BAB IV HASIL DAN PEMBAHASAN

4.1 Hasil Implementasi Database

Pada tahap ini, akan dijelaskan mengenai hasil implementasi *database* yang telah dirancang dan dibangun untuk memenuhi kebutuhan sistem yang telah dijelaskan pada bab sebelumnya. *Database* yang di implementasikan dirancang untuk mendukung operasional dan penyimpanan data yang efisien, serta memungkinkan pengambilan dan pengolahan data secara cepat dan akurat.

4.1.1 Struktur Tabel Log Activity

Untuk meningkatkan kemampuan sistem dalam memonitor dan menganalisis aktivitas yang terjadi, ditambahkan tabel *log activity* dalam struktur *database*.

	#	Name	Туре	Collation	Attributes	Null	Default	Comments	Extra	_
	1	id_log 🔑	int(11)			No	None		AUTO_INCREM	IENT
	2	phys_address	varchar(50)	latin1_swedish_ci		No	None			
	3	status	varchar(20)	latin1_swedish_ci		No	None			
	4	timestamp	datetime			No	None			
t	_	Check all	With selecte	ed: 🗾 Browse	Change)	Drop	Primary	Unique	ह In

Gambar 4.1 Struktur tabel *log activity*

Gambar 4.1 adalah *database* yang berfungsi untuk mencatat setiap aktivitas yang dilakukan oleh pengguna atau sistem, sehingga dapat digunakan untuk keperluan monitoring. Tabel *log activity* dirancang untuk menyimpan informasi detail tentang aktivitas yang terjadi dalam sistem. Adapun atribut-atribut yang terdapat dalam tabel ini adalah sebagai berikut :

1. *id_log* : atribut ini berfungsi sebagai *primary key* yang unik untuk setiap *log activity*. Tipe data yang

digunakan adalah INT dengan *auto-increment*, memastikan setiap *log* memiliki *identifier* yang unik.

- 2. *phys_address*: atribut ini menyimpan alamat fisik (misalnya IP *address*) dari perangkat yang melakukan aktivitas. Tipe data yang digunakan adalah VARCHAR(50) untuk mengakomodasi format IPv4 dan IPv6.
- status: atribut ini mencatat status atau hasil dari aktivitas yang dilakukan, seperti 'ACTIVE', 'INACTIVE', atau deskripsi lainnya yang relevan. Tipe data yang digunakan adalah VARCHAR(20).
- 4. *timestamp*: atribut ini menyimpan waktu terjadinya aktivitas. Tipe data yang digunakan adalah *DATETIME*, memungkinkan pencatatan waktu yang akurat hingga detik.

4.1.2 Struktur Tabel Users

Untuk mengelola informasi pengguna secara lebih detail dan terstruktur, ditambahkan tabel *users* dalam struktur *database*.

	#	Name	Туре	Collation	Attributes	Null	Default	Comments	Extra	
	1	id_user 🔑	int(11)			No	None		AUTO_INCR	EMENT
	2	ip_address	varchar(45)	latin1_swedish_ci		No	None			
	3	name	varchar(45)	latin1_swedish_ci		No	None			
	4	community	varchar(20)	latin1_swedish_ci		No	None			
	5	phys_address	varchar(45)	latin1_swedish_ci		Yes	Unknown			
	6	status	varchar(10)	latin1_swedish_ci		No	inactive			
	7	device_type	int(20)			No	None			
t	_	Check all	With selec	ted: 🔝 Browse	🥜 Change	•	Drop	Primary	Unique	🐖 Inde
			Gam	bar 4.2 St	ruktu	r ta	bel u	sers		

Gambar 4.2 adalah *database* yang berfungsi untuk menyimpan informasi penting tentang setiap pengguna yang berinteraksi dengan sistem, termasuk detail tentang perangkat dan status perangkat. Penambahan tabel ini diharapkan dapat meningkatkan manajemen pengguna dan memberikan informasi yang diperlukan untuk analisis lebih lanjut. Tabel *user* dirancang untuk menyimpan berbagai informasi penting mengenai pengguna. Adapun atribut-atribut yang terdapat dalam tabel ini adalah sebagai berikut :

