

BAB V

IMPLEMENTASI DAN PENGUJIAN

Pada bab ini merupakan tahapan pengaturan dari system yang sudah dianalisa dan dirancang pada bab sebelumnya, dan juga pada bab ini akan dilakukan pengujian terhadap system yang sudah dirancang.

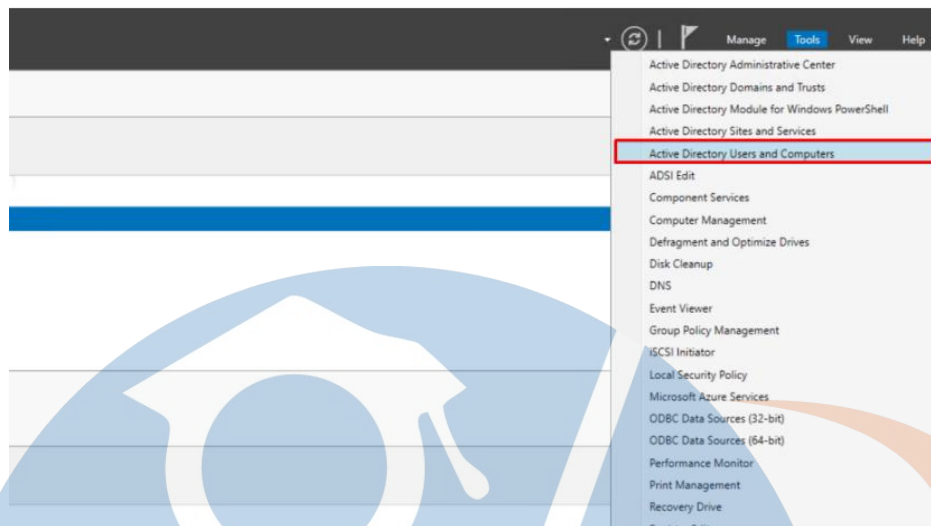
5.1 Implementasi sistem

Tahapan Implementasi sistem merupakan tahap penerjemahan perancangan berdasarkan hasil analisis serta penerapan kebutuhan pada keadaan yang sebenarnya.

5.1.1 Membuat Akun User Baru pada Active Directory

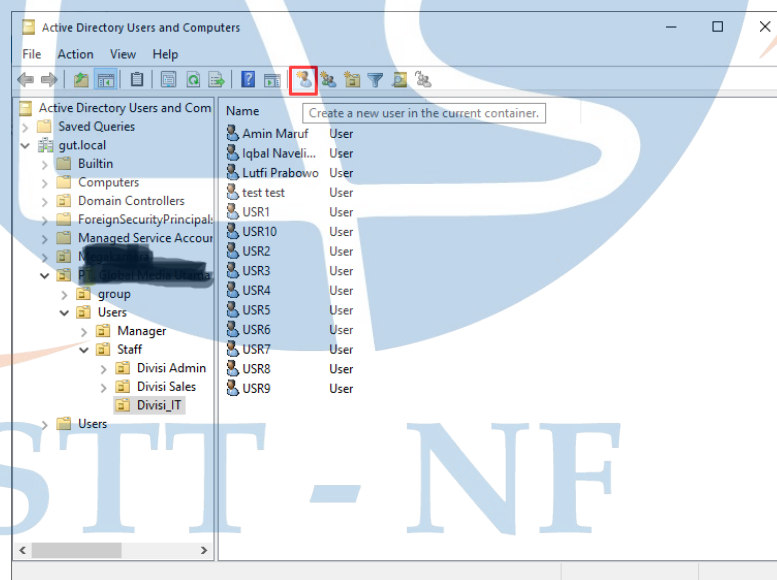
Active Directory yang berfungsi sebagai tempat untuk menyimpan akun dari pengguna merupakan perangkat dan sistem yang sudah ada sebelumnya dan dipergunkana oleh PT.XYZ, penulis pada penelitian ini akan memanfaatkan *Active Directory* untuk menyimpan Akun pengguna yang digunakan untuk autentikasi. Penulis menambahkan 10 akun pengguna baru untuk pengujian efektifitas. Tahapan pertama untuk membuat akun pengguna baru yaitu masuk ke Server *Active Directory*, Setelah penulis berhasil masuk kedalam Server *Active Directory* selanjutnya penulis masuk ke menu ***Server Manager***, kemudian pada bagian menu *Tools* pilih ***Active Directory Users and Computers***.

STT - NF



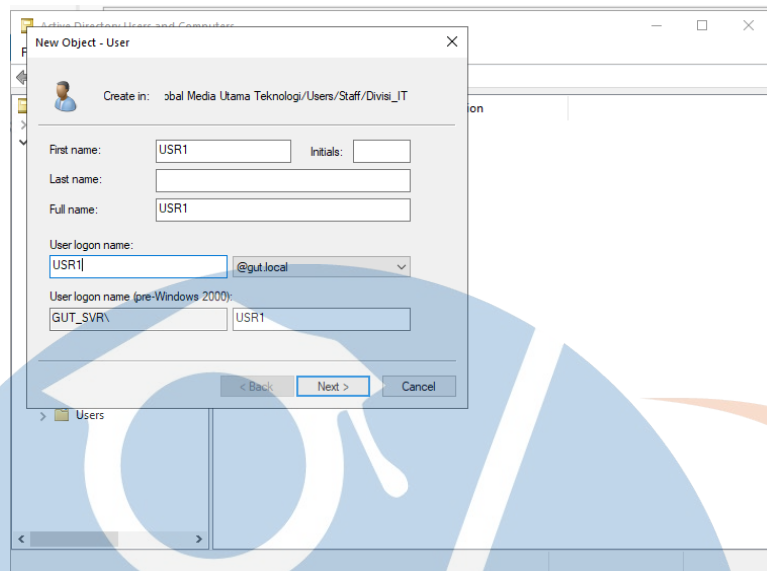
Gambar 5.1 Server Manager

Untuk tahapan selanjutnya setelah masuk di menu *Active Directory Users and Computers* selanjutnya penulis masuk ke menu *Organization Unit* dan grup yang akan ditambahkan Akun pengguna nya.



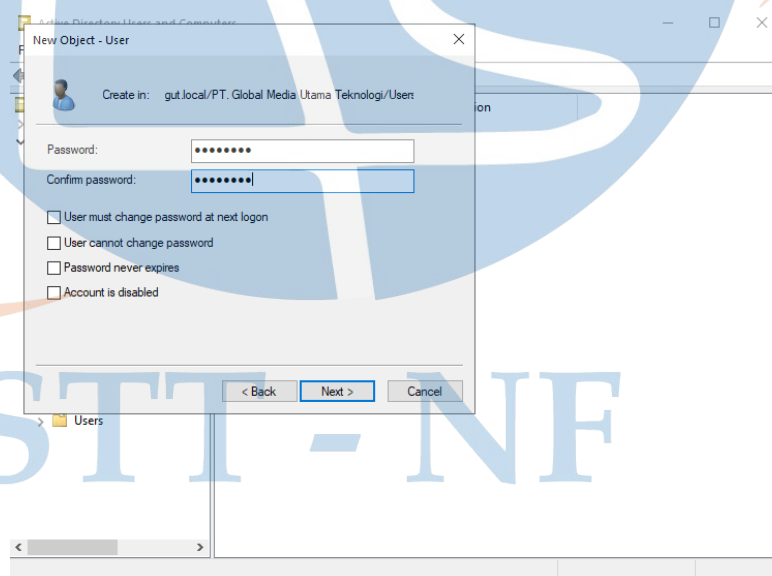
Gambar 5.2 Active Directory Users and Computers

Pada halaman *Active Directory Users and Computers* penulis menambahkan Akun *user* baru dengan cara menekan ikon *Tambah User* baru (*Create a new user in the current container*) pada grup **Divisi_IT**.



