PENERAPAN *FIREWALL* MENGGUNAKAN *FORTIGATE* DI PT. PLN RAYON TAMAN SIDOARJO

KERJA PRAKTIK

Progam Studi

S1 Teknik Komputer

Oleh :

MOHAMMAD FERNANDUZ WILLIAM ANDREAW WAHYU

15410200029

FAKULTAS TEKNOLOGI DAN INFOMATIKA
UNIVERSITAS DINAMIKA
2019

LAPORAN KERJA PRAKTIK

PENERAPAN FIREWALL MENGGUNAKAN *FORTIGATE* DI PT. PLN RAYON TAMAN SIDOARJO

Diajukan sebagai salah satu syarat untuk menempuh ujian Tahap Akhir

Program Strata Satu (S1)

Disusun Oleh :

Nama	:	MOHAMMAD FERNANDUZ W.A.W
Nim	:	15.41020.0029
Program	:	S1 (Strata Satu)
Jurusan	:	Teknik Komputer

UNIVERSITAS DINAMIKA

2019

“Jangan Pernah Berhenti Ketika Kamu Masih Belum Ingin Menyerah”

Kupersembahkan Kepada

ALLAH SWT

Ibu, Bapak, dan semua keluarga tercinta,

Yang selalu mendukung, memotivasi dan menyisipkan nama saya dalam doa-doa terbaiknya.

Beserta semua orang yang selalu membantu, mendukung dan memotivasi agar tetap berusaha menjadi lebih baik.

LEMBAR PENGESAHAN

PENERAPAN FIREWALL MENGGUNAKAN FORTIGATE DI PT.PLN RAYON TAMAN SIDOARJO

Laporan Kerja Praktik oleh

MOHAMMAD FERNANDUZ WILLIAM ANDREAW WAHYU

NIM : 15.410.20.0029

Telah diperiksa, diuji dan disetujui

Surabaya, 31 Desember 2019

Disetujui:

Pembimbing

Musayyanah, S.ST., M.T.
NIDN. 0730069102

Penyelia

Desy Sandra Pamungkas
NIP. 8204012J

Mengetahui:

Ketua Program Studi S1 Teknik Komputer

Fakultas Teknologi dan Informatika
UNIVERSITAS Dinamika

Pauladie Susanto, S.Kom., M.T.
NIDN. 0729047501

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Universitas Dinamika, saya :

Nama : Mohammad Fernanduz William Andreaw

NIM : 15410200029

Program Studi : S1 Teknik Komputer

Fakultas : Fakultas Teknologi dan Informatika

Jenis Karya : Laporan Kerja Praktik

Judul Karya : **PENERAPAN FIREWALL MENGGUNNAKAN *FORTIGATE* PT.PLN RAYON TAMAN SIDOARJO**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Universitas Dinamika Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalti Free Right)* atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialihmediakan dan dikelola dalam bentuk pangkalan data *(database)* untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta
2. Karya tersebut di atas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, 31 Desember 2019

METERAI TEMPEL FEAHF200381257 6000 ENAM RIBU RUPIAH

g menyatakan

Mohammad Fernanduz W.A

NIM :15410200029

iv

ABSTRAK

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan *Fortinet*. *Fortinet* merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan *Fortune Global* 100 tahun 2009. Fortinet merupakan pemimpin pasar untuk *Unified Threat Management* (UTM). *Fortigate* sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai *Network Firewall,* keamanaan pada fortigate harus dikonfigurasi dahulu agar keamanan firewall bisa digunakan pada komputer di PT. PLN Rayon Taman Sidoarjo.

Firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *firewall* mengatur, menyaring dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi di PT. PLN Rayon Taman Sidoarjo.

.

Kata Kunci: WAN, Firewal, Fortigate, Fortinet

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat yang telah diberikan - Nya, sehingga penulis dapat menyelesaikan Laporan Kerja Praktik ini. Penulisan Laporan ini adalah sebagai salah satu syarat menempuh Tugas Akhir pada Program Studi S1 Teknik Komputer Universitas Dinamika.

Dalam usaha menyelesaikan penulisan Laporan Kerja Praktik ini penulis banyak mendapat bantuan dari berbagai pihak baik moral maupun materi. Oleh karena itu penulis mengucapkan terima kasih dan penghargaan setinggi - tingginya kepada :

1. Allah SWT, karena dengan rahmatnya dan hidayahnya penulis dapat menyelesaikan Laporan Kerja Praktik ini.
2. Orang Tua saya tercinta yang telah memberikan dorongan dan bantuan baik moral maupun materi sehingga penulis dapat menempuh dan menyelesaikan Kerja Praktik maupun laporan ini.
3. PLN Rayon Taman Sidoarjo atas segala kesempatan, pengalaman kerja yang telah diberikan kepada penulis selama melaksanakan Kerja Praktik.
4. Kepada Desy Sandra Pamukas selaku penyelia. Terima kasih atas bimbingan yang diberikan sehingga penulis dapat melaksanakan Kerja Praktik di PLN Rayon Taman Sidoarjo.
5. Kepada Pauladie Susanto, S.Kom., M.T. selaku Ketua Program Studi Teknik Komputer Surabaya atas ijin yang diberikan untuk melaksanakan Kerja Praktik di Universitas Dinamika
6. Kepada Musayyanah, S.ST.,M.T selaku pembimbing saya sehingga dapat menyelesaikan laporan Kerja Praktik.

7. Bapak Wahju Priastoto selaku Koordinator Kerja Praktek di Universitas Dinamika. terima kasih atas bantuan yang telah diberikan
8. Teman- teman seperjuangan TK angkatan ’15 dan semua pihak yang terlibat namun tidak dapat penulis sebutkan satu persatu atas bantuan dan dukungannya.

Penulis berharap semoga laporan ini dapat berguna dan bermanfaat untuk menambah wawasan bagi pembacanya. Penulis juga menyadari dalam penulisan laporan ini banyak terdapat kekurangan. Oleh karena itu penulis sangat mengharapkan saran dan kritik untuk memperbaiki kekurangan dan berusaha untuk lebih baik lagi.

Surabaya, 31 Desember 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

Latar Belakang

Semakin besar dan pentingnya pemanfaatan teknologi informasi dan komunikasi memicu meningkatnya kompleksitas sistem informasi yang harus dijaga demi mendukung kinerja secara keseluruhan. Salah satu sistem informasi yang memerlukan penanganan khusus adalah jaringan komputer sebagai urat nadi sistem komputer secara keseluruhan pada era teknologi informasi dan komunikasi seperti sekarang. Banyak cara yang dilakukan dalam meningkatkan efektifitas dan performansi jaringan komputer antara lain menambah perangkat pendukung jaringan komputer serta meningkatkan kapasitas *bandwidth* sebagai penopang transaksi data dan informasi.

Penambahan perangkat pendukung jaringan komputer serta meningkatkan kapasitas bandwidth ternyata tidak menjamin kehandalan transaksi data dan informasi dikarenakan banyak faktor yang harus diperhatikan dalam pengelolaan jaringan komputer. Disinilah dibutuhkan metode, inovasi dan terobosan-terobosan yang cerdas sehingga sistem informasi yang dibangun tidak menjadi percuma dan tidak tertinggal dengan yang lain. Dalam memenuhi tuntutan yang tinggi terhadap ketersediaan jaringan komputer yang aman dan handal, sudah barang tentu tersedia perangkat *firewall* sebagai komponen utama keamanan sistem jaringan, tersedia berbagai jenis *firewall* baik yang bersifat *General Public License* maupun *proprietary*. Contohnya adalah *Fortigate* yang merupakan sebuah *firewall* yang bersifat *proprietary* yang tentunya memiliki banyak keunggulan dibandingkan dengan *firewall* yang bersifat gratis (*open source*), salah satu keunggulan dari

proprietary firewall adalah tersedianya UTM (Unified Threat Management) untuk menjamin *QoS* performansi jaringan komputer. Penggunaan *proprietary firewall* menjadi kurang efektif apabila tidak dilengkapi dengan perangkat yang juga *proprietary* untuk melakukan analisa lalu lintas data jaringan komputer, yang mana fungsi perangkat tersebut selain untuk menganalisa juga sebagai media penyimpan log lalu lintas data yang melewati *proprietary firewall*, harga perangkat *proprietary* yang sangat mahal menjadi kendala, sehingga tidak semuanya mampu menggunakan perangkat yang dimaksud.

Perumusan Masalah

Dalam perumusan masalah yang ada pada kerja praktik yang dilakukan oleh penulis terdapat beberapa permasalahan yang harus diselesaikan. Adapun masalah yang harus diselesaikan berdasarkan latar belakang diatas adalah sebagai berikut:

1. Bagaimana cara konfigurasi *Fortigate* di laboratorium PT. PLN Rayon Taman Sidoarjo
2. Bagaimana cara penerapan *Fortigate* di PT. PLN Rayon Taman SIdoarjo

Batasan Masalah

Melihat permasalahan yang ada, maka penulis membatasi masalah dari kerja praktik, yaitu:

1. Pengaplikasian di tempat masih belum menggunakan mikrotik.
2. Dengan menggunakan *fortigate saja* masih cukup mudah untuk ditembus.

Tujuan

Tujuan umum dari kerja praktik yang dilaksanakan mahasiswa adalah agar mahasiswa dapat melihat serta merasakan kondisi dan keadaan *real* yang ada pada dunia kerja sehingga mendapatkan pengalaman yang lebih banyak lagi dan dapat memperdalam kemampuan pada suatu bidang.

Kontribusi

Adapun kontribusi dari kerja praktik terhadap PLN Rayon Taman Sidoarjo adalah membantu meningkatkan kinerja jaringan dan meningkatkan keamanan pada jaringan yang berada di kantor PLN Rayon Taman Sidoarjo

BAB II

GAMBARAN UMUM PERUSAHAAN

Sejarah Singkat PLN

Berawal di akhir abad 19, bidang pabrik gula dan pabrik ketenagalistrikan di Indonesia mulai ditingkatkan saat beberapa perusahaan asal Belanda yang bergerak di bidang pabrik gula dan pebrik teh mendirikan pembangkit tenaga lisrik untuk keperluan sendiri

Antara tahun 1942-1945 terjadi peralihan pengelolaan perusahaan-perusahaan Belanda tersebt oleh Jepang, setelah Belanda menyerah kepada pasukan tentara Jepang di awal Perang Dunia II

Proses peralihan kekuasaan kembali terjadi di akhir Perang Dunia II pada Agustus 1945, saat Jepang menyerah kepada Sekutu. Kesempatan ini dimanfaatkan oleh para pemuda dan buruh listrik melalui delagasi Buruh/Pegawai Listrik dan Gas yang bersama-sama dengan Pemimpin KNI Pusat berinisiatif menghadap Presiden Soekarno untuk menyerahkan perusahaan-perusahaan tersebut kepada Pemerintah Republik Indinesia. Pada 27 Oktober 1945, Presiden Soekarno membentuk Jawatan Listrik dan Gas di bawah Departemen Pekerjaan Umum dan Tenaga dengan kapasitas pembangkit tenaga listrik sebesar 157,5 MW.

