BAB 4
IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1. Implentasi Sistem

Setelah tahap analisis dan perancangan dilakukan, selanjutnya sistem yang telah dirancang akan diimplementasikan. Adapun tahapan instalasi dan konfigurasi yang dilakukan terhadap *Server Unified Threat Management (UTM) Firewall* Berbasis *Linux* dan *host* pada jaringan komputer Dewan Perwakilan Rakyat Daerah (DPRD) Provinsi Jawa Barat, yaitu:

4.1.1. Perangkat *Server*

Berdasarkan hasil rekomendasi perancangan *Server Unified Threat Management (UTM) Firewall* berbasis *Linux* yang telah dilakukan, Penanggung Jawab IT DPRD Provinsi Jawa Barat telah menyepakati rekomendasi spesifikasi perangkat keras dan lunak tersebut untuk diterapkan pada *Server Unified Threat Management (UTM) Firewall* berbasis *Linux*.

4.1.1.1. Perangkat Keras *Server UTM firewall* Berbasis *Linux*

Berikut adalah spesifikasi perangkat keras *Server UTM firewall* yang digunakan pada jaringan komputer DPRD Provinsi Jawa Barat, yaitu:

Tabel 4.1 Spesifikasi *UTM Firewall*

No	Perangkat	Jumlah	Spesifikasi
1	*CPU*	1	*Clock Speed 3,6 Ghz*
2	*Hard Disk*	1	80 GB dengan kecepatan *7200 RPM*
3	*RAM*	1	*Ukuran 1 GB*
4	*Power Supply*	1	*450 wattt*
5	*LAN Card*	2	*Fast Ethernet 100 Mbps*
6	*Kabel UTP*	2	*CAT.5 SE*
7	*DVD RW*	1	*Standar*
8	*Fan*	2	*Standar*

4.1.1.2. Perangkat Lunak *Server UTM firewall* Berbasis *Linux*

Perangkat lunak yang digunakan pada *Server Unified Threat Management (UTM) Firewall* yaitu sistem operasi berbasis *Linux Endian UTM Software Appliance versi 3.2*

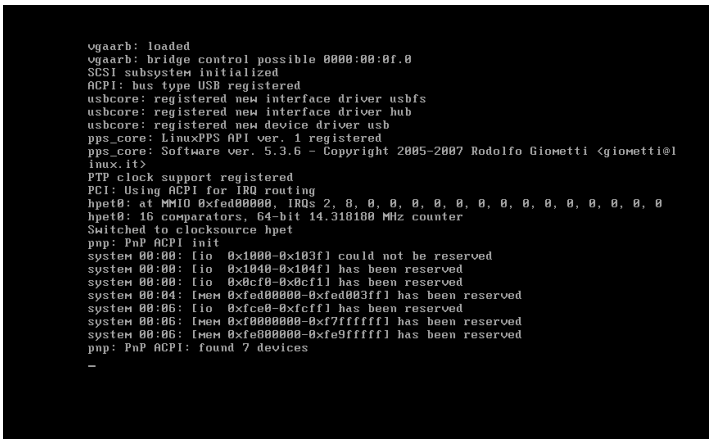
4.1.2. Instalasi dan konfigurasi *Server*

Implementasi selanjutnya yaitu melakukan instalasi dan konfigurasi pada *server UTM Firewall*, berikut adalah tahapan-tahapan yang dilakukan, yaitu :

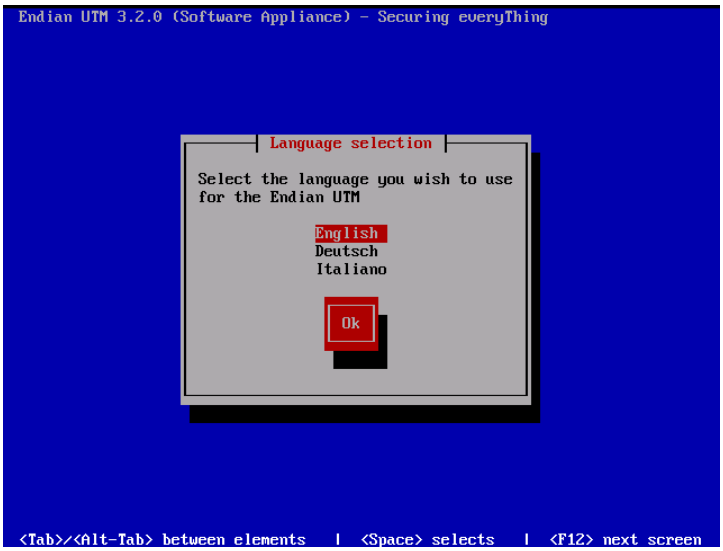
4.1.2.1. Instalasi

Pada *server* sistem operasi yang digunakan adalah *Endian firewall* yang merupakan distribusi berbasis *Linux,* yang berfungsi sebagai *UTM firewall*. *Endian firewall* yang terinstal pada *PC* yang berfungsi sebagai adapter *Local Area Network (LAN)* dan *card* yang lain berfungsi untuk koneksi *Wide Area Network (WAN)* yang dihubungkan dengan *ADSL modem* yang terhubung dengan *internet*. Berikut adalah langkah-langkah instalasi *Endian firewall*:

1. *Booting* dengan CD *Endian* firewall melalui *disk drive.*
2. Saat *booting* akan muncul *command prompt* lalu *enter*, pilih bahasa yang digunakan, kemudian pilih *yes* untuk menginstal dan tunggu proses *copy file*.

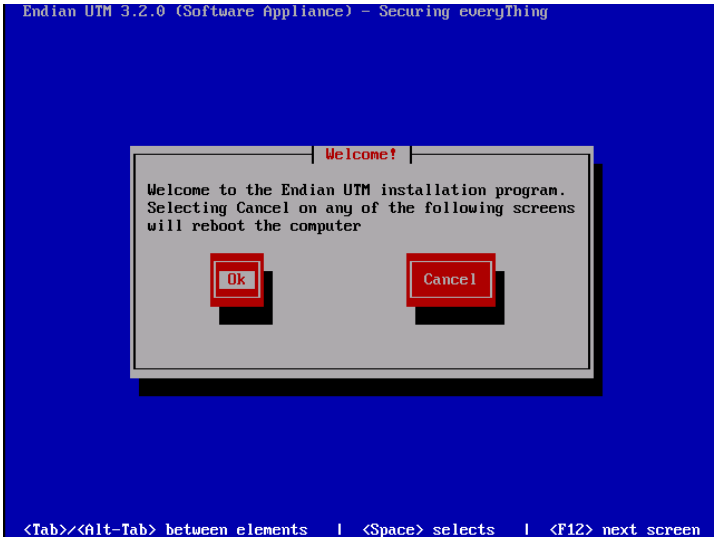


Gambar 4.1 Proses *Booting Instalasi Endian Firewall*



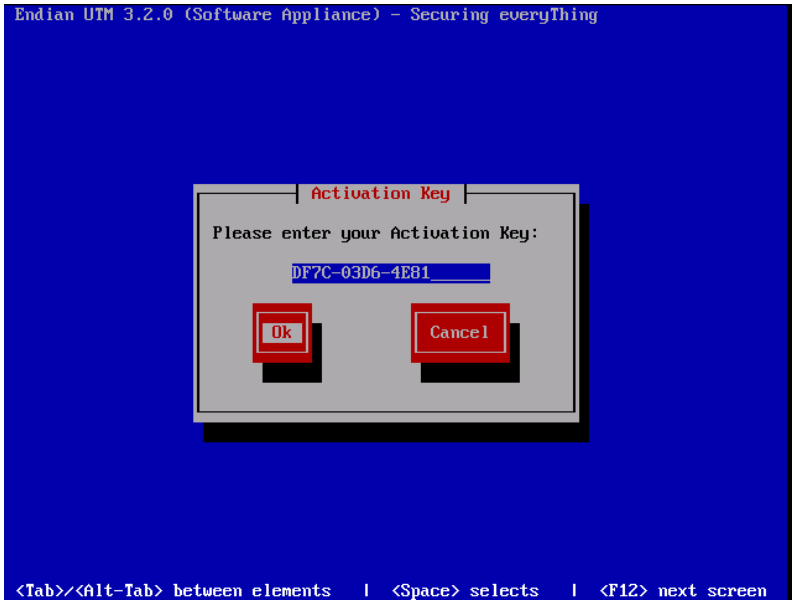
Gambar 4.2 Memilih Bahasa Instalasi *Firewall*

3. Untuk pemilihan bahasa, pilih *English* dan *OK* untuk meneruskan proses installasi



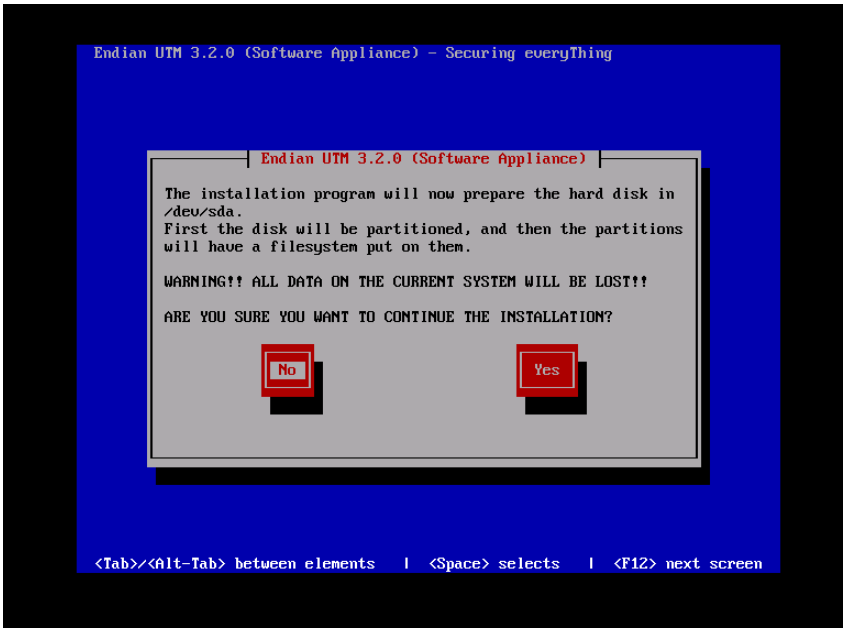
Gambar 4.3 Proses *Agrement Instalasi Endian*

4. Masukan kode aktifasi *UTM firewall* yang valid

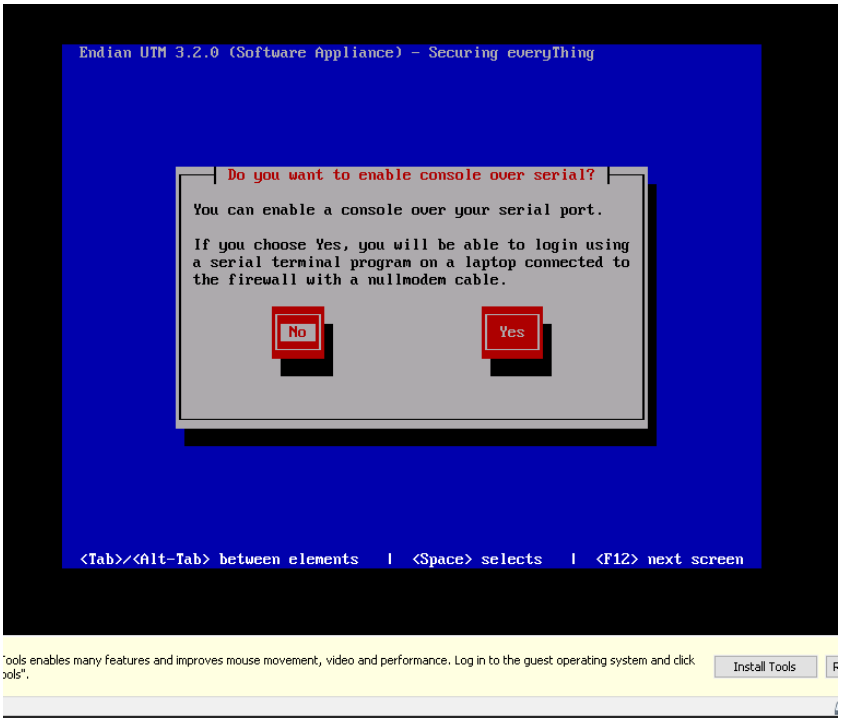


Gambar 4.4 Masukan *Key Activasi*

5. Akan muncul konfirmasi instalasi, semua data pada drive akan terhapus. Klik *Yes* untuk meneruskan instalasi dan klik *Yes* untuk konfirmasi *login* menggukan *serial* program dari laptop

