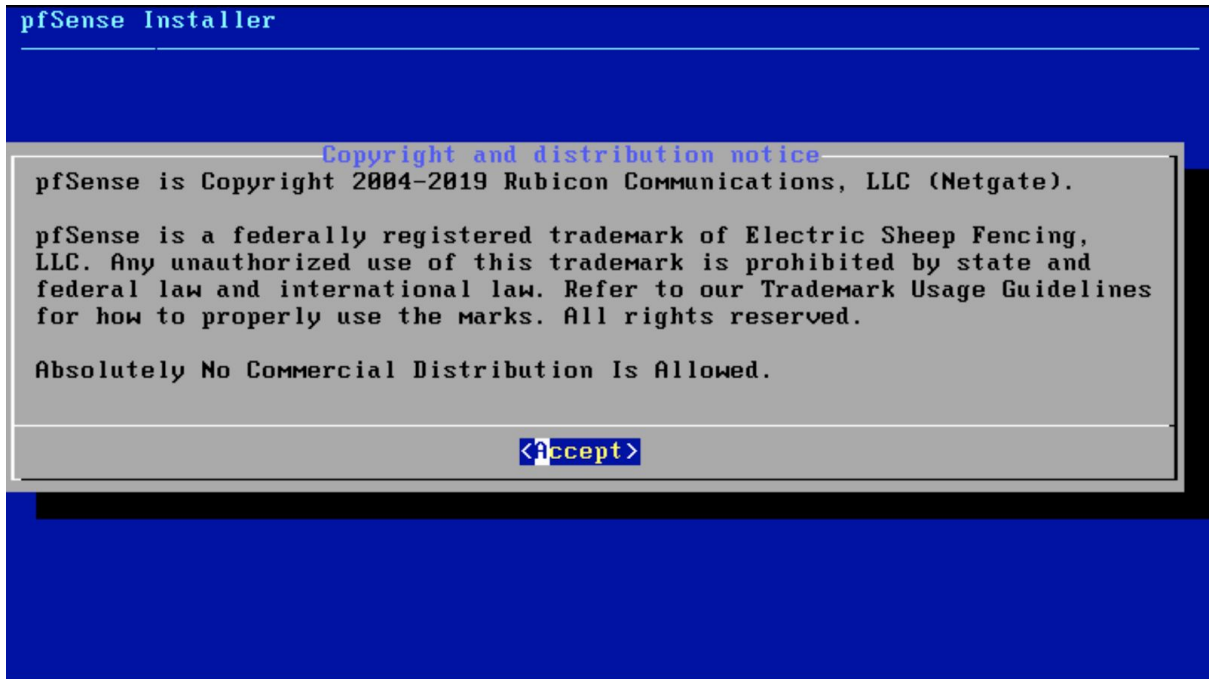


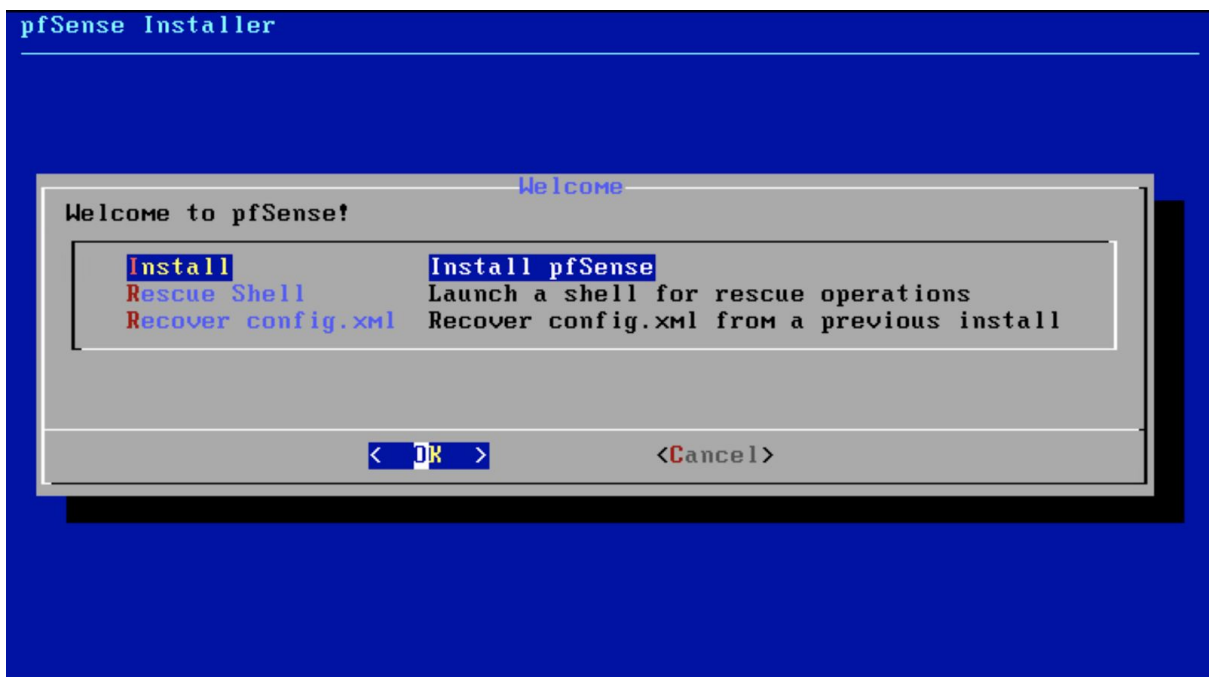
บทที่ 2 ติดตั้ง Server OS pfsense

มีขั้นตอนคร่าวๆ ดังนี้

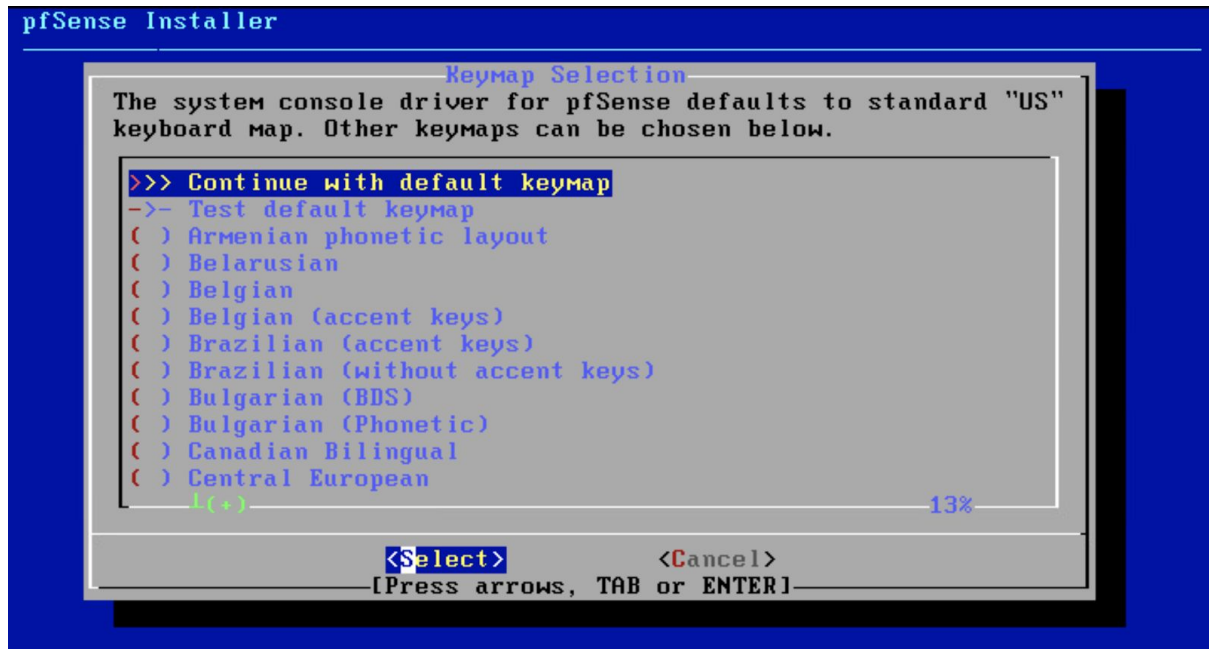
1. กด Accept



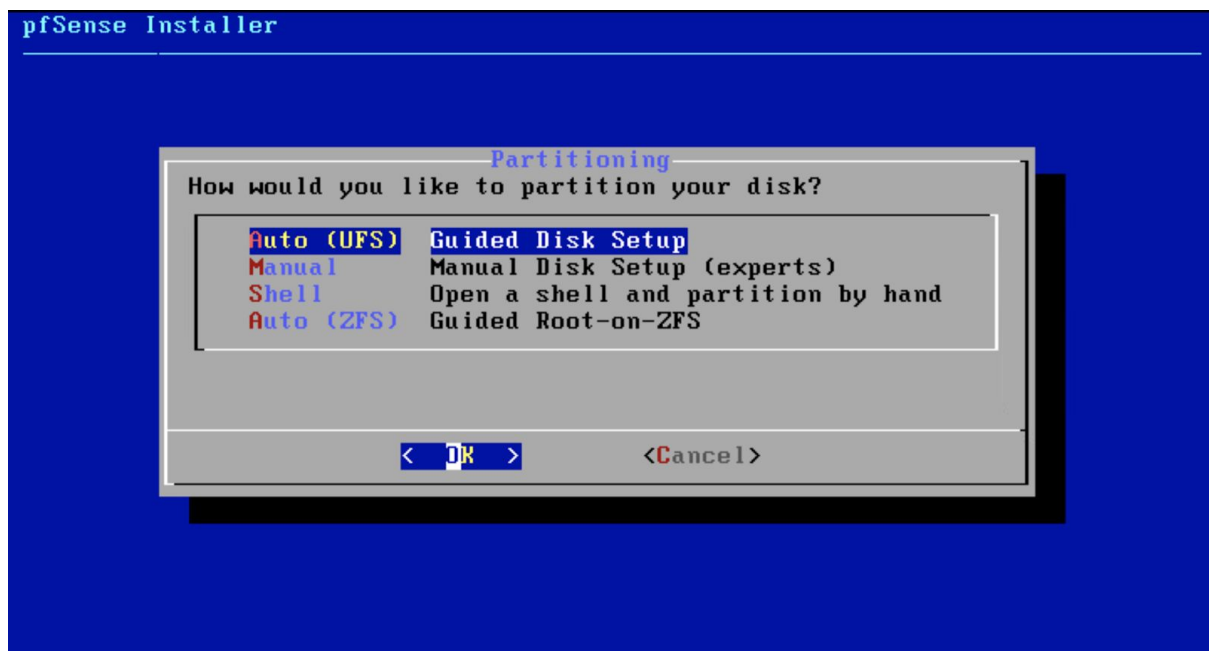
2. เลือกตามภาพข้างบนแล้วกด Ok



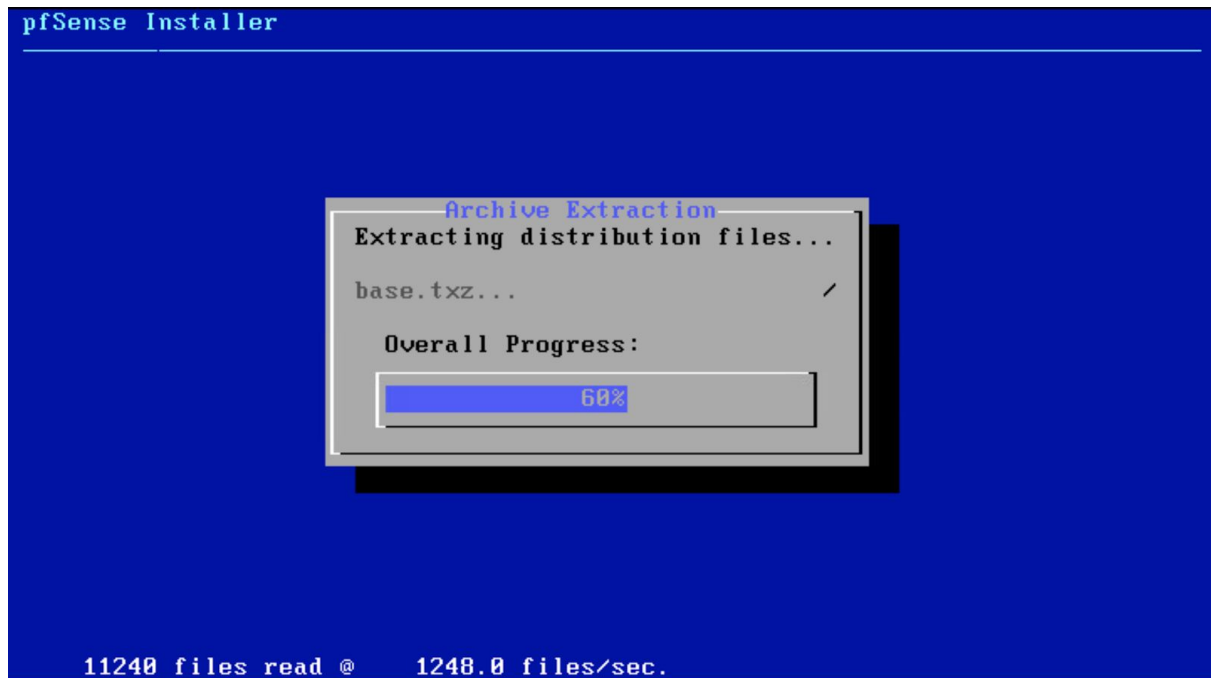