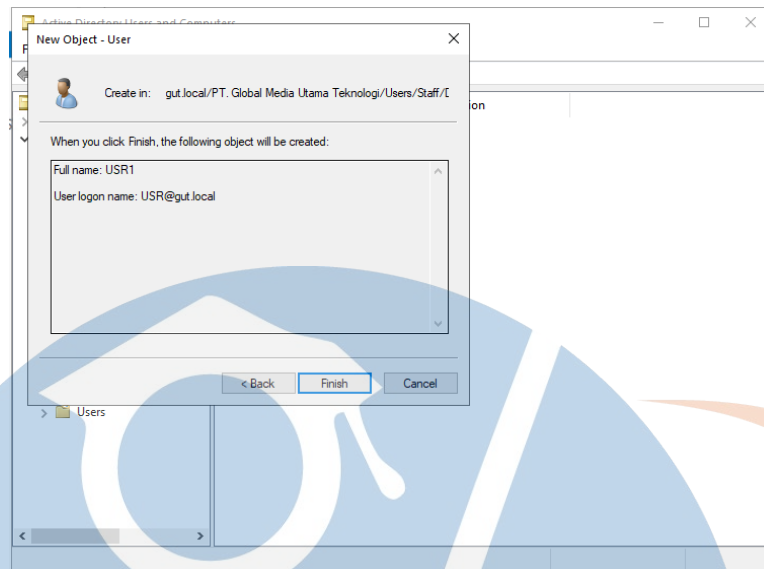
Gambar 5.3 penambahan user baru

Pada gambar di atas setelah halaman *New Object* muncul, pada halaman ini penulis menambahkan identitas dari akun pengguna dan Nama pengguna untuk *Login*, kemudian menekan *Next* untuk melanjutkan ke halaman berikutnya.



Gambar 5.4 password user baru

Pada halaman ini penulis menambahkan *Password* untuk akun pengguna baru tersebut, kemudian menekan *Next* untuk melanjutkan ke halaman berikutnya.



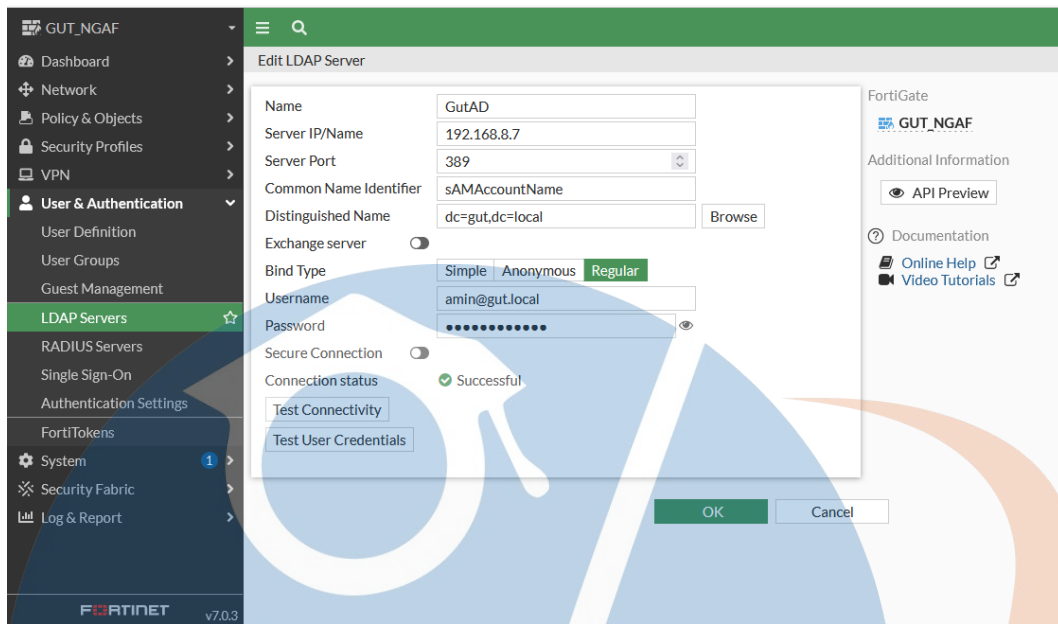
Gambar 5.5 berhasil menambahkan user baru

Pada halaman ini menampilkan bahwa Akun pengguna baru sudah berhasil di buat, kemudian menekan ***Finish*** untuk menyelesaikan pembuatan Akun pengguna baru ini.

5.1.2 Mengintegrasikan Fortinet dengan Active Directory

Untuk mengintegrasikan Fortinet dengan *Active directory* penulis menggunakan fitur **LDAP Server** pada Fortinet yang dimana pada fitur **LDAP Server** ini penulis melakukan pengaturan sebagai berikut.

STT - NF

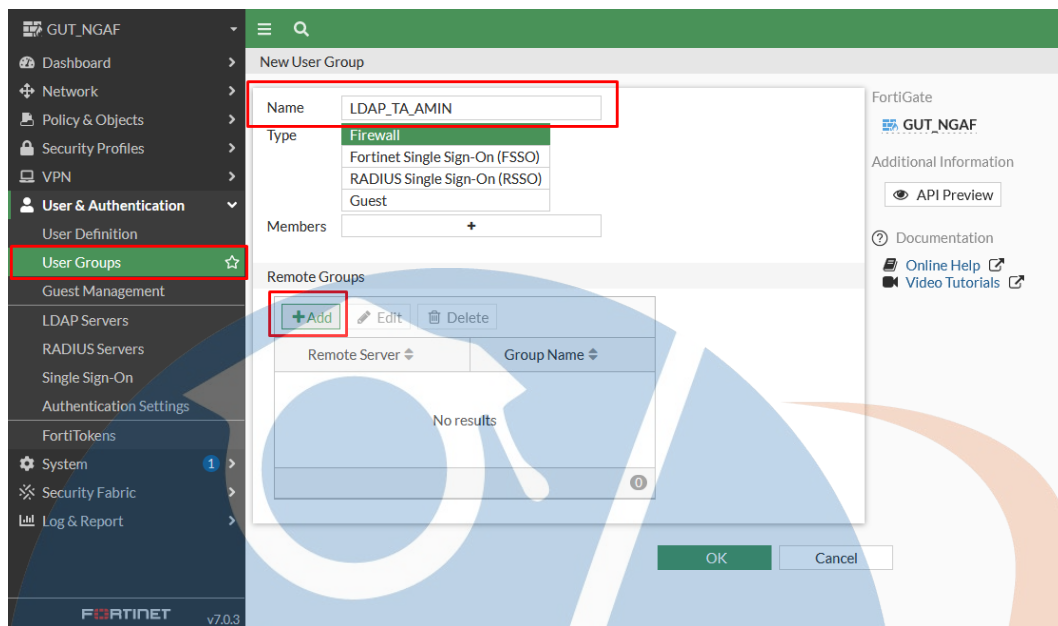


Gambar 5.6 pengaturan ldap server

Pada gambar pengaturan **LDAP Server** di atas, melalui menu **LDAP Server** yang terdapat pada menu **User & Authentication** penulis membuat koneksi baru dari Fortinet ke *Active Directory* yang dinamakan **GutAD** dengan alamat **IP 192.168.8.7** melalui **Port 389** menggunakan akun pengguna amin@gut.local

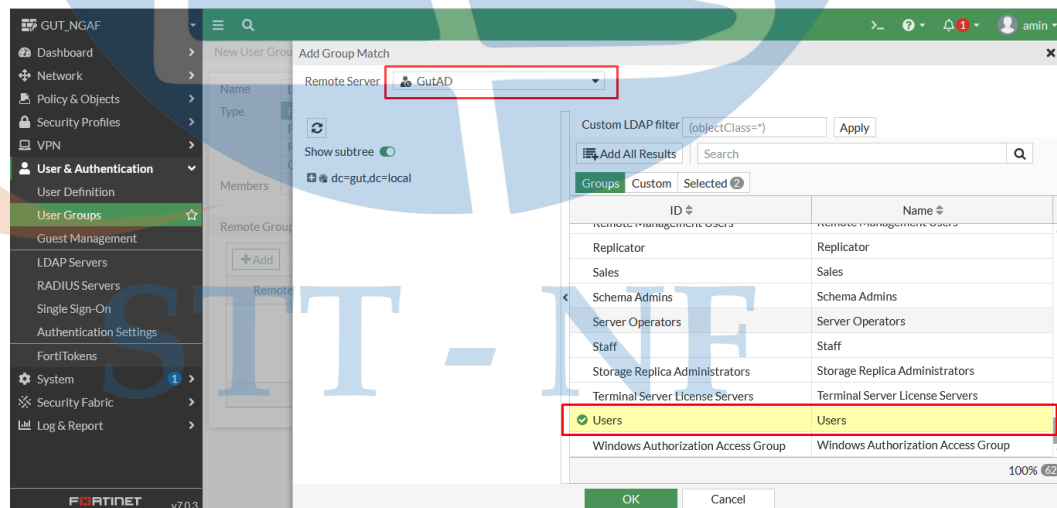
Selanjutnya penulis membuat grup pengguna baru pada menu *User Group* untuk menentukan grup pengguna mana saja yang akan digunakan sebagai Akun pengguna untuk Autentikasi.

