

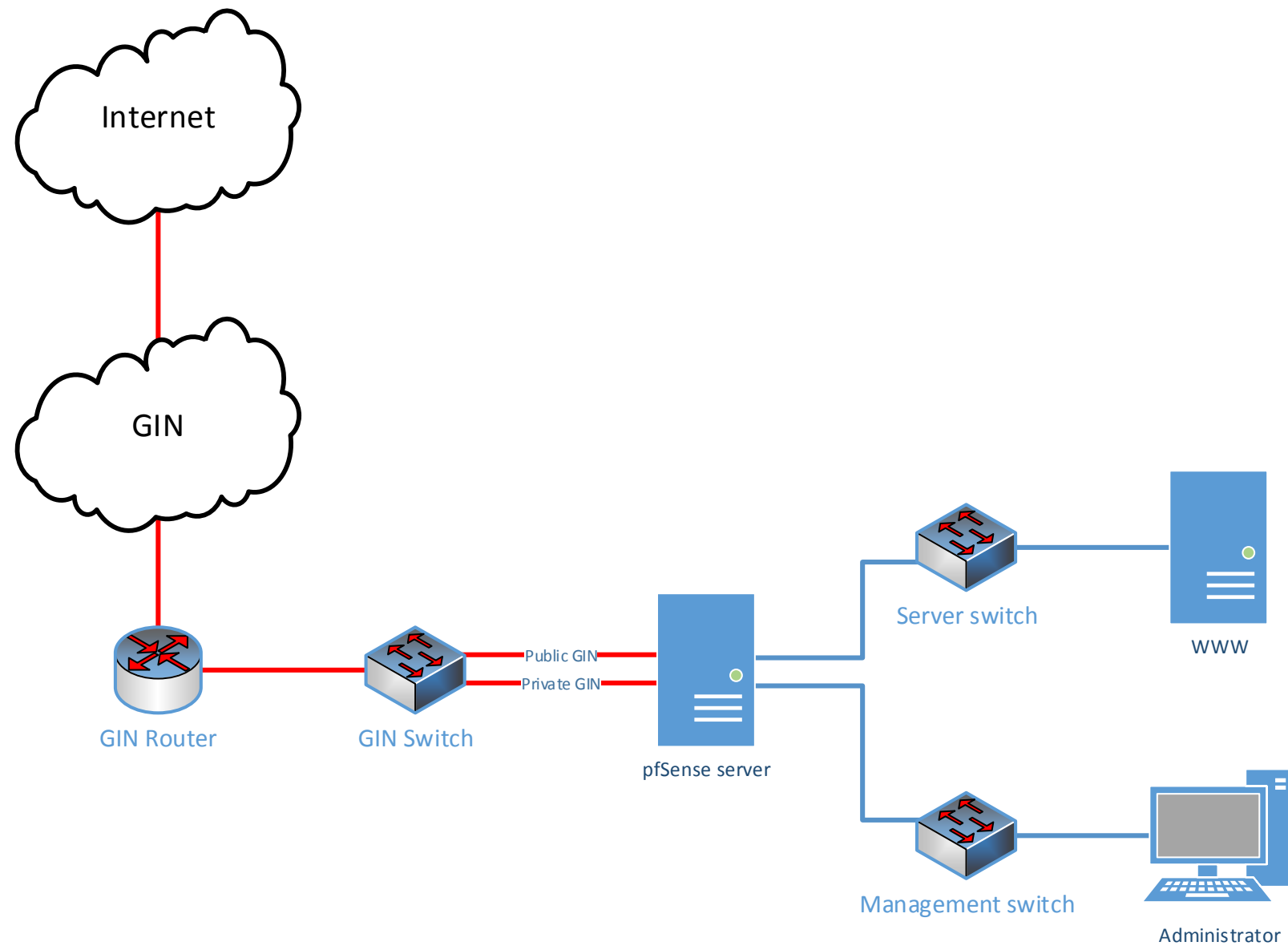
# การใช้งาน pfSense ร่วมกับระบบเครือข่าย GIN

คมกริช คำสวัสดิ์

วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส  
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)