Pada tanggal 1 januari 1961, Jawatan Listrik dan Gas diubah menjadi BPU-PLN (Bada Pemimpin Umum Perusahaan Listrik Negara) yang bergerak di bidang listrik, gas dan kokas yang dibubarkan pada tanggal 1 Januari 1965. Pada saat yang sama, 2 (dua) perusahaan negara yaitu Perusahaan Listrik Negara (PLN) sebagai

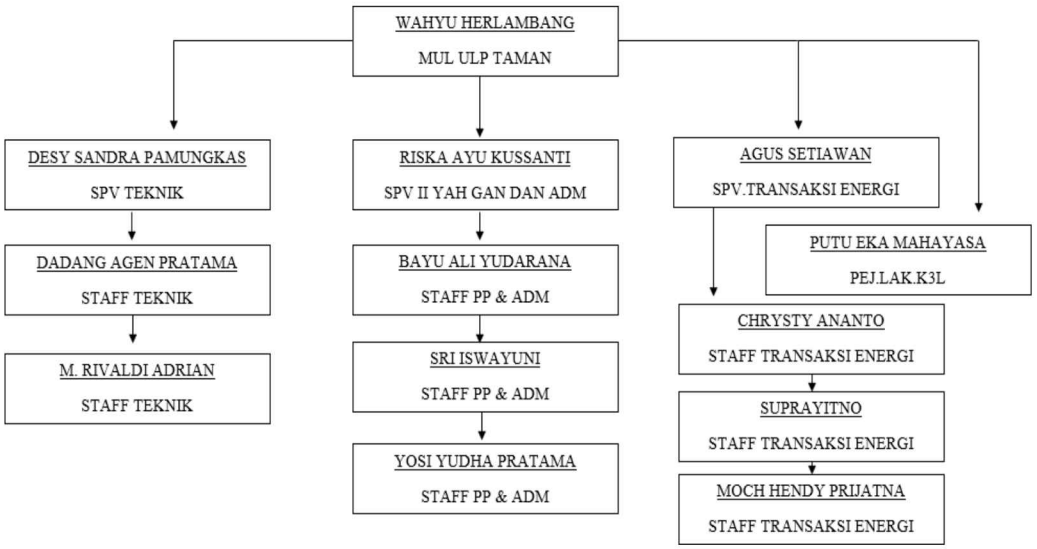
pengelola tenaga listrik milik negara dan Perusahaan Gas Negara (PGN) sebagai pengelola gas diresmikan.

Pada tahun 1972, sesuai dengan Peraturan Pemerintah No. 17, status Perusahaan Listrik Negara (PLN) ditetapkan sebagai Perusahaan Umum Listrik Negara dan sebagai Pemegang Kuasa Usaha Ketenagalistrikan (PKUK) dengan tugas menyediakan tenaga listrik bagi kepentingan umum.

Seiring dengan kebijakan Pemerintah yang memberikan kesempatan kepada sektor swasta untuk bergerak dalam bisnis penyediaan listrik, maka sejak tahun 1994 status PLN beralih dari Perusahaan Umum menjadi Perusahaan Perseroan (Persero) dan juga sebagai PKUK dalam menyediakan listrik bagi kepentingan umum hingga sekarang.

Struktur Organisasi

Struktur Organisasi PT. PLN Rayon Taman Sidoarjo adalah sebagai berikut:



Gambar 2.1 Struktur Organisasi PT.PLN Rayon Taman Sidoarjo

VISI, MISI DAN TUJUAN PLN Rayon Taman Sidoarjo

Visi PLN Rayon Taman Sidoarjo

Diakui sebagai Perusahaan Kelas Dunia yang Bertumbuh kembang, Unggul dan terpercaya dengan bertumpu pada Potensi Insani.

Misi PT.PLN Rayon Taman Sidoarjo

1. Menjalankan bisnis kelistrikan dan bidang lain yang terkait, berorientasi pada kepuasan pelanggan, anggota perusahaan dan pemegang saham.
2. Menjadikan energi listrik sebagai media untuk meningkatkan kualitas kehidupan masyarakat.
3. Mengupayakan akan tenaga listrik menjadi pendorong kegiatan ekonomi.
4. Menjalankan kegiatan usaha yang berwawasan lingkungan

Tujuan PLN Rayon Taman Sidoarjo

Untuk menyelenggarakan usaha penyediaan tenaga listrik bagi kepentingan umum dalam jumlah dan mutu yang memadai serta memupuk keuntungan dan melaksanakan penugasan Pemerintah di bidang ketenagalistrikan dalam rangka menunjang pembangunan dengan menerapkan prinsip-prinsip Perseroan Terbatas.

BAB III

LANDASAN TEORI

Firewall

Pengertian *Firewall*

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar. *Firewall* merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap hardware , software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *Workstation*, *Server*, *Router*, atau *Local Area Network*. (Paul G, 2013)

Fungsi *Firewall*

Fungsi *firewall* sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *firewall* mengatur, menyaring dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak.

a. Alamat IP dari komputer sumber

b. Port TCP/UDP sumber dari sumber.

c. Alamat IP dari komputer tujuan

d. Port TCP/UDP tujuan data pada komputer tujuan

Manfaat *Firewall*

a. Manfaat *firewall* adalah untuk menjaga informasi rahasia dan berharga yang menyelinap keluar tanpa sepengetahuan. Sebagai contoh, *File Transfer Protocol* (FTP) lalu lintas dari jaringan komputer organisasi dikendalikan oleh *firewall*. Hal ini dilakukan untuk mencegah pengguna di jaringan mengirim file rahasia yang disengaja atau tidak sengaja kepada pihak lain.

b. Manfaat *Firewall* sebagai filter juga digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan. Hal ini mencegah pengguna berbagi file, dan bermain-main di jaringan. Aplikasi jenis ini berguna terutama dalam sektor korporasi.

c. Manfaat *firewall* lainnya adalah untuk memodifikasi paket data yang datang di *firewall*. Proses ini disebut *Network Address Translation* (NAT). Ada jenis NAT disebut NAT dasar, di mana alamat IP (*Internet Protocol*) pribadi dari jaringan komputer yang tersembunyi di balik satu alamat IP tertentu. Proses ini disebut sebagai IP samaran. Hal ini membantu pengguna dalam sebuah jaringan yang meliputi sistem tanpa nomor IP publik yang beralamat, untuk mengakses *Internet*.

Cara Kerja *Firewall*

a. Cara Kerja *Firewall* dari komputer adalah menutup *port* kecuali untuk beberapa *port* tertentu yang perlu tetap terbuka. *Firewall* dikomputer bertindak sebagai garis pertahanan terdepan dalam mencegah semua jenis *hacking* ke dalam jaringan, karena, setiap *hacker* yang mencoba untuk menembus ke dalam jaringan computer.

b. *Firewall* dapat berupa perangkat keras atau perangkat lunak namun cara kerja *firewall* optimal bila kedua jenis perangkat digabungkan. Selain membatasi akses ke jaringan komputer, *firewall* juga memungkinkan akses remote ke jaringan privat melalui *secure authentication certificates and logins* (sertifikat keamanan otentikasi dan login).

c. *Hardware firewal* dapat dibeli sebagai produk yang berdiri sendiri, tetapi biasanya pada *router broadband* ditemukan, dan seharusnya dilakukan setting pada perangkat ini untuk akses ke jaringan komputer. Kebanyakan *hardware firewall* adalah memiliki minimal empat *port* jaringan untuk menghubungkan komputer lain.

d. Teknologi *firewall* saat ini sudah sangat canggih. Sebelumnya, cara kerja *firewall* adalah dengan menyaring lalu lintas jaringan yang menggunakan alamat IP, nomor *port*, dan protokol, tapi saat ini *firewall* dapat menyaring data dengan mengidentifikasi pesan konten itu sendiri. Dengan bantuan *firewall*, informasi sensitif atau tidak layak dapat dicegah melalui *interface*. Pastikan sistem keamanan jaringan dilapisi *firewall.*

Fortigate

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan *Fortinet*. *Fortinet* merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan *Fortune* Global 100 tahun 2009. *Fortinet* merupakan pemimpin pasar untuk unified threat management (UTM). *Unified Threat Management* adalah segmen produk jaringan yang dikhususkan untuk menangani fungsi keamanan jaringan secara terpadu. Pada produk UTM ini menghasilkan *Fortigate* yang memiliki fitur-fitur seperti *firewall*,

Intrusion Prevention System, web filter, antivirus yang digabungkan menjadi satu kesatuan dengan tambahan fitur jaringan lain seperti *routing* dalam satu *box hardware*.

Fitur-Fitur *Fortigate*

1. Antarmuka Administrasi

Aktivitas manajemen keamanan jaringan biasanya menuntut banyak interaksi dengan *software* dan *hardware* dari beberapa vendor yang berbeda. Saking banyaknya perangkat yang dipakai, sering mengharuskan kita melakukan berbagai pembaruan terhadap masing-masing perangkat. Hal ini tentu saja akan sedikit ribet dan butuh waktu. Kondisi ini tidak akan diperlukan jika perusahaan IT tersebut memakai *FortiGate*. Karena *FortiGate* sudah mencakup semua kontrol yang dibutuhkan. *FortiGate* adalah perangkat yang menjamin keamanan jaringan secara menyeluruh, sekaligus sebagai *gateaway*, *router*, *firewall*, *hub VPN*, antivirus, antispam, anti *spyware*, *traffic shapping,* dan *proxy*.

Sebagai informasi, *FortiGate* dilengkapi dengan dua antarmuka administratif yang canggih, yakni:

- Manajer berbasis web, yaitu antarmuka grafis yang dapat dipergunakan melalui browser web.
- Antarmuka baris perintah, yaitu antarmuka grafis yang lengkap dan user friendly. Ini artinya ada efisiensi baris perintah. Jadi, Anda tidak perlu mengetikkan berbaris-baris perintah seperti saat tidak menggunakan *FortiGate*.

2. Memiliki tingkat ketahanan yang tinggi dan *high availability*

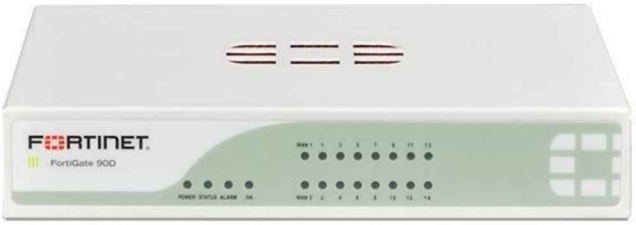
FortiGate sangat fleksibel, karena itu bisa disesuaikan dengan kebutuhan perusahaan. Untuk itu, ada 4 cara berbeda untuk membuat *FortiGate* ini high available, yakni dengan menggunakan desain cluster berikut ini:

- Memakai dua atau lebih unit *FortiGate Cluster Protocol (FGPC)*
- Memakai load balancer eksternal yakni *FortiGate Session Life Support Protocol (FGSP)*
- Mempergunakan solusi ketahanan layar 3, semisal *Virtual Router Redundancy Protocol (VRRP)*
- Menggunakan solusi layer 2 yakni *Fortinet Redundant UTM Protocol (FRUP)*

3. Memiliki fitur *Virtual Domain (VDOMs)*

Virtual domain yang ditawarkan oleh *Fortinet* ini adalah salah satu fitur yang memberi akses menuju beragam perusahaan dengan administrator yang berbeda, namun tetap dengan unit fisik yang sama.

Tujuannya agar masing-masing dapat menjaga konfigurasi yang spesifik, tanpa memberikan dampak berlebihan antara satu dengan yang lain.