STT - NF



Gambar 5.7 pengaturan user grup

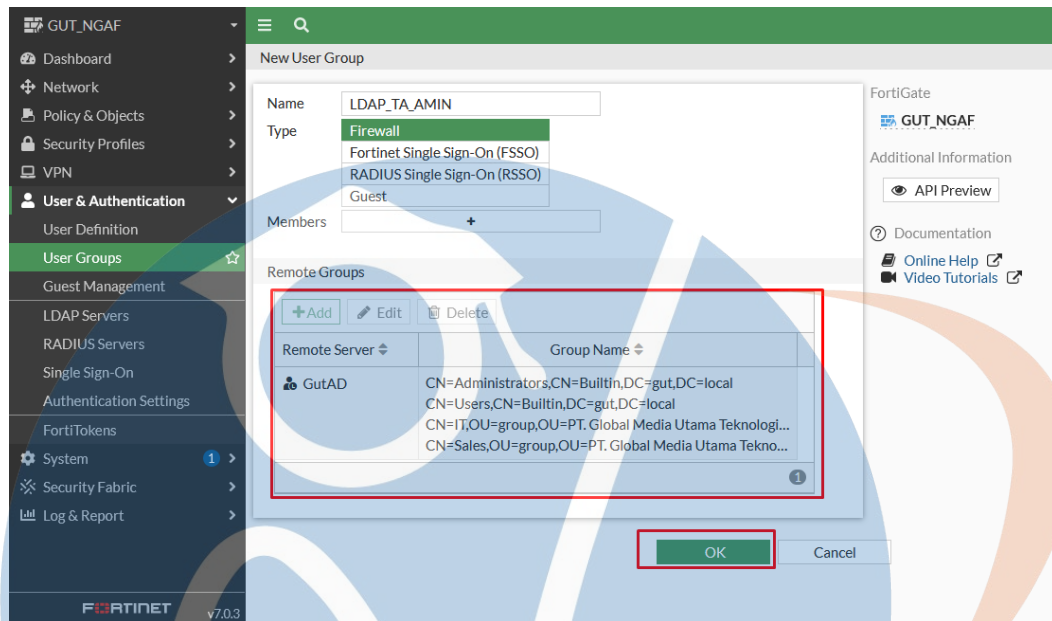
Pada gambar pengaturan *user* grup di atas, pada menu **User Group** penulis menambahkan grup baru dengan nama **LDAP_TA_AMIN** dengan menggunakan type grup **Firewall**, kemudian selanjutnya penulis membuat **Remote Groups** baru.



Gambar 5.8 konfigurasi user grup

Selanjutnya pada bagian **Remote Server** penulis menggunakan **LDAP Server** yang sudah ditambahkan sebelumnya yaitu **GutAD** yang dimana *user* grup *Active Directory*

yang dipilih dan akan digunakan untuk Autentikasi adalah grup *User*, *Administrators*, *IT* dan *Sales*, untuk pengaturannya adalah sebagai berikut.

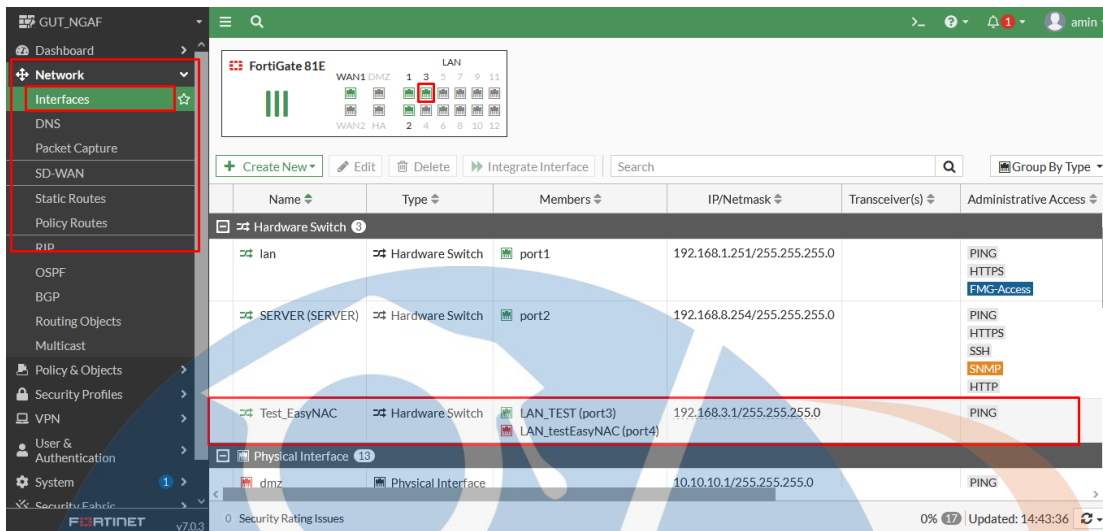


Gambar 5.9 konfigurasi user grup

Berdasarkan dari grup tersebut semua Akun pengguna yang ada di dalam grup tersebut dapat digunakan untuk login ke jaringan *wireless* melalui autentikasi Fortinet.

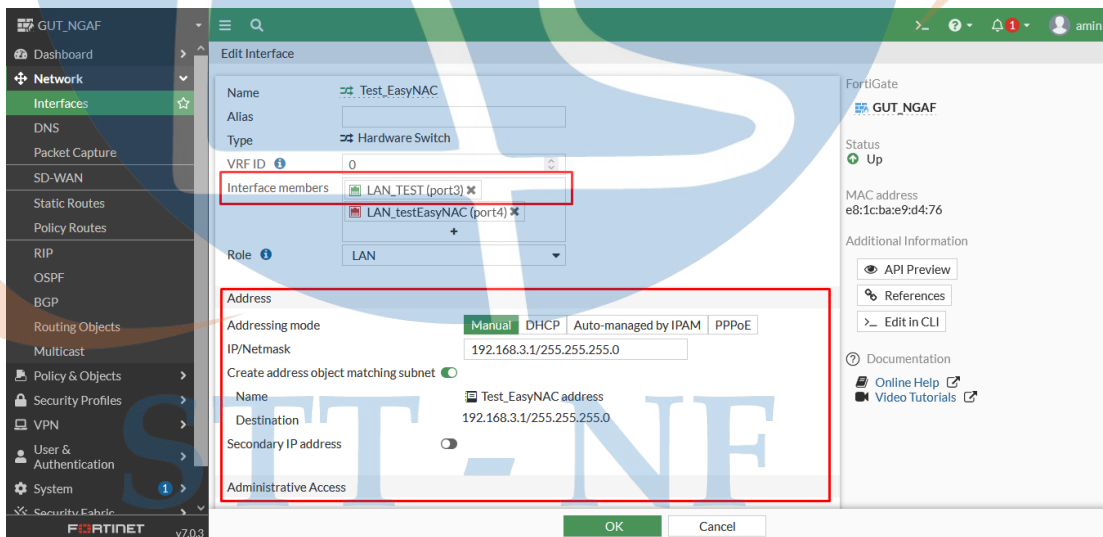
5.1.3 Pengaturan Interfaces

Pada tahapan pengaturan **Interfaces** ini, penulis membuat **Interfaces** baru yang terdapat di menu **Network** pada Fortinet. Yang dimana dalam pengaturan **Interfaces** ini penulis mengaktifkan satu **port** baru pada Fortinet untuk digunakan sebagai **Interfaces** pada jaringan *wireless*, yang dimana terdapat **DHCP Server** untuk pengalamantan IP pengguna, juga mengaktifkan **Security mode** dan **Captive Portal** sebagai Autentikator.