# ผังการเชื่อมต่อระบบเครือข่าย GIN



# การติดตั้ง pfSense



# การติดตั้ง pfSense

```
32-bit compatibility ldconfig path: /usr/lib32
done.
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

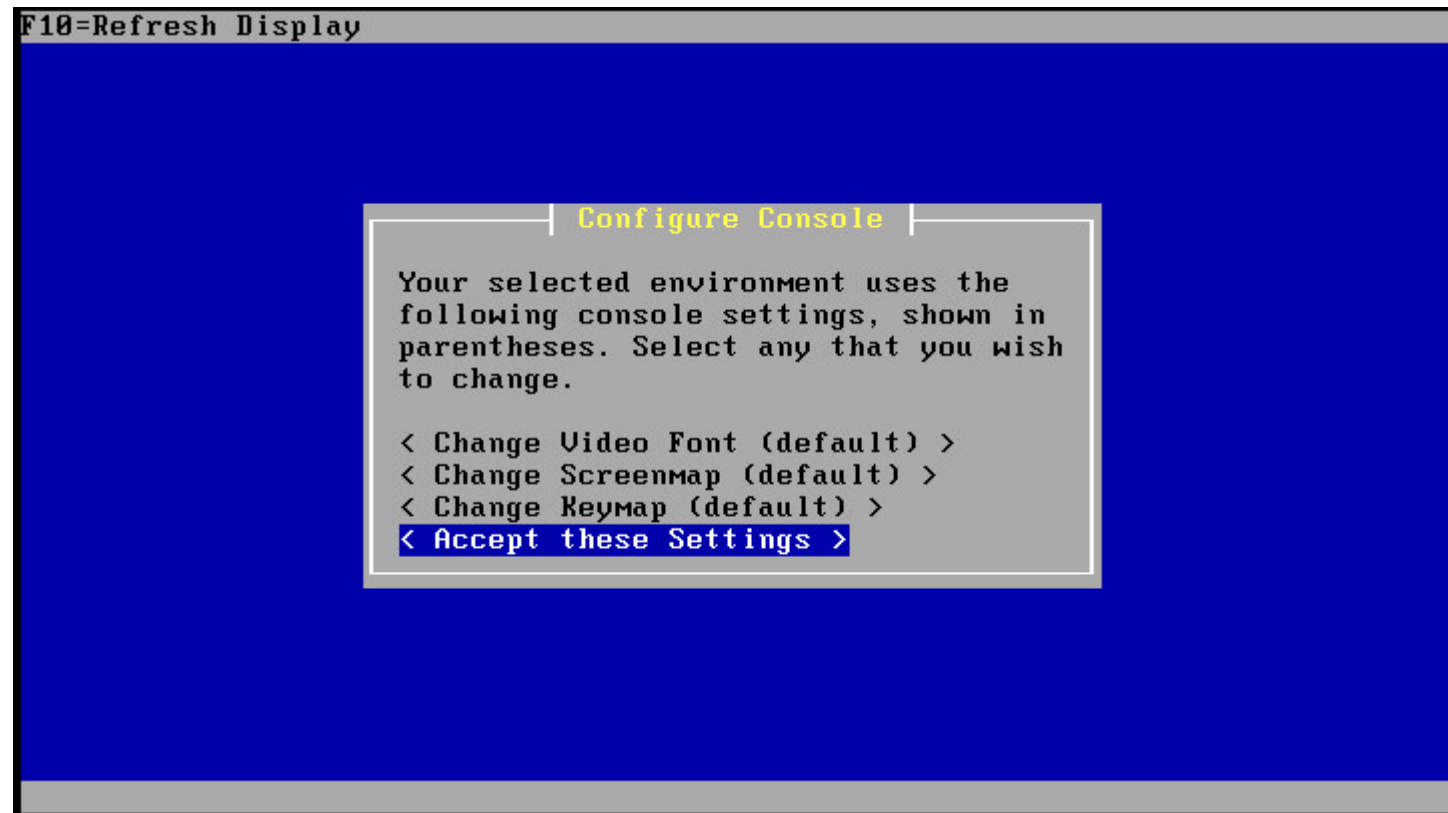
(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C) continues the LiveCD bootup without further pause.