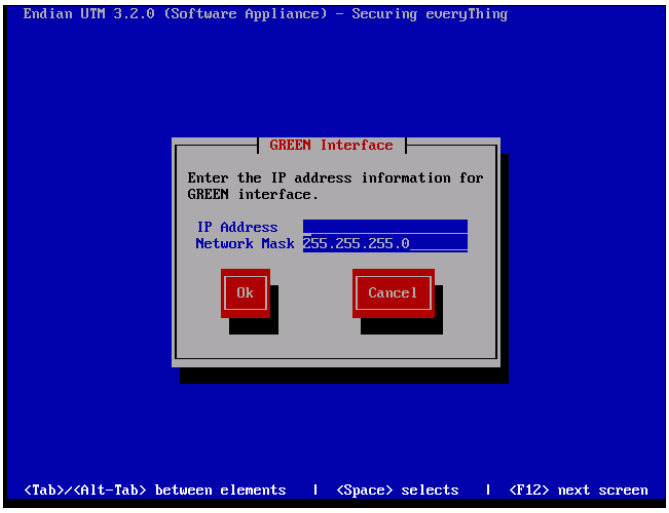


Gambar 4.5 Proses *Agrement format Instalasi Endian*

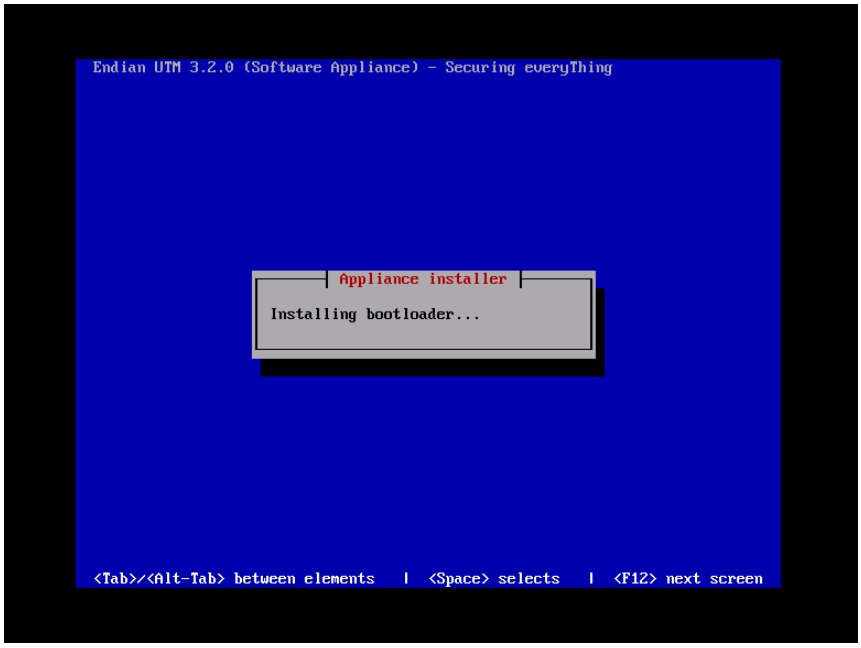


Gambar 4.6 Proses *Agrement Access via consol serial*

6. Masukan *IP Address* 192.168.8.17 beserta dengan subnet, setelah proses instalasi berlangsung.

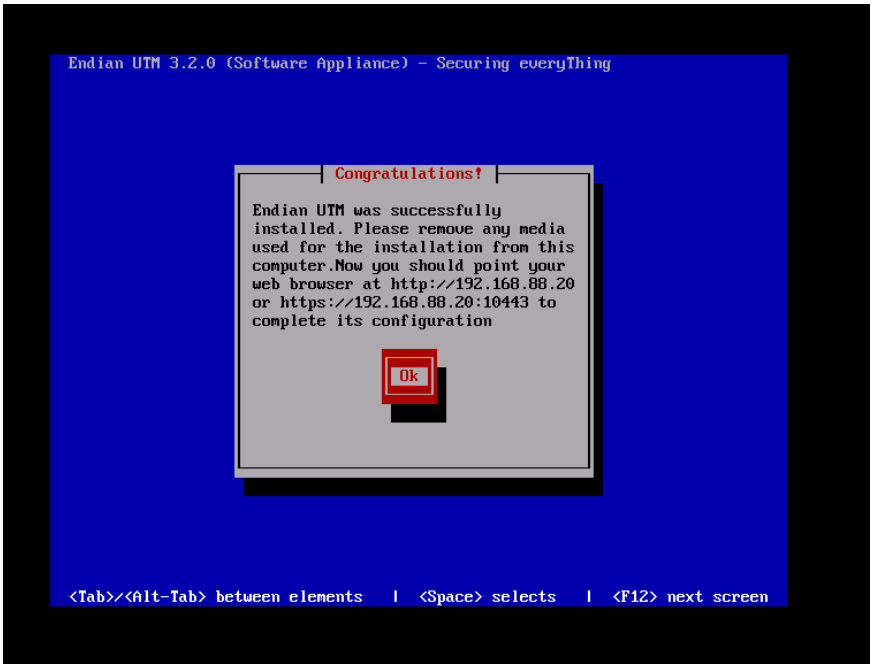


Gambar 4.7 *IP Address Endian Firewall*



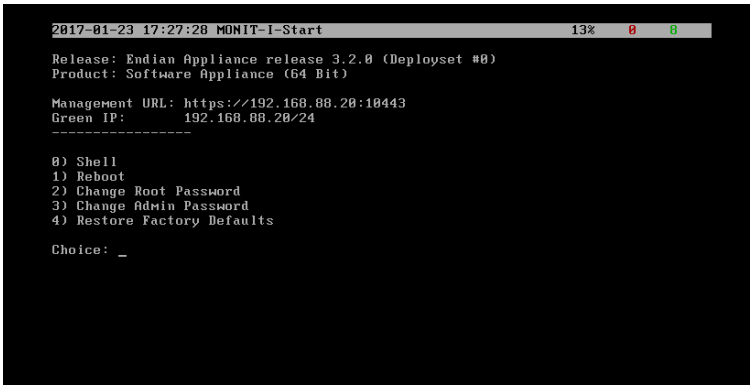
Gambar 4.8 Proses *Copy file data*

1. Setelah Proses instalasi berlansung muncul alamat *IP Address* beserta *port* untuk bisa diakses melalui *LAN Card.*



Gambar 4.9 Proses Instalasi Selesai

2. Tampilan awal ketika sistem sudah berhasil di *install.*

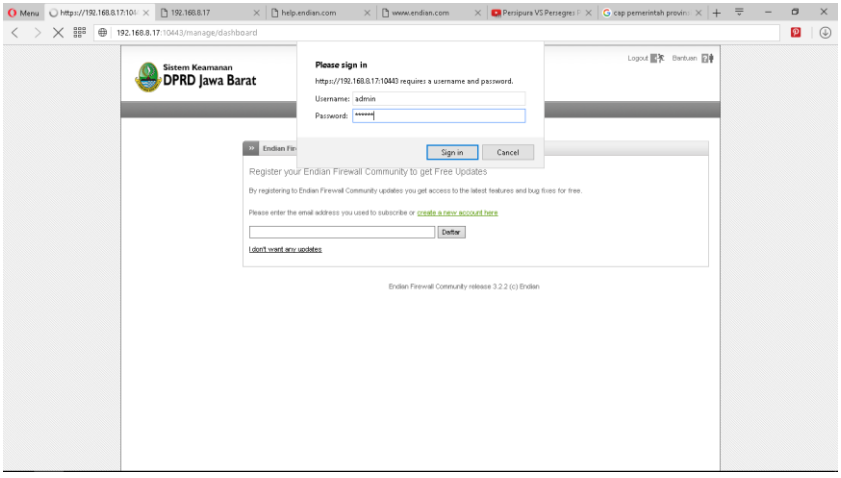


Gambar 4.10 Tampilan *Shell Endian Firewall*

4.1.2.2. Konfigurasi

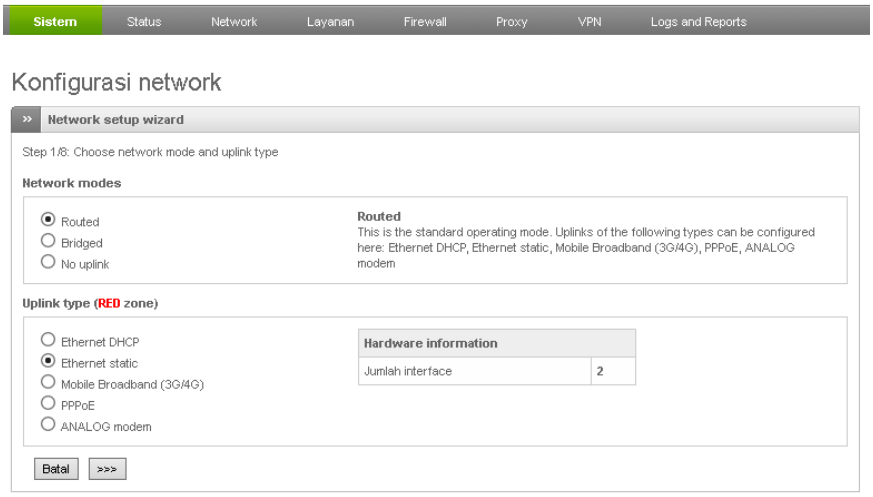
Agar mendapatkan keamanan jaringan yang kita inginkan kita perlu melakukan konfigurasi dengan step-step berikut

1. Buka browser *Mozilla Firefox* dari desktop dan browser ke alamat *IP Address: https://192.168.8.17:10443/* kemudian akan muncul seperti gambar dibawah ini, lalu isi *user name* dengan ‘admin’ *password:* ‘*Endian*’.



Gambar 4.11 Verifikasi *username* dan *password*

2. Pada *Interface RED* pilih alamat *IP Statis* untuk semua *interfaces*, *port RED* adalah *interface* yang berhubungan langsung dari *internet* sehingga banyak ancaman dari luar. Untuk berbagai jenis koneksi *internet* (seperti *ADSL* untuk pengguna rumah atau ISDN untuk bisnis), pilih opsi yang sesuai. Langkah berikutnya akan tetap sama akan tetapi konfigurasi akan berbeda ketika *Endian firewall* akan melempar pengaturan lain nantinya. Sebagai contoh, ketika alamat *IP* yang ditetapkan secara dinamis menggunakan *DHCP*, *Endian* akan perlu dikonfigurasi untuk dapat menjadi *server DHCP*. Pilih opsi 'ETHERNET STATIC' dari beberapa opsi yang muncul. Kemudian klik button '>>>' untuk melanjutkan proses



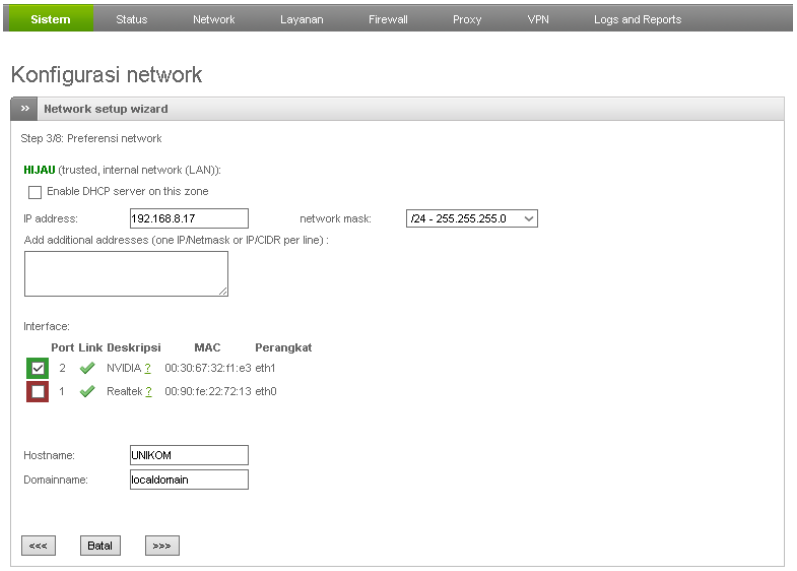
Gambar 4.12 Pemilih *Type Red Interface*

3. Kemudian akan muncul layar dimana memberikan pilihan *network zones*. Pada gambar dibawah kita akan memilih *Interface Orange*, dimana *orange* merupakan *port* yang menghubungkan dengan bagian *Server (DMZ)*. Pilih opsi 'Orange' dari beberapa opsi yang muncul. Kemudian klik button '>>>' untuk melanjutkan proses



Gambar 4.13 Pemilihan *Zone Network*

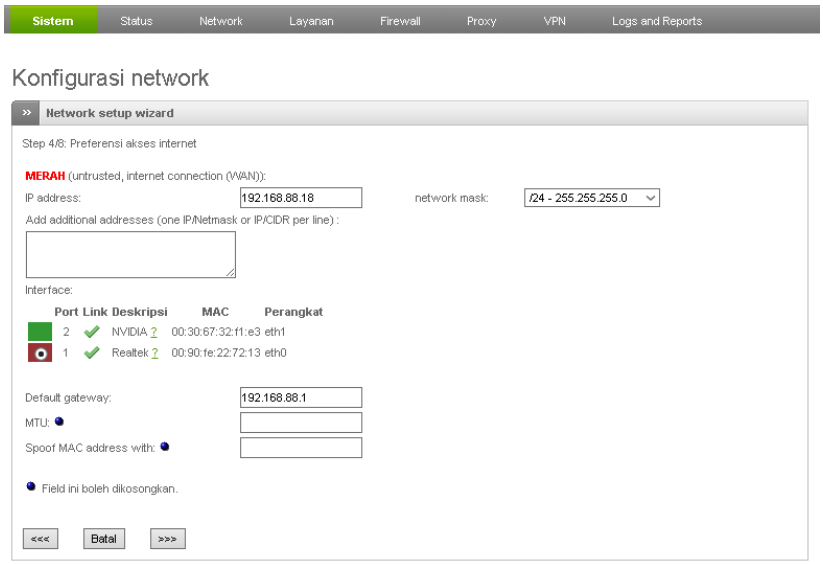
4. Pilih alamat *IP statis* untuk antar muka *GREEN*, antar muka terhubung dengan terpercaya dan dilindungi oleh internal jaringan, perhatikan bahwa kita mengkonfigurasi ulang alamat *IP* sesuai dengan kebutuhan jaringan. *Green Interface IP Address* : 192.168.8.17 *Network Mask* : 255.255.255.0



Gambar 4.14 *Network Preference*

5. *Interface RED* adalah pintu gerbang kedunia luar, yaitu *interface* yang menghubungkan jaringan dalam ke internet. Pada interface ini akan kita beri *IP Address* 192.168.2.2 khusus untuk membedakan dengan *interface GREEN*

dan *ORANYE. RED Interface IP Address* : 192.168.2.2 *Network Mask* : 255.255.255.0 *Default Gateway* : 192.168.2.2 Kemudian klik button '>>>' untuk melanjutkan proses



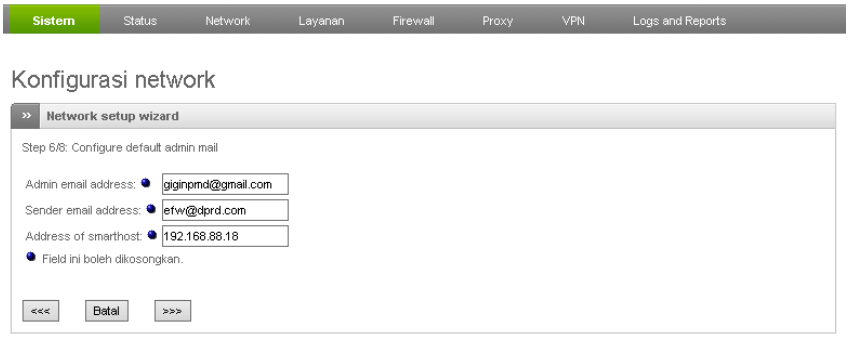
Gambar 4.15 *Preference akses Internet*

6. Masukan *IP Address* 8.8.8.8 sebagai *DNS* di kedua entri, hal ini karena 8.8.8.8 adalah web *server* yang telah dibuat oleh penulis.