Gambar 3.1 Router *Fortigate*

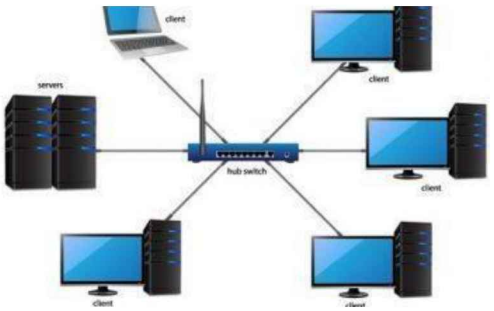
Jaringan

Jaringan Komputer

Jaringan komputer adalah kumpulan komputer dan peralatan lainnya yang saling terhubung dan membentuk suatu kesatuan system". Sebuah jaringan komputer memungkinkan informasi dan data berpindah dari satu jaringan ke jaringan yang lain sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data. Tidak hanya itu, sebuah jaringan komputer juga memungkinkan penggunakanya mencetak pada printer yang sama dan digunakan secara bersama sama. (Indra W, 2012) Jaringan komputer secara umum yaitu sebuah sistem yang terdiri dari atas komputer, *software* dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai tujuan yang sama, setiap bagian komputer meminta dan memberikan layanan *(service)*, jaringan komputer terbagi menjadi tiga kelompok, yaitu:

a. *Local Area Network* (LAN)

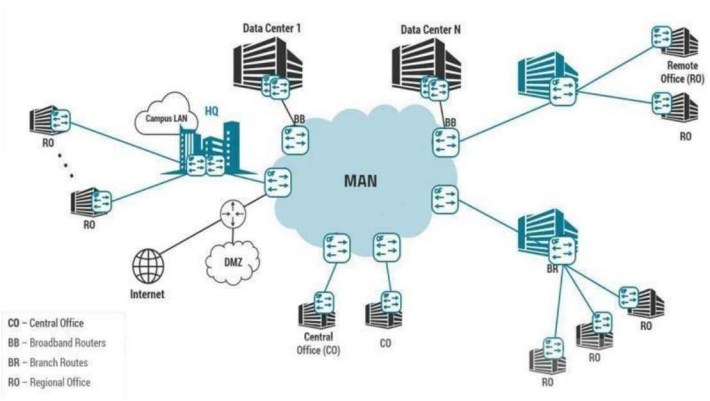
Local Area Network (LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, kantor, gedung atau yang lebih kecil.



Gambar 3.2 Jaringan LAN

b. *Metropolitan Area Network* (MAN)

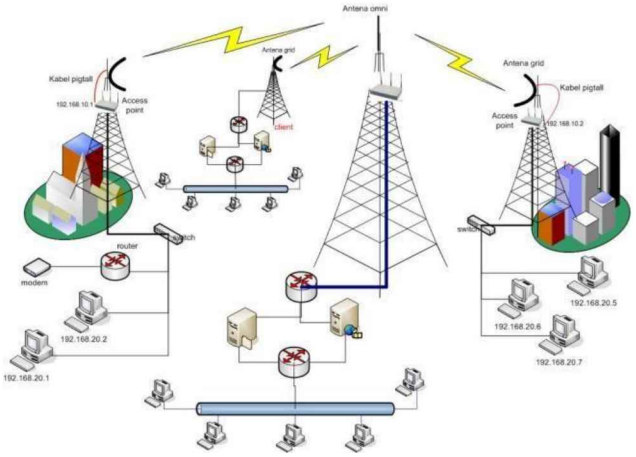
Metropolitan Area Network (MAN) adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antara 10 hingga 50 Km.



Gambar 3.3 Jaringan MAN

c. *Wide Area Network* (WAN)

Wide Area Network (WAN) merupakan jaringan komputer yang mencakup area besar. Jangkauannya mencakup daerah geografis yang luas, sebagai contoh yaitu jaringan komputer antar wilayah, antar kota, antar negara, bahkan benua.



Gambar 3 4 Jaringan WAN

Tujuan Membangun Jaringan Komputer

Tujuan dibangunnya suatu jaringan komputer adalah membawa informasi secara tepat dan tanpa adanya kesalahan dari sisi pengirim (*transmitter*) menuju ke sisi penerima (*receiver*) melalui media komunikasi.

Ada beberapa kendala dalam membangun jaringan komputer, yaitu:

1. Masih mahalnya fasilitas komunikasi yang tersedia dan bagaimana memanfaatkan jaringan komunikasi yang ada secara efektif dan efisien.
2. Jalur transmisi yang digunakan tidak benar-benar bebas dari masalah gangguan (*noise*).

Manfaat Jaringan Komputer

Manfaat yang didapat dalam membangun jaringan komputer yaitu:

1. *Sharing Resources*

Sharing Resources bertujuan agar seluruh program, peralatan atau *peripheral* lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai.

2. Media Komunikasi

Jaringan Komputer memungkinkan terjadinya komunikasi antar pengguna, baik untuk mengirim pesan atau informasi penting lainnya.

3. Integrasi Data

Jaringan Komputer dapat mencegah ketergantungan pada komputer pusat, karena setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya. Oleh sebab itu maka dapat terbentuk data

yang terintegrasi yang memudahkan pemakai untuk memperoleh dan mengola informasi setiap saat.

4. Pengembangan dan Pemeliharaan

Pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer juga memudahkan pemakai dalam merawat *harddisk* dan peralatan lainnya.

5. Keamanan Data

Sistem Jaringan Komputer dapat memberikan perlindungan terhadap data. Karena pemberian dan pengaturan hak akses kepada para pemakai, serta teknik perlindungan terhadap *hardisk* sehingga data mendapatkan perlindungan yang efektif.

6. Sumber Daya Lebih Efisien dan Informasi Terkini

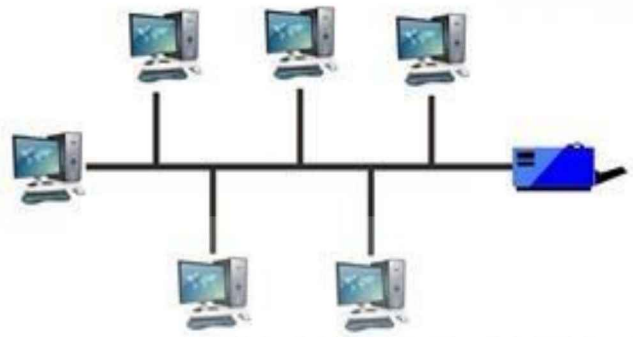
Dengan pemakaian sumber daya secara bersama-sama, akan mendapatkan hasil yang maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera langsung diketahui oleh setiap pemakai.

Topologi

Topologi Jaringan adalah sebuah pola interkoneksi dari beberapa terminal komputer. Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) yang menunjukan posisi pemasangan kabel secara fisik dan topologi logika (*logical topology*) yang menunjukan bagaimana suatu media diakses oleh *host*.

Topologi *Bus*

Topologi ini menggunakan satu *segment* (panjang kabel) *backbone*, yaitu yang menyambungkan semua *host* secara langsung. Apabila komunikasinya dua arah di sepanjang *ring*, maka jarak maksimum antara dua simpul pada *ring* dengan n simpul adalah n/2.Topologi ini cocok untuk jumlah prosesor yang relatif sedikit dengan komunikasi data minimal.



Gambar 3.5 Topologi Bus

A. Keuntungan Topologi *Bus*:

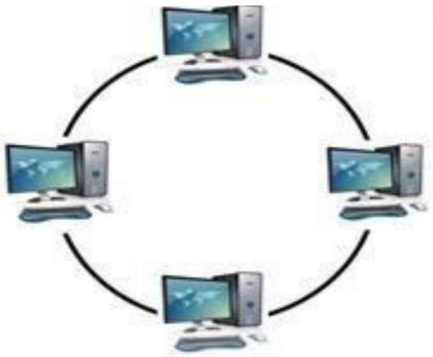
1. Jarak LAN tidak terbatas
2. Kecepatan pengiriman tinggi.
3. Tidak diperlukan pengendali pusat.
4. Kemampuan pengandalan tinggi

B. Kerugian Topologi *Bus*:

1. Operasi jaringan LAN tergantung tiap perangkat.
2. Deteksi dan isolasi kesalahan sangat kecil.
3. Bila salah satu *client* rusak, maka jaringan tidak bisa berfungsi.
4. Diperlukan *repeater* untuk jarak jauh.

Topologi *Ring*

Topologi ini menghubungkan satu *host* ke *host* setelah dan sebelumnya. Secara fisik jaringan ini berbentuk *ring* (lingkaran). Topologi cincin juga merupakan topologi jaringan dimana setiap titik terkoneksi ke dua titik lainnya, membentuk jalur melingkar membentuk cincin.



Gambar 3.6 Topologi Ring

Pada topologi cincin, komunikasi data dapat terganggu jika satu titik mengalami gangguan. Jaringan FDDI mengantisipasi kelemahan ini dengan mengirim data searah jarum jam dan berlawanan dengan arah jarum jam secara bersamaan.

A. Keuntungan Topologi *Ring*:

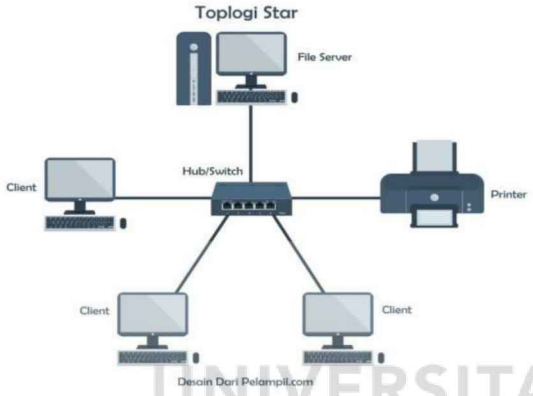
1. Hemat Kabel.
2. Tidak terjadi tabrakan saat pengiriman data.

B. Kerugian Topologi *Ring*:

1. Peka kesalahan.
2. Pengembangan jaringan lebih kaku.

Topologi *Star*

Menghubungkan semua kabel pada *host* ke satu titik utama. Titik ini biasanya menggunakan *Hub* atau *Switch*. Topologi bintang merupakan bentuk topologi jaringan yang berupa konvergensi dari *node* tengah ke setiap *node* atau pengguna. Topologi jaringan bintang termasuk topologi jaringan dengan biaya menengah.



Gambar 3.7 Topologi Star

A. Keuntungan Topologi *Star*:

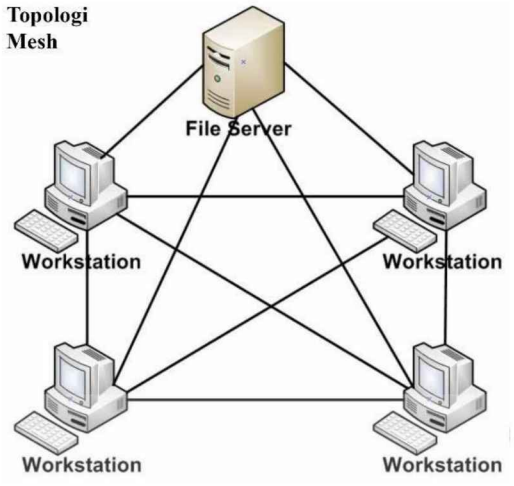
1. Kerusakan pada satu saluran hanya akan mempengaruhi jaringan pada saluran tersebut dan *station* yang terpaut.
2. Tingkat keamanan termasuk tinggi.
3. Tahan terhadap lalu lintas jaringan yang sibuk.
4. Penambahan dan pengurangan *station* dapat dilakukan dengan mudah.

B.* Kerugian Topologi *Star:

1. Jika *node* tengah mengalami kerusakan, maka seluruh jaringan akan terhenti.
2. Penggunaan kabel terlalu boros.

Topologi *Mesh*

Topologi *Mesh* adalah suatu topologi yang memang didisain untuk memiliki tingkat restorasi dengan berbagai alternatif *rute* atau penjaluran yang biasanya disiapkan dengan dukungan perangkat lunak atau *software*



Gambar 3.8 Topologi Mesh

A. Kelebihan Topologi *Mesh*:

1. Jika ingin mengirimkan data ke komputer tujuan, tidak membutuhkan komputer lain (langsung sampai ke tujuan).
2. Memiliki sifat *robust*, yaitu: jika komputer A mengalami gangguan koneksi dengan komputer B, maka koneksi komputer A dengan komputer lain tetap baik.
3. Lebih aman.
4. Memudahkan proses identifikasi kesalahan.