Timeout before auto boot continues (seconds): 8i
Installer mode selected...
Launching pfSense Installer...

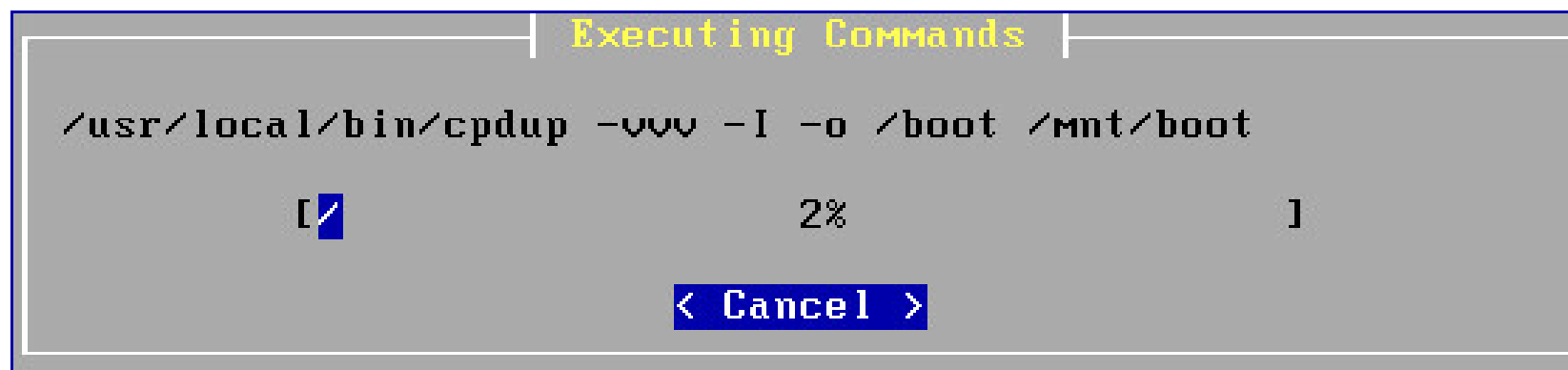
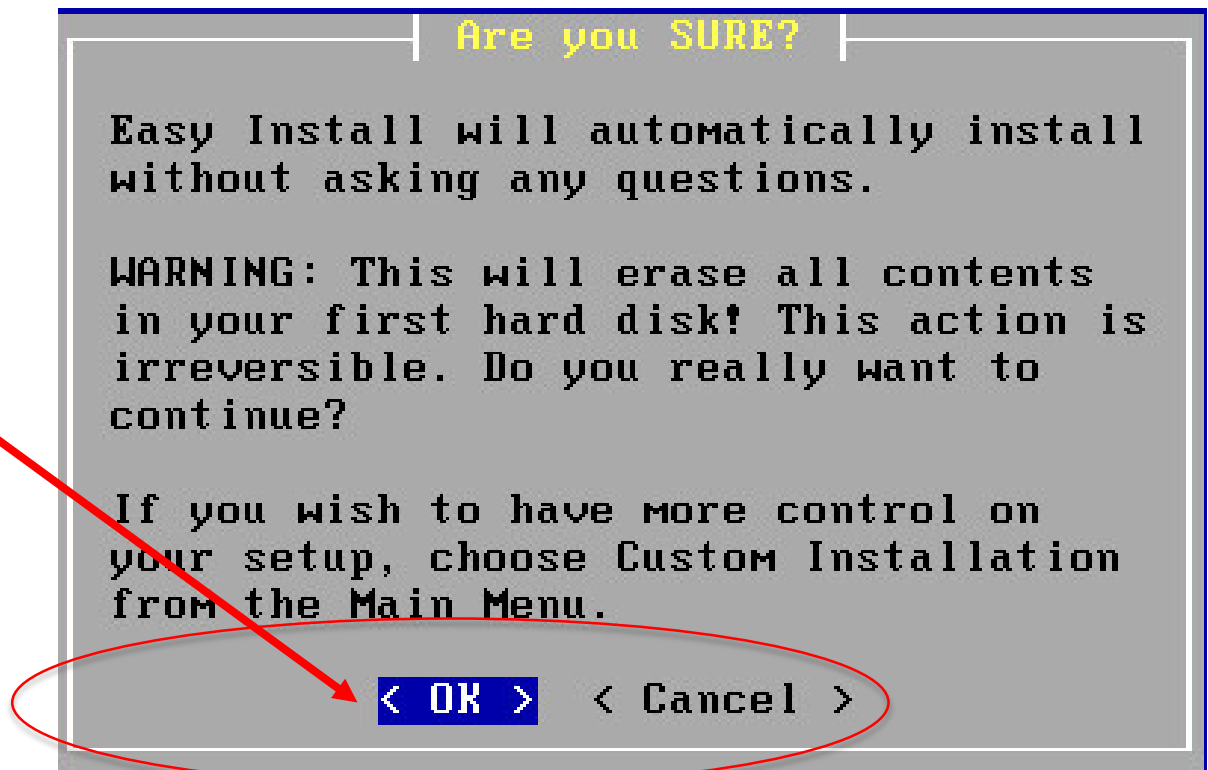
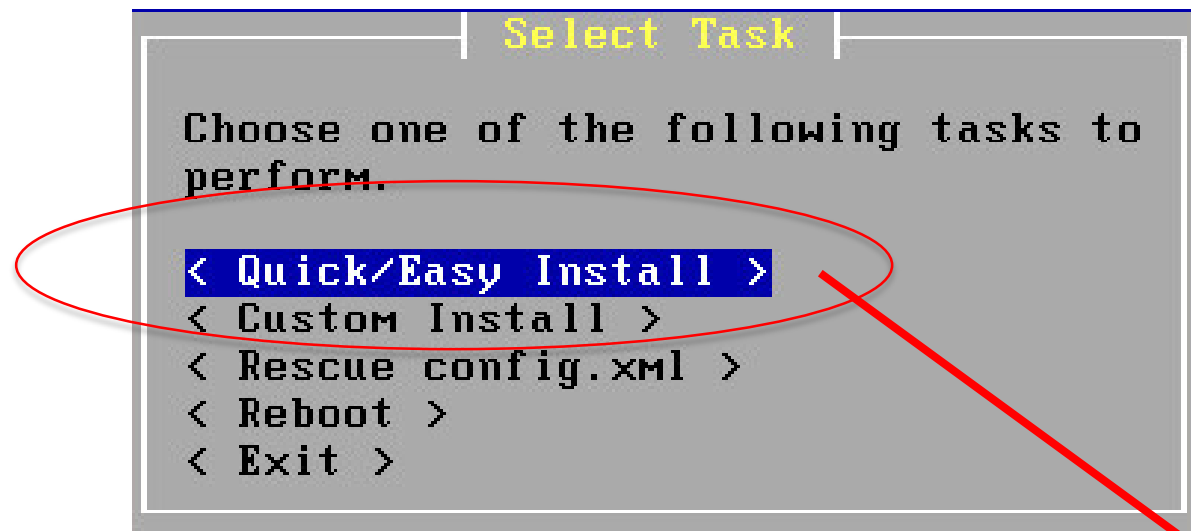
kern.geom.debugflags: 0 -> 16
VMware detected. The installer will make changes to tune this host....
```