- id_user: atribut ini berfungsi sebagai primary key yang unik untuk setiap pengguna. Tipe data yang digunakan adalah INT dengan auto-increment, memastikan setiap pengguna memiliki identifier yang unik.
- 2. *ip_address*: atribut ini menyimpan alamat IP dari perangkat yang digunakan oleh pengguna. Tipe data yang digunakan adalah VARCHAR(45) untuk mengakomodasi format IPv4 dan IPv6.
- 3. *name*: atribut ini menyimpan nama pengguna. Tipe data yang digunakan adalah VARCHAR(45), memungkinkan penyimpanan nama pengguna dengan panjang yang memadai.
- 4. *community*: atribut ini menyimpan informasi tentang komunitas atau grup yang diikuti oleh pengguna. Tipe data yang digunakan adalah VARCHAR(20).
- 5. *phys_address*: atribut ini menyimpan alamat fisik dari perangkat pengguna, seperti MAC *address*. Tipe data yang digunakan adalah VARCHAR(45).

- 6. status: atribut ini mencatat status dari pengguna, seperti '*ACTIVE*', '*INACTIVE*', atau status lainnya yang relevan. Tipe data yang digunakan adalah VARCHAR(20).
- *device_type*: atribut ini menyimpan jenis perangkat yang digunakan oleh pengguna, seperti '*MOBILE*', '*DESKTOP*', atau '*TABLET*. Tipe data yang digunakan adalah VARCHAR(20).

4.2 Hasil Implementasi Sistem Monitoring

Dalam tahap ini akan menjelaskan bagaimana sistem monitoring di implementasikan. Implementasi sistem ini meliputi petunjuk penggunaan *website* dan tampilannya sehingga administrator dapat memahami fitur yang tersedia pada *website* monitoring.

4.2.1 Halaman Login Administrator

Halaman *login* pada sistem monitoring kinerja jaringan merupakan langkah pertama dalam menjaga keamanan dan integritas sistem. Pada tahap awal, pengguna diharuskan memasukkan *hostname* dan *community* atau nama lingkup yang dimonitoring, yaitu Zaha.net. Ini adalah langkah awal yang membantu memastikan bahwa hanya pengguna dengan pengetahuan tentang lingkungan yang spesifik yang dapat mencoba mengakses sistem. Pada tahap awal *login*, perlu adanya informasi yang harus di *input* yaitu data SNMP yang di monitoring. Informasi tersebut di *input* seperti pada Gambar 4.3.

Zaha.n	iet		
Sign in to start your session			
192.168.52.93	8		
Community	<u>:</u>		
	Sign In		

Gambar 4.3 Halaman login SNMP

Untuk mendapatkan IP address yang diperlukan untuk login pada sistem monitoring Zaha.net, pengguna perlu melakukan pengecekan melalui terminal atau command line interface (CLI) pada perangkat jaringan, yaitu router. IP address ini merupakan alamat unik yang diberikan kepada perangkat dalam jaringan untuk memungkinkannya berkomunikasi dengan perangkat lain di dalam atau di luar jaringan. Pada router utama, pengguna dapat menggunakan perintah seperti ipconfig (untuk Windows) atau *ifconfig* (untuk Linux/Unix) untuk melihat konfigurasi jaringan termasuk IP address yang diberikan kepada router, pengecekan melalui address terminal dapat menggunakan IP print. Informasi IP address ini kemudian digunakan sebagai hostname saat login ke halaman sistem monitoring, memastikan bahwa komunikasi antara perangkat yang dimonitor dan sistem monitoring berjalan dengan benar

dan aman. Gambar 4.4 menunjukkan cara melakukan pengecekan IP *address* perangkat.

5 8.8.8.	8		56	114	45ms
6 8.8.8.	.8		56	114	50ms
7 8.8.8.	.8		56	114	112ms
8 8.8.8.	8		56	114	42ms
9 8.8.8.	8		56	114	74ms
10 8.8.8.	8		56	114	80ms
11 8.8.8.	8		56	114	88ms
12 8.8.8.	8		56	114	40ms
13 8.8.8.	8		56	114	80ms
14 8.8.8.	8		56	114	83ms
15 8.8.8.	8		56	114	61ms
16 8.8.8.	8		56	114	82ms
17 8.8.8.	8		56	114	65ms
18 8.8.8.	8		56	114	74ms
19 8.8.8.	8		56	114	72ms
sent=20	received=20	packet-loss=0%	min-rtt=38ms	avg-	-rtt=69ms
max-rtt=1	46ms				
adminOMikro	Tikl > ip ad	ldress print			
lags: X – d	lisabled, I -	- invalid, D - d	lynamic		
# ADDRESS	5	NETWURK	INTERFACE		
0 192.168	8.10.1/24	192.168.10.0	ether2		
1 D 192.168	3.52.93/24	192.168.52.0	ether1		
adminOMikro	Tik1 >				

