BAB IV

ANALISIS DAN PERANCANGAN

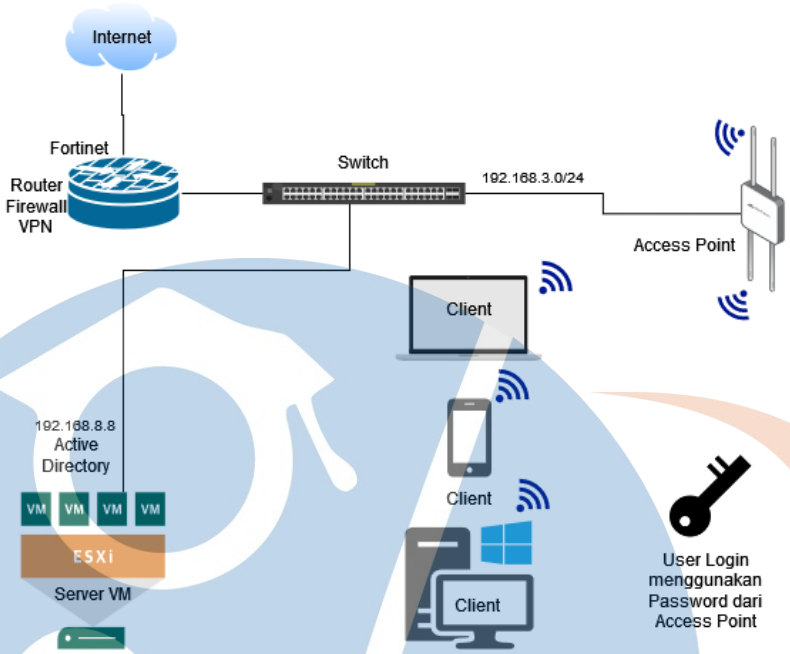
Pada bab ini berisikan langkah-langkah untuk mendapatkan informasi dari sistem yang akan diterapkan berdasarkan hasil pengumpulan data yang dibutuhkan melalui observasi sistem yang telah digunakan sebelumnya. Informasi dan data yang didapatkan akan di analisis dan digunakan untuk mempermudah mengidentifikasi suatu permasalahan sistem yang sebelumnya sudah diterapkan serta kebutuhan sistem yang diharapkan dapat membantu proses implementasi.

4.1 Analisis Sistem Yang Sedang Berjalan

Pada tahapan ini proses yang dilakukan adalah observasi terhadap lingkungan jaringan *wireless* pada PT.XYZ yang dimana untuk mendapatkan permasalahan yang sedang dialami pada keamanan jaringan *wireless* serta untuk mendapatkan jawaban atas solusi yang akan diterapka untuk menjawab permasalahan tersebut.

Oleh karena itu observasi ini telah dilakukan peneliti dan menghasilkan beberapa acuan dasar pengetahuan seperti alur dari sistem jaringan *wireless* yang sedang berjalan serta proses keamanan jaringan *wireless* yang saat ini digunakan PT.XYZ untuk bisa menjadi bahan yang dibutuhkan guna penelitian ini. Terdapat beberapa hasil dari kegiatan observasi, diantaranya:

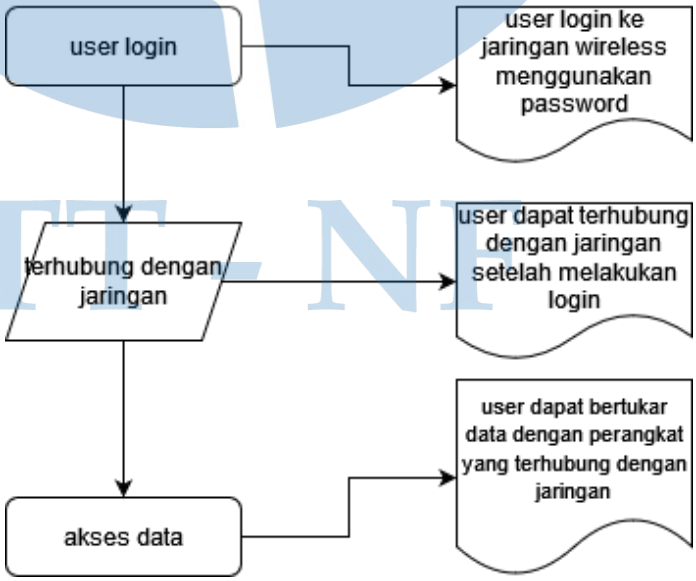
1. Topologi dari sistem jaringan *wireless* yang sedang berjalan pada PT.XYZ saat ini adalah sebagai berikut:



Gambar 4.1 Topologi jaringan sebelumnya

Pada gambar 4.1 merupakan topologi dari jaringan pada PT.XYZ yang saat ini sedang berjalan dan dipergunakan.

2. Proses keamanan jaringan *wireless* yang saat ini digunakan PT.XYZ



Gambar 4.2 keamanan jaringan yang sedang berjalan

Pada gambar 4.2 merupakan alur dari prosedur keamanan pada jaringan *wireless* PT.XYZ yang saat ini digunakan, yang mana masih menggunakan keamanan WPA yang hanya membutuhkan *password* untuk dapat masuk ke jaringan *wireless*. Pada jaringan *wireless* yang sedang berjalan belum menggunakan mekanisme yang terpusat sehingga penulis dalam penelitian ini akan menerapkan keamanan pada jaringan *wireless* PT.XYZ dengan mekanisme yang terpusat.

4.2 Analisis Kebutuhan Sistem

Pada tahapan ini akan dijelaskan mengenai analisis kebutuhan terhadap perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian ini. Adapun Spesifikasi perangkat keras yang akan digunakan oleh penulis dalam penelitian ini adalah sebagai berikut:

Table 4.1 Spesifikasi perangkat keras

Nama Perangkat	Fungsi	Spesifikasi	Jumlah
Server Dell PowerEdge R250	Sebagai Server VM yang digunakan untuk Server Windows Active Directory	• Intel Xeon E-2300 (8 core) • 128GB Memory • 4TB Hard Drive SAS	1
Fortinet tipe FortiGate 81E	Berfungsi sebagai router dan firewall yang sudah berjalan sebelumnya. Penulis menambahkan fungsi sebagai Autentikator pada jaringan wireless	• GE RJ45/SFP Shared Media Pairs 2 ports • GE RJ45 PoE/+ Ports 12 ports • GE RJ45 DMZ/HA Ports 2 ports • USB Ports 1 ports • Console (RJ45) 1 ports • Internal Storage 1x 128 GB SSD	1
Access Point TP-LINK TR-MR3420	Digunakan sebagai penyedia SSID pada jaringan wireless	• Interface: 1 USB 2.0 Port for LTE/HSPA+/HSUPA/HSDPA/UMTS/EVDO USB Modem 1 10/100Mbps WAN Port, 4 10/100Mbps LAN Ports, support the auto-Negotiation and auto-MDI/MDIX • Wireless Standards IEEE 802.11b, IEEE 802.11g, IEEE 802.11n	1

		• Wireless Security Support 64/128 bit WEP, WPA-PSK/WPA2-PSK, Wireless MAC Filtering	

Sedangkan Kebutuhan perangkat lunak (software) yang dibutuhkan dalam melakukan proses intruksi atau menjalankan perangkat keras untuk mendukung implementasi penerapan autentikasi terpusat ini antara lain:

Table 4.2 Spesifikasi perangkat lunak

Nama Perangkat Lunak	Fungsi	Versi
Windows Active Directory	Berfungsi sebagai tempat untuk menyimpan akun dari user yang akan digunakan untuk login ke jaringan	2016
FortiOS	Berfungsi sebagai penyedia portal layanan Autentikasi menggunakan fitur Captive Portal	7.0.0