B. Kekurangan Topologi *Mesh*:

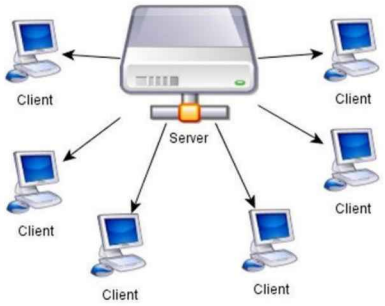
1. Membutuhkan banyak kabel.
2. Instalasi & konfigurasi sulit.
3. Perlunya *space* yang memungkinkan.

Tipe Jaringan

Secara garis besar tipe jaringan dibagi menjadi dua macam, yaitu tipe jaringan *Peer-to-Peer* dan *Client-Server*.

Jaringan *Peer To Peer*

Pada jaringan tipe ini, setiap komputer yang terhubung dalam jaringan dapat saling berkomunikasi dengan komputer lainnya secara langsung tanpa perantara. Bukan hanya komunikasi langsung tetapi juga sumber daya komputer dapat digunakan oleh komputer lainnya tanpa ada pengendali dan pembagian hak akses. Setiap komputer dalam jaringan *Peer to Peer* mampu berdiri sendiri sekalipun komputer yang tidak bekerja atau beroperasi. Masing-masing komputer tidak terikat dan tidak tergantung pada komputer yang lainnya. Komputer yang digunakan pun bisa beragam dan tidak harus setara, karena fungsi komputer dan keamanannya diatur dan dikelola sendiri oleh masing-masing komputer.



Gambar 3.9 Jaringan *Peer To Peer*

B. Keunggulan Jaringan *Peer To Peer*:

1. Antar Komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya serperti: *harddisk, drive,* fax/*modem, printer*.

2. Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan *client-server*, salah satunya karena tidak memerlukan adanya *server* yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.
3. Kelangsungan kerja jaringan tidak tergantung pada satu *server*. Sehingga bila salah satu komputer atau *peer* mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.

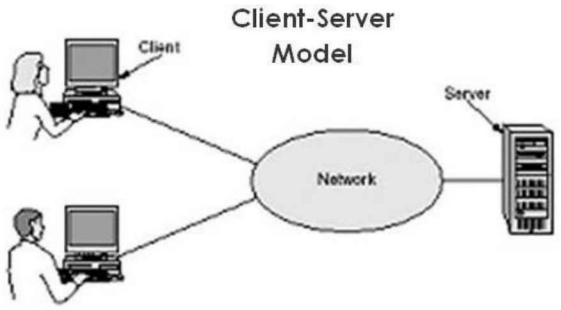
C. Kelemahan Jaringan *Peer To Peer*:

1. *Troubleshooting* jaringan relatif lebih sulit, karena pada jaringan tipe *peer to peer* setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan *client-server*, komunikasi adalah anatara *server* dengan *workstation*.
2. Unjuk kerja lebih rendah dibandingkan dengan jaringan *client-server*, karena setiap komputer atau *peer* disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
3. Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur masing-masing fasilitas yang dimiliki.

Jaringan *Client-Server*

Sesuai dengan namanya, jaringan komputer tipe ini memperlukan sebuah (atau lebih) komputer yang difungsikan sebagai pusat pelayanan dala jaringan yang disebut *server*. Komputer-komputer lain disebut sebagai *Client* atau *Workstation*. Sesuai sebutannya, komputer *server* bertugas melayani semua kebutuhan komputer

lain yang berada dalam jaringan. Semua fungsi jaringan dikendalikan dan diatur oleh komputer *server*, termasuk masalah keamanan jaringan seperti hak akses data, waktu akses, sumber daya dan sebagainya.



Gambar 3.10 Jaringan *Client-Server*

A. Keunggulan Jaringan *Client-Server*:

1. Memberikan keamanan yang lebih baik.
2. Lebih mudah pengaturannya bila *network* nya besar karena administrasinya di sentralkan.
3. Semua data dapat di backup pada satu lokasi sentral.

B. Kelemahan Jaringan *Clien-Server*:

1. Membutuhkan hardware yang lebih tinggi dan mahal untuk mesin *server.*
2. Mempunyai satu titik lemah jika menggunakan satu *server*, data user menjadi tidak ada jika *server* mati.

Protokol Jaringan

Protokol adalah serangkaian aturan yang mengatur unit fungsional agar komunikasi bisa terlaksana. Misalnya mengirim pesan, data, dan informasi. Protokol juga berfungsi untuk memungkinkan dua atau lebih komputer dapat berkomunikasi dengan bahasa yang sama. Secara umum fungsi dari *protocol* adalah untuk menghubungkan sisi pengirim dan penerima dalam berkomunikasi serta

dalam bertukar informasi agar dapat berjalan dengan baik dan benar dengan kehandalan yang tinggi.

IP *Address*

Alamat IP (*Internet Protocol Address* atau sering disingkat IP) adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* yang berada dalam jaringan internet. Panjang dari angka ini adalah 32-bit (untuk IP versi 4) dan 128-bit (untuk IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan internet berbasis TCP/IP. IP *address* yang terdiri dari bilangan biner 32-bit tersebut dipisahkan oleh tanda titik pada setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet, bentuk IP address dapat dituliskan sebagai berikut:

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx jadi IP *address* ini mempunyai *range* dari 00000000.00000000.00000000.00000000. sampai 11111111.11111111.11111111.11111111. Notasi IP *address* dengan bilangan seperti ini susah untuk digunakan, sehingga sering ditulis dalam 4 bilangan *decimal* yang masing-masing dipisahkan 4 buah titik yang lebih dikenal dengan "notasi desimal bertitik". Setiap bilangan desimal merupakan nilai dari satu oktet IP *address*. Contoh hubungan suatu IP *address* dalam format biner dan desimal:

A. Kelas-kelas IP *Address*

IP *address* dapat dipisahkan menjadi 2 bagian, yakni bagian *network* (*net* ID) dan bagian *host* (*host* ID). *Net* ID berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *host* ID berperan untuk identifikasi *host* dalam suatu *network.*

1. Bit pertama IP *address* kelas A adalah 0, dengan panjang *net* ID 8 bit dan panjang *host* ID 24 bit. Jadi *byte* pertama IP *address* kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 *network* dengan tiap *network* dapat menampung sekitar 16 juta *host* (255x255x255x255).
2. Dua bit IP *address* kelas B selalu diset 10 sehingga *byte* pertamanya selalu bernilai antara 128-191. *Network* ID adalah 16 bit pertama dan 16 bit sisanya adalah *host* ID sehingga kalau ada komputer mempunyai IP *address* 192.168.26.161, *net* ID = 192.168 dan *host* ID = 26.161. Pada IP *address* kelas B ini mempunyai *range* IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx yakni berjumlah 65.255 *network* dengan jumlah *host* tiap *network* 255x255 *host* atau sekitar 65 ribu *host*.
3. IP *address* kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP *address* kelas C selalu diset 111. *Network* ID terdiri dari 24bit dan *host* ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta *network* dengan masing-masing *network* memiliki 256 *host*.

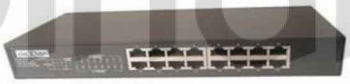
Network Device

3.6.5 *Switch*

Switch tidak digunakan untuk membuat *internetwork* tapi digunakan untuk memaksimalkan jaringan LAN. Tugas utama dari *switch* adalah membuat LAN bekerja dengan lebih baik dengan mengoptimalkan unjuk kerja (*performance*), menyediakan lebih banyak bandwidth untuk penggunaan LAN. *Switch* tidak seperti *router, switch* tidak meneruskan paket ke jaringanlain. *Switch* hanya menghubung-hubungkan *frame* dari satu *port* ke *port* yang lainnya di jaringan mana dia berada.

Secara default, *switch* memisahkan *collision domain*. Istilah *collision domain* adalah istilah di dalam *Ethernet* yang menggambarkan sebuah kondisi *network* dimana sebuah alat mengirimkan paket pada sebuah *segment network*, kemudian memaksa semua alat yang lain di segment tersebut untuk memperhatikan paketnya. Pada saat yang bersamaan, alat yang berbeda mencoba mengirimkan paket yang lain, yang mengakibatkan terjadinya *collision*. Paket yang dikirim menjadi rusak akibatnya semua alat harus melakukan pengiriman ulang paket, sehingga seperti ini menjadi tidak efisien.

Switch dapat dikatakan sebagai *multi-port brigde* karena mempunyai *collision domain* dan *broadcast domain* tersendiri, dapat mengatur lalu lintas paket yang melalui *switch* jaringan. Cara menghubungkan komputer ke *switch* sangat mirip dengan cara menghubungkan komputer atau *router* ke *hub*. *Switch* dapat digunakan langsung untuk menggantikan *hub* yang sudah terpasang pada jaringan.



Gambar 3.11 *Switch*

Hub

Hub biasanya titik koneksi pertama antara sebuah titik koneksi jaringan dan sebuah LAN.Variasi hub sangat luas dalam fungsi dan kapabilitasnya. *Hub* yang paling sederhana tidak lebih dari koneksi pemasangan terpusat pada titik tunggal dan biasanya dinamakan *Wiring Concentrator*.

Jaringan *hub* sesuai dengan perkembangan teknik mutakhir lebih tidak dapat bekerja sama dengan fungsi *routing, bridges* dan *switching. Hub* untuk *token ring* LAN lebih *sophisticated* dari hub untuk tipe LAN karena mereka harus

mengenerate sebuah *token* ketika jaringan dimulai atau jika *token* asli hilang dan sekitar jalur transmisi ulang terputus atau gagal terhubung. Jalur transmisi yang dihubungkan ke sebuah NIU atau jaringan *hub* dengan standar konektor. Konektor RJ-45 seperti konektor telepon RJ-11 kecuali lebih besar dan menghubungkan 8 kabel, ada beberapa standar untuk konektor *fiber optic* termasuk ST,SC,LT and MT-RJ. Standar MT-RJ telah mendukung peralatan vendor termasuk Cisco dan 3com.

Gambar 3.12 *Hub*

Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau *network operating system*. Server juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat penectak (*printer*) dan memberikan akses kepada *workstation* anggota jaringan.

Umumnya, di atas sistem operasi *server* terdapat aplikasi-aplikasi yang menggunakan arsitektur *client/server*. Contoh dari aplikasi ini adalah DHCP *Server, Mail* Server, *HTTP Server*, FTP *Server*, DNS *Server* dan lain sebagainya. Setiap

sistem operasi *server* umumnya *membundle* layanan-layanan tersebut atau layanan tersebut juga dapat diperoleh dari pihak ketiga. Setiap layanan-layanan tersebut akan merespon terhadap *request* dari klien. Sebagai contoh, *client* DHCP akan memberikan *request* kepada *server* yang menjalankan *server* DHCP, ketika sebuah *client* membutuhkan alamat IP, klien akan memberikan perintah atau *request* kepada *server*, dengan bahasa yng dipahami oleh *server* DHCP, yaitu *protocol* DHCP itu sendiri.