กด i

# การติดตั้ง pfSense



# การติดตั้ง pfSense



# การติดตั้ง pfSense

## Install Kernel

You may now wish to install a custom Kernel configuration.

< Standard Kernel >

< Embedded kernel (no VGA console, keyboard) >

## Executing Commands

```
if [ -f /etc/installed_filesystem.mtree ]; then /usr/sb...
```

[ 95% ]

< Cancel >

## Reboot

This machine is about to be shut down. After the machine has reached its shutdown state, you may remove the CD from the CD-ROM drive tray and press Enter to reboot from the HDD.

< Reboot > < Return to Select Task >

# การติดตั้ง pfSense

pfSense is now rebooting

After the reboot is complete, open a web browser and enter `https://192.168.1.1` (or the LAN IP Address) in the location bar.

You might need to acknowledge the HTTPS certificate if your browser reports it as untrusted. This is normal as a self-signed certificate is used by default.

\*DEFAULT Username\*: admin  
\*DEFAULT Password\*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.  
Rebooting in 4 seconds. CTRL-C to abort.  
Rebooting in 3 seconds. CTRL-C to abort.  
Rebooting in 2 seconds. CTRL-C to abort.  
Rebooting in 1 second.. CTRL-C to abort.

pfSense is now rebooting.





# การติดตั้ง pfSense

```
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.2.2-RELEASE amd64 Mon Apr 13 20:10:22 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)          -> em0          ->
LAN (lan)           -> em1          -> v4: 192.168.1.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

# การกำหนด Network Interface

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
```

```
*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      ->
```

```
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
```

```
0) Logout (SSH only)
```

```
9) pfTop
```

```
1) Assign Interfaces
```

```
10) Filter Logs
```

```
2) Set interface(s) IP address
```

```
11) Restart webConfigurator
```

```
3) Reset webConfigurator password
```

```
12) pfSense Developer Shell
```

```
4) Reset to factory defaults
```

```
13) Upgrade from console
```

```
5) Reboot system
```

```
14) Enable Secure Shell (sshd)
```

```
6) Halt system
```

```
15) Restore recent configuration
```

```
7) Ping host
```

```
16) Restart PHP-FPM
```

```
8) Shell
```

```
Enter an option: 1█
```

# การกำหนด Network Interface

Valid interfaces are:

```
em0      00:0c:29:2a:1b:54    (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em1      00:0c:29:2a:1b:5e    (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em2      00:0c:29:2a:1b:68    (down) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em3      00:0c:29:2a:1b:72    (down) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
```

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y:n]? n

# การกำหนด Network Interface

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]? n

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(or nothing if finished): em2

Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> em0  
LAN -> em2

Do you want to proceed [y!n]? y

# การกำหนด Network Interface

```
The interfaces will be assigned as follows:
```

```
WAN -> em0
```

```
LAN -> em2
```

```
Do you want to proceed [y|n]?y
```

```
Writing configuration...done.
```

```
One moment while we reload the settings... done!
```

```
*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***
```

```
WAN (wan) -> em0 ->
```

```
LAN (lan) -> em2 -> v4: 192.168.1.1/24
```

```
0) Logout (SSH only)
```

```
9) pfTop
```

```
1) Assign Interfaces
```

```
10) Filter Logs
```

```
2) Set interface(s) IP address
```

```
11) Restart webConfigurator
```

```
3) Reset webConfigurator password
```

```
12) pfSense Developer Shell
```

```
4) Reset to factory defaults
```

```
13) Upgrade from console
```

```
5) Reboot system
```

```
14) Enable Secure Shell (sshd)
```

```
6) Halt system
```

```
15) Restore recent configuration
```

```
7) Ping host
```

```
16) Restart PHP-FPM
```

```
8) Shell
```

```
Enter an option: █
```

# การกำหนด IP address ให้ WAN Interface

```
*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em2      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em2 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n
```

# การกำหนด IP address ให้ WAN Interface

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
```

```
> 123.242.1.2
```

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
```

```
e.g. 255.255.255.0 = 24
```

```
     255.255.0.0   = 16
```

```
     255.0.0.0     = 8
```

```
Enter the new WAN IPv4 subnet bit count (1 to 31):
```

```
> 24
```

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
```

```
For a LAN, press <ENTER> for none:
```

```
> 123.242.1.1
```

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n
```

```
Enter the new WAN IPv6 address. Press <ENTER> for none:
```

```
>
```

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

# การกำหนด IP address ให้ WAN Interface

```
Please wait while the changes are saved to WAN...
```

```
Reloading filter...
```

```
Reloading routing configuration...
```

```
DHCPD...
```

```
The IPv4 WAN address has been set to 123.242.1.2/24
```

```
Press <ENTER> to continue.
```

```
*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4: 123.242.1.2/24
LAN (lan)      -> em2      -> v4: 192.168.1.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

```
Enter an option: █
```



# การกำหนด IP address ให้ LAN Interface

Enter an option: 2

Available interfaces:

- 1 - WAN (em0 - static)
- 2 - LAN (em2 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:

> 172.17.12.151

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.

e.g. 255.255.255.0 = 24

255.255.0.0 = 16

255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):

> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

> █

# การกำหนด IP address ให้ LAN Interface

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 172.17.12.151/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://172.17.12.151/

Press <ENTER> to continue. █
```

# การกำหนด IP address ให้ LAN Interface

```
The IPv4 LAN address has been set to 172.17.12.151/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://172.17.12.151/
```

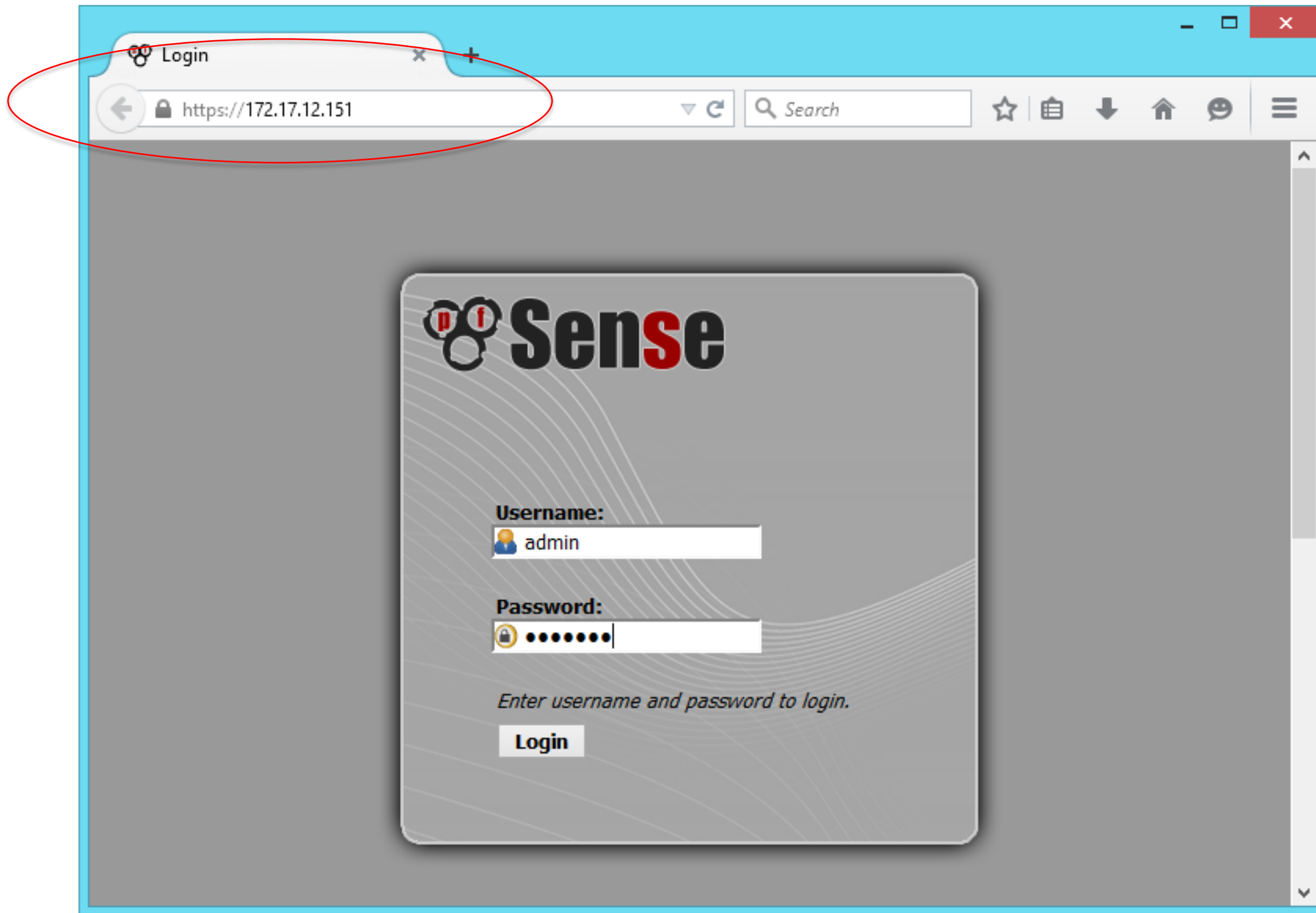
```
Press <ENTER> to continue.
```

```
*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***
```