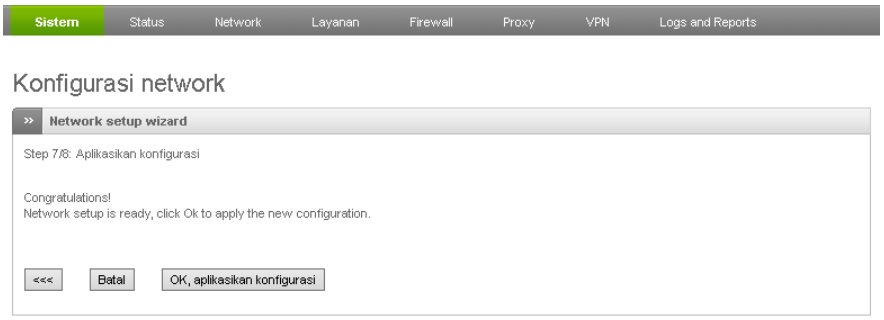
Gambar 4.16 *Setup DNS*

7. Layar berikutnya akan menampilkan permintaan alamat email dari admin *Endian Firewall*



Gambar 4.17 Setup email admin

8. Jika konfigurasi yang diinginkan sudah di *set-up* maka klik OK, dan *Endian firewall* sudah bisa berjalan. Kemudian menunggu sampai dengan 20 detik sampai keluar gambar seperti dibawah ini.



Gambar 4.18 Konfirmasi Penerapan Konfigurasi

4.1.3. Perangkat *Client*

Berikut adalah spesifikasi perangkat keras *client* yang digunakan pada jaringan komputer DPRD Provinsi Jawa Barat, yaitu:

Tabel 4.2 Perangkat *client*

No	Perangkat	Jumlah	Spesifikasi
1	*CPU*	1	*Clock Speed 2.4 Ghz*
2	*Hard Disk*	1	80 GB dengan kecepatan 7200 RPM
3	*RAM*	1	Ukuran 1 GB
4	*Power Supply*	1	*450 wattt*
5	*LAN Card*	1	*Fast Ethernet 100 Mbps*
6	*Kabel UTP*	1	*CAT.5 SE*

4.2. Pengujian Sistem

Setelah tahap instalasi dilakukan, selanjutnya yaitu tahap pengujian terhadap jaringan komputer *LAN* dan *WLAN* serta *Server UTM firewall* yang telah dibangun di DPRD Provinis Jawa Barat. Pengujian ini dilakukan untuk membuktikan seberapa baik kualitas keamanan jaringan komputer *LAN* dan *WLAN* serta seberapa baik *Server UTM firewall* dalam menjamin *packet data* pada lalu lintas jaringan internal.

Berikut adalah beberapa pengujian yang dilakukan untuk memenuhi tujuan dari penelitian ini menggunakan pengujian *Black box* dengan pengujian *alpha* dan pengujian *beta.*

4.2.1. Pengujian Alpha

Pengujian dilakukan untuk menjamin kualitas dan juga mengetahui kesalahan dari keamanan jaringan komputer yang dibangun. Tujuan dari pengujian ini adalah untuk menjamin bahwa keamanan jaringan komputer yang dibangun memiliki kualitas yang handal.

4.2.1.1. Rancangan Pengujian

Pengujian jaringan komputer ini menggunakan metode pengujian *Black box*. Pengujian *Black box* berfokus pada persyaratan fungsional jaringan komputer yang dibangun.

Berikut adalah penjelasan pada tabel 4.3 rancangan pengujian *alpha:*

Tabel 4.3 Rancangan pengujian

Konfigurasi Uji	Detail Pengujian	Sistem Operasi	Jenis Pengujian
IP Address	Ping ke *IP Address client* dari *UTM Firewall*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Ping ke *IP Address UTM firewall* dari *IP Address client*		
	Ping ke google.com dari *IP Address client*		
Firewall	Melakukan *DOS* terhadap	*Endian UTM*	*Black Box*

	web server	*firewall* dan Windows 7	
	Mengakses jaringan yang tidak valid		
	Melakukan *spoofing* dengan *winarpattacker*		
Intrusion Prevent System	*Import database snort rule*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Melakukan *host scanning* dengan aplikasi *Angry IPScan*		
	Melakukan *port scanning* dengan aplikasi *nmap*		
	Melakukan *HTTP attacking* pada *database Server*		
	Melakukan pengaksesan terhadap web *Server* dari komputer *client*		
	Melakukan pengaksesan terhadap *database Server* dari computer *client*		
Anti-Virus	*Import database virus clamav*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Memasukan jenis virus yang berasal dari sumber **eircar.com** melalui alamat *port http*		
Anti-Spam	Data *training spam*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Mengirimkan *mail spam*		
Web Conten Filtering	Mengakses *website* langsung dari *url*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Mengakses *website* sesuai pencarian *keyword*		
Virtual Private Network	*Username* dan *password* untuk *account VPN*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Ping IP Address *VPN Server*		
	Username dan *password* untuk akses *VPN*		
Control Central Management	Mengaktifkan semua fungsi *security*	*Endian UTM firewall* dan Windows 7	*Black Box*
	Mengaktifkan fungsi		

	notification email		
	Menampilkan *logs* dan *report*		
	Mengaktifkan fungsi *backup*		

Tabel 4.4 *IP Address UTM firewall* dan Komputer *Client*

Komputer	TCP/IP
1 *(Server)*	*1. IP Address 192.168.137.18* *2. IP Address 192.168.8.17*
2 *(Client)*	*1. IP Address 192.168.137.1* *2. IP Address 192.168.8.17*

4.2.1.2. Kasus dan Hasil Pengujian

Berdasarakan rencana pengujian yang telah disusun, diperoleh hasil pengujian sebagai berikut:

1. *IP Address*

Pengujian *IP Address* dimana dalam scenario pengujian ini melibatkan 2 komputer client sesuai gambar 4.19. Pengujian ini bertujuan untuk mengetahui konektifitas antar *device.*



Gambar 4.19 Skenario *IP Address*

Pada skenario pengujian normal dapat dilihat di tabel. 4.5 sedangkan untuk pengujian tidak normal dilakukan scenario pada tabel 4.6 berikut ini

Tabel 4.5 Pengujian *IP Address* normal

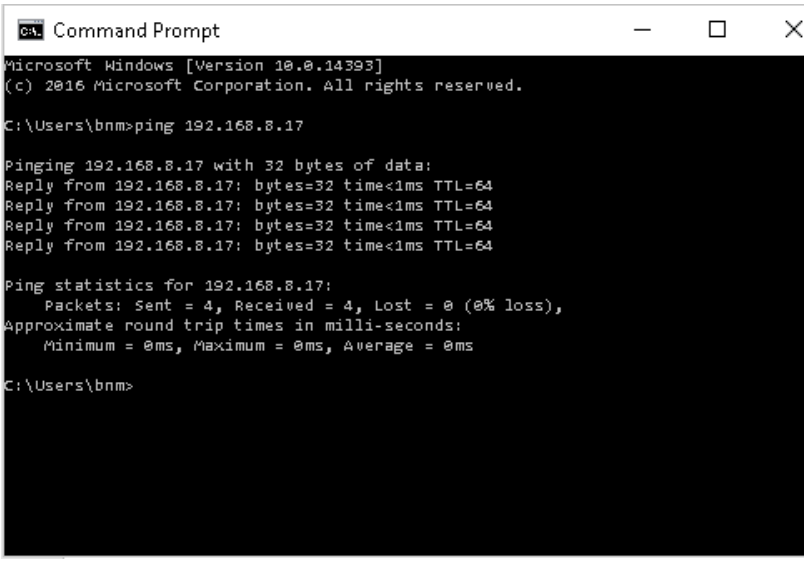
Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Ping ke *IP Address client* dari *UTM Firewall*	Komunikasi terjalan dengan *IP Address* berhasil	Komputer *client* merespon *ping* dari *UTM firewall*	Diterima
Ping ke *IP Address UTM firewall* dari *IP Address client*	Komunikasi terjalan dengan *IP Address* berhasil	*UTM Firewal* merespon *ping* dari *client*	Diterima
Ping ke google.com dari *IP Address client*	Komunikasi terjalan dengan *IP Address* berhasil	Komputer *client* merespon ping ke **google.com**	Diterima

Tabel 4.6 Pengujian *IP Address* tidak normal

Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Ping ke *IP Address client* dari *UTM Firewall*	Komunikasi tidak berjalan antara *UTM firewall* dengan komputer *client*	*IP Address* tidak terdaptar pada network zone configuration	Diterima
Ping ke *IP Address UTM firewall* dari *IP Address client*	Komunikasi tidak berjalan antara *client* dengan komputer *UTM firewall*	*IP Address* benar satu jaringan, tetapi beda *gateway*	Diterima
Ping ke google.com dari *IP Address client*	Komputer *client* tidak bisa mengkases internet	*IP Address*, gateway dan DNS benar, tetapi network *zone configuration* tidak benar.	diterima

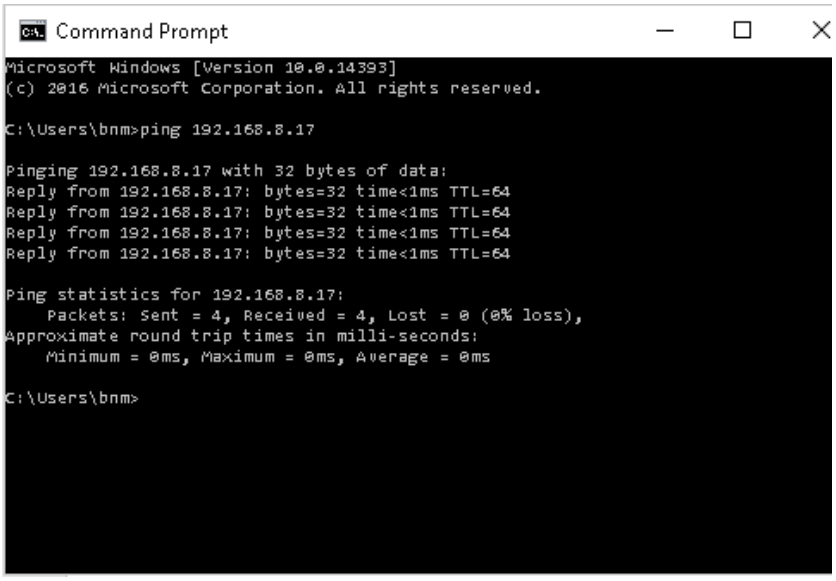
Pengujian data tidak normal pada *IP Address* untuk komunikasi *UTM firewall* dengan komputer *client* terjadi karean *network zone configuration* belum melakukan pengaturan yang benar dan gateway pada komputer *client* tidak sama.

Untuk hasil pengujian *Ping IP address client to UTM firewall dapat dilihat pada gambar 4.20* dimana komunikasi berhasil terjalin.



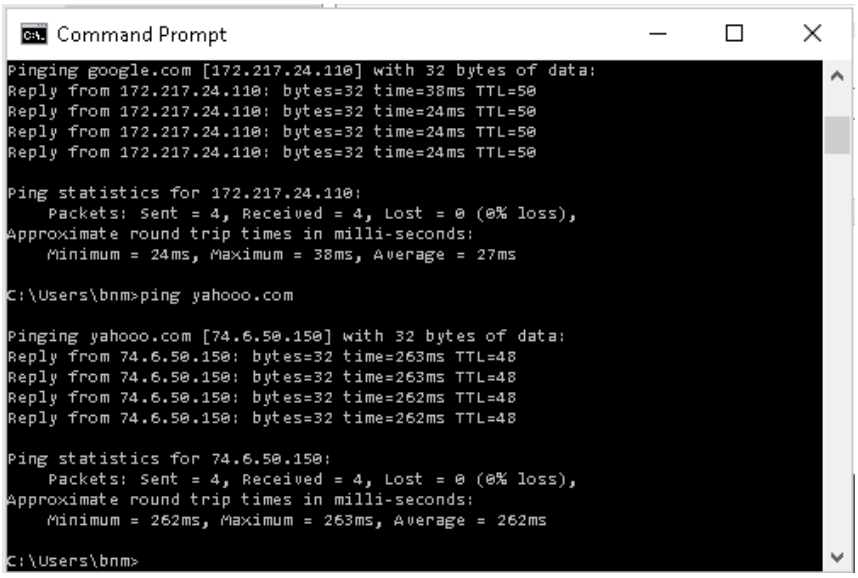
Gambar 4. 20 *ping client to UTM*

Sedangkan untuk hasil pengujian *Ping IP address UTM firewall to client* dapat dilihat pada gambar 4.21 dimana komunikasi berhasil terjalin.