Contoh sistem operasi *server* adalah Windows NT 3.51, dan dilanjutkan dengan Windows NT 4.0. Saat ini sistem yang cukup popular adalah Windows 2000 *Server* dan Windows *Server* 2003, kemudian Sun Solaris, Unix dan GNU/Linux. *Server* biasanya terhubung dengan client dengan kabel UTP dan sebuah *Network Card*. Kartu jaringan ini biasanya berupa kartu PCI atau ISA. Fungsi *server* sangat banyak, misalnya untuk situs internet, ilmu pengetahuan atau sekedar penyimpanan data. Namun yang paling umum adalah untuk mengkoneksikan komputer *client* ke *Internet*.

BAB IV

DESKRIPSI KERJA PRAKTIK

Pada bab ini akan membahas tentang bagaimana proses instalasi dan konfigurasi *FortiGate* yang telah di diterapkan selama Kerja Praktik berlangsung.

Konfigurasi *Fortigate*

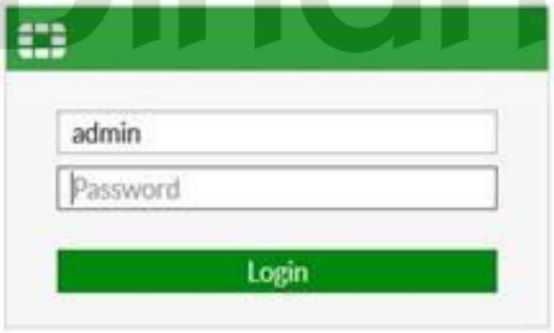
Pengenalan Tentang *FortiGate*

1. Untuk mengaksesnya *Fortigate* kita bisa mengunakan web.

   Colok kabel lan ke port 1 pada *fortigate*, *IP Default Fortigate* 192..168.1.99/24 akses di browser

   User Name : admin

   Password : dikosongkan (Dikosongkan karena default dari fortigate)



Gambar 4.1 Akses Web *Fortigate*

2. Di menu *Dashboard* tersebut terlihat

   Unit Operation: Menampilkan unit yang digunakan)

   System Information: Menampilkan sistem yang dipakai pada device)

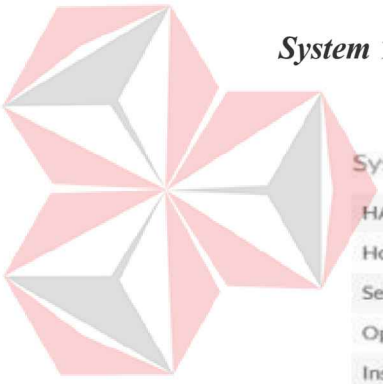
   apabila tidak tampil bisa di tambahkan pada menu ***Add Widget*** disisi kanan bawah.

   Di *System Informartion* kita dapat *merubah*

   Host Name : Nama komputer.

   Inspection Mode : Merupakan bagian dari Web Development Tools yang memungkinkan untuk mengubah tampilan web atau debug secara sementara sampai halaman tersebut di refresh / reload.

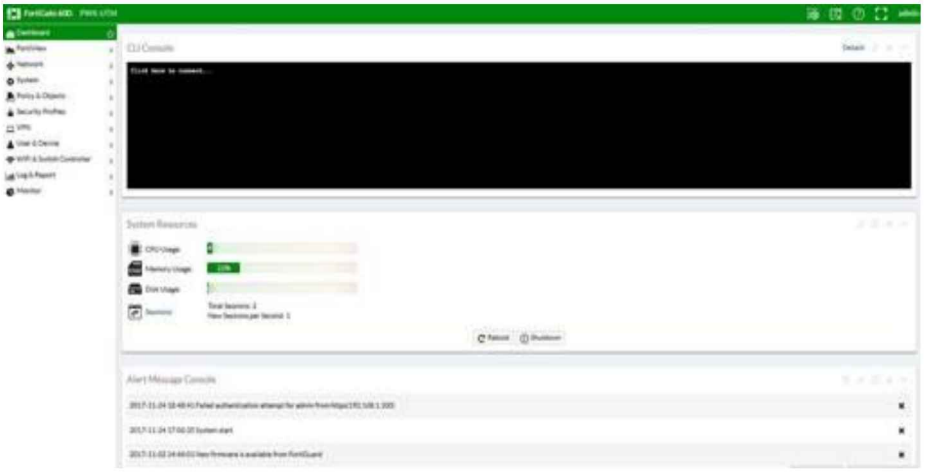
   System Time : Untuk mengatur waktu.



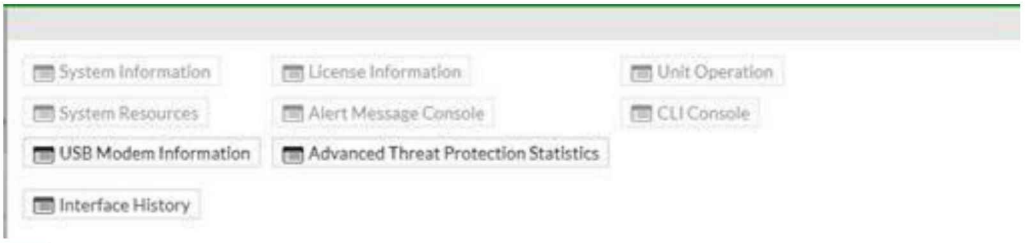
System Information

HA Status:	Standalone [Configure]
Host Name:	FG100D3G12812324 [Change]
Serial Number:	FG100D3G12812324
Operation Mode:	NAT
Inspection Mode:	Proxy-based [Change]
System Time:	Fri Jan 29 15:00:50 2016 (FortiGuard) [Change]
Firmware Version:	v5.4.0,build1011 (GA) [Update]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password] /2 in Total [Details]
Uptime:	13 day(s) 23 hour(s) 51 min(s)
Virtual Domain:	Disabled [Enable]

Gambar 4.2 Sistem Informasi

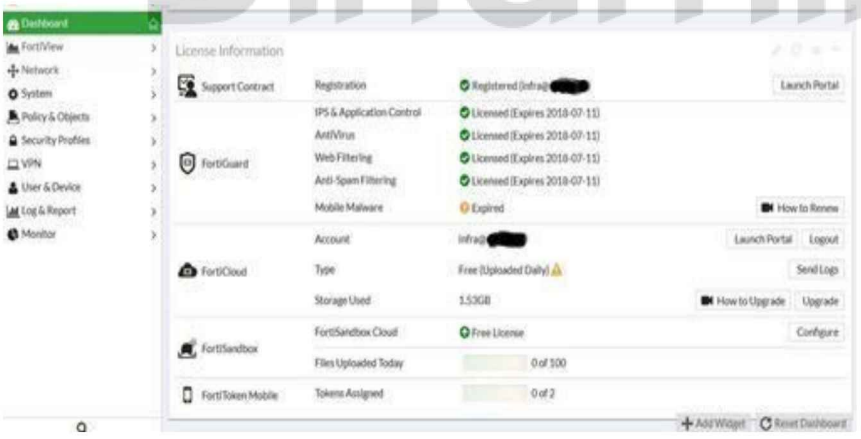


Gambar 4.3 CLI *Console*



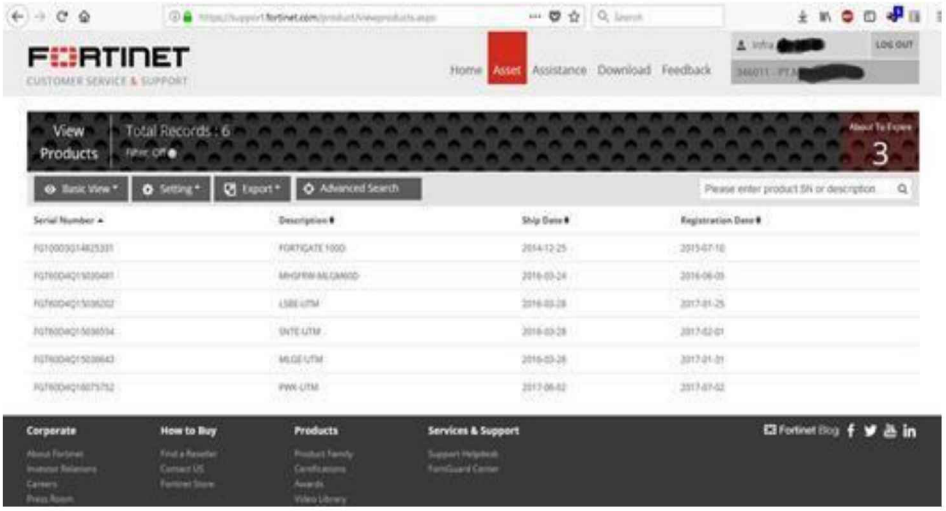
Gambar 4.4 Informasi Pada Dashboard

3. Terlihat juga informasi *License*, perlu di ketahui *license fortiget* berbayar pertahunnya dan harus diregistrasikan di *website fortunate*.



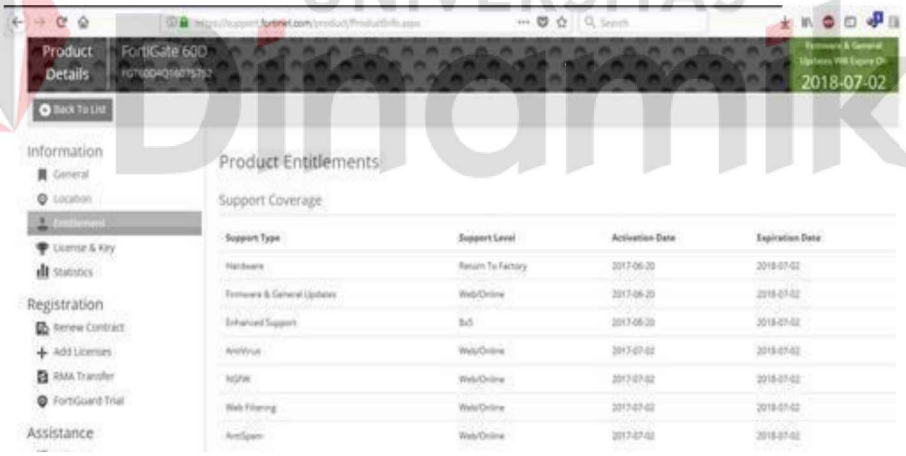
Gambar 4.5 Informasi Lisensi

4. Informasi fitur-fitur *device fortigate* yang telah diregistrasikan.



Gambar 4.6 fitur-fitur *Fortigate* yang sudah di regristasikan

5. Berikut ini fitur-fitur jika *fortigate* diregistrasikan, *AntiVirus, AntiSpam, Firmware,Web Filtering*, dll. semua itu akan diupdate secara otomatis keserver *fortigate*, kita juga akan terima sertifikat *license*nya.