3. เลือก Select



4. เลือกตามภาพ ด้านบนแล้วกด Ok



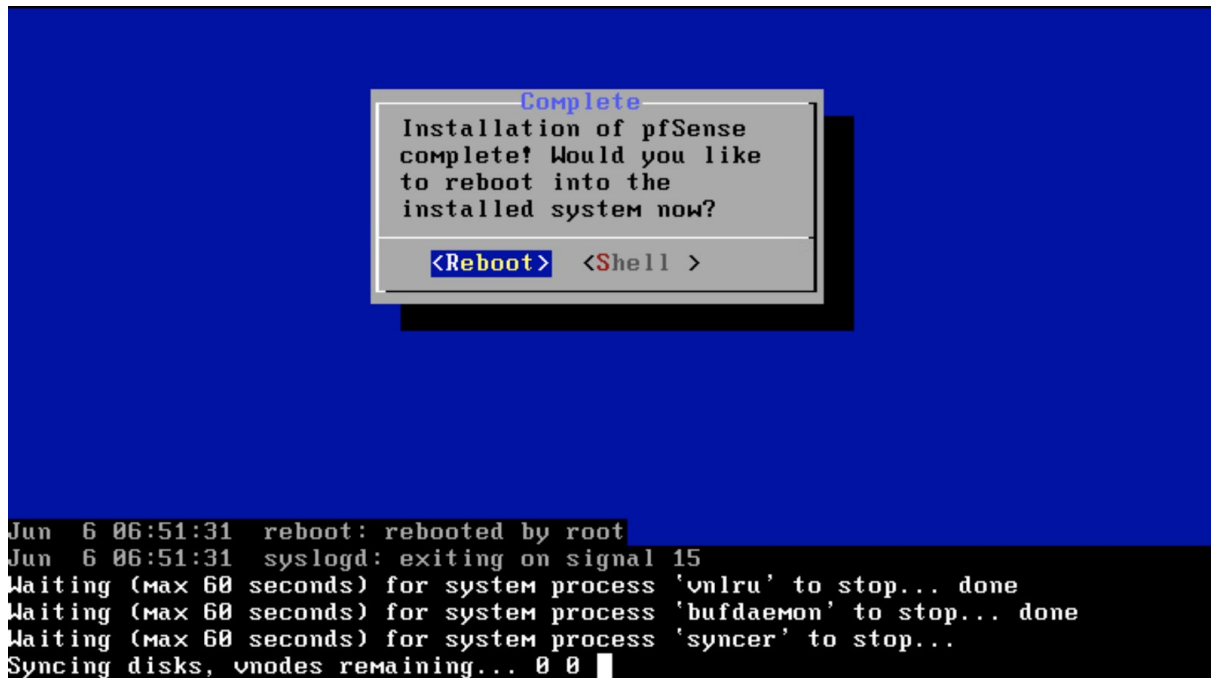
5. จากนั้นก็รอจนติดตั้งเสร็จ



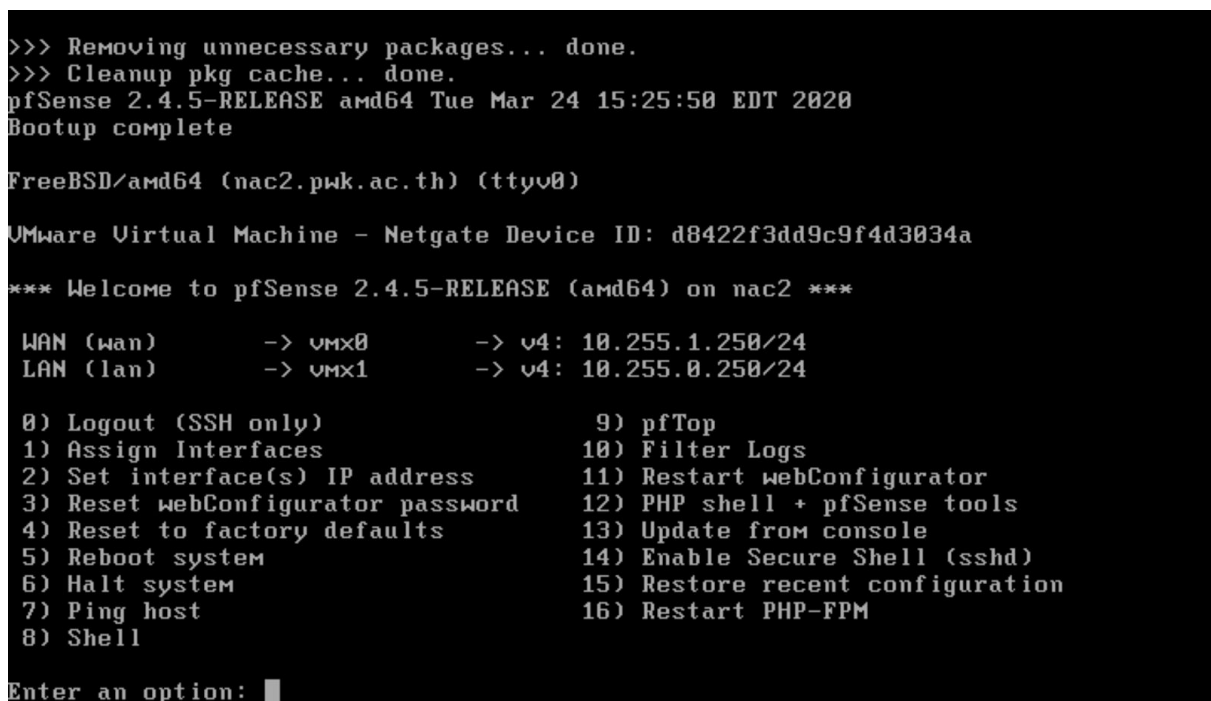
6. เลือก No เพื่อให้เครื่องทำการ Reboot



7. เครื่องทำการ Reboot



8. เมื่อทำการ Boot เสร็จก็กำหนดค่า IP Wan และ Lan ตามที่ใช้งาน



การกำหนดค่าในการเชื่อมกับ Server Radius

1. สร้าง Captive Portal ไปที่ Services -----> Captive Portal

Not Secure | 10.255.1.250/services_captiveportal_zones_edit.php

pfSense
COMMUNITY EDITION

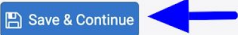
System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name PwkTest
Zone name. Can only contain letters, digits, and underscores (.) and may not start with a digit.

Zone description Pwk-NAC2020
A description may be entered here for administrative reference (not parsed).



ตั้งชื่อที่ต้องการแล้วกด Save & Continue

2. คลิกที่ enable Captive Portal จะได้ตามภาพและกำหนดค่าเบื้องต้น ซึ่งจะกำหนดตามตัวอย่างหรือปรับตามที่ต้องการได้

- ภาพที่ 2.1

Not Secure | 10.255.1.250/services_captiveportal_zones_edit.php

pfSense
COMMUNITY EDITION

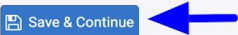
System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name PwkTest
Zone name. Can only contain letters, digits, and underscores (.) and may not start with a digit.