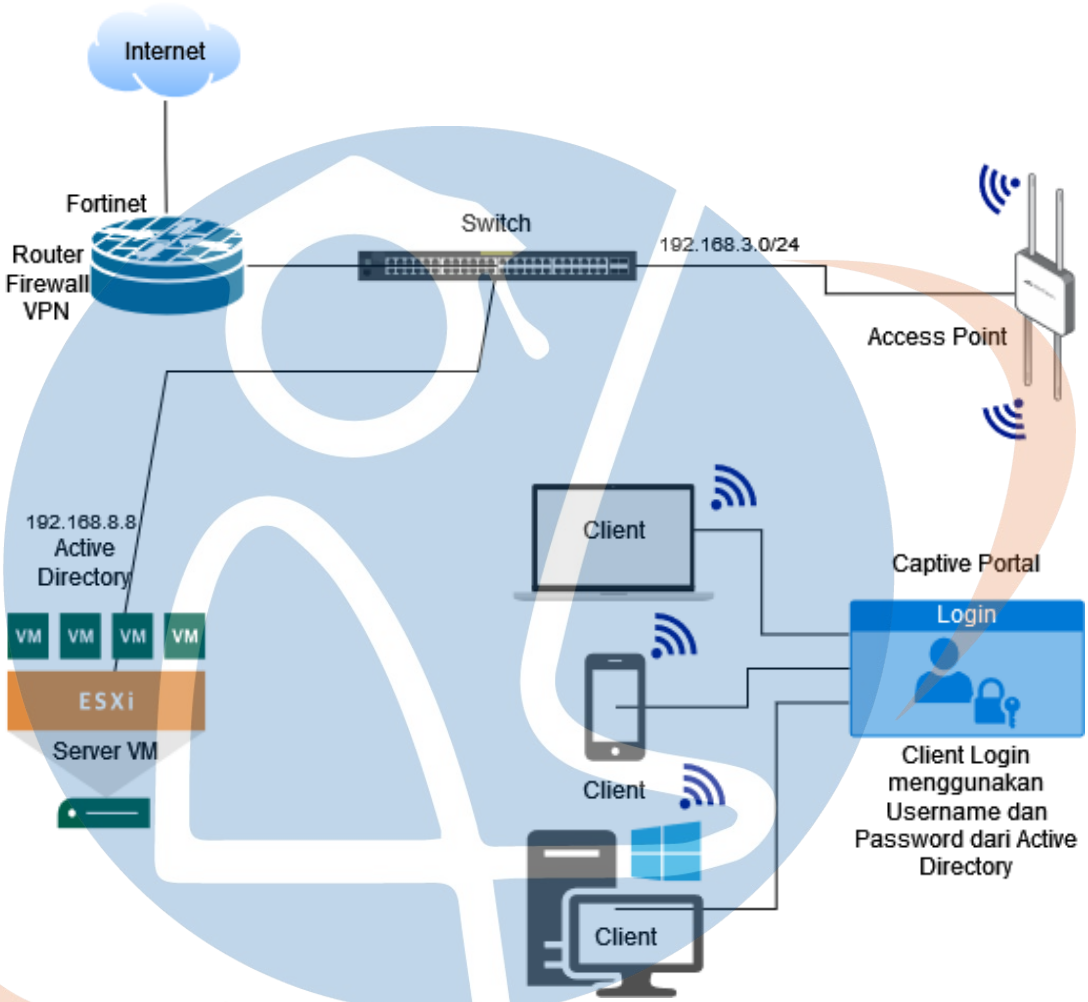
4.3 Perancangan Sistem

Pada perancangan sistem ini akan dijelaskan mengenai rancangan jaringan usulan serta rancangan arsitektur sistem yang digunakan peneliti dalam mengimplementasikan Penerapan Autentikasi Terpusat Untuk Keamanan Jaringan *Wireless* Menggunakan Perangkat Fortinet Terintegrasi Dengan Windows *Active Directory*.