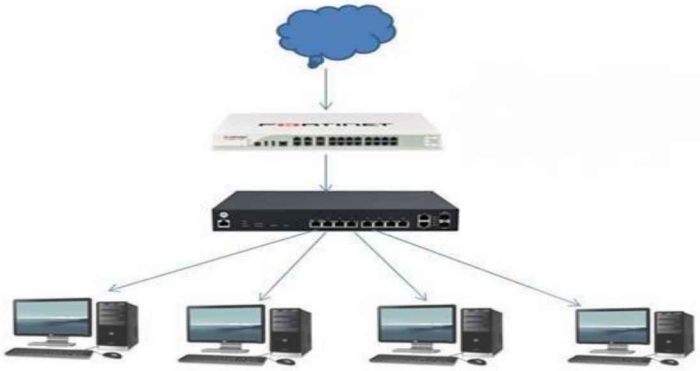


Gambar 4.7 Fitur-Fitur *Fortigate* Yang sudah terregristasi

Konfigurasi Dasar *Fortigate*

Create New User Login

1. Pada konfigurasi dasar ini kita akan mengunakan topologi yang sederhana dimana dari ISP menuju port WAN 1 *Fortigate*, dan Port 2 *Fortigate* ke Switch, dari switch ke masing— masing pc

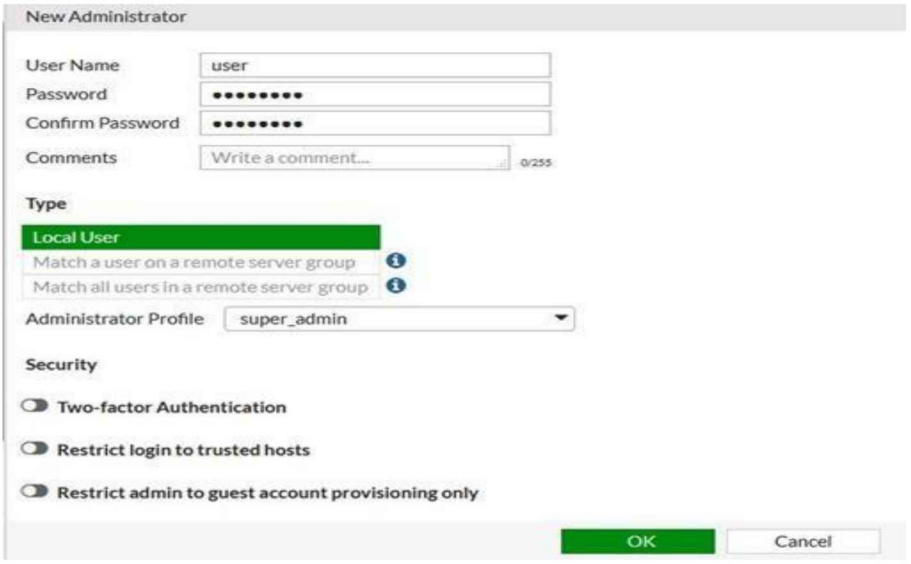


Gambar 4.8 Topologi Sederhana

2. Kita bisa menambahkan user administrator di menu ***System →Administrators →Create New***

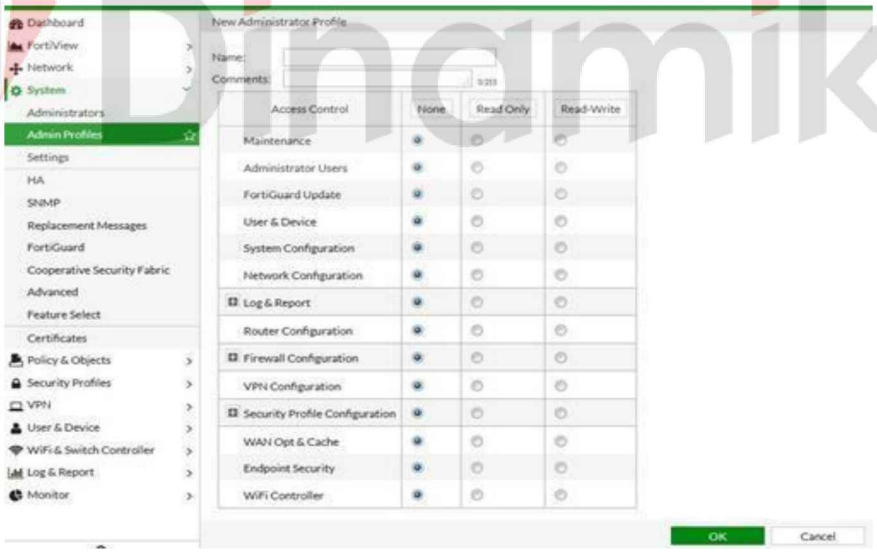
Gambar 4.9 Administrasi

3. *Adminstrator Profile* ***super_admin.***



Gambar 4.10 Membuat Administasi Baru

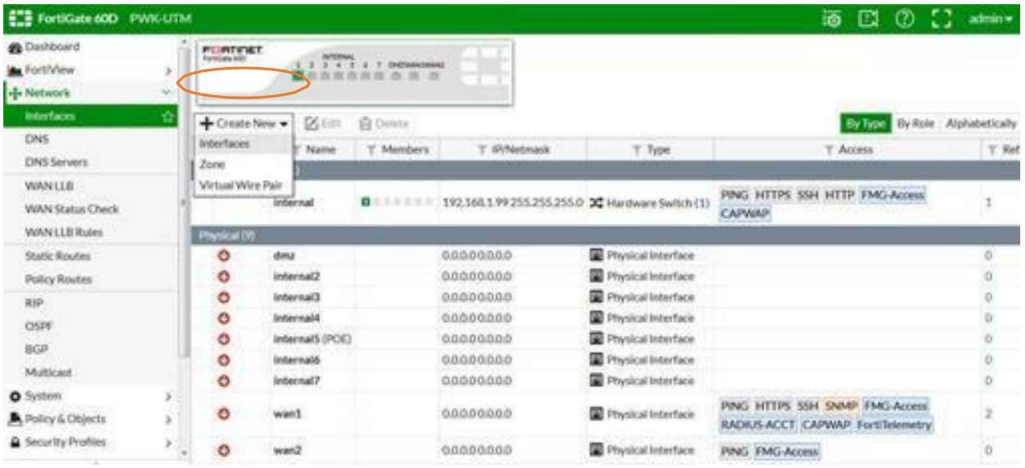
4. Kita juga dapat membuat akses untuk user biasa yang dibatasi permissionnya, kita buat dahulu *Admin Profile* di menu ***System → Admin Profile →Create New***



Gambar 4.11 New Admin Profil

Setting IP Address

1. Klik Menu *Network* →*Interfaces* →*Create New*



Gambar 4.12 Untuk Membuat Interface Baru

2. Isikan *Interface Name, Type, Physcal Interface Member, Role, Address, DHCP Server, Device Detection* (berfungsi untuk jika ada pc yang konek informasi tentang pc tersebut akan diketahui windownya, usernya, IP nya).

Address : isikan *ip address* lokal disini 10.10.XXX.XXX/24

Restrict Access : memberi ijin pada *network* 10.10.XXX.XXX agar bisa akses *fortigate* dengan cara *https, ping, ssh, snmp*

DHCP Server : jika enable akan memberikan ip ke *client* secara dhcp, jika disable maka *ip client* diset manual

Network Devices : — ***Devices Detection*** (akan mendeteksi perangkat apa saja yang terhubung kejaringan pc,laptop,iphone,android,tablet)

- ***Active Scanning*** (akan mengscan perangkat apa saja yang terhubung kejaringan pc,laptop,iphone,android,tablet)

jika sudah klik **OK**

Gambar 4.13 Gambar Hasil Dari Interface Baru

3. Selanjutnya kita edit port WAN 1

Klik **WAN 1 → Edit**

isikan

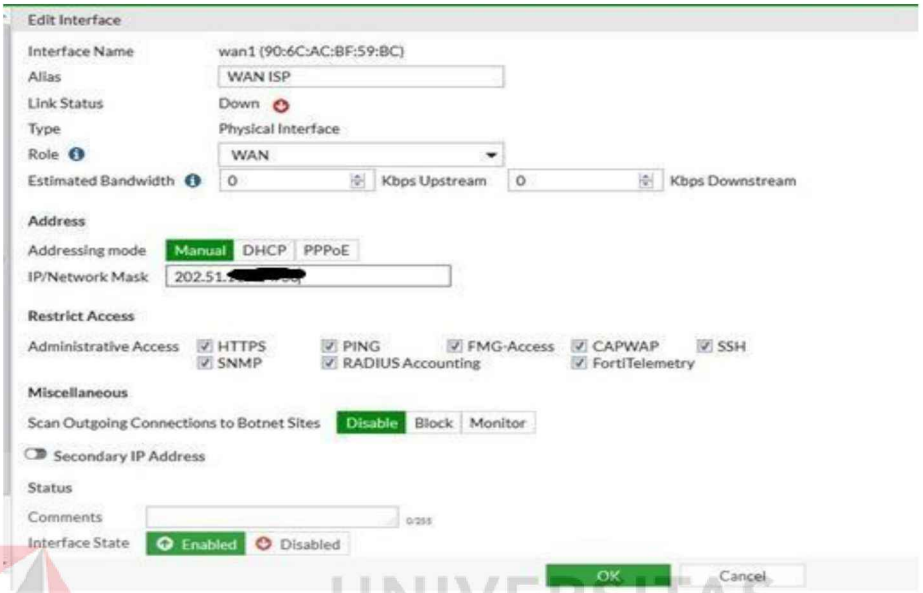
Alias : nama alias

Role : *WAN*

Address : *IP Public ISP*

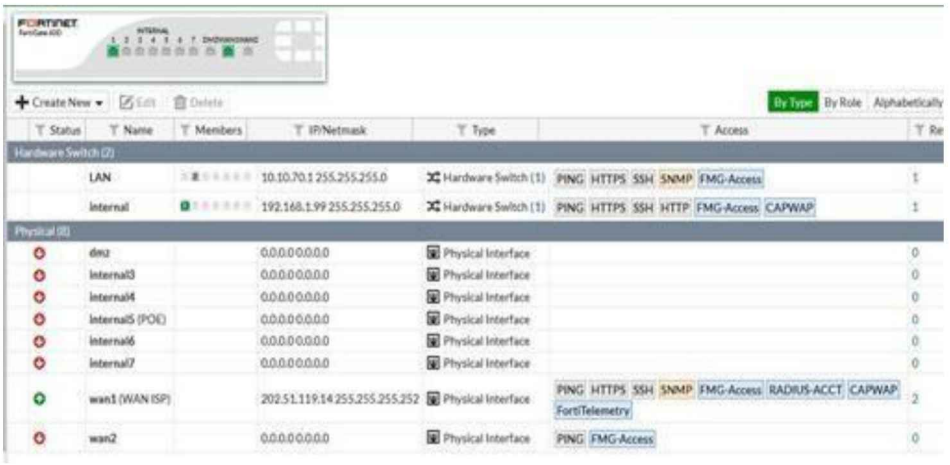
Restrict Access : memberi ijin pada network luar agar bisa akses *fortigate* dengan cara *https, ping, ssh, snmp*

Secondary IP Address : digunakan apabila mempunyai *IP Public* lain dari ISP yang sama atau dari ISP yang berbeda, jadi bisa diakses mengunakan 2 *IP Public* sesuai dengan WAN anda, jika sudah klik **OK**



Gambar 4.14 Membuat WAN Baru

4. Jika sudah maka di *interface* akan terlihat LAN 1 dan WAN 1 nyala warna hijau.



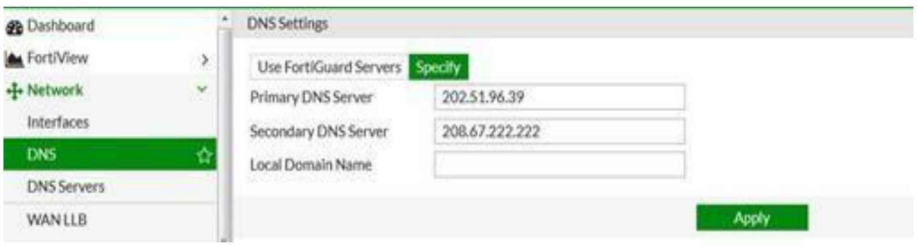
Gambar 4.15 Hasil Dari Interface Lan dan Wan