Gambar 4.21 *Ping UTM firewall to client*

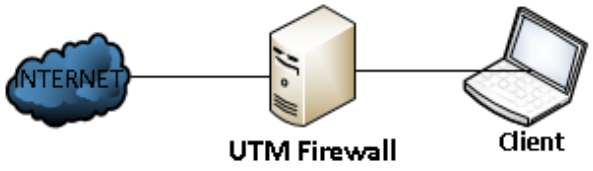
Pada gambar 4.22 berikut ini merupakan hasil percobaan pengaksesan ke *internet* dari *IP address client*



Gambar 4.22 *client* berhasil mengkases *internet* melewati *UTM firewall*

2. Firewall

Pada tabel 4.7 dan tabel 4.8 adalah pengujian normal dan tidak normal firewall pada *UTM firewall* dengan melibatkan komputer *client* sesuai scenario pada gambar 4.7



Gambar 4.23 Skenario *Firewall*

Tabel 4.7 Pengujian *Firewall* Normal

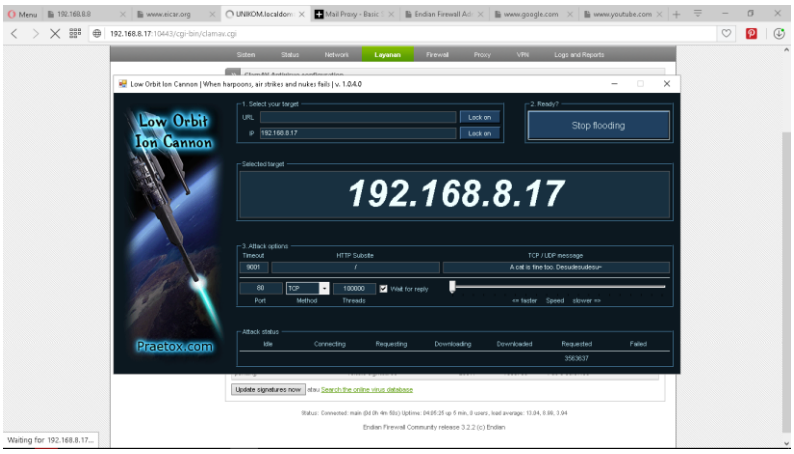
Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Melakukan spam *DOS* terhadap *web Server*	Bisa mengatasi respon yang lebih banyak	Dengan *tools PHP DOS* dan target IP Address 127.0.0.1 dengan time 665000 serta port 445	Diterima
Melakukan *Flooding* dengan mengirimkan data permili detiknya 65000	Bisa mengatasi ancaman *Flooding*	*Flooding* dilakukan dengan menggunakan tool *ping flood* terhadap UTM firewall	Diterima
Melakukan *spoofing* dengan *winarpattacker*	Bisa mengatasi *spoofing*	*Spoofing* dilakukan dengan *tool winarpattacker* dan memilih serangan type *spoofing*	Diterima

Tabel 4.8 Pengujian *firewall* tidak normal

Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Melakukan spam *DOS* terhadap *web Server*	Tidak Bisa mengatasi respon yang lebih banyak	Dengan *tools PHP DOS* dan target IP Address 127.0.0.1 dengan time 665000 serta port 445	Diterima
Melakukan *Flooding* dengan mengirimkan data per mili detiknya 65000	Tidak Bisa mengatasi ancaman *Flooding*	*Flooding* dilakukan dengan menggunakan tool ping flood terhadap UTM	Diterima

		firewall	
Melakukan *spoofing* dengan *winarpattacker*	Tidak Bisa mengatasi *spoofing*	*Spoofing* dilakukan dengan *tool winarpattacker* dan memilih serangan type spoofing	Diterima

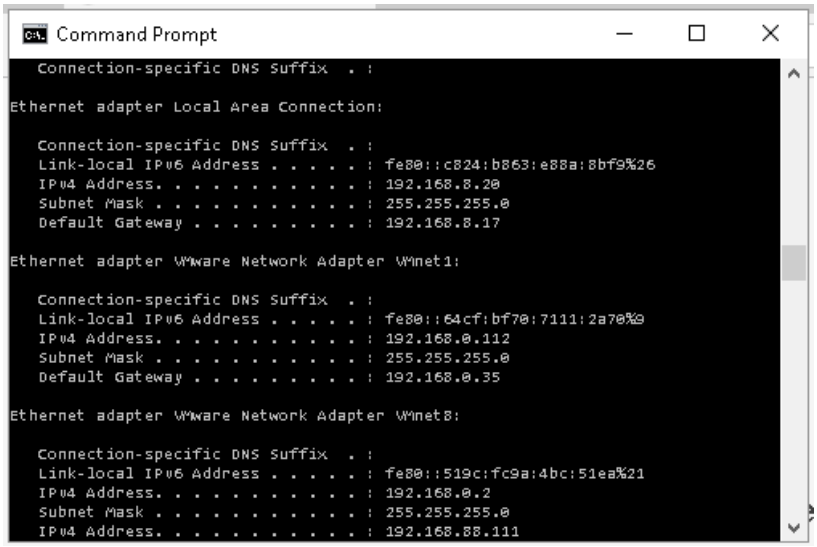
UTM firewall berhasil mengatasi serangan Ddos dimana Hasil pengujian dari tindakan *DDos* ini, menggunakan *tool* yaitu *Loic* dengan angka *threat* 100000 dan *method TCP* terlihat pada gambar 4.23



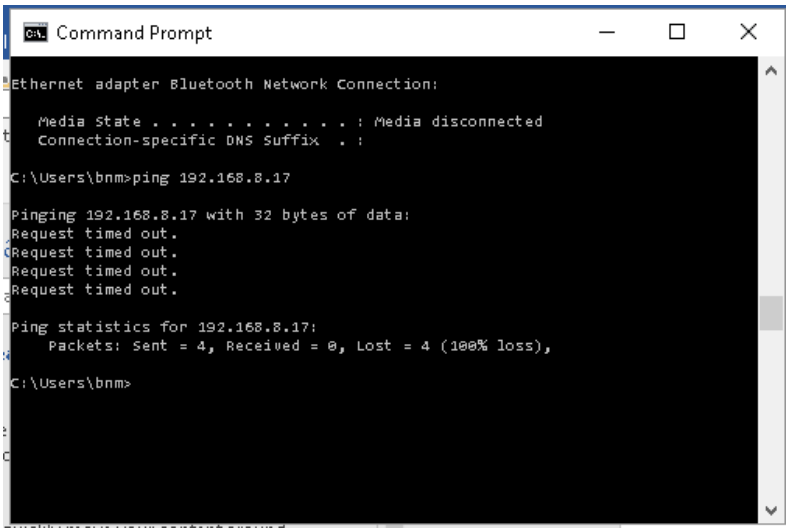
Gambar 4.24 *DDos, Floading Loic* terhadap *UTM Firewall*

UTM firewall berhasil bertahan terhadap *DDos* tersebut sehingga masih bisa diakses terhadap *web server*.

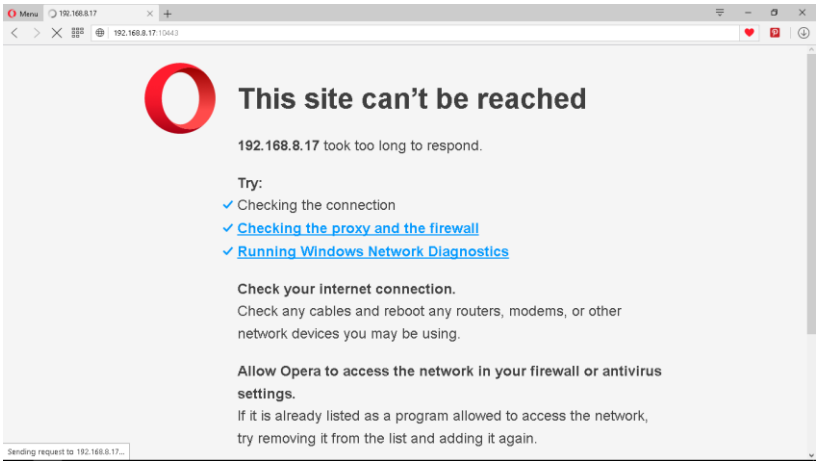
Pengaksesan pada *IP Address* yang tidak *valid* dapat dicegal oleh *UTM firewall* ini. Hasil pengujian dari *IP Address* yang tidak valid dapat dilihat pada gambar 4.24, gambar 4.25 dan gambar 4.26



Gambar 4.25 *IP address* tidak valid

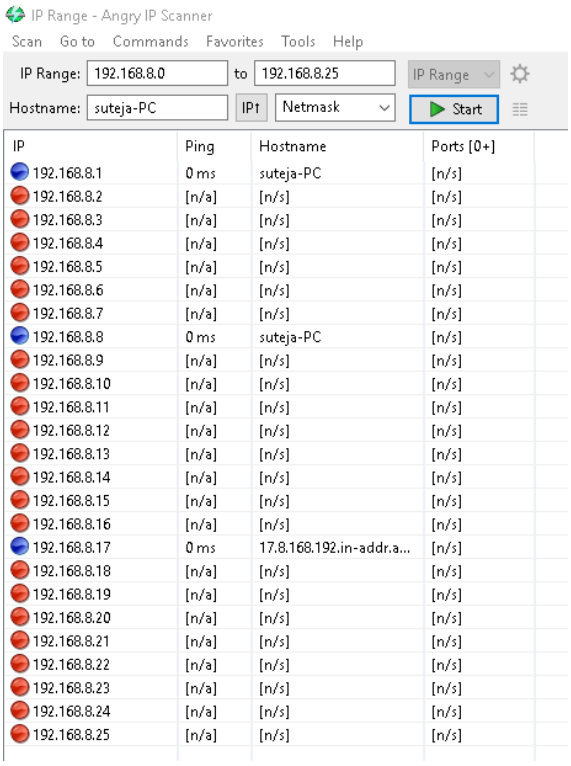


Gambar 4 26 percobaan *ping* dari *IP address* tidak valid



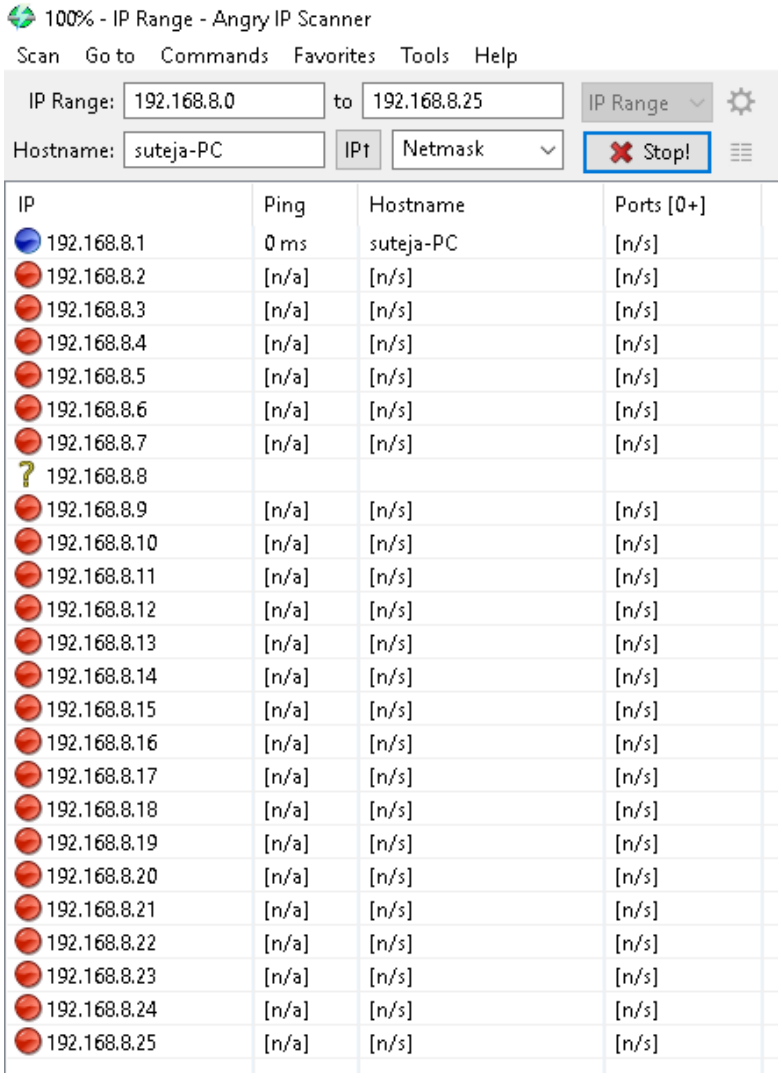
Gambar 4.27 hasil dari *IP address* tidak valid

Adapun untuk tindakan spoofing pada gambar 4.28 berikut ini, tindakan spoofing berhasil dijalankan dengan melihat data *IP address* ketika keamanan firewall dan IPS non-aktifkan



Gambar 4. 28 *spoofing* berhasil ketika *firewall* dan *IPS* di non-aktifkan

Sedangkan pada gambar 4.29 tindakan *spoofing* tidak berhasil dan *UTM firewall* berhasil mengatasi terhadap *spoofing* tersebut dengan mengkombinasikan antara *firewall* dan *IPS.*



Gambar 4.29 *Spoofing* tidak berhasil ketika *Firewall* dan *IPS* di aktifkan

3. *Instrusion Prevent Sysem (IPS)*

Pada tabel 4.9 adalah pengujian *IPS* dengan mendeteksi spoofing, malware dan packet data mencurigakan dan pengaksesan terhadap *server* dengan scenario sesuai gambar 4.30



Gambar 4.30 Skenario Pengujian *IPS*

Tabel 4. 9 Pengujian IPS Normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Import database snort rule	*Database snort* tersimpan	Proses upload snort database berhasil	Diterima
Melakukan *host scanning* dengan aplikasi *Angry IPScan*	Hasil *IP scanning* tidak diketahui	Hasil scanning jaringan dari *IP Address* 192.168.88.1 samap 192.168.88.10 tidak berhasil	Diterima
Melakukan *port scanning* dengan aplikasi *nmap*	Hasil *port scanning* tidak diketahui	Hasil *port scanning* terhadap *port* yang terbuka pada *web server* dan *database server* dengan *tool nmap* tidak berhasil	Diterima
Melakukan *HTTP attacking* pada	*Access* ke *database server*	Proses access ke database *server* dengan *web*	Diterima

database server	gagal	browser google chrome tidak berhasil ketika *IPS* diaktifkan	
Melakukan pengaksesan terhadap *web server* dari komputer *client*	*Web server* tidak berhasil diakses	Akses terhadap *web server* dari komputer *client* tidak bisa dengan web browser	Diterima
Melakukan pengaksesan terhadap *database aerver* dari computer *client*	Database *server* tidak berhasil diakses	Akses terhadap database *server* dari komputer *client* tidak bisa dengan menggunakan *web browser*	Diterima
Melakukan *Deniel of sevice* berupa *Ping of Death*	Menghentikan ping berkelanjutan	Ping of death dilakukan oleh komputer *client* terhadap *UTM firewall*	diterima
Melakukan serangan *sql injection* dengan *tool Havij SQL Injection*	Dapat mencegah *sql injection*	Pengeksekusian *query* terhadap *web server* tidak berhasil dilakukan	diterima

Adapun untuk pengujian tidak normal terhadap *IPS* ini, tertera pada tabel 4.10 beriktu ini.

