BAB V

IMPLEMENTASI DAN PENGUJIAN

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



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.

New Object - User	obal Media Utama Teknolo	ai/Users/Staff/Divisi IT	×		
First name:	USR1	Initials:	ion		55
Last name: Full name:	USR1				
USR1	@gut.local	~			
	CBack	Next > Cancel			
Users					
	,				

Gambar 5.3 penambahan user baru

Pada gambar di atas setelah halaham *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.

	New Object - User	amoutare	×		>	×
1	Create in: gut.k	ocal/PT. Global Media Utama Teknologi/U	Jser			_
	Password:	•••••				
	Confirm password:	•••••				
	User must change password User cannot change pass Password never expires	ord at next logon word				
	Account is disabled					
C		< Back Next >	Cancel			
	Users	_		F		
	<	>				

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.

🗱 GUT_NGAF 🗸	≡ Q.			;
Dashboard	Edit LDAP Server			
 ✤ Network ➢ Policy & Objects 	Name	GutAD		FortiGate
Security Profiles	Server IP/Name Server Port	192.168.8.7 389		Additional Information
Luser & Authentication	Common Name Identifier Distinguished Name	sAMAccountName dc=gut,dc=local	Browse	API Preview
User Definition User Groups	Exchange server			⑦ Documentation
Guest Management	Bind Type Username	Simple Anonymous Regular amin@gut.local		Video Tutorials
LDAP Servers 🗘 RADIUS Servers	Password Secure Connection	••••••		
Single Sign-On Authentication Settings	Connection status	Successful		
FortiTokens	Test User Credentials			
♥ System 1 > ※ Security Fabric >	l			
Log & Report >			OK Cancel	
V/	Gambar	5.6 pengaturan ldap serv	ver	

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 <u>amin@gut.local</u>

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

GUT_NGAF -	≡ Q	
Dashboard >	New User Group	
	Name I DAD TA AMIN	FortiGate
Policy & Objects		B GUT_NGAF
Security Profiles	Fortinet Single Sign-On (FSSO)	Additional Information
₽ VPN >	RADIUS Single Sign-On (RSSO)	ADI Draviour
💄 User & Authentication 🛛 🗸	Guest	C API PI Eview
User Definition	Members +	⑦ Documentation
User Groups 🔂	Remote Groups	Doline Help
Guest Management		Video Iutorials
LDAP Servers	+Add / Edit Delete	
RADIUS Servers	Remote Server 🗢 Group Name 🗢	
Single Sign-On		
Authentication Settings	No resulta	
FortiTokens	Notesuits	
🗘 System 1 >		
🔆 Security Fabric 🔹 🔉		
네 Log & Report >		
	ОК С	incel
FURTIDET		
V/.0.3		
	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.

	≡ Q.				>_
Dashboard	New User Grou Add Grou	ip Match			×
A Network	Remote	Server 🔒 GutAD	_	•	
🛃 Policy & Objects 🔷 🔹 🔸	Name				
🔒 Security Profiles 🔷 🔷	Type			Custom LDAP filter (objectClass=*)	Apply
모 VPN >	Show sul	btree 🜑		Add All Results Search	0
💄 User & Authentication 🛛 🗸	D @ dc=	=gut.dc=local			
User Definition	Members	0		Groups Custom Selected	
User Groups 🖒	Pomoto Grour				Name \$
Guest Management	Keniote Group			Replicator	Replicator
LDAP Servers	+Add			Sales	Sales
RADIUS Servers	Remote			Schema Admins	Schema Admins
Single Sign-On			Ì	Server Operators	Server Operators
Authentication Settings				Server Operators	
FortiTokens			7	Starr	Stati
🗘 System 🚺 🔰				Storage Replica Administrators	Storage Replica Administrators
☆ Security Fabric >				Terminal Server License Servers	Ierminal Server License Servers
Log & Report >				✓ Users	Users
				Windows Authorization Access Group	Windows Authorization Access Group
					100% 🚱
				OK Cancel	

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.