4.3.1 Rancangan Sistem Jaringan Usulan

Pada perancangan arsitektur sistem jaringan usulan ini akan menjelaskan bagaimana rancangan dari Autentikasi terpusat menggunakan Fortinet terintegrasi dengan windows *active directory* untuk keamanan jaringan *wireless*. Dalam penelitian ini penulis menggunakan Arsitektur sistem yang sama dengan sebelumnya, hal ini dikarenakan topologi yang ada sekarang sudah sangat baik dan dari pihak perusahaan PT.XYZ tidak memberikan izin untuk merubah dari sisi Arsitektur sistem yang sedang berjalan, penulis hanya menambahkan rancangan Autentikasi Terpusat pada jaringan *wireless*, yang dimana memanfaatkan fitur dari Fortinet yaitu *Captive Portal* sebagai

portal untuk login ke jaringan *wireless* dengan meng integrasikannya dengan *Active Directory* sebagai wadah dari *Account* client.



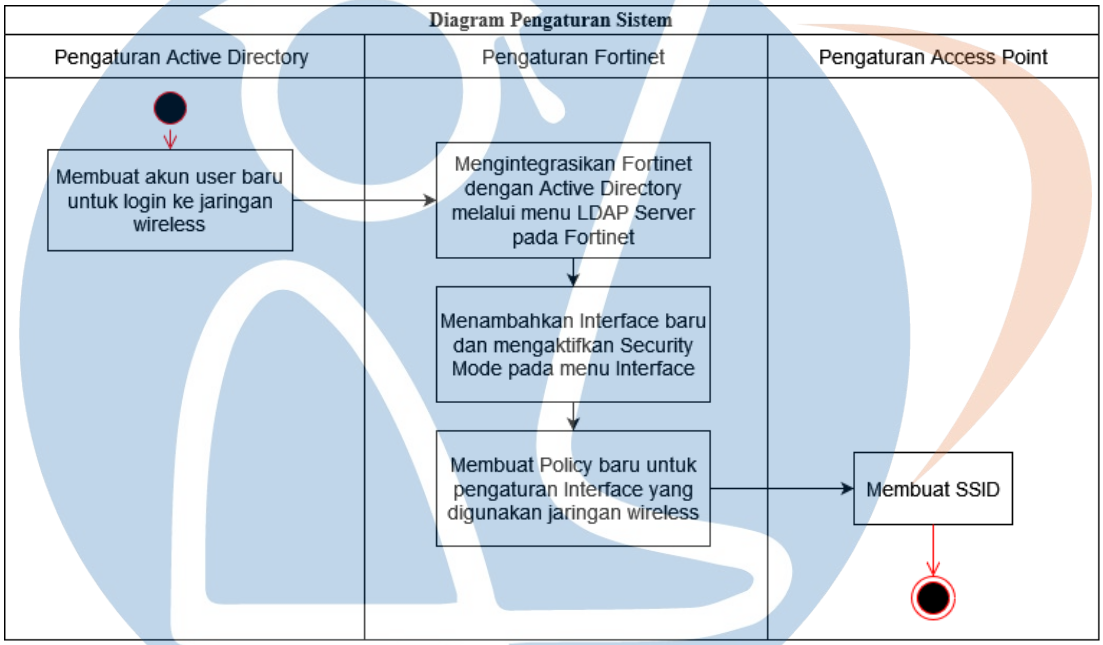
Gambar 4.3 arsitektur sistem fisik

Pada gambar diatas tentang rancangan system jaringan usulan dijelaskan bahwa:

1. *User* melakukan koneksi ke jaringan melalui SSID dari *Access poit*.
2. Fortinet akan megirimkan webpage portal login kepada *user* untuk memasukan *username* dan *password*.
3. Fortinet akan meneruskan akun *user* ke *active directory* untuk di verifikasi.

4. *Active directory* akan mengecek apakah akun tersebut telah terdaftar di database atau belum, Jika akun terdaftar maka Fortinet akan memberikan akses kepada *user* untuk bisa masuk kedalam jaringan lokal dan internet.

Selanjutnya akan menjelasakan bagaimana rancangan dari tahapan yang akan diterapkan pada *Active Directory* dan perangkat Fortinet. Adapun kegiatan yang ada divisualisasikan ke dalam diagram dibawah ini.