Gambar 4.4 Cek IP address

Setelah sistem memverifikasi identitas SNMP yang dimasukkan valid, administrator kemudian diarahkan ke halaman *login router* dan kemudian mengisi *username* dan *password* perangkat yang berfungsi sebagai *Simple Network Management Protocol* (SNMP) yang dimonitor. Gambar 4.5 menunjukaan halaman *login router*, proses *login* ganda ini memiliki beberapa keuntungan penting, yaitu :

- 1. Keamanan ganda : dengan mengharuskan dua kali *login*, sistem menambahkan lapisan keamanan ekstra. Bahkan jika akses untuk *login* pertama diketahui oleh pihak yang tidak berwenang, mereka masih harus melewati *login* kedua untuk mendapatkan akses ke sistem monitoring.
- 2. Verifikasi pengguna: *login* pertama dengan *hostname* dan *community* memastikan bahwa hanya pengguna yang terkait dengan Zaha.net yang dapat

melanjutkan ke tahap berikutnya. Ini mengurangi risiko akses oleh pengguna dari luar organisasi.

- 3. Kendali akses : *login* kedua yang memerlukan akses ke perangkat *router* memastikan bahwa hanya administrator yang memiliki izin untuk mengelola perangkat jaringan yang dapat mengakses halaman *dashboard*. Ini penting untuk mencegah perubahan yang tidak sah atau tindakan berbahaya terhadap perangkat jaringan.
- 4. Pengurangan risiko akses tidak dikenal : dengan dua kali *login*, kemungkinan akses tidak dikenal berkurang signifikan. Ini karena akses memerlukan dua informasi yang berbeda, yang meningkatkan kesulitan bagi orang yang tidak bertanggung jawab untuk mendapatkan akses penuh sistem monitoring.

Login Mikrotik ×
admin
Password
Close
Login

Gambar 4.5 Login router

4.2.2 Halaman Dashboard

Halaman *dashboard* adalah halaman utama atau halaman awal yang menampilkan ringkasan informasi

penting dan ditampilkan setelah berhasil *login*. Gambar 4.6 adalah halaman dashboard dari sistem yang telah di buat.



Gambar 4.6 Halaman dashboard

4.2.3 Widget Informasi Perangkat

Gambar 4.7 dan Gambar 4.8 menampilkan informasi data perangkat berupa nama perangkat, sistem operasi, IP *address* perangkat dan *physical address* perangkat yang kemudian akan menampilkan informasinya dengan menggunakan tombol *detail*.



Gambar 4.7 Informasi perangkat

Data Perangkat				
Mikrotik				
Nama Perangkat "MikroTik"	3 Firmware "RouterOS x86"			
器 Ip Address 192.168.52.93	O Physical Address			
	08: 0:0 :27: A:D :08: 7:9			
Close				

Gambar 4.8 Data perangkat

4.2.4 Widget Uptime Perangkat

Gambar 4.9 yang terletak pada halaman *dashboard* menampilkan informasi mengenai waktu operasional atau ketersediaan sebuah perangkat jaringan dalam periode tertentu. *Uptime* mengindikasikan durasi atau waktu sejak perangkat terakhir kali dinyalakan atau dimulai, atau dalam konteks monitoring, sejak terakhir kali perangkat tersebut dikonfirmasi aktif. Informasi ini penting karena memberikan gambaran tentang keandalan dan ketersediaan perangkat dalam infrastruktur jaringan.

Uptime perangkat menjadi indikator utama dalam menilai performa dan stabilitas jaringan serta dalam mengidentifikasi masalah jika *uptime* perangkat menurun atau terjadi *downtime*.