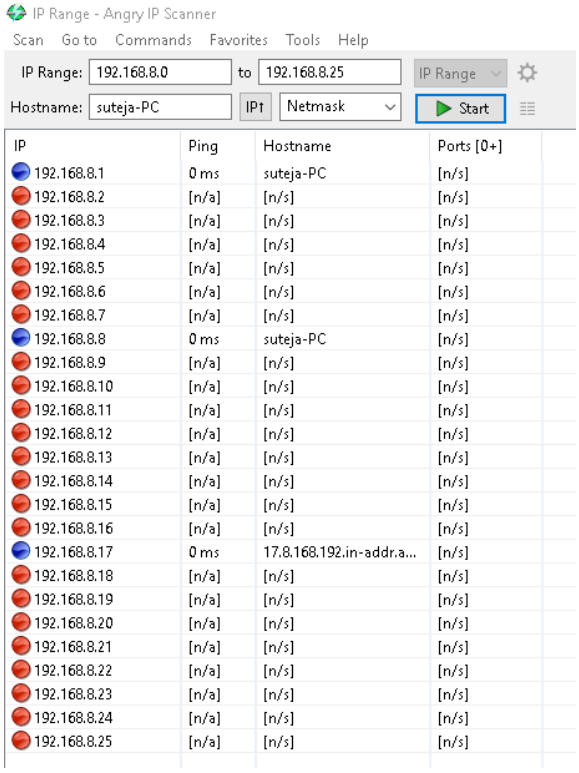
Tabel 4.10 Pengujian *IPS* tidak normal

Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Melakukan *host scanning* dengan aplikasi *Angry IPScan*	Hasil *IP scanning* tidak diketahui	Kondisi *IPS* tidak aktif	Diterima
Melakukan *port scanning* dengan	Hasil *port scanning* tidak	Kondisi *IPS* tidak	Diterima

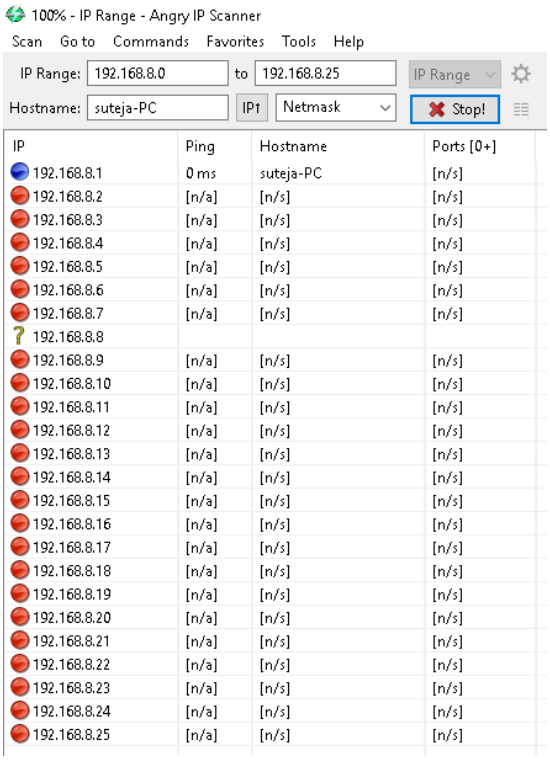
aplikasi *nmap*	diketahui	aktif	
Melakukan HTTP attacking pada database *server*	*Access* ke *database server* gagal	Kondisi *IPS* tidak aktif Proses access ke	Diterima
Melakukan pengaksesan terhadap *web server* dari komputer *client*	*Web server* tidak berhasil diakses	Kondisi *IPS* tidak aktif	Diterima
Melakukan pengaksesan terhadap *database server* dari komputer *client*	*Database server* tidak berhasil diakses	Kondisi *IPS* tidak aktif	Diterima
Melakukan *Deniel of sevice* berupa *Ping of Death*	Menghentikan ping berkelanjutan	Kondisi *IPS* tidak aktif	diterima
Melakukan serangan *sql injection* dengan *tool Havij SQL Injection*	Tidak dapat mencegah *sql injection*	*Rule snort* tidak tersedia untuk sql injection terbaru	diterima

Dalam pengujian tidak normal tersebut, *IPS* tidak bekerja karena beberapa factor diantaranya tidak aktifnya *IPS* itu sendiri dan tidak melakukan *update database* terhadap *file snort*

Hasil dari pengujian *IPS* dinon-aktifkan terdapat pada gambar 4.31 dimana *spoofing* berhasil dilakukan. Sedangkan ketika *IPS* di-aktifkan berhasil mengatasi *spoofing* yang terdapat pada gambar 3.32 berikut ini

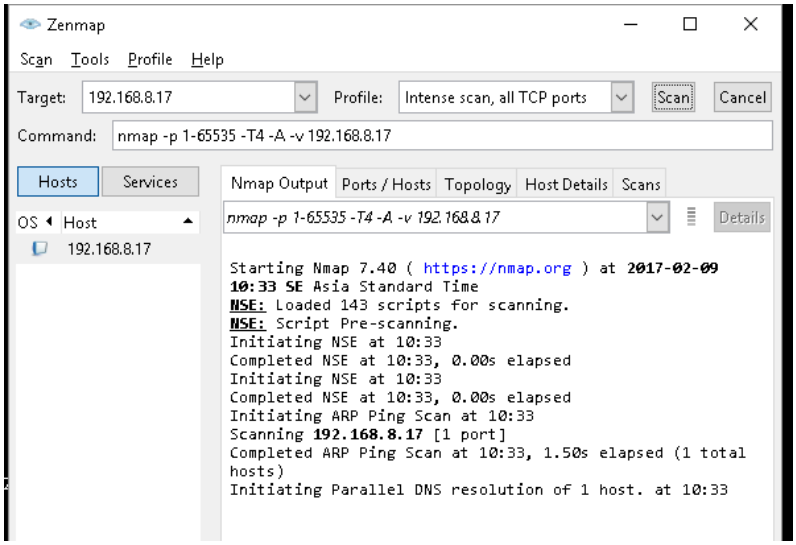


Gambar 4.31 *Spoofing* berhasil dilakukan



Gambar 4. 32 Spoofing berhasil dicegah

Untuk pencegahan *spoofing* dengan memamfaatkan *port* yang terbuka, pada pengujian ini dilakukan dengan menggunakan *tool zenmap*. Adapun untuk tindakan *scanning port* ketika *UTM firewall* difungsikan sebagai *IPS* maka tindakan *scanning port* tersebut berhasil dicegah seperti gambar 4.33 berikut ini. Adapun pada gambar 4.37 merupakan tindakan *scanning port* yang berhasil dilakukan disebabkan fungsi *IPS* di non-aktifkan

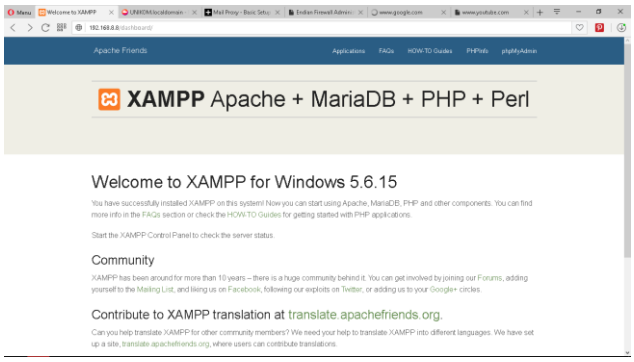


Gambar 4. 33 *port scanning* berhasil di cegah

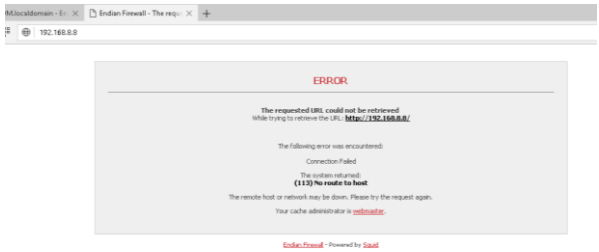


Gambar 4. 34 *port scanning* berhasil dilakukan

Adapun pengaksesan *illegal* terhadap *database server* dapat dicegah dengan *UTM firewall* yang difungsikan sebagai *IPS*. Pada *database server* diberikan dua *IP Address* yaitu 127.0.0.0 dan 192.168.8.8. Pada pengujian ini *IP address* 127.0.0.0 tidak dilakukan pengamanan sehingga bisa diakses seperti gambar 4.35 berikut ini. Sedangkan pada gambar 4.36 yaitu *IP address* 192.168.8.8 diberikan pengaman dengan aturan yang berlaku sehingga tidak bisa diakses sembarang dengan *IP address* yang tidak *valid*.

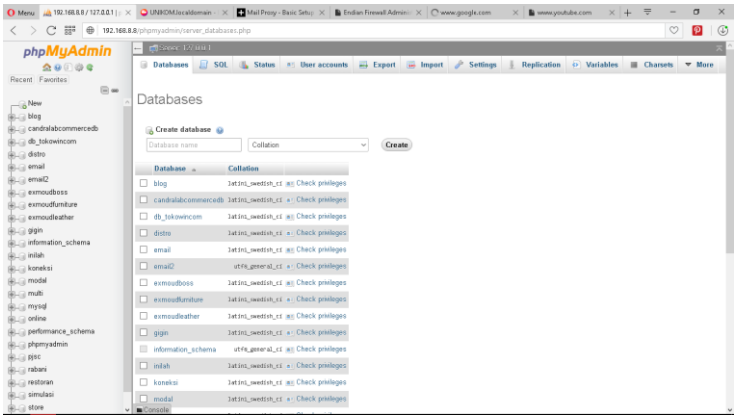


Gambar 4. 35 *IP Address database* 127.0.0.0



Gambar 4. 36 *Database server* tidak bisa diakses oleh sembarang *IP address*

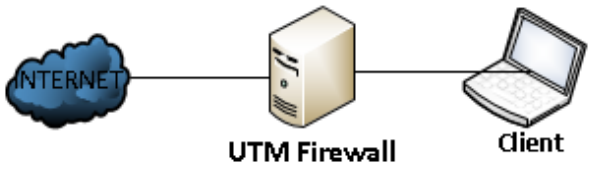
Ketika fungsi *IPS* tidak dijalankan maka pengaksesan *database server* berhasil dilakukan meskipun dengan *IP Address* tidak *valid* yang terdapat pada gambar 4.37



Gambar 4. 37 *Database* berhasil diakses ketika *IPS* dinon-aktifkan

4. Anti-Virus

Pada pengujian ini yang dilihat pada tabel 4.11 dengan harapan sesuai fungsioanl sebagai antivirus terhadap ancaman dari internet sesuai scenario pada gambar 4.22



Gambar 4. 39 Skenario Anti-Virus

Untuk skenario pengujian normal dan pengujian tidak normal dapat dilihat pada tabel 4.11 dan tabel 4.12 berikut ini.

