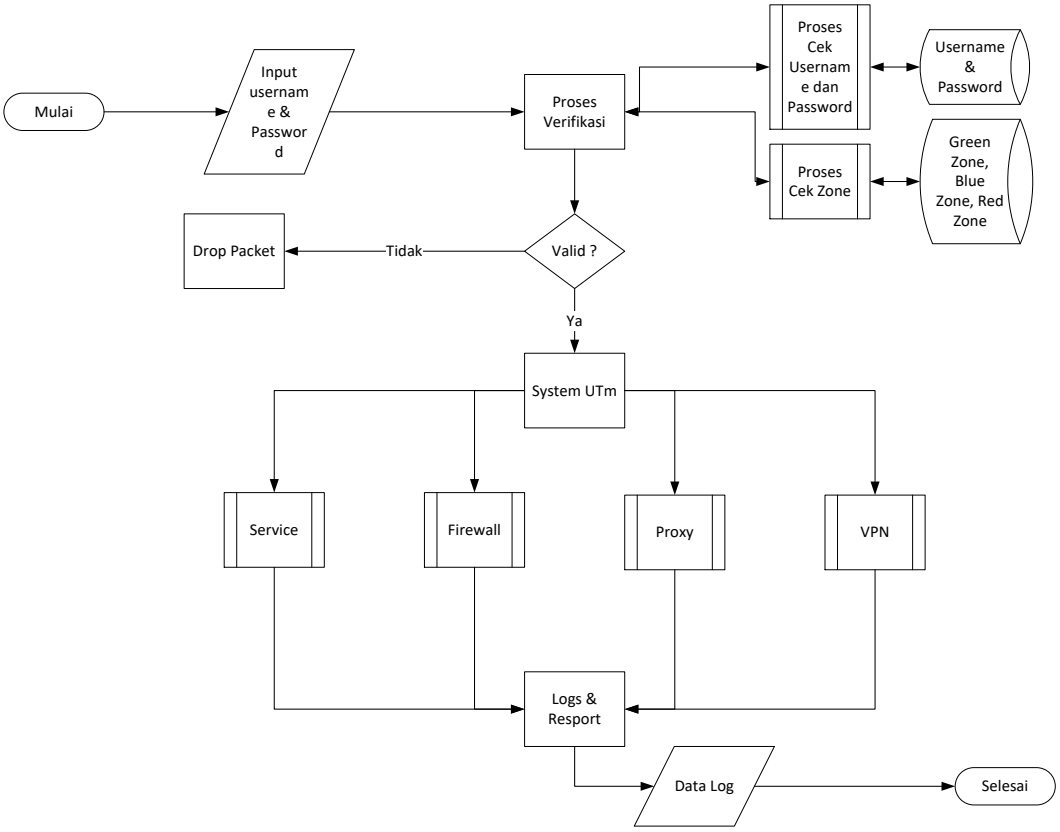
Tabel 3. 41 Rule Anti-Virus

Anti-archive bomb	Ukuran
Max. archive size *	50
Max. nested archives *	5
Max. files in archive *	1000
Max compression ratio *	1000

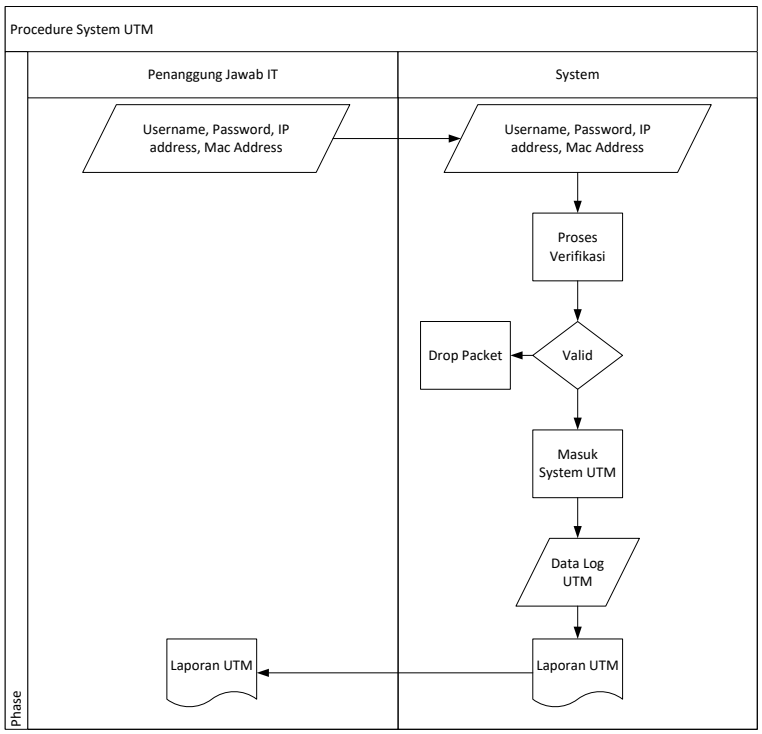
3.2.5.8. Aplikasi control

Berdasarkan hasil analisi sistem yang berjalan dimana untuk monitoring router dan server masih bersifat terpisah – pisah, maka pada gambar 3.52

merupakan *flowchart* yang menggambarkan bagaimana aplikasi control ini dapat melakukan monitoring dan konfigurasi secara terpusat.



Gambar 3. 53 *flowchart* Aplikasi Control Center



Gambar 3. 54 Procedure Akses Sistem *UTM Firewall*

3.2.5.8. Event Notification

Event Notification ini adalah sebagai tanda pemberitahuan telah terjadi pada sistem keamanan unified treat management ini. Dengan event *Notification* ini dapat memudahkan penanggung jawab IT dalam mengawali sistem jaringan. Adapun aturan dalam *evenet Notification* ini tertera pada tabel 3.42 berikut ini

Tabel 3.42 Data *Notification*

No	Event ID	Keterangan
1	10100011	*Raid device failed*
2	10100026	*Raid array rebuilt*
3	10100038	*Starting raid recovery*
4	20100016	*Uplink went online*
5	20100024	*Uplink went offline*
6	20100036	*System started*
7	20100044	*System shutting down*
8	20100054	*System reboot*