Setting DNS

1. Setting DNS dengan cara klik ***Network → DNS***, masukan DNS ISP dan dns open dns

   DNS pertama : milik ISP

   DNS kedua : milik opendns



Gambar 4.16 Setting DNS

2. *Setting Static Route*

Setting Static Routes dengan cara klik ***Network → Static Routes***

Device : WAN

Gateway : IP *gateway* milik ISP

Comments : *Route to* internet

jika suda klik OK

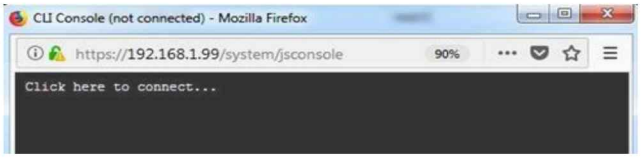
Gambar 4.17 Edit Static Route

3. Tes koneksi

sekarang kita tes koneksi denga CLI, klik kanan atas pada nama user login → klik ***CLI Console***

Gambar 4.18 Ip *Address* dari WAN 1

Setelah muncul pencet enter

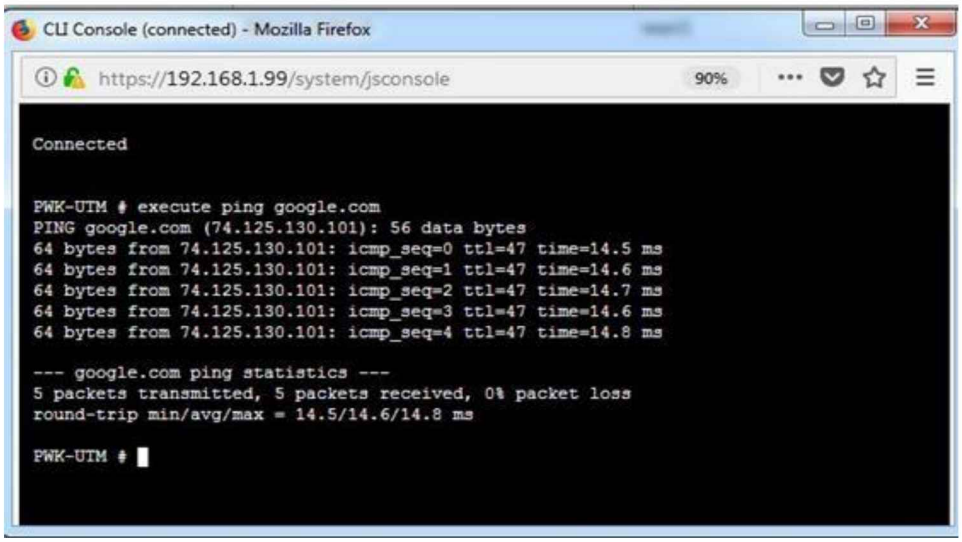


Gambar 4.19 Tes koneksi

jalankan *syntax* untuk ping

excute ping google.com

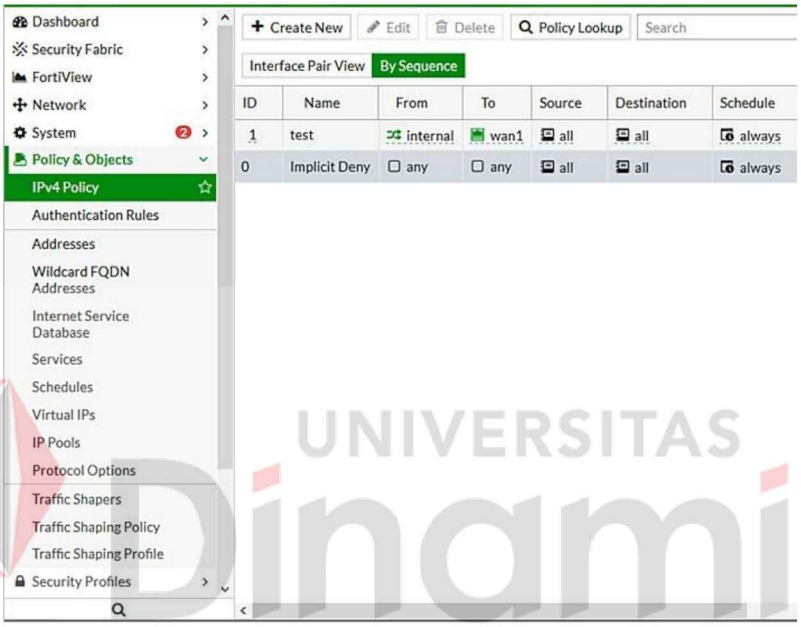
jika DNS dan route nya sudah benar akan tampil seperti ini



Gambar 4.20 Hasil Ping dari google.com

4. ***Setting Policy & Object*** (*S*ebuah alat bantu yang dapat digunakan untuk mengatur keamanan dan beberapa kebijakan lainnya) perlu diperhatikan settingan *Policy & Object* urutan yang akan dibaca dari atas kebawah, untuk menambahkannya

   klik ***Policy & Objects → IPv4 Policy → Create New***



Gambar 4.21 Menambahkan Ipv4 baru

5. Masukan

   Name : LAN to WAN

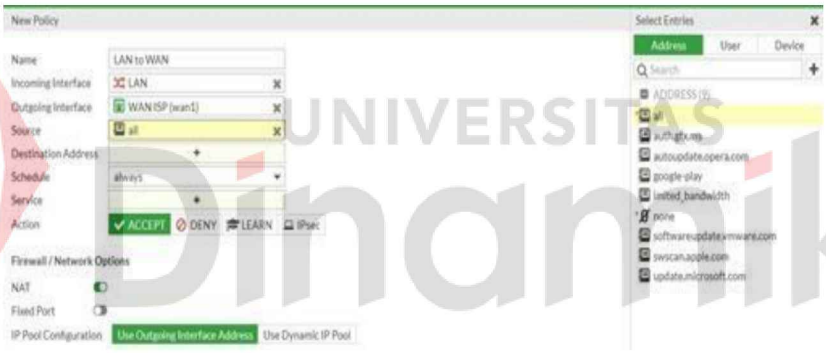
   Incoming Interface : LAN (yang telah kita buat sebelumnya)

Gambar 4.22 Incoming Interface (LAN)

6. ***Outgoing Interface*** *:* WAN ISP (yang telah kita buat sebelumnya)

Gambar 4.23 *Outgoing* interface (WAN1)

ource *: all*

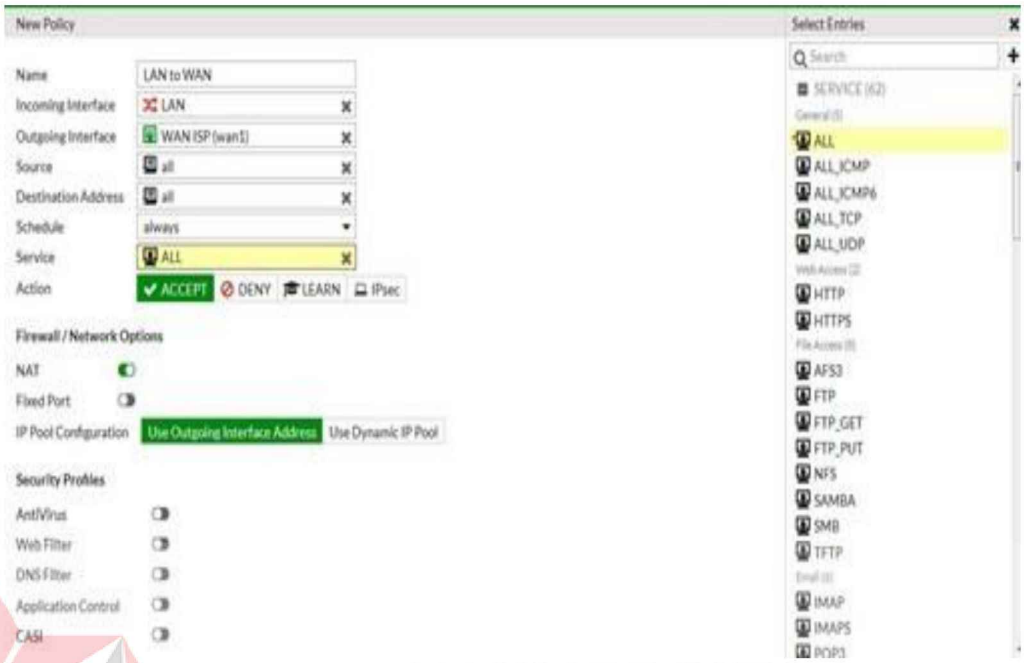


Gambar 4.24 Source

Destination Address *: all*

Gambar 4.25 Alamat Destinasi

7. ***Serivce*** : *ALL* (bisa disesuaikan jika hanya ingin mengijinkan *service http,https,ftp,ping,imap,pop3,smtp)*



Gambar 4.26 Servis

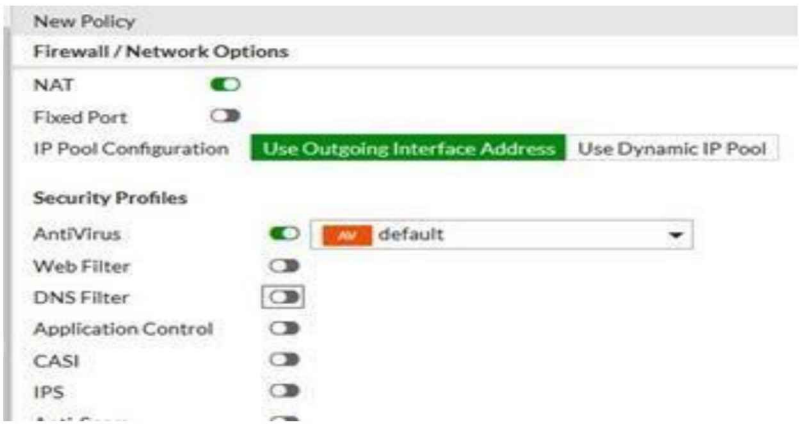
8. **NAT** : *enable*

Security Profiles : AntiVirus

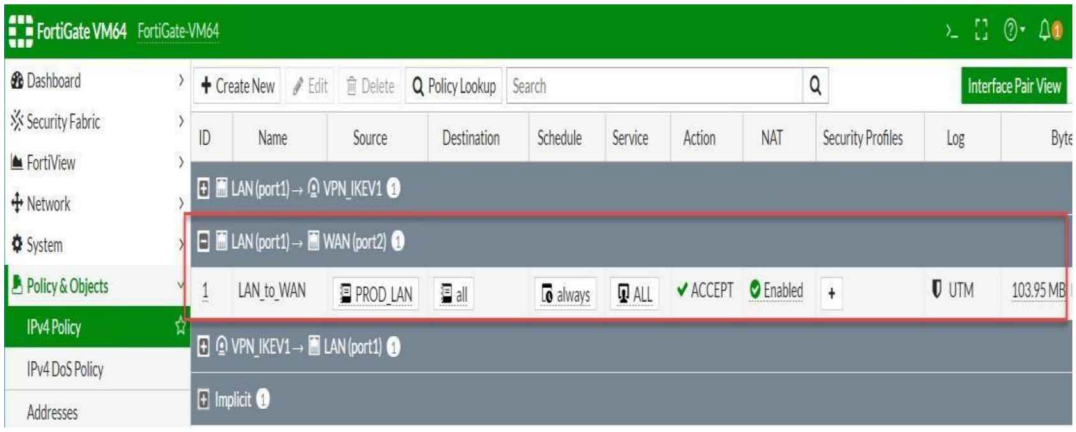
untuk *Security Profile* akan dibahas pada pembahasannya selanjutnya