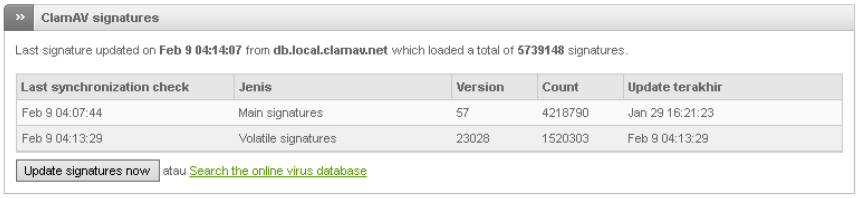
Tabel 4. 11 Pengujian *Anti-Virus* normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Import database virus clamav	Database berhasil di update	Muncul pesar success upload pada UTM Firewall	Diterima
Memasukan jenis virus yang berasal dari sumber **eircar.com** melalui alamat *port http*	Virus berhasil di deteksi dari luar jaringan	Virus tidak sampai ke komputer *client* dengan menggunakan file sharing	Diterima

Tabel 4.12 Pengujian *Anti-virus* tidak normal

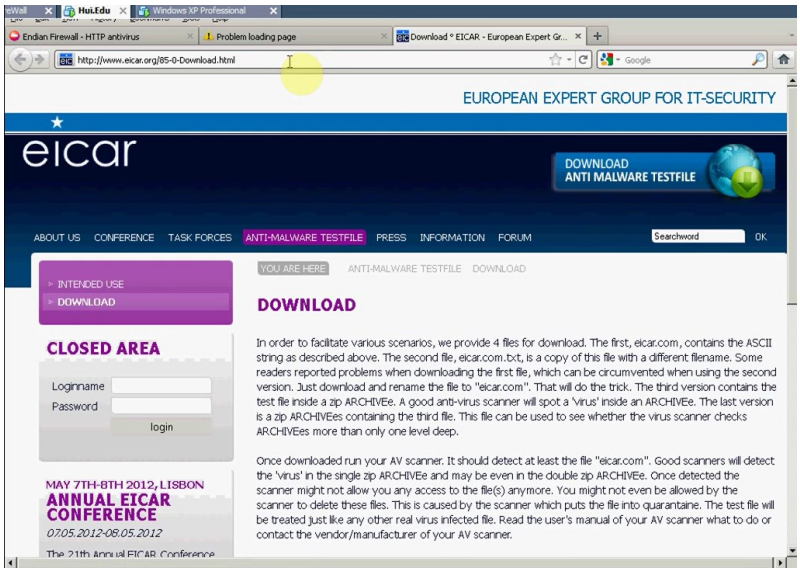
Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengirim virus ke komputer *client*	Virus tidak terdeteksi	Database virus clamave tidak di upload	Diterima
Memasukan jenis virus yang berasal dari sumber **eircar.com** melalui alamat *port http*	Virus tidak berhasil di deteksi dari luar jaringan	Anti virus tidak di aktifkan	Diterima

Pada gambar adala hasil pengujian terhadap *update database virus* pada anti virus di *UTM firewall* ini.

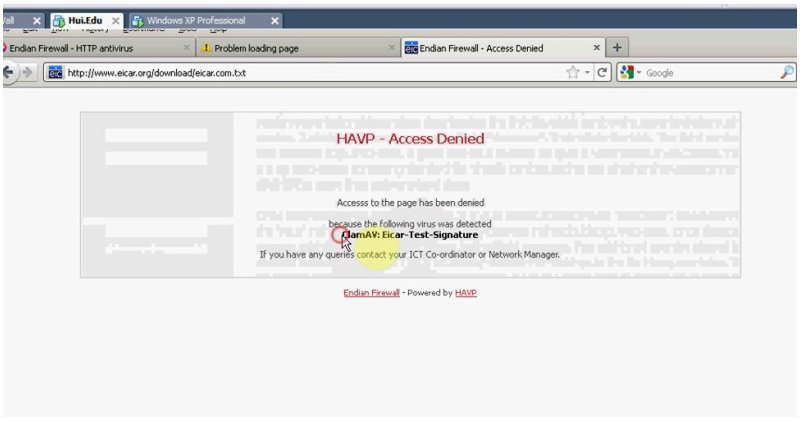


Gambar 4. 40 *Update database* virus berhasil

Untuk pengujian antivirus berjalan pada *UTM firewall* ini dilakukan pengujian dengan menggunakan website **eircar.com** dimana situs ini merupakan situs pengetesan terhadap antivirus. Pada pengujian ini dilakukan oleh komputer *client* dimana mencoba untuk mengakses **situs eircar.com**. pada gambar adalah hasil dari *UTM firewall* berhasil mengatasi dan mendeteksi virus dari sebuah *website*

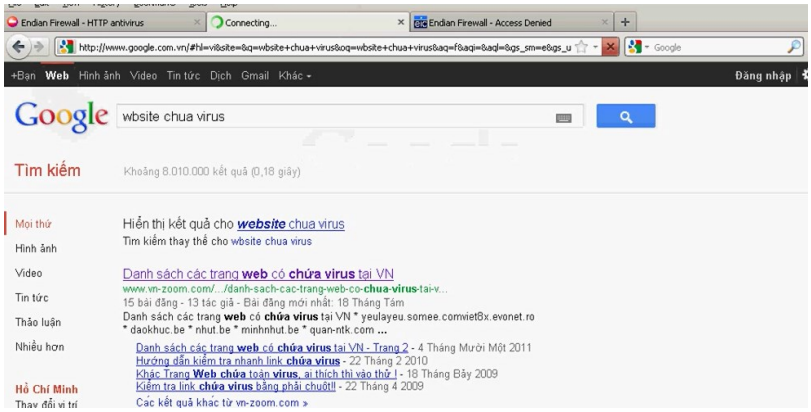


Gambar 4. 41 *website eircar.com* diakses



Gambar 4. 42 *website eircar.com* berhasil terdeteksi

Selain langsung mengkases terhadap *url* tersebut. Pada pengujian kali *UTM firewall* berhasil memblok situs yang berisikan *malware* dengan menuliskan *keyword* di mesin pencara yang dapat dilihat pada gambar 4.43



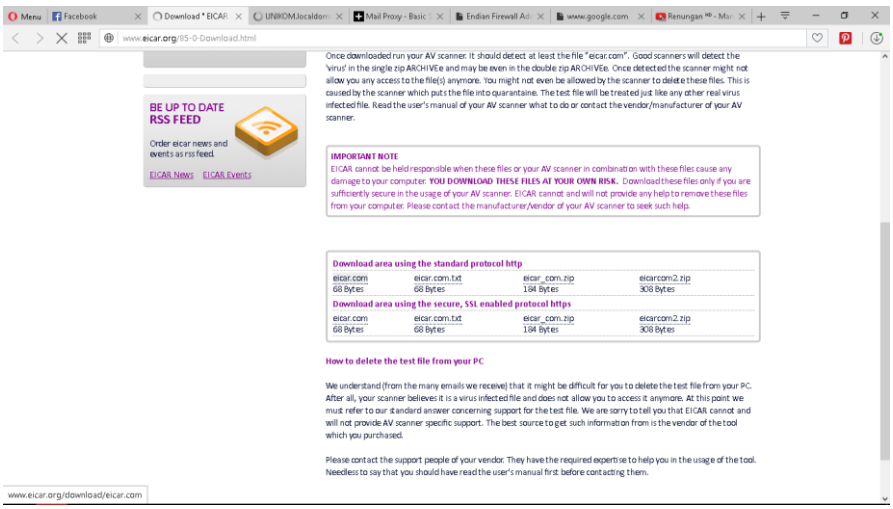
Gambar 4. 43 *website* yang berisi *malware*



Gambar 4. 44 *website* diblock yang berisi *malware*

Dalam pengujian tidak normal dilakukan dengan pengujian dengan menon-aktifkan anti-virus dan dilakukan pengaksesan oleh komputer client

terdapada situs **eircar.com** yang dapat dilihat pada gamabar 4.45 dimana bisa diakses tanpa diatifkanya *anti-virus*



Gambar 4. 45 *werbsite* berhasil di akses

5. *Anti-Spam*

Pengujian anti-spam untuk mengetahui fungsioanl anti-spam pada *UTM firewall* yang tertera pada tabel 4.13 dengan scenario sesuai gambar 4.23



Gambar 4. 46 Skenario Anti-Spam

Dalam pengujian kasus normal dan kasus tidak normal dapat dilihat pada tabel 4.13 dan tabel 4.14

Tabel 4. 13 Pengujian *Anti-Spam* Normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Data *training spam*	Data *training spam* berhasil disimpan	Data *training spam* berhasil di *testing*	Diterima

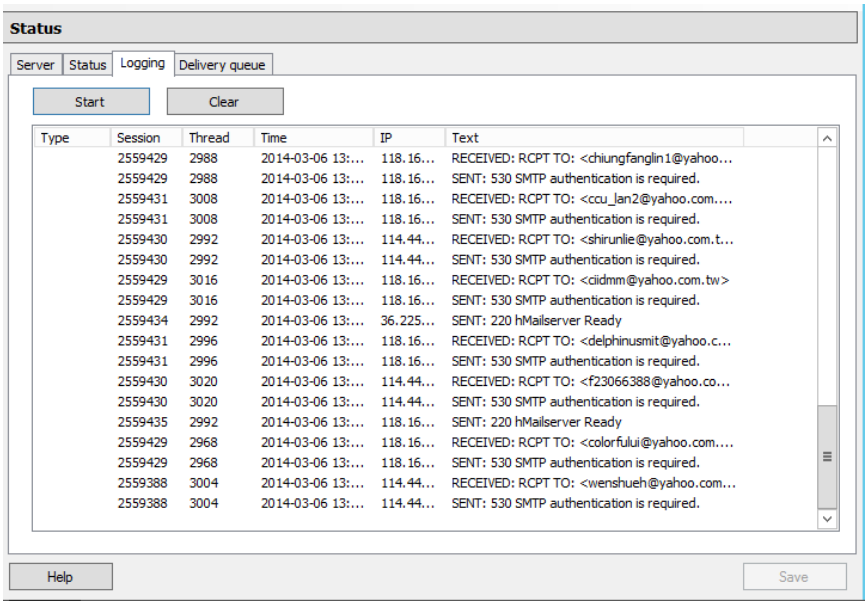
Mengirimkan *mail spam*	*Email spam* terdeteksi	*Mail spam* tertampung pada daftar *mail quarantine* di *UTM firewall*	Diterima

Tabel 4. 14 Pengujian *Anti-Spam* tidak normal

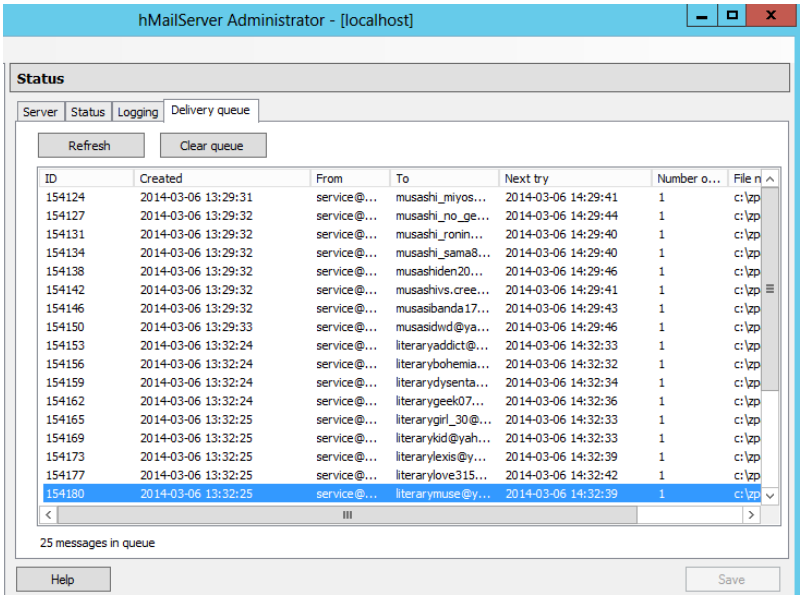
Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengirimkan *mail spam*	*mail spam* tidak terdeteksi	Data *training* masukan tidak berhasil	Diterima
Mengirimkan *mail spam*	*mail spam* tidak terdeteksi	*Mail spam* tidak terdaftar di *Blacklist mail*	Diterima
Mengirimkan *mail spam*	*mail spam* terdeteksi	*Feature anti-spam* tidak diaktifkan	Diterima

UTM firewall tidak bekerja terhadap spam mail *server* dikarenakan data *trainning* masukan tidak ada ataupun data training tidak sesuai, karena spam filtering ini membutuhkan data training terlebih dahulu.

Hasil pengujian mail spam filtering pada *UTM firewall* dapat dilihat di gambar dan gambar dimana *UTM firewall* berhasil melakukan mail filtering sesuai aturan yang di terapkan



Gambar 4. 47 *mail spam* yang berhasil terekam di *logs file*

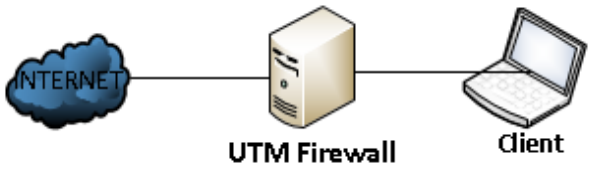


Gambar 4. 48 *mail spam* yang berhasil dicegah

Adapaun *mail spam* yang lolos *filtering* disebabkan beberapa factor diantaranya tidak terdaptar pada *white-list dan black-list mail* dan juga *keyword* tidak terdapatar pada *mail spam filtering.*

6. Web Content Filtering

Pengujian anti-spam untuk mengetahui fungsioanl anti-spam pada *UTM firewall* yang tertera pada tabel 4.15 dengan sekario sesuai gambar 4.24



Gambar 4. 49 Skenario Web Content Filtering

Tabel 4. 15 Pengujian *Content* Normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengakses *website* langsung dari *url*	*Website* diblokir	Komputer *client* melakukan akses *website* langsung dengan mengetikan *url* di *web browser*	Diterima
Mengakses *website* sesuai pencarian *keyword*	*Website* diblokir	Komputer *client* melakukan akses *website* dari hasil *keyword* pada mesin pencari	Diterima

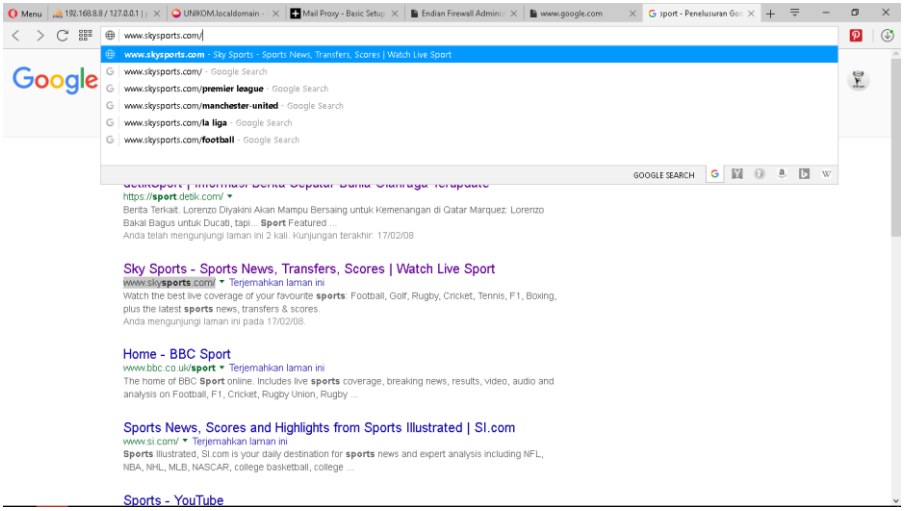
Tabel 4. 16 Pengujian *Content* tidak normal

Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengakses *website* langsung dari url	Website bisa diakses	Alamat *url* tidak terdaftar pada *list block* site di *UTM Firewall*	Diterima
Mengakses *website* sesuai pencarian	Website bisa diakses	*Keyword* yang dimasukan tidak terdaptar pada	Diterima

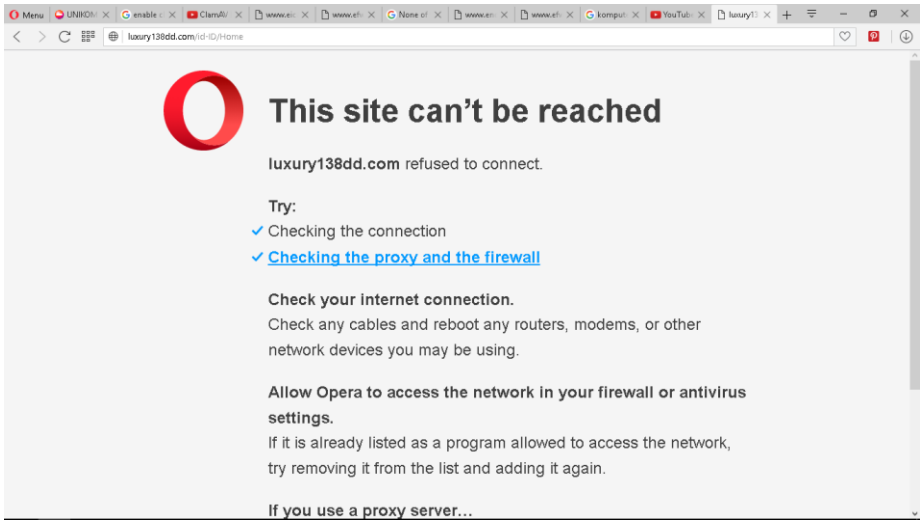
keyword		semua kategori yang di *block*	

Ketika sebuah *content* lolos dari *filtering UTM firewall* ada beberapa penyababnya antara lain *keyword* tidak terdaptar ke dalam list-content ataupn *URL website* tersebut mempunyai content beragam sehingga tidak terdeteksi sebagai *content* yang diblock

Dalam pengujian content filtering ini dilakukan dengan pengaksesan *url* secara langsung dan pengaksesan url dengan menggukan keyword pada mesin pencari. Pada gambar adalah hasil pengujian dimana *UTM firewall* berhasil mengatasi content yang sudah diterapkan sebelumnya baik secara pengaksesan langsung maupun pengaksesan dengan menggunakan keyword pada mesin pencari.

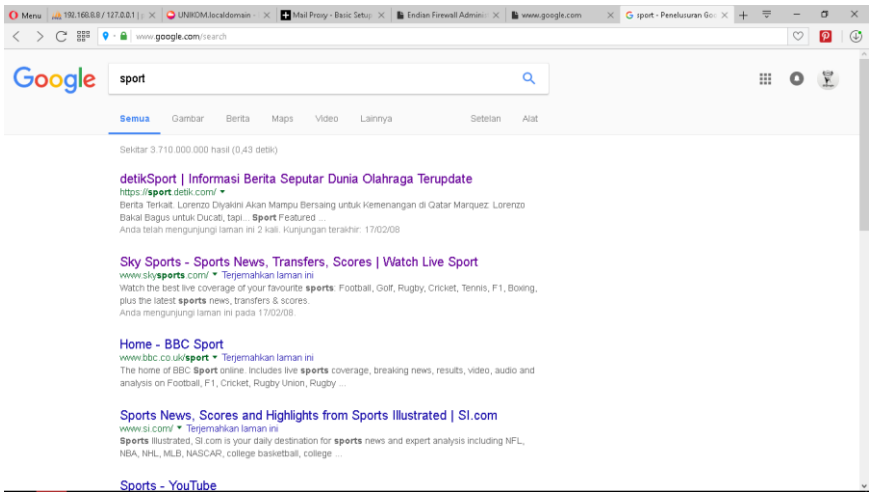


Gambar 4. 50 pengaksesan secara langsung lewat *url*

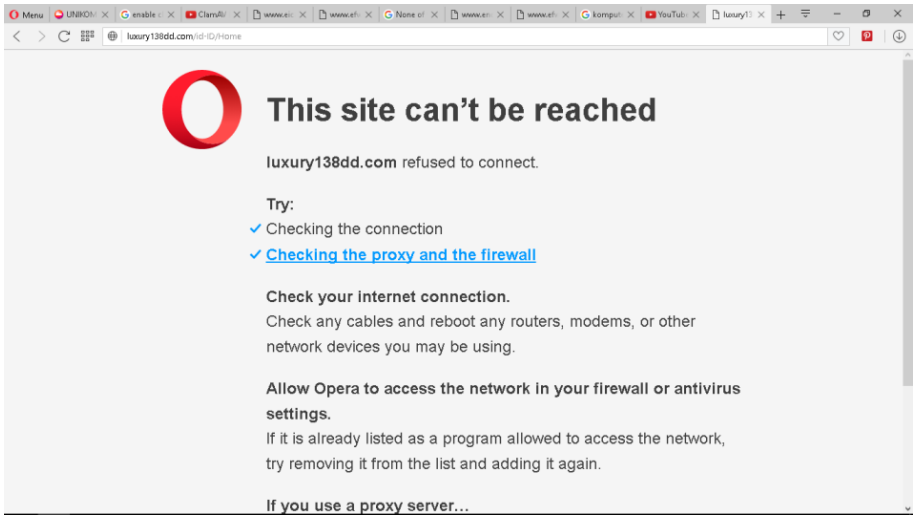


Gambar 4. 51 *UTM firewall* berhasil memblock *traffic* tersebut

Untuk hasil pengujian *content filtering* dengan melalui *keyword* pada mesin pencari, *UTM firewall* berhasil *block content* melalui *keyword* yang sudah diterapkan sebelumnya.



Gambar 4. 52 pengaksesan *content* melalui *keyword*



Gambar 4. 53 *UTM firewall* berhasil memblock *traffic* tersebut

7. Virtual Private Network (VPN)

Pengujian *VPN* ini dilakukan oleh Penanggung Jawab IT dimana untuk melakukan romote dari luar jaringan untuk monitoring keamanan jaringan tersebut dengan scenario pada gambar 4.25 dan kasuk uji pada tabel 4.17



Gambar 4. 54 Skenario VPN

Tabel 4. 17 Pengujian *VPN* Normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Username dan *password* untuk *account VPN*	*Username* dan password terdaptar di *VPN Server*	*Username* dan *password* berhasil disimpan pada *VPN Server*	Diterima
Ping IP Address VPN Server	Koneksi *VPN* berhasil	*Ping IP Address VPN Server* 192.168.88.18 dari komputer *client* dengan respon *Replay TTL*	Diterima
Username dan *password* untuk akses *VPN*	Berhasil *login VPN*	Tool yang digunakan *OpenVPN* dengan memasukan *username* dan *password* yang valid	Diterima

Tabel 4. 18 Pengujian *VPN* tidak normal

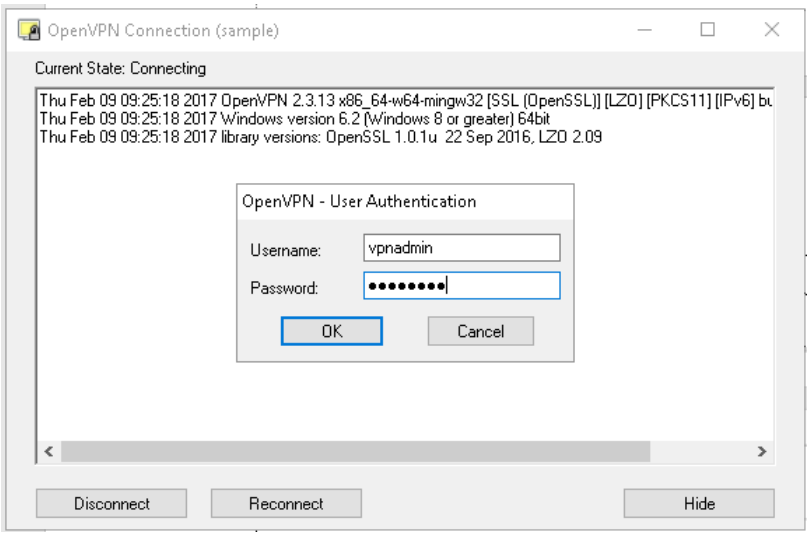
Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Username dan *password* untuk account *VPN*	Username dan password gagal terdaptar di *VPN Server*	*Username* menggunakan spasi	Diterima
Ping IP Address VPN Server	Koneksi *VPN* tidak berhasil	*VPN* tidak diaktifkan	Diterima
Username dan *password* untuk akses *VPN*	Tidak berhasil *login VPN*	*VPN* tidak diaktifkan	Diterima

Dalam penerapan VPN ini harus terlebih dahulu melakukan *register* terhadap *username* dan *password* yang akan dijadikan akses untuk terhadap *VPN Server*. Pada gambar adalah hasil *username* dan *password* berhasil disimpan pada *UTM firewall.*

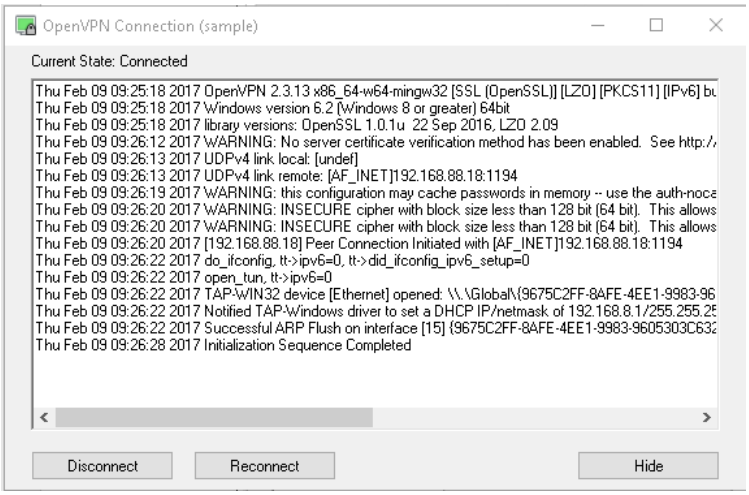


Gambar 4. 55 *username* dan *password* berhasil disimpan

Sistem yang dibangun menggunakan keamanan autentikasi user pada saat log in. Dalam hal ini akan dilakukan pengujian jika user akan mencoba *log in* dengan password yang benar pada gambar 4.56.

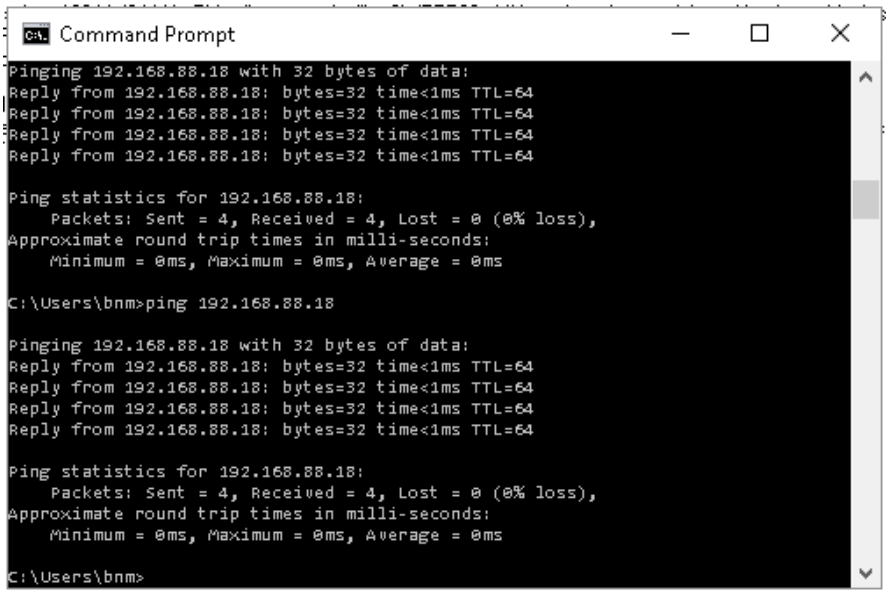


Gambar 4. 56 *username* dan *password* valid



Gambar 4. 57 berhasil masuk ke *VPN*

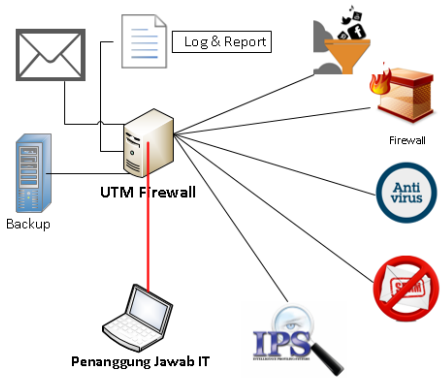
Hasil dari pengujian *VPN* berjalan dengan baik dapat dilihat pada gambar 4.58 dimana dilakukan pengujian *IP address* dari *client*



Gambar 4. 58 Berhasil Pengetesan terhadap *VPN*

8. Control Central Management

Pengujian ini dengan scenario pada gambar 4.25 dan tabel 4.27 untuk mengetahui fungsional dari masing – masing sistem keamana pada *UTM firewall* ini.