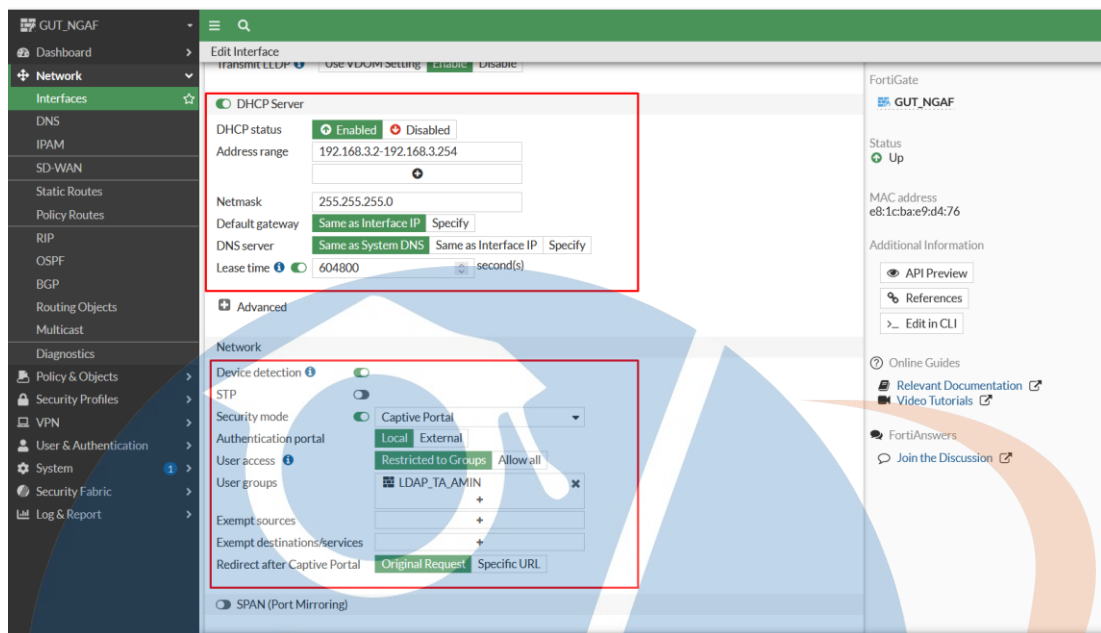
Gambar 5.10 konfigurasi interface

Pada Gambar diastas merupakan **Port interfaces** yang digunakan sebagai **DHCP Server** untuk pengalaman IP pengguna dan **Interfaces port 3** yang digunakan untuk jaringan *wireless* PT.XYZ



Gambar 5.11 konfigurasi interface

Pada bagian **Address**, **Addressing mode** yang digunakan adalah **Manual** melalui IP/Netmask **192.168.3.1/255.255.255.0**



Gambar 5.12 konfigurasi interface

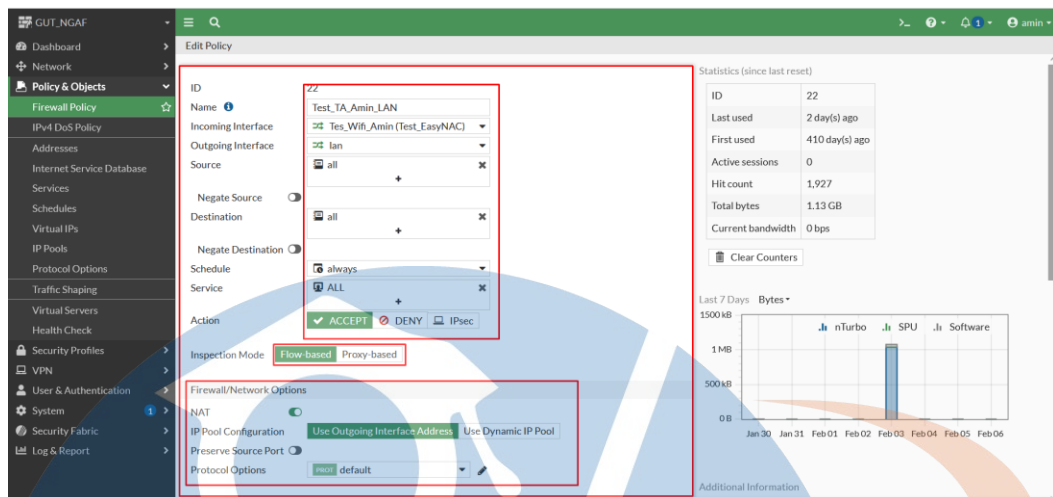
untuk **DHCP Server** range IP yang digunakan adalah **192.168.3.2-192.168.3.254** menggunakan Subnet Mask **255.255.255.0** dengan **Lease Time 604800 second** sebagai batas waktu penggunaan IP dari masing-masing *User*, pada bagian **Device detection** diaktifkan agar tersedia local MAC address filtering, untuk **Security mode** di aktifkan menggunakan **Captive Portal** sebagai antar muka Login *User* menggunakan **Local Authentication portal**, dan untuk *User Account* menggunakan *User Account* dari *Active Directory* yang sudah di daftarkan berdasarkan *User Group* **LDAP_TA_AMIN** yang sudah dibuat sebelumnya.

5.1.4 Pengaturan Policy

Tahapan yang selanjutnya yaitu pembuatan Policy (Kebijakan), Penulis membuat 3 Policy untuk mengatur kebijakan bagi *User* pengguna jaringan *wireless* diantaranya yaitu:

1. Policy jaringan *Wireless* ke LAN

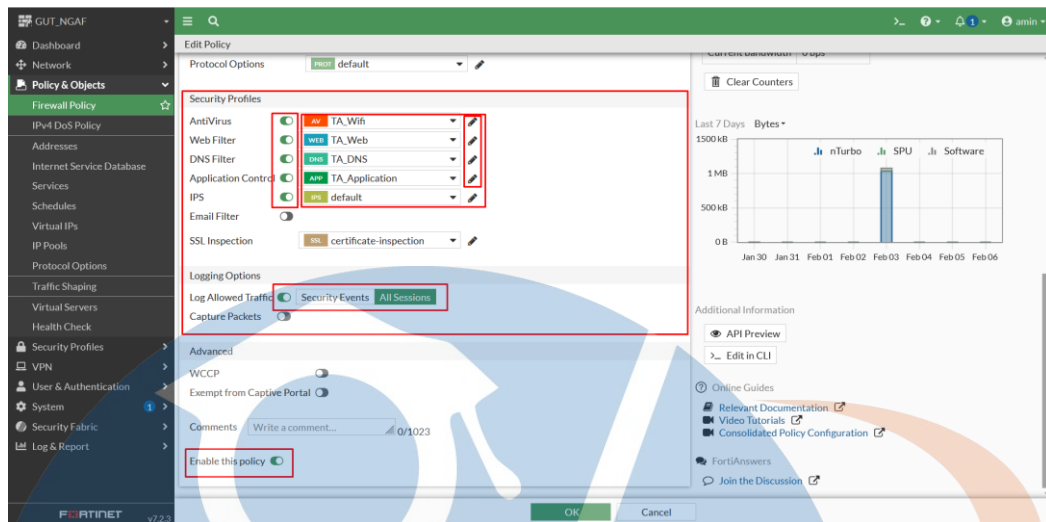
Policy pertama ini dibuat untuk mengatur lalu lintas penggunaan jaringan dari *user* ke jaringan local (LAN),



Gambar 5.13 policy LAN

Pada menu **Policy & Objects** di menu **Firewall Policy** menambahkan kebijakan baru dengan nama **Test_TA_Amin_LAN** yang mana akan digunakan sebagai kebijakan *user* saat mengakses jaringan local (LAN), pada halaman pernama berisikan nama **policy**, **incoming interface**, **outgoing interface**, **source**, **destination**, **schedule**, **service**, **action**, **inspection mode**, dan **firewall/network option**. Yang dimana untuk **incoming** nya berasal dari jaringan *wireless* dan **outgoing** nya menuju ke jaringan **LAN**, untuk **Source** yang digunakan adalah semua resource yang ada (**ALL**) dan untuk **Destination** nya juga ke semua (**ALL**) untuk **schedule** nya dibuat **Always**, **service** dijakankan semua (**ALL**) dan untuk **inspection** nya menggunakan **flow-based**.