Logging Options : *All Sessions*

jika sudah klik **OK**



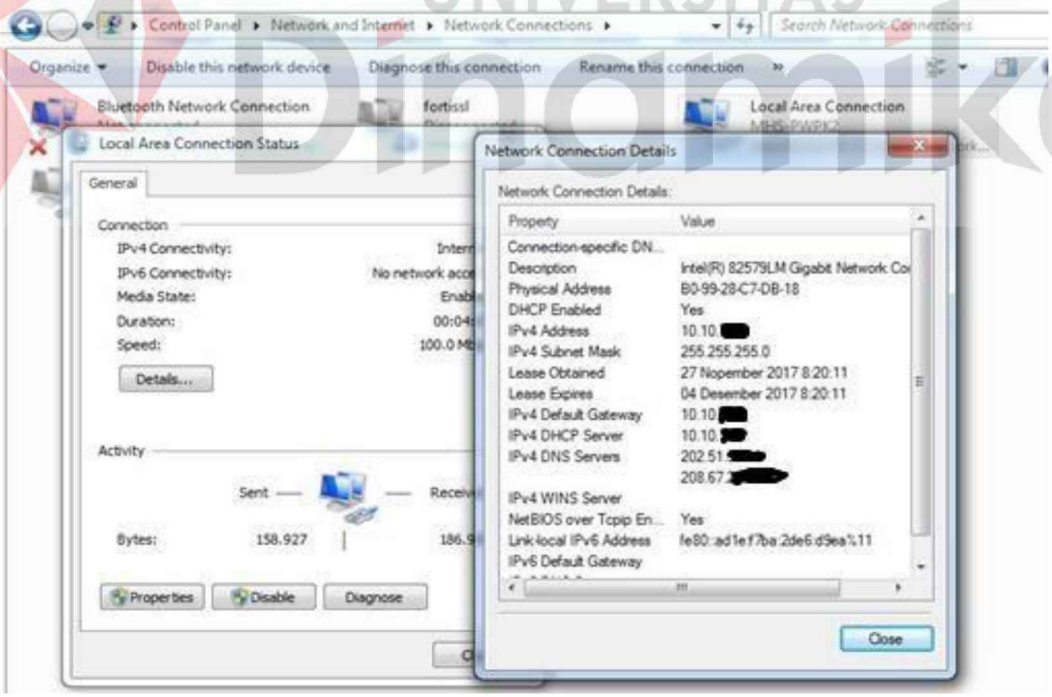
Gambar 4.27 Form untuk mengaktivkan antivirus



Gambar 4.28 Lan dan Wan sudah terhubung

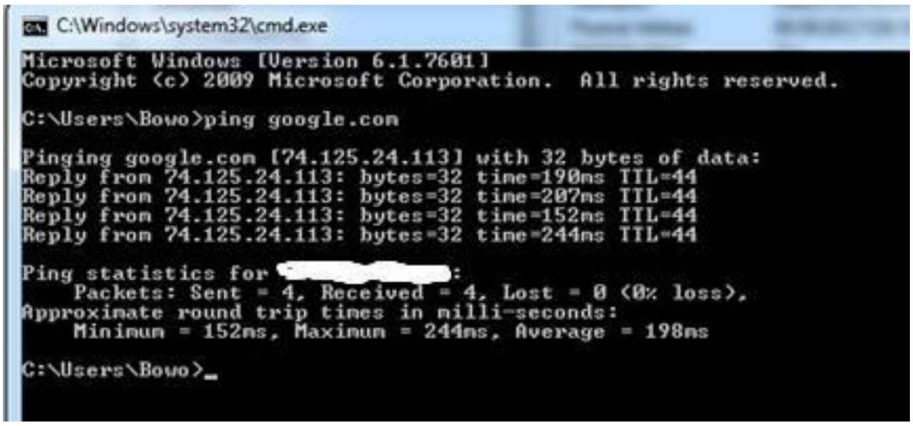
Sekarang kita lihat hasilnya, colok kan kabel Lan ke Port 2 *Fortigate* ke PC/Laptop

IP *Address* sudah mendapatkan DHCP 10.10.XXX.XXX/24



Gambar 4.29 Cek Ip di Pc

sekarang kita coba ping ke google.com, kemudian coba *browsing* beberapa situs



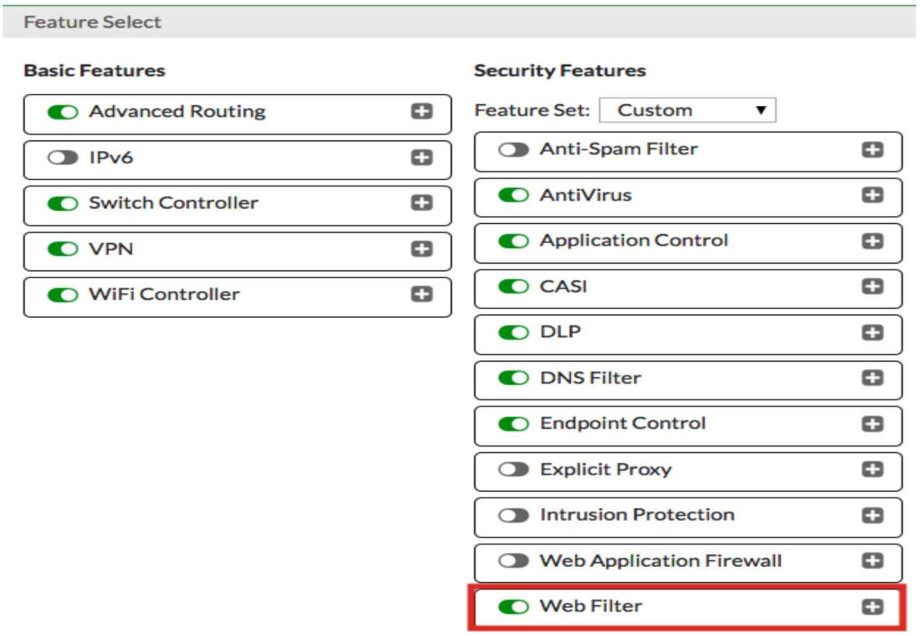
Gambar 4.30 Ping google.com

jika sudah bisa browsing pada tahap ini *fortigate* sudah bisa digunakan

Block Facebook* lewat *FortiGate

1. *Enable Web Filtering*

Pergi ke *System*> *Feature Select* untuk mengaktifkan fitur ***Web Filter***.



Gambar 4.31 Feature Select

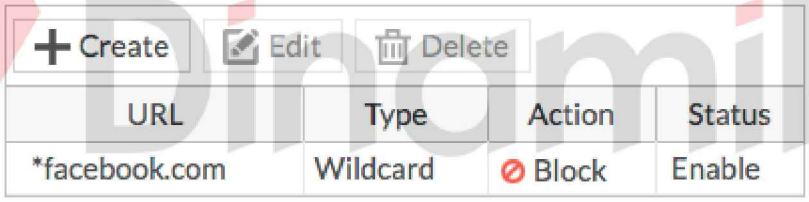
2. Mengedit profil *Filter Web default*

Buka ***Security Profiles*** > ***Web Filter*** dan edit profil Web Filter default.

Untuk memblokir Facebook, buka ***Static URL filter***, pilih ***URL Filter***, lalu klik ***Create***

Gambar 4.32 Static URL Filter

Setel ***URL*** ke * facebook.com. Setel ***Type*** ke ***Wildcard***, atur ***Action*** untuk **Diblokir**, dan atur **Status** ke *Enable*



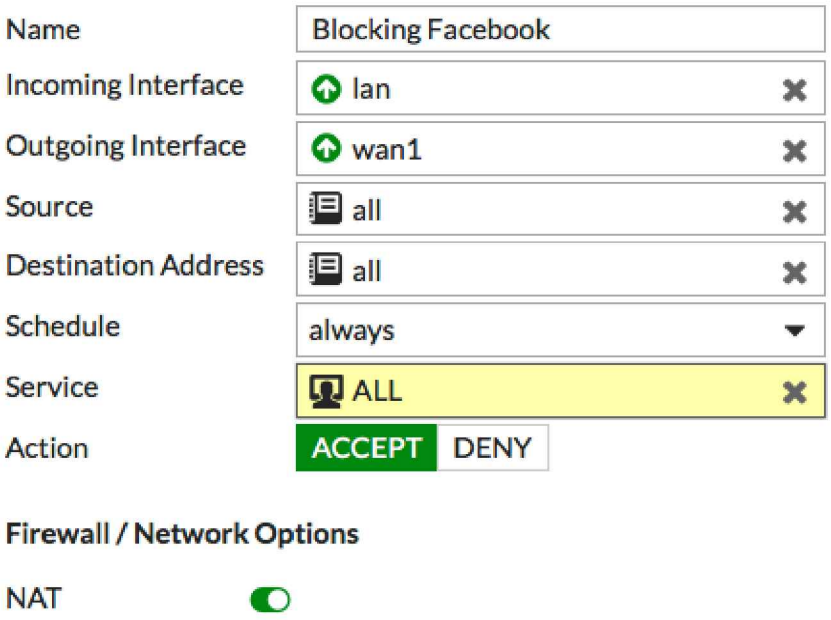
Gambar 4.33 Url yang telah diblokir

3. Creating Web filtering *security policy*

Pergi Ke ***Policy & Objects*** > ***IPv4 Policy***, dan klik ***Create New*** Beri nama *policy* yang mengidentifikasi pengguna.

Atur ***Incoming Interface*** ke jaringan internal dan atur ***Outgoing Interface*** ke antarmuka yang menghadap Internet.

Enable **NAT**.



Gambar 4.34 Web filtering *security policy*

Di bawah ***Security Profiles*** Aktifkan ***Web Filter*** dan pilih ***Default*** *Web Filter Profile*

Gambar 4.35 *Security Profile*

Enable ***certificate-inspection*** dari menu *dropdown*. Ini memungkinkan ***FortiGate*** untuk memeriksa dan menerapkan ***Web Filter*** ke *HTTPS traffic*

Gambar 4.36 penerapan web filter ke https

Kebijakan baru harus menjadi yang pertama dalam daftar untuk diterapkan pada *Internet traffic*. Konfirmasikan ini dengan melihat kebijakan

Konfirmasikan ini dengan melihat kebijakan.

Gambar 4.37 halaman untuk memblokir situs

4. Hasil dari Pemblokiran Facebook

Visit facebook.com

HTTPS secara otomatis diterapkan ke facebook.com, meskipun tidak dimasukkan di bilah alamat. muncul mesan (Halaman *Web FortiGuard Diblokir!*)

Gambar 4.38 hasil Pemblokiran facebook.com

Kunjungi subdomain Facebook, misalnya, attachments.facebook.com.

Halaman *Web FortiGuard* Diblokir! Muncul pesan, memblokir *subdomain*.

Gambar 4.39 hasil Pemblokiran attachments.facebook.com.

BAB V

KESIMPULAN

Firewall merupakan hal yang tak boleh dilewatkan sebelum mengakses internet, elemen ini memastikan anda dapat berselancar di internet tanpa khawatir terpapar virus atau mengalami pencurian data, oleh karena itu diperusahaan ini dibutuhkan device yang bernama fortigate untuk bisa mengkonfigurasi firewall agar data dan mengakses internet bisa aman.

DAFTAR PUSTAKA

Indra, W. (2012, 12 14). *Pengenalan Mikrotik*. Diambil kembali dari ilmukomputer.org: https://ilmukomputer.org/author/indra-wicaksono/

Paul, G. (14. Maret 2013). *Manual:Firs t time startup*. Noudettu osoitteesta http//wiki.mikrotik.com: https://wiki.mikrotik.com/wiki/Manual:Firs_t_time_startup

Setio, D. (2003). Bandwidth and throughput. *Artikel Populer IlmuKomputer.Com* .