Gambar 4.9 Uptime perangkat

4.2.5 Widget Total Users

Gambar 4.10 yang terlatak pada halaman *dashboard* sistem monitoring menampilkan informasi tentang jumlah keseluruhan pengguna atau perangkat yang terhubung atau terdaftar dalam jaringan atau sistem yang sedang dimonitor. Informasi ini penting untuk memahami skala penggunaan atau pengelolaan infrastruktur jaringan. *Widget* ini membantu pengelola untuk dengan cepat melihat dan memantau skala penggunaan atau kelompok perangkat dalam jaringan.



Gambar 4.10 Total users

4.2.6 Widget Active Users

Pada Gambar 4.11 dan 4.12 menampilkan informasi total *active users* (perangkat aktif) yang terkoneksi ke jaringan secara *real-time*, yang kemudian akan menampilkan tabel *active users* ketika menggunakan tombol *detail*.

Salah satu *widget* yang terdapat di *dashboard* adalah *widget* "*active users*," yang memberikan informasi tentang pengguna aktif yang sedang menggunakan jaringan. *Widget* "*active users*" berfungsi untuk memantau dan menampilkan data mengenai pengguna yang saat ini sedang terhubung ke jaringan. Informasi ini sangat penting bagi pengelola jaringan untuk memahami beban jaringan secara *real-time* dan memastikan tidak ada masalah yang mengganggu konektivitas pengguna. Data yang disajikan oleh *widget* ini bisa mencakup jumlah pengguna aktif, IP *address* perangkat, *physical address*, dan status perangkat.



Gambar 4.11 Active users

Active	Active							
No	Name	IP Address	Phys. Address	Community	Status	Opsi		
1	-	192.168.52.129	14: D:4 :24: 3:0 :76: C:F	zaha.net	•	Edit Log Activity Delete		
2	-	192.168.10.11	08: 0:0 :27: 3:A :53: 1:E	zaha.net	•	Edit Log Activity Delete		
3	-	192.168.10.50	08: 0:0 :27: D:D :05: 9:7	zaha.net		Edit Log Activity Delete		
4	-	192.168.52.174	12: D:A :6C: 1:5 :4B: 7:B	zaha.net	•	Edit Log Activity Delete		

Gambar 4.12 Tabel *active users*

4.2.7 Grafik Users

Salah satu komponen utama yang terdapat di halaman dashboard adalah grafik *users* berupa diagram lingkaran (*pie chart*). Grafik ini memberikan representasi visual yang jelas tentang status pengguna jaringan dalam tiga kategori yaitu *users active, users inactive,* dan total keseluruhan *users*. Warna hijau menunjukkan jumlah total pengguna aktif, warna merah menunjukkan jumlah total pengguna tidak aktif, dan warna biru menunjukkan jumlah total keseluruhan pengguna. Gambar 4.13 menunjukkan representasi visual yang jelas tentang status pengguna jaringan.





Gambar 4.13 Grafik users

4.2.8 Last Inactive Users

Informasi mengenai *last inactive users* pada sebuah sistem monitoring kinerja jaringan adalah krusial untuk memantau keandalan perangkat dalam jaringan. Ketika sebuah perangkat menjadi *inactive* atau mengalami gangguan, tampilan ini memberikan detail seperti alamat fisik perangkat untuk identifikasi yang lebih tepat, status terakhir perangkat ketika gangguan terjadi, dan waktu spesifik (tanggal dan jam) ketika perangkat terakhir kali

tercatat mengalami masalah. Hal ini membantu pengelola untuk segera merespons dan mengatasi masalah, menjaga kestabilan dan ketersediaan jaringan secara keseluruhan. Dengan informasi ini, tim pengelola dapat melakukan analisis lebih lanjut untuk memperbaiki perangkat atau sistem yang terpengaruh, serta memastikan bahwa dapat diminimalkan gangguan untuk mendukung operasional kelancaran jaringan. Gambar 4.14 menunjukkan informasi last inactive user yang terjadi di dalam sistem monitoring yang telah dibuat.