STT - NF



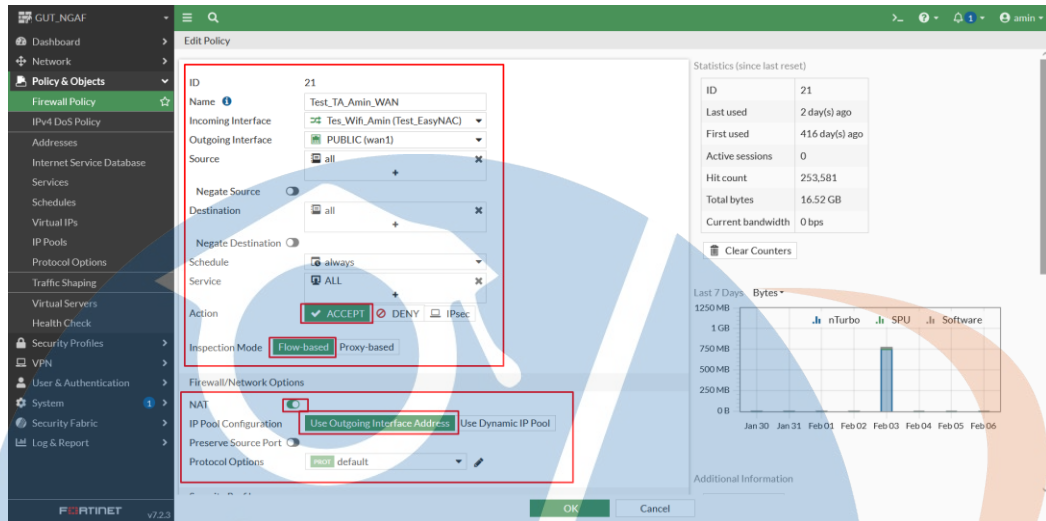
Gambar 5.14 policy LAN

Pada halaman kedua untuk memilih *service security* apa saja yang akan di aktifkan dan membuat atau menggunakan *profile* yang sudah tersedia, berikut ini *service* yang dijalankan diantaranya yaitu:

- AntiVirus
untuk memfilter setiap lalulintas yang keluar dan masuk agar terhindar dari virus
- Web Filter
untuk memfilter konten-konten yang berbasis web seperti situs-situs illegal, pornografi dan yang lainnya, untuk action nya dapat berupa **Allowed**, **Monitoring** dan **block**
- DNS Filter
untuk memfilter konten-konten berdasarkan kategori yang sudah tersedia pada Fortinet, untuk action nya dapat berupa **Allowed**, **Monitoring** dan **block**
- Application Control
untuk memfilter aplikasi-aplikasi berdasarkan kategori yang sudah disediakan Fortinet, untuk action nya dapat berupa **Allowed**, **Monitoring** dan **block**.

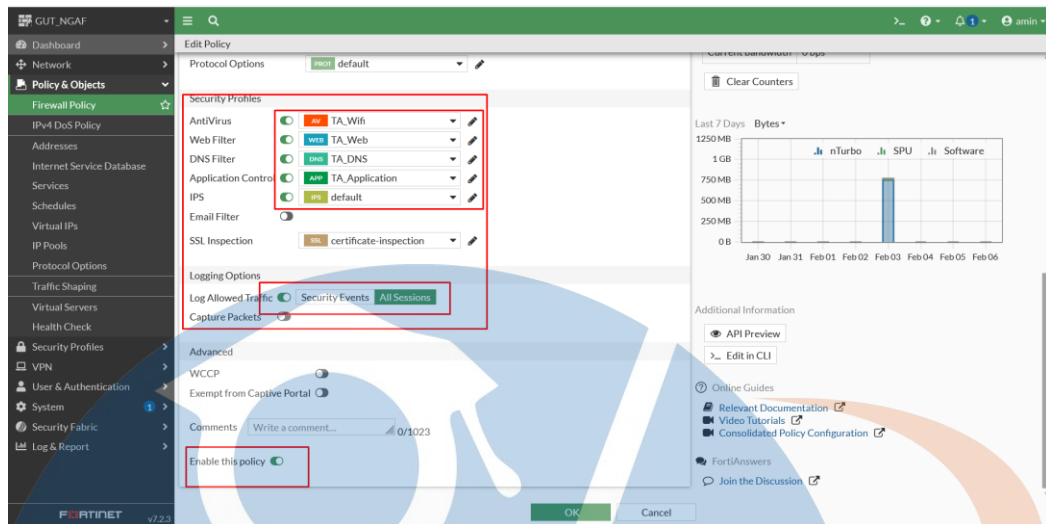
2. Policy Jaringan *Wireless* ke Internet

Policy yang kedua ini dibuat untuk mengatur lalulintas jaringan dari Jaringan *Wireless* ke *Public* (internet),



Gambar 5.15 policy WAN

Pada menu **Policy & Objects** di menu **Firewall Policy** menambahkan kebijakan baru dengan nama **Test_TA_Amin_WAN** yang mana akan digunakan sebagai kebijakan user saat mengakses jaringan local (LAN), pada halaman pernama berisikan nama **policy, incoming interface, outgoing interface, source, destination, schedule, service, action, inspection mode, dan firewall/network option**. Yang dimana untuk **incoming** nya berasal dari jaringan *wireless* dan **outgoing** nya menuju ke jaringan **Public (WAN)**, untuk **Source** yang digunakan adalah semua resource yang ada (**ALL**) dan untuk **Destination** nya juga ke semua (**ALL**) untuk **schedule** nya dibuat **Always**, **service** diizinkan semua (**ALL**) dan untuk **inspection** nya menggunakan **flow-based**.



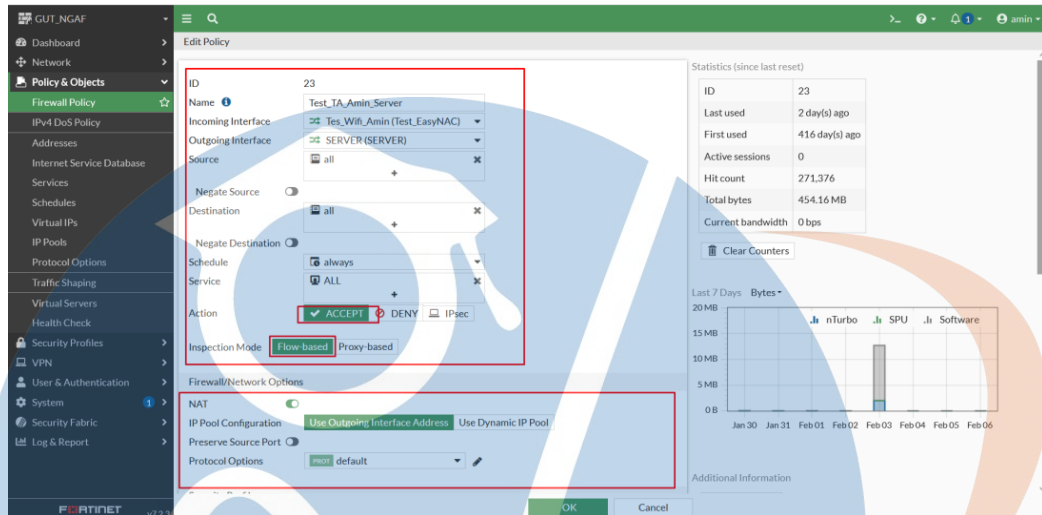
Gambar 5.16 policy WAN

Pada halaman kedua ini sama seperti pada policy **Tes_TA_Amin_LAN** yaitu untuk memilih *service security* apa saja yang akan di aktifkan dan membuat atau menggunakan *profile* yang sudah tersedia, berikut ini *service* yang dijalankan diantaranya yaitu:

- AntiVirus
untuk memfilter setiap lalulintas yang keluar dan masuk agar terhindar dari virus
- Web Filter
untuk memfilter konten-konten yang berbasis web seperti situs-situs ilegal, pornografi dan yang lainnya, untuk action nya dapat berupa **Allowed, Monitoring dan block**
- DNS Filter
untuk memfilter konten-konten berdasarkan kategori yang sudah tersedia pada Fortinet, untuk action nya dapat berupa **Allowed, Monitoring dan block**
- Aplication Control
untuk memfilter aplikasi-aplikasi berdasarkan kategori yang sudah disediakan Fortinet, untuk action nya dapat berupa **Allowed, Monitoring dan block.**

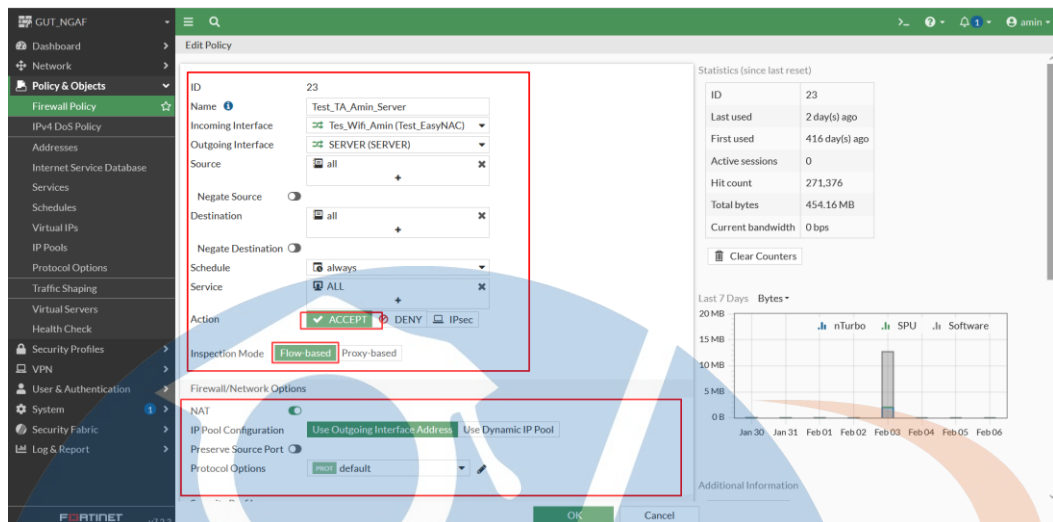
3. Policy Jaringan *Wireless* ke Server

Policy yang ketiga ini dibuat untuk mengatur lalulintas jaringan dari Jaringan *Wireless* ke Server



Gambar 5.17 policy server

Pada menu **Policy & Objects** di menu **Firewall Policy** menambahkan kebijakan baru dengan nama **Test_TA_Amin_Server** yang mana akan digunakan sebagai kebijakan user saat mengakses jaringan local (LAN), pada halaman pernama berisikan nama **policy**, **incoming interface**, **outgoing interface**, **source**, **destination**, **schedule**, **service**, **action**, **inspection mode**, dan **firewall/metwork option**. Yang dimana untuk **incoming** nya berasal dari jaringan *wireless* dan **outgoing** nya menuju ke jaringan **Server**, untuk **Sorce** yang digunakan adalah semua resource yang ada (**ALL**) dan untuk **Destination** nya juga ke semua (**ALL**) untuk **schedule** nya dibuat **Always**, **setvice** diizinkan semua (**ALL**) dan untuk **inspection** nya menggunakan **flow-based**.



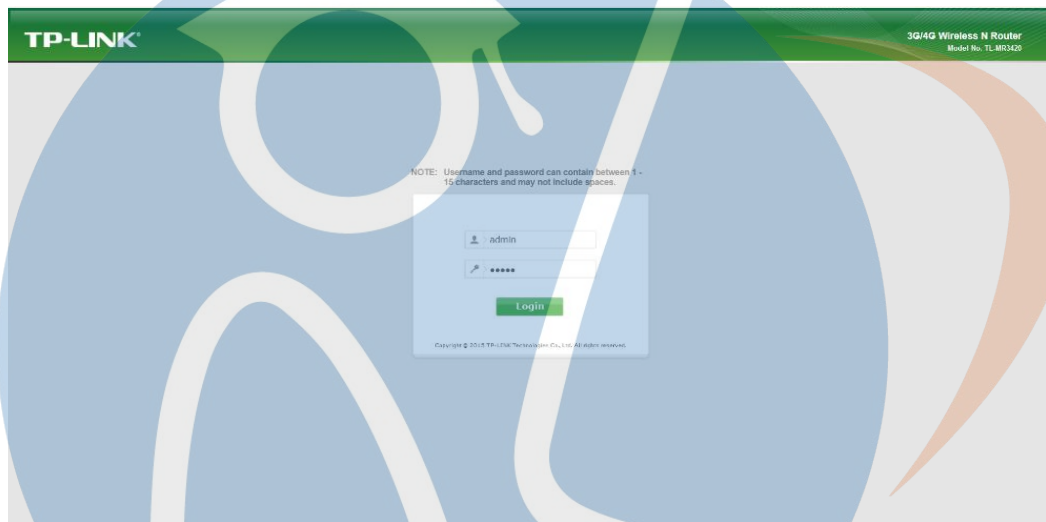
Gambar 5.18 policy server

Pada halaman kedua ini sama seperti pada *policy Tes_TA_Amin_LAN* dan *Tes_TA_Amin_WAN* yaitu untuk memilih *service security* apa saja yang akan di aktifkan dan membuat atau menggunakan *profile* yang sudah tersedia, berikut ini *service* yang dijalankan diantaranya yaitu:

- AntiVirus
untuk memfilter setiap lalulintas yang keluar dan masuk agar terhindar dari virus
- Web Filter
untuk memfilter konten-konten yang berbasis web seperti situs-situs ilegal, pornografi dan yang lainnya, untuk *action* nya dapat berupa **Allowed, Monitoring** dan **block**
- DNS Filter
untuk memfilter konten-konten berdasarkan kategori yang sudah tersedia pada Fortinet, untuk *action* nya dapat berupa **Allowed, Monitoring** dan **block**
- Application Control
untuk memfilter aplikasi-aplikasi berdasarkan kategori yang sudah disediakan Fortinet, untuk *action* nya dapat berupa **Allowed, Monitoring** dan **block**.

5.1.5 Pengaturan SSID pada Access Point TP-LINK

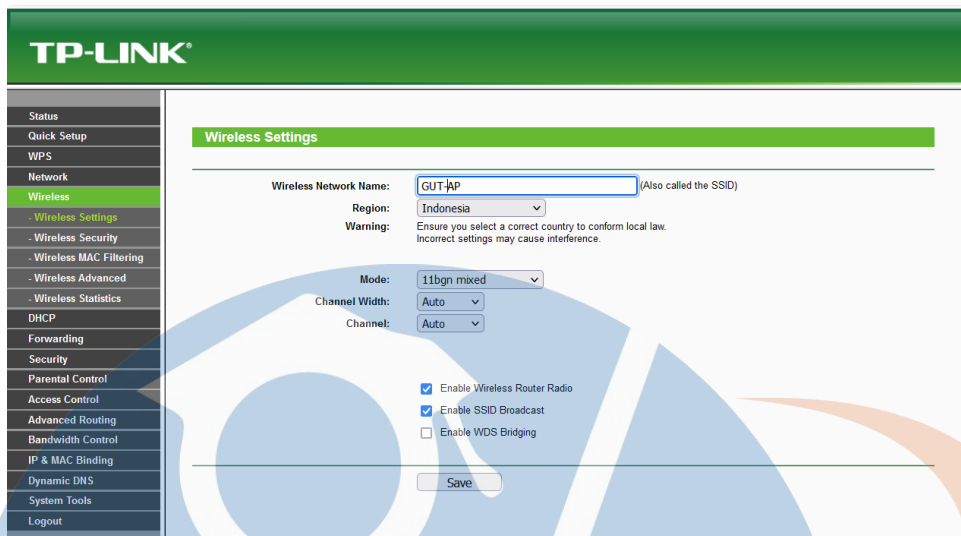
Untuk pengalamatan jaringan wireless agar dapat ditemukan oleh perangkat *user* dan dapat dibedakan dengan alamat jaringan wireless yang lainnya, maka pada tahapan ini penulis membuat SSID bagi jaringan *wireless* PT.XYZ, pertama penulis masuk ke pengaturan dari *Access Point* melalui Browser dengan cara mengakses alamat IP dari *Access Point*.