🗱 GUT_NGAF 🗸 👻	≡ Q.	
Dashboard >	New User Group	
✤ Network >		FortiGate
Policy & Objects >	Name LDAP_IA_AMIN	🗰 GUT_NGAF
Security Profiles	Type Firewall Fortinet Single Sign-On (ESSO)	Additional Information
🖵 VPN 📏	RADIUS Single Sign-On (RSSO)	Additional mormation
💄 User & Authentication 🛛 👻	Guest	API Preview
User Definition	Members +	⑦ Documentation
User Groups 🛛 🏠	Remote Groupe	🗐 Online Help 🖸
Guest Management	Keinote Groups	Video Tutorials
LDAP Servers	+Add Selit Delete	
RADIUS Servers	Remote Server 🗢 Group Name 🗢	
Single Sign-On	GutAD CN=Administrators.CN=Builtin.DC=gut.DC=local	
Authentication Settings	CN=Users,CN=Builtin,DC=gut,DC=local	
FortiTokens	CN=IT,OU=group,OU=PT. Global Media Utama Teknologi	
💠 System 1 💈	CIV-sales,OO-group,OO-PT. Global Media Otama Tekno	
☆ Security Fabric >	0	
년 Log & Report >		
	ОК Салсе	el

Berdasarkan dari grup tersebut semua Akun pengguna yang ada di dalam grup tersebut dapat diguanakan 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.

Ē	GUT_NGAF	•	≣ Q.				>_ @) 🔹 🗘 🕇 🕘 amin '
Ø	Dashboard >	î (EartiGate 915	LAN				
¢	Network 🗸		WAN1	DMZ 135791	1			
	Interfaces ☆				<u>*</u>			
	DNS		WAN2	HA 2 4 6 8 10 1	12			
	Packet Capture							
	SD-WAN		Create New ▼	dit 🛍 Delete 🕨 I	ntegrate Interface Search		Q	Group By Type 🔻
	Static Routes		Name 🗢	Type 🌩	Members \$	IP/Netmask ≑	Transceiver(s) =	Administrative Access \$
	Policy Routes		🖸 🚅 Hardware Switch ③)				
	RIP		⊐⊄ lan	⊐‡ Hardware Switch	port1	192.168.1.251/255.255.255.0		PING
	OSPF							HTTPS
	BGP							FMG-Access
	Routing Objects		SERVER (SERVER)	⊐	m port2	192.168.8.254/255.255.255.0		PING
	Multicast							SSH
B	Policy & Objects							SNMP
≙	Security Profiles							HTTP
묘	. VPN >		⊐⊄ Test_EasyNAC	⊐⊄ Hardware Switch	LAN_TEST (port3)	192.168.3.1/255.255.255.0		PING
	User &	l ba			LAN_testEasyNAC (port4)			
	Authentication		-] 🛗 Physical Interface 🔃	3)				
*	System (1) >	. <	M dmz	Physical Interface		10.10.10.1/255.255.255.0		PING
		0.3	0 Security Rating Issues				0% 🚺	Updated: 14:43:36 2 -
				Gambar 5.1	0 konfigurasi in	terface		

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

GUT_NGAF	= Q	>_ 😧 • 🗘 • શ amin
Dashboard	Edit Interface	
Network	News Tot EscubleC	FortiGate
Interfaces ☆	Name 24 ICSC Lasy VIC	GUT_NGAF
DNS	Airas	
Packet Capture		Status O Up
SD-WAN	Interface members	
Static Routes	I LAN testEasyNAC (nort4) *	MAC address e8:1c:ba:e9:d4:76
Policy Routes	+	
RIP	Role 🖲 LAN 👻	Additional Information
OSPF		API Preview
BGP	Address	% References
Routing Objects	Addressing mode Manual DHCP Auto-managed by IPAM PPPoE	>_ Edit in CLI
Multicast	IP/Netmask 192.168.3.1/255.255.255.0	 Documentation
🖹 Policy & Objects 🔹 🕨	Create address object matching subnet C	
A Security Profiles	Name 🔤 Test_EasyNAC address	Video Tutorials
🖵 VPN 💦	Destination 192.168.3.1/255.255.0	
User & Authentication	Secondary IP address	
🕸 System 🚺 🔰	Administrative Access	
Security Eahric Y FtaRTINET v7.0.3	OK Cancel	