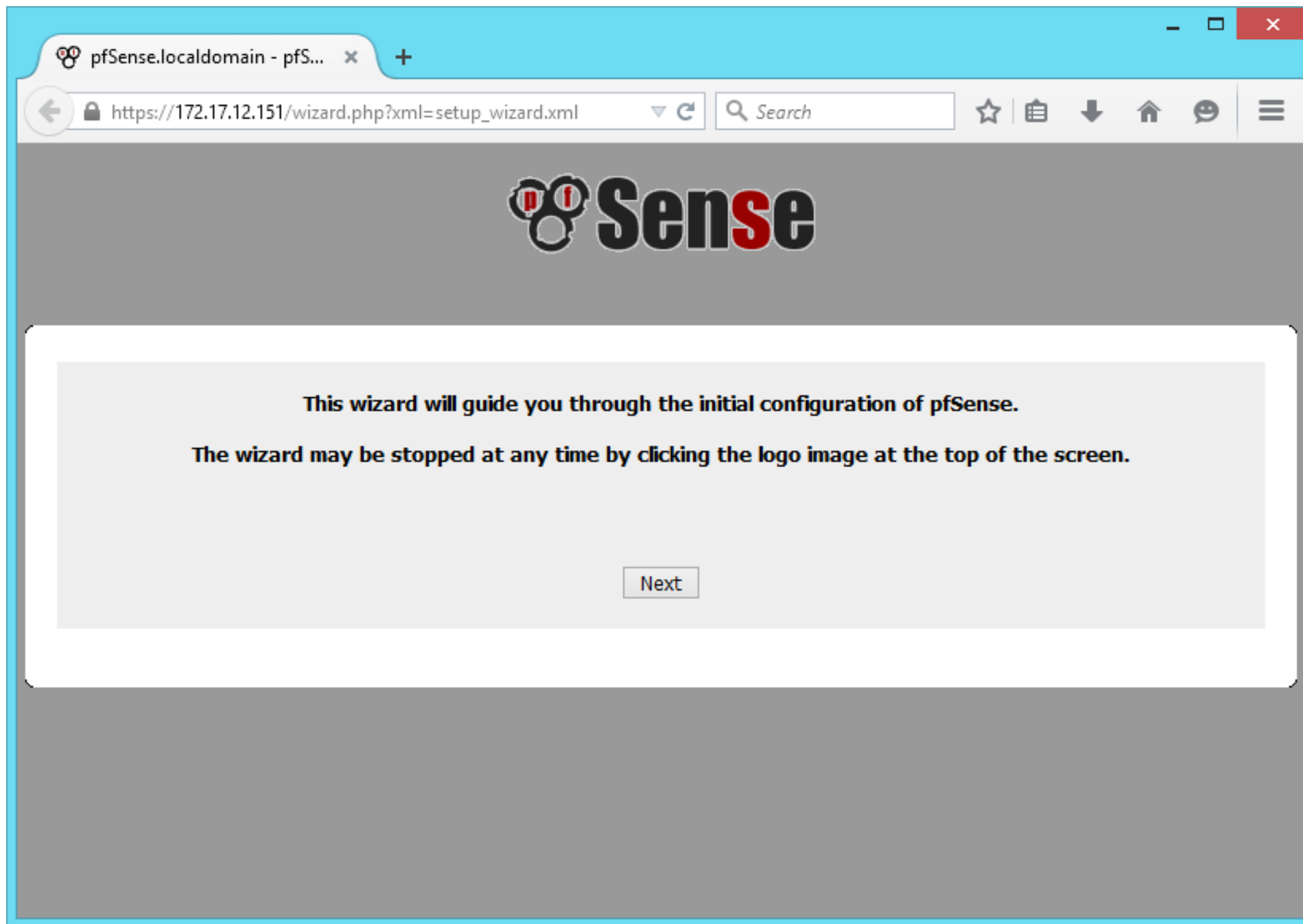
```
WAN (wan)      -> em0      -> v4: 123.242.1.2/24
LAN (lan)      -> em2      -> v4: 172.17.12.151/24
0) Logout (SSH only)      9) pfTop
1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
```

```
Enter an option: █
```