Zone description Pwk-NAC2020
A description may be entered here for administrative reference (not parsed).



- ภาพที่ 2.2

Not Secure | 10.255.1.250/services_captiveportal.php?zone=pwctest

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Captive Portal / PwkTest / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers File Manager

Captive Portal Configuration

Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="Pwk-NAC2020"/> A description may be entered here for administrative reference (not parsed).
Interfaces	<div><div>WAN</div><div>LAN</div></div> Select the interface(s) to enable for captive portal.
Maximum concurrent connections	<input type="text"/> Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)	<input type="text"/> Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)	<input type="text"/> Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Traffic quota (Megabytes)	<input type="text"/> Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately.

- ภาพที่ 2.3

ot Secure | 10.255.1.250/services_captiveportal.php?zone=pwctest

Waiting period to restore pass-through credits. (Hours)	<input type="text"/> Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.
Reset waiting period	<input type="checkbox"/> Enable waiting period reset on attempted access If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURLS variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
Concurrent user logins	<input type="checkbox"/> Disable Concurrent user logins If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.
Pass-through MAC Auto Entry	<input type="checkbox"/> Enable Pass-through MAC automatic additions When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.

- ภาพที่ 2.4

ot Secure | 10.255.1.250/services_captiveportal.php?zone=pwctest

- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server

PwkTest2020
Local Database

You can add a remote authentication server in the [User Manager](#).

Secondary authentication Server

PwkTest2020
Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

NAS Identifier

Specify a NAS identifier to override the default value (CaptivePortal-pwctest)

Reauthenticate Users

☒ Reauthenticate connected users every minute
If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

Session timeout

☒ Use RADIUS Session-Timeout attributes
When enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute.

Traffic quota

☒ Use RADIUS pfSense-Max-Total-Octets attribute
When enabled, clients will be disconnected after exceeding the amount of traffic, inclusive of both downloads and uploads, retrieved from the RADIUS pfSense-Max-Total-Octets attribute.

Per-user bandwidth restrictions

☒ Use RADIUS pfSense-Bandwidth-Max-Up and pfSense-Bandwidth-Max-Down attributes
When enabled, the bandwidth assigned to a client will be limited to the values retrieved from the RADIUS pfSense-Bandwidth-Max-Up and pfSense-Bandwidth-Max-Down attributes or from the comparable WISPr attributes.

- ภาพที่ 2.5

ot Secure | 10.255.1.250/services_captiveportal.php?zone=pwctest

Accounting

RADIUS

☒ Send RADIUS accounting packets.
If enabled, accounting request will be made for users identified against any RADIUS server.

Accounting Server

PwkTest2020

You can add a Radius Accounting server in the [User Manager](#).

Send accounting updates

☐ No updates ☐ Stop/Start ☐ Stop/Start (FreeRADIUS) ☒ Interim

This field set the way Accounting Updates should be done :
- If "No updates" is selected, then only one "Accounting Start" and one "Accounting Stop" request will be sent, when any user get connected and disconnected.
- If "Interim" is selected, then "Accounting Update" requests will be send regularly (every minute) to the RADIUS server, for each connected user.
- In some rare cases, you would like to simulate users to disconnect and reconnect every minute (eg, to send an Accounting Stop then an Accounting Start) instead of sending Accounting updates, this is the purpose of "Stop/Start" option. FreeRADIUS does not support this option very well, you should select "Stop/Start (FreeRADIUS)" instead.