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

GUT_NGAF	≡ Q	
Dashboard	Edit Interface	
• Network ~		FortiGate
Interfaces 🖍	C DHCP Server	5 GUT_NGAF
DNS	DHCP status O Enabled O Disabled	
IPAM	Address range 192.168.3.2-192.168.3.254	Status
SD-WAN	0	O Op
Static Routes	Netmask 255 255 0	MAC address
Policy Routes	Default gateway Same as Interface IP Specify	e8:1c:ba:e9:d4:76
RIP	DNS server Same as System DNS Same as Interface IP Specify	Additional Information
OSPF	Lease time 0 C 604800 second(s)	ADI Demuiour
		API Preview
Routing Objects	Advanced	* References
Multicast		> Edit in CLI
Diagnostics	Network	(2) Online Guides
Policy & Objects	Device detection 1	Relevant Documentation
Security Profiles	STP O	Video Tutorials
므 VPN >	Security mode Captive Portal	- FantiAutorea
User & Authentication >	Authentication portal Local External	C lain the Discussion
🕸 System 🔹 🤉	User access Restricted to Groups Allow all	Join the Discussion La
Security Fabric >	User groups III LDAP_IA_AMIN	
🔟 Log & Report 💦 💊	Exempt sources +	
	Exempt destinations/services +	
	Redirect after Captive Portal Original Request Specific URL	
	SPAN (Port Mirroring)	

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 Acount* menggunakan *User Acount* 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 utuk mengatur lalulintas penggunaan jaringan dari *user* ke jaringan local (LAN),

27	GUT_NGAF	• = Q			>_ 0·	4 1 -	\rm e amin 🕶
Ð		> Edit Policy					
÷		>	Statistics (since last res	et)			Â
₽	Policy & Objects	V ID 22	ID	22			
	Firewall Policy	Name 1 Test_TA_Amin_LAN	Lastused	2 day(s) ago			
	IPv4 DoS Policy	Incoming Interface Incoming	First used	410 day(s) ago			
		Outgoing Interface Interface Interface	A stiller services	-10 uay(s) ago			
		Source 🔤 all 🗰	Active sessions	0			
		Negate Source	Hit count	1,927			
		Destination 🔤 all	Total bytes	1.13 GB			
		+	Current bandwidth	0 bps			
		Negate Destination 🕥	Clear Counters				
	Protocol Options	Schedule Co always					
	Traffic Shaping	Service I ALL X	Last 7 Days Bytes •				
			1500 kB				-
				.lı nTurbo	.li SPU .li S	oftware	
۵		Inspection Mode Flow-based Proxy-based	1 MB				
묘		,					
-		Firewall/Network Options	500 KB				
٠		NAT O	ов				
۲		IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool	Jan 30 Jan 3	Feb 01 Feb 02	Feb03 Feb04 Fe	b05 Feb0	6
ш		Preserve Source Port					
		Protocol Options					
			Additional Information			_	

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/metwork option**. Yang dimana untuk **incoming** nya berasal dari jaringan *wireless* dan **outgoing** nya menuju ke jaringan **LAN**, untuk **Sorce** yang digunakan adalah semua resource yang ada (ALL) dan untuk **Destination** nya juga ke semua (ALL) untuk **schedule** nya dibuat **Always, setvice** dijakankan semua (ALL) dan untuk **inspection** nya menggunakan **flow-based**.