Gambar 4.4 Diagram pengaturan sistem

Pada rancangan system jaringan usulan ini penulis menggambarkan rancangan pengaturan system pada gambar diagram pengaturan system diatas yang diantaranya adalah sebagai berikut.

1. Membuat Akun User Baru pada Active Directory

   Untuk login ke jaringan *wireless* memerlukan *Username* dan *Password* dari *Active Directory*, oleh karena itu penulis menambahkan 10 akun baru pada *Active Directory* yang akan digunakan sebagai akun untuk mengakses jaringan *wireless*
2. Pengaturan LDAP Server pada Fortinet

Untuk meng integrasikan Fortinet dengan *Active Directori*, penulis menggunakan fitur LDAP Server pada Fortinet, dan membuat *user* grup dari akun *user* yang sudah di buat pada *Active Directory*.

3. Membuat Interfaces Baru pada Fortinet

   Setelah membuat gruping tahapan yang selanjutnya adalah pembuatan interfaces baru untuk memberikan IP Address terhadap *user wireless* dan menggunakan fitur Captive Portal sebagai Autentikator.

4. Menbuat *Policy*

   Untuk selanjutnya pembuatan policy pada Fortinet, penulis membuat 3 policy untuk mengakses jaringan LAN, Internet dan mengakses Server. Policy yang dibuat merupakan jembatan penghubung bagi *user* supaya dapat terkoneksi dengan jaringan lokal, mengakses internet dan juga dapat mengakses Server.

5. Membuat SSID

   Tahapan berikutnya yaitu membuat SSID pada Access Point tanpa mengaktifkan fitur keamanan apapun, hanya menjadikannya sebagai SSID saja.

4.3.2 Rancangan Pengujian Efektifitas

Pada rancangan pengujian ini peneliti melakukan pengujian terhadap Efektifitas dari Autentikasi Terpusat untuk keamanan jaringan *wireless* menggunakan perangkat Fortinet terintegrasi dengan Windows *Active Directory*. Dalam rancangan pengujian efektifitas ini akan dilakukan serangkayan percobaan Autentikasi dengan cara melakukan prosedur sebagai berikut:

1. Melakukan Autentikasi menggunakan perangkat Laptop dan Handphone untuk tersambung ke jaringan *wireless* yang sudah di konfigurasi dengan memasukan *user* name dan password dari *Active Directory*. Melihat hasil Autentikasi apakah berhasil atau tidak.
2. Dilakukan beberapa kali uji coba sebanyak 10 kali menggunakan variasi *user* yang berbeda dan menggunakan variasi perangkat yang berbeda. Berikut form pengujian berdasarkan variasi 10 *user* menggunakan perangkan Laptop:

Table 4.3 Pengujian Efektifitad dengan variasi user

Nama User	Autentikasi		Keterangan
	Gagal	Sukses	
USR1		✓	Berhasil terkoneksi ke jaringan
USR2			
USR3			
USR4			
USR5			
USR6			
USR7			
USR8			
USR9			
USR10			

Setelah dilakukan uji coba menggunakan variasi *user*, selanjutnya akan dilakukan uji coba menggunakan variasi perangkat menggunakan 10 perangkat yang berbeda yang terdiri dari 5 perangkat laptop dan 5 perangkat Smart Phone menggunakan akun *user* USR1. Berikut ini tabel pengujian Autentikasi berdasarkan variasi perangkat:

Table 4.4 Pengujian Efektifitas dengan variasi perangkat

Perangkat		Hasil Autentikasi		Keterangan
Jenis Perangkat	Sistem Operasi	Gagal	Sukses	
Laptop	Windows 10		✓	Berhasil terkoneksi ke jaringan
Laptop	Windows 10			
Laptop	Windows 11			
Laptop	Ubuntu 20			
Laptop	Ubuntu 20			
Handphone	Android			
Handphone	Android			
Handphone	IOS			
Handphone	IOS			
Handphone	IOS			