Accounting style

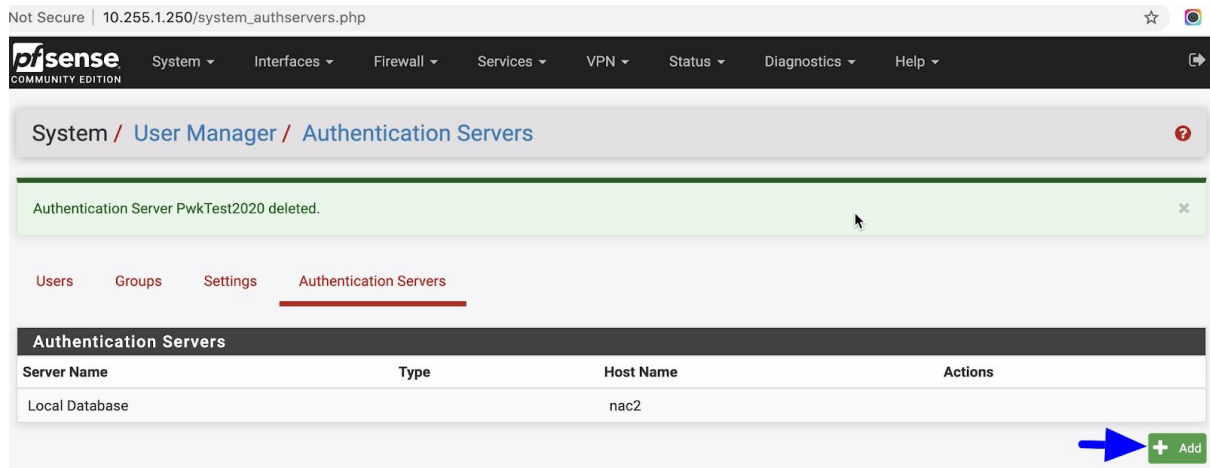
☒ Invert Acct-Input-Octets and Acct-Output-Octets
When enabled, data counts for RADIUS accounting packets will be taken from the client perspective, not the NAS. Acct-Input-Octets will represent download, and Acct-Output-Octets will represent upload.

Idle time accounting

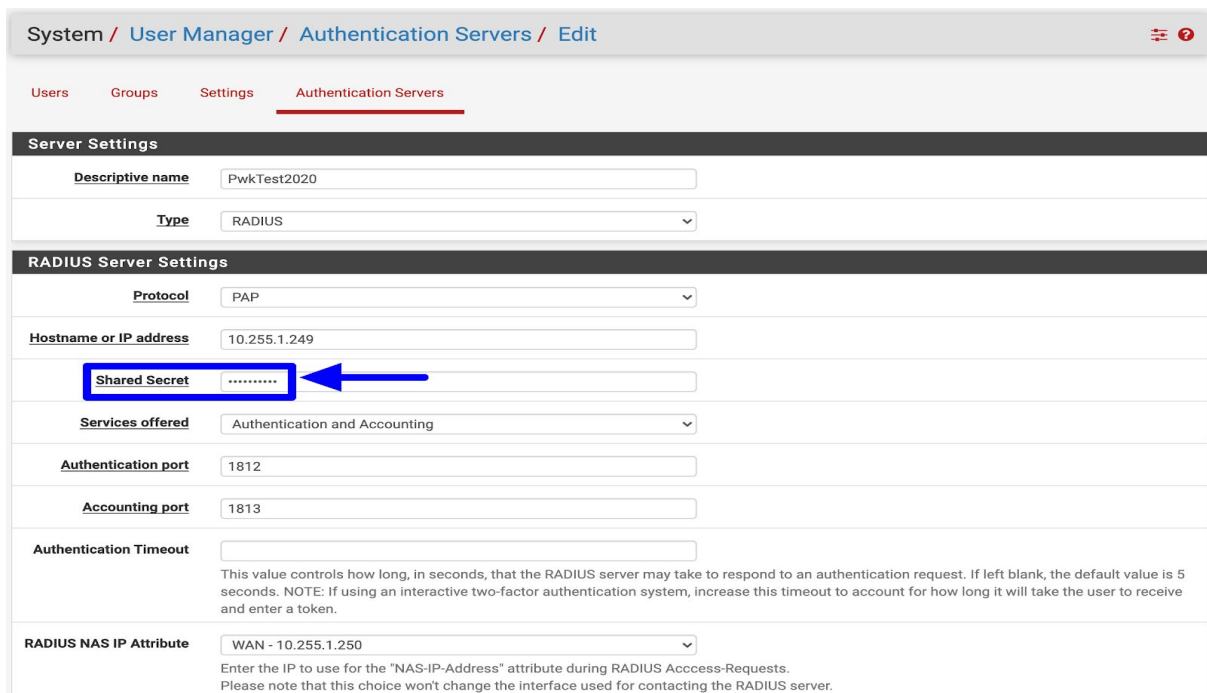
☒ Include idle time when users get disconnected due to idle timeout
This setting change the stop time that will be send in the Accounting Stop request, when a user get disconnected after exceeding the idle timeout. If not checked, the sent stop time will be the last activity time.