Gambar 5.19 login Access Point

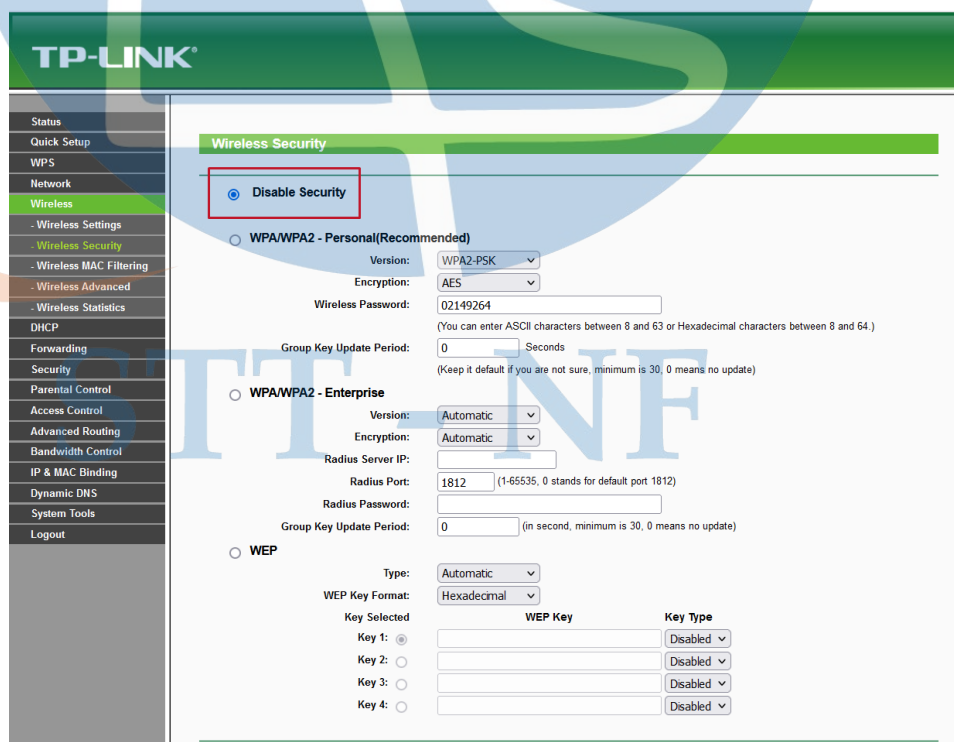
Kemudian setelah masuk ke menu pengaturan pilih menu **Wireless**, selanjutnya pilih **Wireless Setting**. Pada menu **Wireless Network Name** penulis memasukan Nama SSID yang akan digunakan, disini penulis menggunakan SSID dengan nama GUT-AP.

STT - NF



Gambar 5.20 Nama SSID

Selanjutnya pada menu *Wireless Security* penulis memilih untuk *Disable Security* karena tidak akan menggunakan fitur *Security* pada SSID, yang dimana penulis akan menggunakan Autentiikasi *Captive Portal* dari Fortinet.

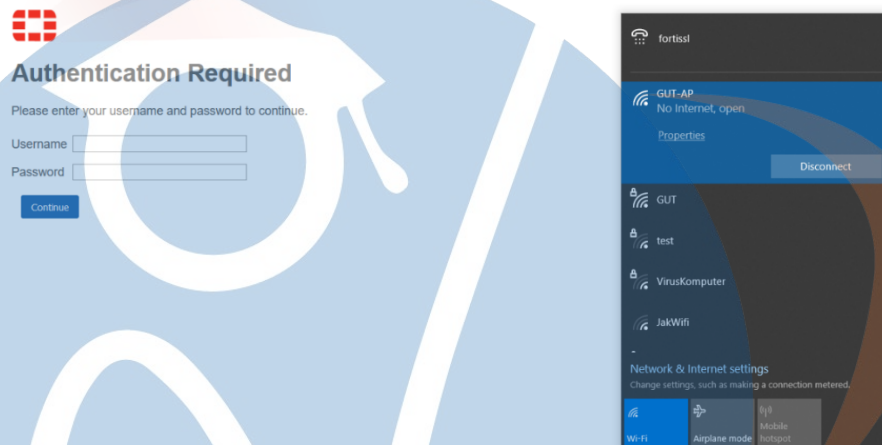


Gambar 5.21 Disable Security

5.2 Pengujian Efektifitas

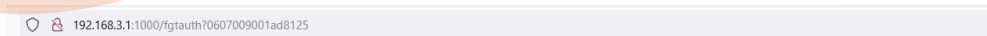
5.2.1 Pengujian Autentikasi

Pada tahapan pengujian Autentikasi ini penulis mencoba untuk masuk dan *login* ke jaringan *wireless* PT.XYZ melalui perangkat Komputer.

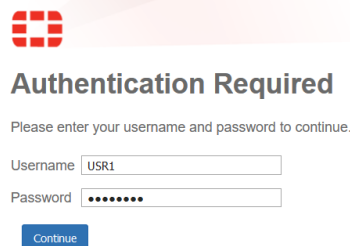


Gambar 5.22 uji koneksi laptop

Penulis masuk ke jaringan *wireless* **Test_TA_Amin** dan belum melakukan login menggunakan *username* dan *password* dari *Active Directory*, terpantau koneksi masih **No Internet** (belum terhubung ke internet),



STT - NF



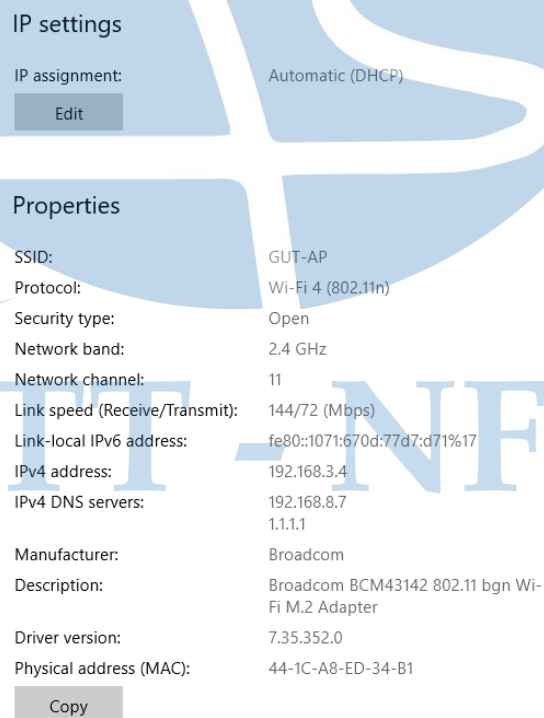
Gambar 5.23 autentikasi laptop

Penulis melakukan Autentikasi dengan cara memasukan *Username* dan *Password Active Directory* pada **login page** yang ter **popup** di browser,



Gambar 5.24 connected jaringan

Setelah melakukan Autentikasi, terpantau bahwa penulis sudah terkoneksi dan mendapatkan akses internet,



Gambar 5.25 mendapatkan alaman ip

User sudah mendapatkan alamat IP dari DHCP Server. Kemudian test ping ke internet dan server lokal

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2604]
(c) Microsoft Corporation. All rights reserved.