Log Activity (Inactive) - Newest					
Phys Address	Status	Timestamp	*		
7E: A:D :34: 6:7 :EF: 9:A	inactive	2024-06-25 18:14:59			
12: D:A :6C: 1:5 :4B: 7:B	inactive	2024-06-25 12:14:44			
ST:RI:NG:: :"::R?:???"	inactive	2024-06-24 13:23:08			
CC: 2:D :E0: 0:3 :10: D:5	inactive	2024-06-24 13:20:34			
3A: 5:2 :9B: 9:B :AD: F:E	inactive	2024-06-24 12:10:11			

Gambar 4.14 *Last inactive users*

4.2.9 Halaman Users

Pada Gambar 4.15 menampilkan informasi total keseluruhan perangkat, baik yang terkoneksi maupun tidak. Pada halaman ini juga menampilkan informasi status perangkat, jika status berwarna hijau maka perangkat terkoneksi, sedangan jika status berwarna merah maka koneksi perangkat terputus.

ter b	y Status:						
All							
No	Name	IP Address	Phys. Address	Community	Status	Opsi	
1	÷	192.168.52.129	14: D:4 :24: 3:0 :76: C:F	zaha.net	•	Edit Log Activity Delete	
2		192.168.10.11	08: 0:0 :27: 3:A :53: 1:E	zaha.net	•	Edit Log Activity Delete	
3		192.168.10.50	08: 0:0 :27: D:D :05: 9:7	zaha.net	•	Edit Log Activity Delete	
4	•	192.168.52.174	12: D:A :6C: 1:5 :4B: 7:B	zaha.net	•	Edit Log Activity Delete	
5		192.168.72.251	7E: A:D :34: 6:7 :EF: 9:A	zaha.net	•	Edit Log Activity Delete	
6		192 168 100 1	CC: 2:D :E0: 0:3 :10: D:5	zaha.net		Edit Los Activity Delete	

Gambar 4.15 All users

4.2.10 Edit, Log Activity & Delete

Opsi "edit" memungkinkan administrator atau pengelola untuk mengubah informasi yang terkait dengan perangkat yang terdaftar dalam sistem. Ini adalah fitur penting untuk memastikan bahwa data perangkat tetap akurat dan terkini. Ketika opsi ini dipilih, sebuah form akan muncul yang berisi informasi perangkat saat ini, seperti IP address, physical address, status dan community. Pengguna dapat memperbarui informasi sesuai ini Misalnya, kebutuhan. jika ada perubahan dalam konfigurasi jaringan atau jika perangkat dipindahkan ke lokasi baru dengan alamat IP yang berbeda, informasi ini dapat diperbarui melalui opsi "edit device." Memastikan bahwa informasi perangkat selalu akurat membantu dalam memantau dan mengelola jaringan secara efektif. Gambar 4.16 menampilkan halaman edit device.

Edit Device

Name		
Laptop William		
IP Address		
192.168.52.129		
Phys. Address		
14: D:4 :24: 3:0 :76: C:F		
Community		
zaha.net		
Status		
active		
	Close Save chang	es

×

Gambar 4.16 Edit info perangkat

Opsi "Log Activity" dalam konteks sistem monitoring jaringan merupakan fitur penting yang memungkinkan pengguna untuk mengakses dan menganalisis aktivitas yang terjadi pada suatu perangkat jaringan. Log activity ini mencatat informasi waktu kapan perangkat aktif (up) dan tidak aktif (down). Informasi ini penting untuk memahami seberapa sering perangkat mengalami gangguan atau downtime yang dapat mempengaruhi ketersediaan jaringan. Gambar 4.17 menunjukkan log activity dari sebuah device.

Activity Log

Timestamp	Status
2024-06-13 10:02:28	inactive
2024-06-13 10:02:27	active
2024-06-13 06:19:04	inactive
2024-06-13 06:19:03	active
2024-06-13 06:04:24	inactive
2024-06-13 05:56:38	active

Gambar 4.17 Log activity

Selanjutnya adalah opsi "*delete*" memungkinkan pengelola untuk menghapus perangkat dari sistem monitoring. Ini mungkin diperlukan jika perangkat tersebut tidak lagi digunakan, digantikan oleh perangkat lain, atau jika perangkat tersebut dipindahkan ke jaringan lain yang tidak dipantau oleh sistem ini. Ketika opsi ini dipilih, sistem biasanya akan meminta konfirmasi untuk memastikan bahwa penghapusan dilakukan secara sengaja dan bukan sebagai kesalahan. Penghapusan perangkat akan menghilangkan semua data terkait perangkat tersebut dari sistem monitoring, termasuk log aktivitas.