3. กำหนด Authentication Server ให้กดที่ User Manager ตามภาพที่ 2.4

3.1 เลือก Authentication Servers แล้วกดที่ Add



3.2 ตั้งค่าตามตัวอย่าง และตรง Shares Secret กำหนดให้ตรงกับ Radius Server ในที่นี้จะกำหนดเป็น testing123 สุดท้ายกด Save



3.3 ไปที่ Diagnostic -----> Authentication จะได้ตามภาพล่าง ทำการทดสอบ Authen โดยใช้ User ใน Radius Server

Not Secure | 10.255.1.250/diag_authentication.php

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Diagnostics / Authentication

User admin authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server PwkTest2020
Select the authentication server to test against.

Username admin

Password

Test

4. การจัดการหน้า Login ใน Captive Portal

4.1 เลือก Services -----> Captive Portal



Not Secure | 10.255.1.250/services_captiveportal_zones.php

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
PwkTest	LAN	0	Pwk-NAC2020	 

+ Add

4.2 กดแก้ไข จากนั้นเลือกแถบ File Manger แล้วกด Add

Not Secure | 10.255.1.250/services_captiveportal_filemanager.php?zone=pwktest

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / PwkTest / File Manager

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers **File Manager**

Installed Files

Name	Size	Actions
------	------	---------

+ Add

4.3 ทำการ upload ไฟล์หน้า Login ที่จัดเตรียมไว้จนครบ

Services / Captive Portal / PwkTest / File Manager

Configuration

MACs

Allowed IP Addresses

Allowed Hostnames

Vouchers

File Manager

Installed Files

Name	Size	Actions
captiveportal-avatar.png	82 KiB	
captiveportal-error.html	19 KiB	
captiveportal-img-01.png	82 KiB	
captiveportal-jquery-3.2.1.min.js	85 KiB	
captiveportal-Kanit-Regular.ttf	157 KiB	
captiveportal-logout.html	22 KiB	
captiveportal-portal.html	19 KiB	
Total	465 KiB	

+ Add

4.3 เลือกแถบ Configuration เพื่อกำหนดหน้า Login โดยที่ไป enable to use a custom captive portal login page จากนั้นเลือกไฟล์เพื่อกำหนด Portal page contents , Auth error page contents , Logout page contents แล้วเลื่อนมาล่างสุด กด Save

Use custom captive portal page ☒ Enable to use a custom captive portal login page
If set a portal.html page must be created and uploaded. If unchecked the default template will be used

HTML Page Contents

Portal page contents portal.html

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL_ACTION\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.
Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="zone" type="hidden" value="$PORTAL_ZONE$">
  <input name="accept" type="submit" value="Continue">
</form>
```

ส่วนที่ต้องกำหนด

Auth error page contents error.html

The contents of the HTML/PHP file that is uploaded here are displayed when an authentication error occurs. It may include "\$PORTAL_MESSAGE\$", which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout page contents logout.html

The contents of the HTML/PHP file that is uploaded here are displayed on authentication success when the logout popup is enabled.

4.4 ตรวจสอบสถานะการทำงานของ captive portal โดยไปที่ Status ---> Services

Not Secure 10.255.1.250/status_services.php			
pfSense COMMUNITY EDITION			
System	Interfaces	Firewall	Services
VPN	Status	Diagnostics	Help
Status / Services			
Services			
Service	Description	Status	Actions
captiveportal	Captive Portal: PwkTest	✓	
dpinger	Gateway Monitoring Daemon	✓	
ntpd	NTP clock sync	✓	
syslogd	System Logger Daemon	✓	
unbound	DNS Resolver	✓	