C:\Users\amin>ping google.com

Pinging google.com [142.251.12.101] with 32 bytes of data:
Reply from 142.251.12.101: bytes=32 time=893ms TTL=107
Reply from 142.251.12.101: bytes=32 time=1104ms TTL=107
Reply from 142.251.12.101: bytes=32 time=754ms TTL=107
Reply from 142.251.12.101: bytes=32 time=941ms TTL=107

Ping statistics for 142.251.12.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 754ms, Maximum = 1104ms, Average = 923ms

C:\Users\amin>ping 192.168.8.7

Pinging 192.168.8.7 with 32 bytes of data:
Reply from 192.168.8.7: bytes=32 time=734ms TTL=127
Reply from 192.168.8.7: bytes=32 time=785ms TTL=127
Reply from 192.168.8.7: bytes=32 time=740ms TTL=127
Reply from 192.168.8.7: bytes=32 time=658ms TTL=127

Ping statistics for 192.168.8.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 658ms, Maximum = 785ms, Average = 729ms

C:\Users\amin>
```

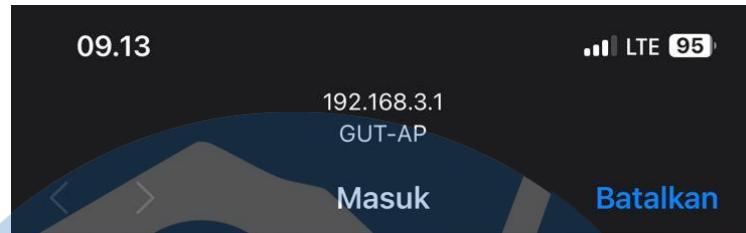
Gambar 5.26 test ping

Selanjutnya penulis melakukan uji coba koneksi dari perangkat Handphone



Gambar 5.27 Test autentikasi Iphone

Penulis masuk ke jaringan menggunakan perangkat Iphone melalui SSID GUT-AP



Authentication Required

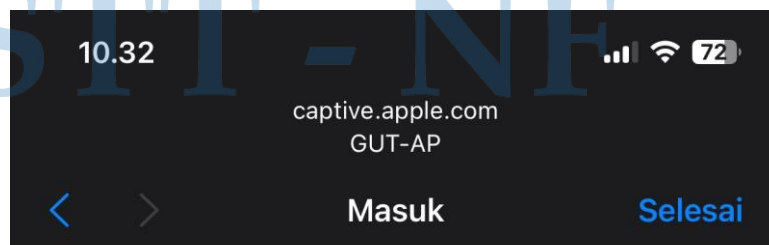
Please enter your username and password to continue.

Username

Password

Gambar 5.28 user login iphone

Penulis melakukan Autentikasi menggunakan *Username* dan *Password* yang terdaftar pada *Active Directory*



Success

Gambar 5.29 iphone terkoneksi

Setelah Autentikasi berhasil, pada gambar diatas terpantau bahwa penulis berhasil login dan mendapatkan akses internet.

5.2.2 Pengujian Efektifitas Berdasarkan Variasi User dan Variasi Perangkat

Setelah melakukan pengujian koneksi jaringan, selanjutnya penulis melakukan pengujian efektifitas dari rancangan Autentikasi Terpusat yang sudah di implementasikan dengan cara melakukan *login* ke jaringan menggunakan 10 akun *user* dan 10 perangkat yang berbeda, berikut hasil dari pengujian efektifitas:

1. Pengujian berdasarkan variasi user

Berikut ini adalah tabel hasil uji coba Autentikasi berdasarkan variasi 10 *user* yang berbeda didalam satu perangkat:

Table 5.1 Uji coba Autentikasi Variasi User

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

Dari tabel uji coba Autentikasi berdasarkan variasi 10 user berbeda didalam satu perangkat yang sama di atas, semua pengujiannya berhasil tanpa adanya kegagalan dalam login ke jaringan.

#	User	Date/Time	Action	Group	Destination	Status	Message
1	USR1	2023/03/03 09:37:10	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
2	USR2	2023/03/03 09:36:56	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR2 succeeded in authentication
3	USR3	2023/03/03 09:36:36	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR3 succeeded in authentication
4	USR4	2023/03/03 09:36:19	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR4 succeeded in authentication
5	USR5	2023/03/03 09:36:04	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR5 succeeded in authentication
6	USR6	2023/03/03 09:35:30	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR6 succeeded in authentication
7	USR7	2023/03/03 09:35:08	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR7 succeeded in authentication
8	USR8	2023/03/03 09:34:36	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR8 succeeded in authentication
9	USR9	2023/03/03 09:34:02	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR9 succeeded in authentication
10	USR10	2023/03/03 09:33:26	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR10 succeeded in authentication

Gambar 5.30 Hasil uji coba berdasarkan variasi user

Gambar diatas merupakan log dari Fortinet hasil uji coba berdasarkan variasi 10 user yang berbeda.

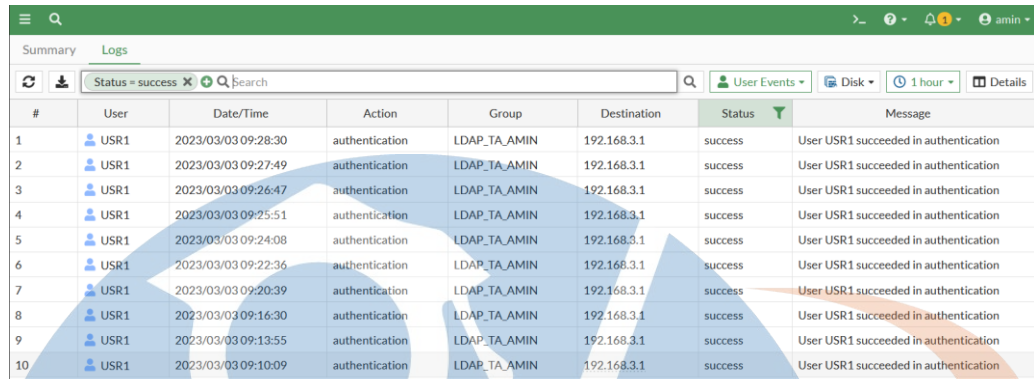
2. Pengujian berdasarkan variasi perangkat

Selanjutnya pengujian Autentikasi berdasarkan variasi 10 perangkat yang berbeda menggunakan akun USR1 untuk *login* ke jaringan, berikut ini tabel hasil uji coba berdasarkan variasi 10 perangkat yang berbeda:

Table 5.2 Uji coba Autentikasi variasi perangkat

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

Berdasarkan dari tabel diatas hasil dari uji coba autentikasi berdasarkan variasi 10 perangkat yang berbeda berhasil dan efektif.



The screenshot shows a log viewer interface with a table of authentication events. The table has columns for #, User, Date/Time, Action, Group, Destination, Status, and Message. All 10 entries show successful authentication for user USR1 from the group LDAP_TA_AMIN to destination 192.168.3.1.

#	User	Date/Time	Action	Group	Destination	Status	Message
1	USR1	2023/03/03 09:28:30	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
2	USR1	2023/03/03 09:27:49	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
3	USR1	2023/03/03 09:26:47	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
4	USR1	2023/03/03 09:25:51	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
5	USR1	2023/03/03 09:24:08	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
6	USR1	2023/03/03 09:22:36	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
7	USR1	2023/03/03 09:20:39	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
8	USR1	2023/03/03 09:16:30	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
9	USR1	2023/03/03 09:13:55	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
10	USR1	2023/03/03 09:10:09	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication

Gambar 5.31 Uji coba Autentikasi Variasi Perangkat

Gambar diatas merupakan log dari Fortinet hasil uji coba berdasarkan varias 10 Perangkat yang berbeda. Berdasar hasil uji coba sebanyak 10 kali menggunakan variasi user yang berbeda dan menggunakan variasi perangkat yang berbeda 100% berhasil dilakukan dan efektif.

STT - NF