Gambar 4. 59 Skenario *Control Management*

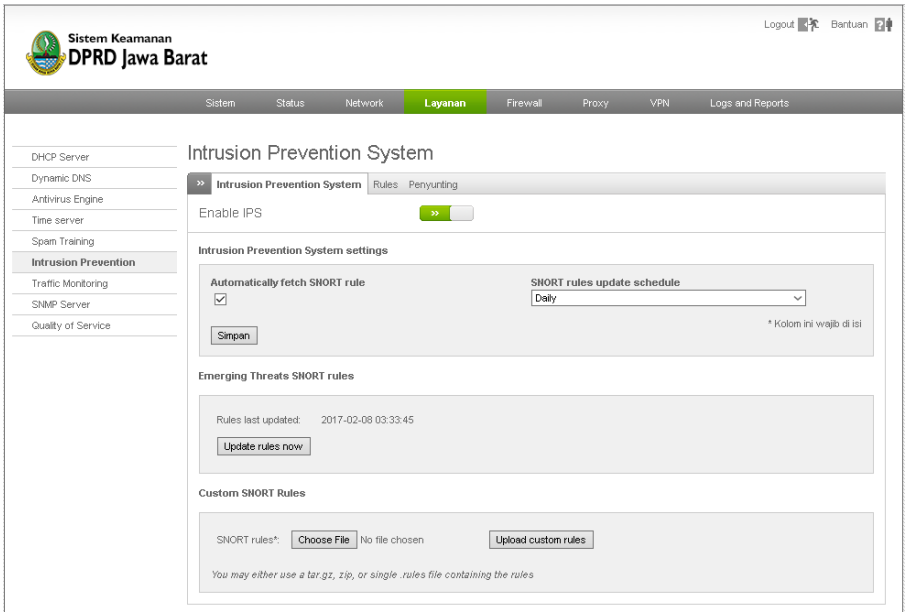
Tabel 4. 19 Pengujian *Control Central Management* normal

Kasus dan Hasil Uji (Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengaktifkan semua fungsi *security*	Semua fungsi bisa berjalan	Semua fungsi berjalan ditandai dengan indicator warna hijau	Diterima
Mengaktifkan fungsi *notification email*	Notifikasi berhasil	Notifikasi berhasil lewat *email* ketika ada aturan yang dilakukan	Diterima
Menampilkan *logs* dan *report*	*Logs* dan *report* ditampilkan	Semua aktifita dapat di *monitoring* pada bagian *logs* dan *report*	Diterima
Mengaktifkan fungsi *backup*	Fungsi *backup* berhasil sesuai jadwal yang telah di atur	Fungsi *backup* berhasil dilakukan sesuai jadwal yang telah di atur	

Tabel 4. 20 Control Management tidak normal

Kasus dan Hasil Uji (Tidak Normal)			
Data Masukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Mengaktifkan semua fungsi *security*	beberapa fungsi tidak bisa berjalan	*System crush*	diterima
Mengaktifkan fungsi *notification email*	Notifikasi tidak berhasil	*System crush*	diterima
Menampilkan *logs* dan *report*	Beberapa *Logs* dan report tidak ditampilkan	*System crush*	diterima
Mengaktifkan fungsi *backup*	Fungsi *backup* tidak berhasil sesuai jadwal yang telah di atur	*System crush*	diterima

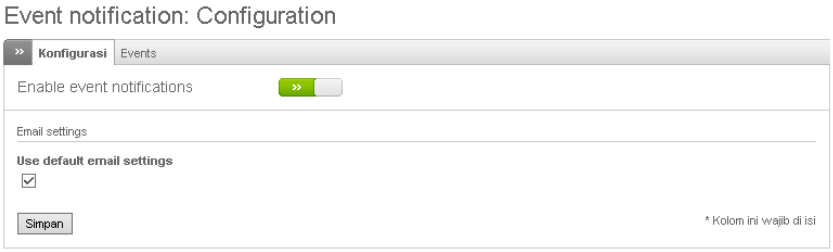
Sistem keamanan pada *UTM firewall* berhasil difungsikan dengan baik dapat terlihat pada gambar 4.60 berikut ini.



Gambar 4. 60 fungsi keamanan *IPS* berhasil dijalankan

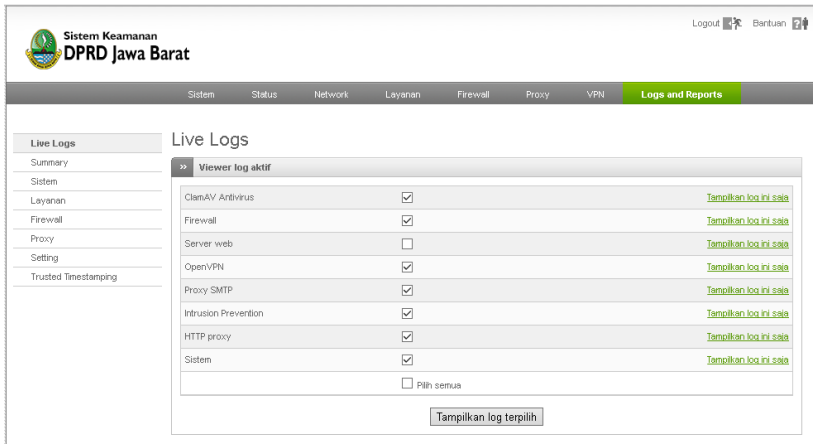
Adapaun untuk fungsi *notification email* dimana fungsi ini bertujuan agar administrator dapat mengetahui dengan segera yang terjadi pada *UTM firewall* ini. Pada gambar 4.61 *UTM firewall* berhasil mengaktifkan fungsi notification mail

Mengaktifkan fungsi notification email



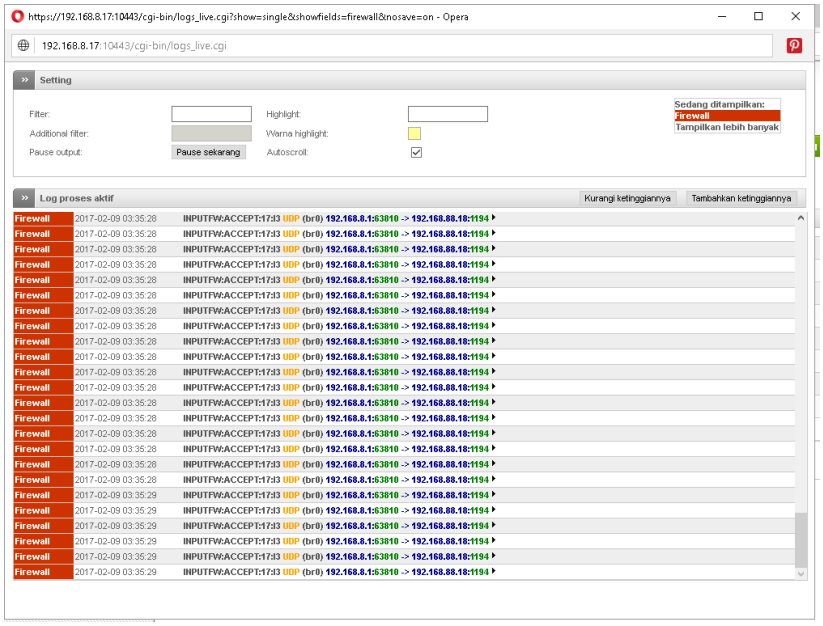
Gambar 4. 61 *notification* email berhasil dilakukan

Hasil dari pengujian *UTM firewall* sebagai contral management center yang bisa menampilkan *logs* dan *report secara menyeluruh dari sistem keamanan yang diterapkan seperti firewall, IPS, anti-virus, anti-spam, content-management,* dan *VPN* dapat dilihat pada *live logs* gambar 4.62 berikut ini.



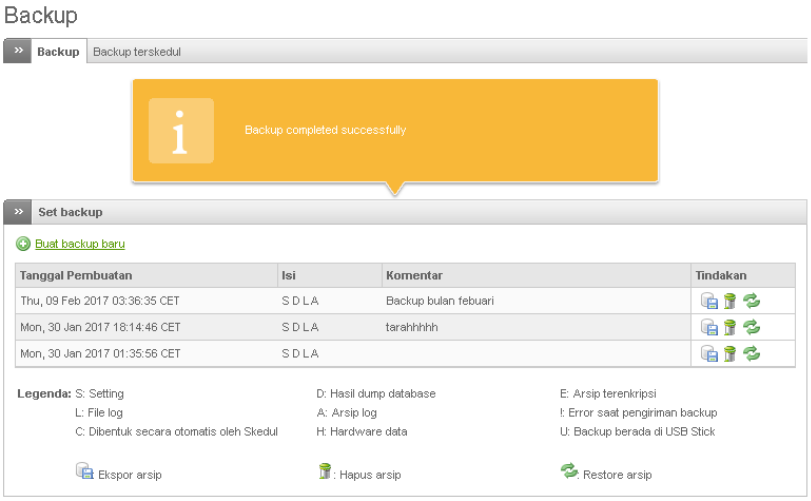
Gambar 4. 62 semua sistem keamanan berhasil di aktifkan

UTM firewall Berhasil menampilkan *logs* dan *report* secara *spesifik* yaitu *firewall* yang terdapat pada gambar 4.63



Gambar 4.63 *Monitoring file logs* berhasil dilakukan

Fungsi *backup* pada *UTM firewall* ini berhasil berjalan dengan baik bisa dilihat pada gambar 4.64 berikut ini



Gambar 4. 64 fungsi *Backup* berhasil dilakukan

4.2.1.3. Kesimpulan Hasil Pengujian Alpha

Dari hasil pengujian sebelumnya bahwa *UTM firewall* dapat melakukan fungsinya sebagai perangkat keamana jaringan sesuai penerapan *rule security*

yang diharapkan. Adapun untuk hasil pengujian tidak normal dapat disebabkan beberapa factor dengan keterbatasan pada sistem ini.

4.2.2. Pengujian Beta

Pengujian beta adalah pengujian yang dilakukan secara objektif dengan kata lain pengujian ini adalah pengujian secara langsung di lapangan atau tempat dimana aplikasi yang dibuat diimplementasikan. Pengujian ini menggunakan kuisioner yang terdiri dari 15 pertanyaan yang ditanyakan kepada Penanggung Jawab IT DPRD Provinsi Jawa Barat.

Tabel 4. 21 Pengujian Beta

No	Pertanyaan	Sangat Setuju	Setuju	Tidak Setuju	Sangat Tidak Setuju
1	Dengan penggabungan beberapa sistem keamanan jaringan menjadi satu seperti *UTM Firewal* apakah anda setuju bisa berfungsi firewall berjalan dengan baik dari pengujian?		[✓]		
2	Spesifikasi *Hardware* yang baik sangat diperlukan dalam penerapan sistem keamanan ini, Apakah anda setuju?		[✓]		
3	Apakah anda setuju kemudahan dalam *maintenance* dan pembaharuan aturan dapat dengan mudah dilakukan di *UTM firewall* dari hasil pengujian?		[✓]		
4	*UTM firewall* mempunyai kemampuan sebagai managemen *network* disamping sebagai security system. Apakah anda setuju semua *management network* dan *security* difungsikan pada UTM *Server*?				[✓]
5	*Feature Anti-virus* pada *UTM Server* sama baiknya dengan Anti-virus pada umumnya. Apakah anda setuju dengan itu?			[✓]	

6	Apakah anda setuju dengan aplikasi berbasis web yang diterapkan pada *UTM firewall* ini dapat mempermudah Penanggung Jawab IT dalam monitoring jaringan. ?	[✓]			
7	Apakah anda setuju dengan adanya *feature update* dapat memberitahu dengan mudah informasi terbaru mengenai ancaman serangan.?	[✓]			
8	Apakah anda setuju penerapan sistem keamanan *UTM firewall* harus mempunyai *license* yang *valid* atau berbayar?	[✓]			
9	Apakah anda setuju fungsi *IPS* pada sistem keamanan ini berjalan dengan baik		[✓]		
10	Apakah anda setuju fungsi *anti-Spam* berjalan sesuai yang diharapkan?			[✓]	
11	Apakah anda setuju sistem keamanan jaringan ini dapat mengatasi untu *content filtering*?		[✓]		
12	Dari hasil pengujian spoofing, apakah anda setujua sistem keamanan ini dapat meminalkan ancaman terhadap spoofing?		[✓]		
13	Apakah anda setuju dengan menggunakan *UTM firewall* ini dapat mengurangi biaya infrastruktur keamanan dalam jaringan ini?	[✓]			
14	Apakah anda setuju dengan adanya *UTM firewall* ini untuk monitoring sistem keamanan jaringan menjadi sederhana?	[✓]			
15	Apakah anda setuju dengan adanya feature event *Notification* pada *UTM firewall* ini dapat memberitahu informasi ancaman penyerangan?		[✓]		

Berdasarkan tabel 4.21 sebanyak 12 pertanyaan yang diajukan kepada penanggung jawab IT DPRD Provinsi Jawa Barat menyatakan setuju terhadap kinerja sistem keamanan jaringan *UTM firewall* ini. Pada 2 pertanyaan tidak

setuju karena beberapa Sistema keamana masih belum sesuai yang diharapkan. Untuk 1 pertanyaan sangat tidak setuju dikarena factor insfrastruktur IT, dimana sebelumnya tidak melakukan perubahan yang signifikan.

Berdasarkan hasil kuisioner tersebut dapat disimpulkan bahwa dengan keamanan jaringan menggunakan UTM firewall dapat bekerja sesuai fungsional yang diharakan serta lebih menyederhanakan monitoring dan maintenance dari PenanggungJawab IT.