GUT_NGAF -	≡ α	>_ 😧 • 🗘 1 • 😝 amin •
Dashboard >	Edit Policy	
Network >	Protocol Options PROT default 🔹 🖋	Currene bandwiddi 0 ops
💄 Policy & Objects 🛛 🗸 🗸		Clear Counters
	Security Profiles	
IPv4 DoS Policy	AntiVirus 🔍 📈 TA_Wifi 👻 🖍	Last 7 Days Bytes -
Addresses	Web Filter 🜑 🚾 TA_Web 🔹 🖋	1500 kB
	DNS Filter C DNS TA_DNS 🗸	
	Application Control 🔘 🗛 TA_Application 🔹 🖉	1MB
Schedules	IPS 💽 📴 default 👻 🇨	500 kB
	Email Filter	
IP Pools	SSL Inspection 🔹 🖉	08
Protocol Options		Jan 30 Jan 31 Feb 01 Feb 02 Feb 03 Feb 04 Feb 05 Feb 06
Traffic Shaping	Logging Options	
Virtual Servers	Log Allowed Traffic O Security Events All Sessions	Additional Information
Health Check	Capture Packets	
Security Profiles	A Second S	API Preview
	Advanced	> Edit in CLI
Liser & Authentication	WCCP	(2) Online Guides
System	Exempt from Captive Portal	Relevant Documentation
Security Fabric	Comments Write a comment	Video Tutorials 🗹
H Log & Report	0/1823	Consolidated Policy Configuration
	Enable this policy 🔘	Se FortiAnswers
		♀ Join the Discussion I
	OK Cancel	
	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 lainya, 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**.
- 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/metwork option**. Yang dimana untuk **incoming** nya berasal dari jaringan *wireless* dan **outgoing** nya menuju ke jaringan **Pulic (WAN),** untuk **Sorce** yang digunakan adalah semua resource yang ada (ALL) dan untuk **Destination** nya juga ke semua (ALL) untuk **schedule** nya dibuat **Always, setvice** dijakankan semua (ALL) dan untuk **inspection** nya menggunakan **flow-based**.

GUT_NGAF	≡ Q	>_ 😧 • 🗘 1 • 😝 amin •
Dashboard	Edit Policy	
Network	Protocol Options 🛛 🕶 🅜	
💄 Policy & Objects 🛛 🗸		Clear Counters
Firewall Policy 🖒	Security Profiles	
IPv4 DoS Policy	AntiVirus 🔍 📈 TA_Wifi 👻 🖌	Last7Days Bytes*
Addresses	Web Filter 🔍 Mts TA_Web 🔹	1250 MB
Internet Service Database	DNS Filter C DNS TA_DNS V	1 GB
Services	Application Control 🔘 🛺 TA_Application 👻 🖋	750 MB
Schedules	IPS 🖸 🗾 default 👻 🌶	500 MB
Virtual IPs	Email Filter	250 MB
IP Pools	SSL Inspection 🔹 Certificate-inspection 👻	0 B
Protocol Options		Jan 30 Jan 31 Feb 01 Feb 02 Feb 03 Feb 04 Feb 05 Feb 06
Traffic Shaping	Logging Options	
Virtual Servers	Log Allowed Traffic O Security Events All Sessions	Additional Information
Health Check	Capture Packets	ADI Drawinu
Security Profiles	Advanced	API Preview
묘 VPN	WCCD	>_ Edit in CLI
🚨 User & Authentication 💦 🌙	Exempt from Capital O	⑦ Online Guides
🕸 System 🔹 🕥	Exclipt from captive fortain Ca	Relevant Documentation
Security Fabric	Comments Write a comment	Video Tutorials C
🗠 Log & Report 💦 🔪		Constructed Forcy configuration B
	Enable this policy 🔘	PortiAnswers
ENETIDET	OK Cancel	
v7.23		

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 illegal, pornografi dan yang lainya, 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 dijakankan semua (ALL) dan untuk inspection nya menggunakan flow-based.