Oleh karena itu, opsi ini harus digunakan dengan hati-hati untuk menghindari kehilangan data penting yang mungkin masih diperlukan untuk analisis atau audit di

Close

masa mendatang. Gambar 4.18 menampilkan halaman konfirmasi *delete*.



Gambar 4.18 Delete device

4.3 Pengujian Sistem

Pengujian sistem menggunakan metode *blackbox* dilakukan berdasarkan kebutuhan fungsionalitas untuk memastikan bahwa *output* sesuai dengan yang diharapkan. Pengujian ini melibatkan skenario yang dilakukan oleh pengguna dalam memantau jaringan dan mengelola data perangkat pemantauan.

4.3.1 Pengujian Login

Pada pengujian *login*, administrator harus mengisi data SNMP, memasukkan *username* dan *password* dengan benar. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

No	Skenario	Hasil Yang	Keterangan
	Pengujian	Didapatkan	
1	Jika data SNMP	Maka tidak dapat	Berhasil
	tidak ada	login router	
2	Jika data SNMP	Maka dapat <i>login</i>	Berhasil
	ada	router	
3	Jika <i>username</i> &	Maka tidak dapat	Berhasil
	password salah	<i>login</i> ke halaman	

Tabel 4.1 Pengujian login

		dashboard	
4	Jika <i>username</i> &	Maka berhasil	Berhasil
	password benar	<i>login</i> ke halaman	
		dashboard	

4.3.2 Pengujian View Status

Pada pengujian *view status*, administrator harus menampilkan *status device* yang di monitoring. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

No	Skenario	Hasil Yang	Keterangan
	Pengujian	Didapatkan	
1	Jika data SNMP	Maka perbarui	Berhasil
	dan <i>database</i>	status <i>device</i>	
	sama	menjadi active	
2	Jika data hanya	Maka perbarui	Berhasil
	ada di <i>database</i>	status <i>device</i>	
		menjadi <i>inactive</i>	

4.3.3 Pengujian Log Activity

Pada pengujian *log activity*, administrator harus menampilkan *log* atau histori kondisi jaringan yang terjadi. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

No	Skenario	Hasil Yang	Keterangan
	Pengujian	Didapatkan	
1	Jika log activity	Maka log activity	Berhasil

Tabel 4.2 Pengujian log activity

	phys_address	tidak ditampilkan	
	tidak ada di		
	database		
2	Jika <i>log activity</i>	Maka log activity	Berhasil
	<i>phys_address</i> ada	ditampilkan	
	di database		

4.3.4 Pengujian Edit

Pada pengujian edit, administrator harus dapat mengubah atau menambah nama *device*. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

Tabel 4.4 Pengujian edit

No	Skenario	Hasil Yang	Keterangan
	Pengujian	Didapatkan	
1	Jika mengubah	Maka	Berhasil
	atau menambah	menampilkan <i>form</i>	
	nama <i>device</i>	edit device	
2	Jika menekan	Maka perubahan	Berhasil
	tombol save	tersimpan	
	changes		

4.3.5 Pengujian Delete

Pada pengujian *delete*, administrator harus bisa menghapus daftar atau data *device*. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

Tabel 4.5 Pengujian delete

No	Skenario	Hasil Yang	Keterangan

	Pengujian	Didapatkan	
1	Jika <i>device</i> di	Maka	Berhasil
	delete	menampilkan form	
		delete	
2	Jika konfirmasi	Maka device	Berhasil
	<i>delete</i> di benarkan	berhasil di <i>delete</i>	
3	Jika device sudah	Maka data device	Berhasil
	di <i>delete</i>	termasuk log	
		activity terhapus	

4.3.6 Pengujian View Device

Pada pengujian *view device*, administrator harus bisa menampilkan daftar *total users* atau *device*, dan melakukan filter berdasarkan status yang diminta. Kemudian, dilakukan pengujian dan hasil yang di dapatkan untuk memastikan sistem berjalan sesuai yang diharapkan.

Tabel 4.5 Pengujian view device

No	Skenario	Hasil Yang	Keterangan
	Pengujian	Didapatkan	
1	Jika ke menu	Maka	Berhasil
	users	menampilkan	
		semua daftar	
		device	
2	Jika ke menu	Maka	Berhasil
	users dan di filter	menampilkan	
	berdasarkan	daftar device	
	status active atau	berdasarkan status	
	inactive	active atau inactive	