🛱 GUT_NGAF 🗾 👻	≡ Q					>_ 0 •	4 1 •	9
Dashboard >	Edit Policy							
Network >			•	Statistics (since last res	set)			
Policy & Objects 🗸 🗸	ID	23		ID	22			
Firewall Policy 🔂	Name 🚯	Test_TA_Amin_Server		10	23			
IPv4 DoS Policy	Incoming Interface			Last used	2 day(s) ago			
Addresses	Outgoing Interface	⇒ SERVER (SERVER) ▼		First used	416 day(s) ago			
Internet Service Database	Source	🗉 all 🛛 🗙		Active sessions	0			
Services		+		Hit count	271,376			
Schedules	Negate Source			Total bytes	454.16 MB			
Virtual IPs	Destination	i≌ all X		Current bandwidth	0 bps			
IP Pools	Negate Destination (
Protocol Options	Schedule	always -		Clear Counters				
Traffic Shaping	Service	ALL ×						
Virtual Servers		+		Last 7 Days Bytes -				
Health Check	Action	ACCEPT 🕐 DENY 😐 IPsec		20 MB	.h nTurbo	.li SPU .li Sc	oftware	
Security Profiles		The second second		15 MB				
VPN	Inspection Mode Flo	Proxy-based		10 MB				
User & Authentication	Firewall/Network Ontio	ns		EMP				
System (1)	NAT			JMD		_		
Security Fabric	IP Pool Configuration	Use Outgoing Interface Address Use Dynamic	IP Pool	OB	Color Color		05 5-1-04	_
Log & Report	Preserve Source Port	Ose outgoing internace Autorest Ose of Inamic		Jan 30 Jan 31	FebU1 FebU2 I	Feb 03 Feb 04 Feb	US FEDUC	,
Log anapore -	Protocol Options	reor default						
				Additional Information				
	A							
FURTINET v7.2.3			OK Cancel					
		Gambar 5.18 p	olicy server					
		in the P						

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 illegal, pornografi dan yang lainya, 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.**

5.1.5 Pengaturan SSID pada Access Point TP-LINK

Untuk pengalamatan jaringan wireless agar dapat ditemukan oleh perangkat *user* dan dapat dibendakan dengan alamat jaringan wireless yang lainnnya, 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*.



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.

Status		
Quick Setup	Vireless Settings	
WPS		
Network	Wireless Network Name	(Also called the SSID)
Wireless	Pagion	
- Wireless Settings	Warning:	Ensure you select a correct country to conform local law
- Wireless Security		Incorrect settings may cause interference.
- Wireless MAC Filtering		
- Wireless Advanced	Mode:	11bgn mixed 🗸
- Wireless Statistics	Channel Width:	Auto 🗸
DHCP	Channel:	Auto 🗸
Forwarding		
Security		
Parental Control		Enable Wireless Router Radio
Access Control		Enable SSID Broadcast
Advanced Routing		Enable WDS Bridging
Bandwidth Control		
IP & MAC Binding		
Dynamic DNS		Save
System Tools		
Logout		

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

atus			
lick Setup	Wireless Security		
PS			
twork	Disable Security		
ireless	°		
Vireless Settings	WPA/WPA2 - Personal/Recomm	nended)	
Vireless Security	Version	WPA2-DSK Y	
Vireless MAC Filtering	Encryption	AEC	
Vireless Advanced	Witeless Destructu	AL3 *	
Vireless Statistics	Wifeless Fassword.	Vou on optor ASCII characters between	9 and 62 or Hevedenimal obstractors between 9 and 64)
	Group Koy Undate Period:	Seconde	o and 05 or riexadecimal characters between o and 04.)
rwarding	Gloup Key opuale Period.	Ween it default if you are not ours minim	um is 20.0 means as undate)
urental Control		(Reep it deladit if you are not sure, minim	um is 30, o means no update)
cess Control	WPA/WPA2 - Enterprise		
vanced Routing	version:	Automatic V	
ndwidth Control	Encryption:	Automatic V	
& MAC Binding	Radius Server IP:		
namic DNS	Radius Port:	1812 (1-65535, 0 stands for defau	It port 1812)
stem Tools	Radius Password:		
gout	Group Key Update Period:	0 (in second, minimum i	s 30, 0 means no update)
	○ WEP		
	Туре:	Automatic 🗸	
	WEP Key Format:	Hexadecimal V	
	Key Selected	WEP Key	Кеу Туре
	Key 1: 💿		Disabled V
	Key 2: 🔿		Disabled V
	Key 3: 🔘		Disabled V
	Key 4:		Disabled x

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.



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



Gambar 5.25 mendapatkan alaman ip

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



Gambar 5.27 Test autentikasi Iphone

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

	09.13		•11 LTE (95)	
		192.168.3.1 GUT-AP		
	3	Masuk	Batalkan	
	Authe	ntication R	equired	
	Please enter	your username and pa	ssword to continue.	
	Username u	SR1		
	Password	••••••		
	Continue			
		Gambar 5 28 user login i	phone	1
		Sundu 5.20 user login i	Pirono	
Penuls melak	ukan Autentika	asi menggunakan User	name dan Password	<i>d</i> 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:

Nama User	Aute	ntikasi	Keterangan				
	Gagal	Berhasil	Ketterangan				
USR1		~	Berhasil terkoneksi ke jaringan				
USR2		\checkmark	Berhasil terkoneksi ke jaringan				
USR3		\checkmark	Berhasil terkoneksi ke jaringan				
USR4		\checkmark	Berhasil terkoneksi ke jaringan				
USR5		\checkmark	Berhasil terkoneksi ke jaringan				
USR6		\checkmark	Berhasil terkoneksi ke jaringan				
USR7		~	Berhasil terkoneksi ke jaringan				
USR8		~	Berhasil terkoneksi ke jaringan				
USR9			Berhasil terkoneksi ke jaringan				
USR10		\checkmark	Berhasil terkoneksi ke jaringan				

Table 5.1 Uji coba Autentikasi Variasi User

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.

≣ Q							>_ 🕜 • ♀ 1 • ⊖ amin •
Summar	y Logs						
C 1	Status = succe	ss 🗙 🔁 🔍 þearch				Q User Eve	ents 🔹 🕼 Disk 👻 🕓 1 hour 👻 🗖 Details
#	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	LUSR9	2023/03/03 09:34:02	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR9 succeeded in authentication
10	LUSR10	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 varias 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:

Perangkat		Hasil Au	tentikasi		
Jenis Perangkat	Sistem Operasi	Gagal	Sukses	Keterangan	
Laptop	Windows 10		<	Berhasil terkoneksi ke jaringan	
Laptop	Windows 10		>	Berhasil terkoneksi ke jaringan	
Laptop	Windows 11	_		Berhasil terkoneksi ke jaringan	
Laptop	Laptop Ubuntu 20		X	Berhasil terkoneksi ke jaringan	
Laptop	Laptop Ubuntu 20		$\mathbf{\hat{\mathbf{x}}}$	Berhasil terkoneksi ke jaringan	
Handphone Android			<	Berhasil terkoneksi ke jaringan	
Handphone Android			~	Berhasil terkoneksi ke jaringan	
Handphone IOS			<	Berhasil terkoneksi ke jaringan	
Handphone	Iandphone IOS		\checkmark	Berhasil terkoneksi ke jaringan	
Handphone	IOS		\checkmark	Berhasil terkoneksi ke jaringan	

Table 5.2	Uii co	ba Autentil	kasi variasi	perangkat
1 4010 0.2	0 1 00	ou i iacontin	aubi variabi	perangian

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

≣ ଦ							>_ 🕜 • 🗘 🕽 • \varTheta amin •
Summary	Logs						
C 1	Status = succe	ss 🗙 🖸 🔍 þearch			Q	Luser Event	s 🔹 🕞 Disk 🔹 🕓 1 hour 🔹 🖬 Details
#	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	LUSR1	2023/03/03 09:24:08	authentication	LDAP_TA_AMIN	192.168.3.1	success	User USR1 succeeded in authentication
6	LUSR1	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	LUSR1	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.