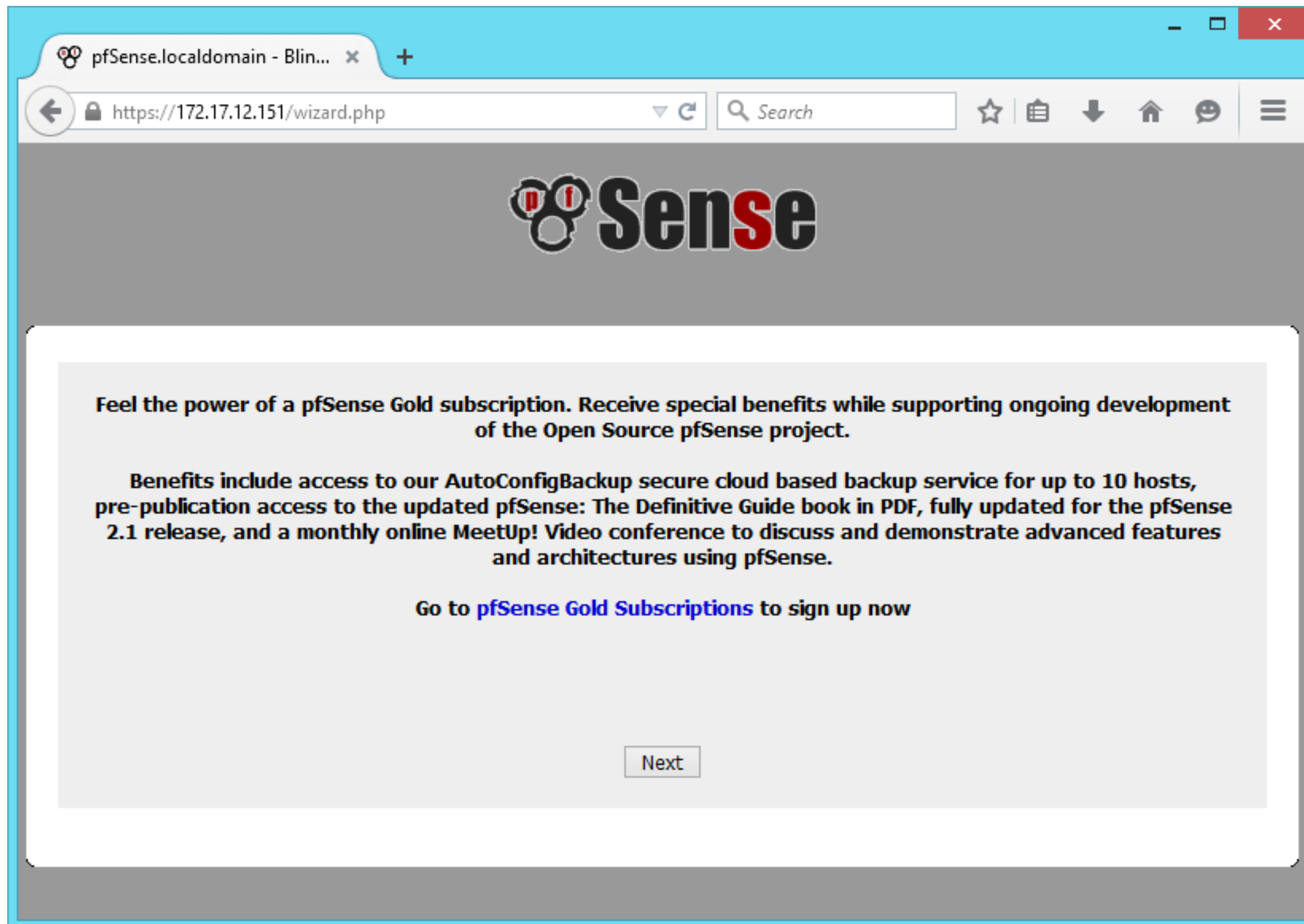
# การเข้าใช้งาน pfSense



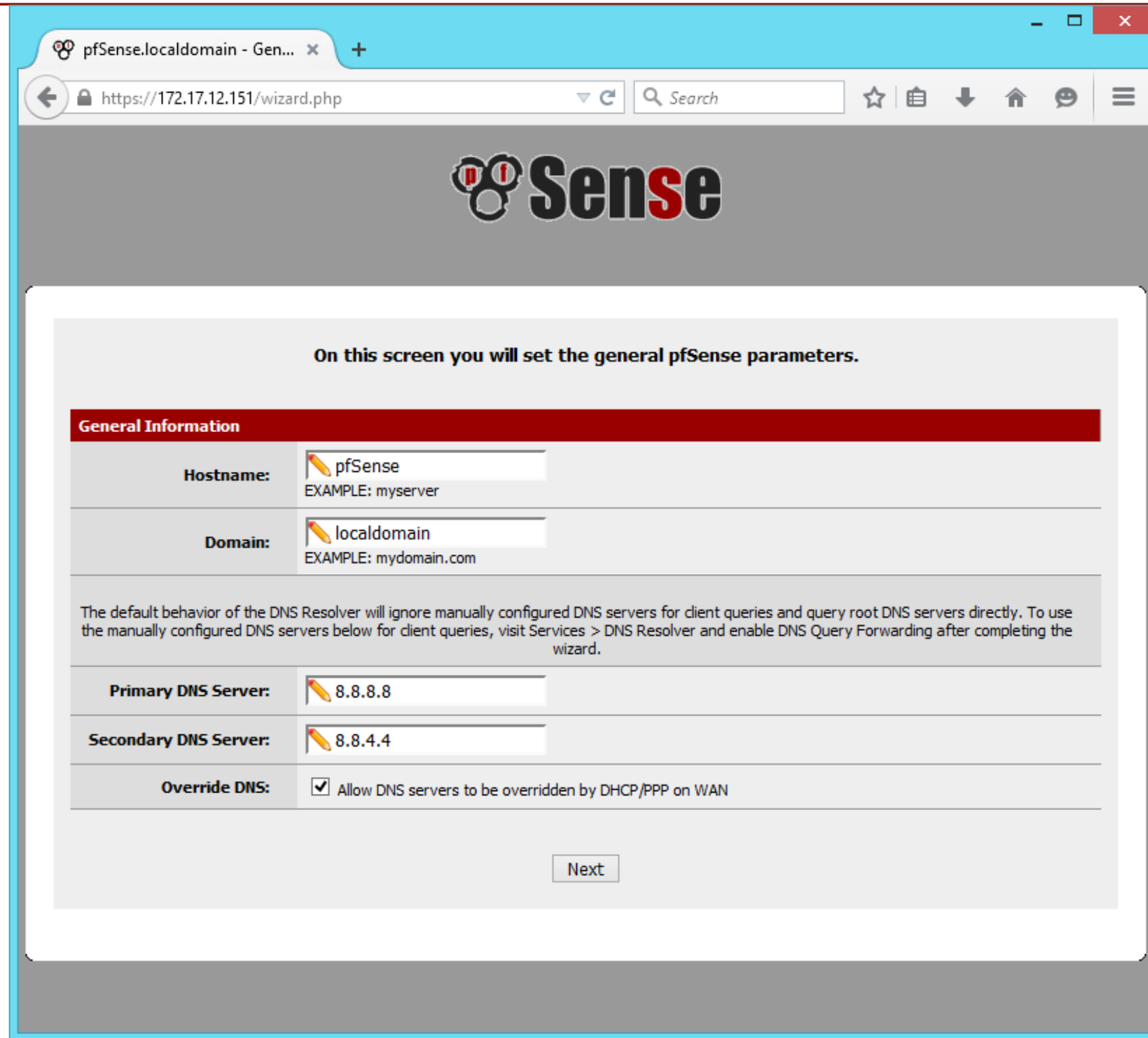
# การเข้าใช้งาน pfSense



# การเข้าใช้งาน pfSense



# การเข้าใช้งาน pfSense



The screenshot shows a web browser window with the address bar displaying "https://172.17.12.151/wizard.php". The page features the pfSense logo at the top. Below the logo, a message states: "On this screen you will set the general pfSense parameters." The main content area is titled "General Information" and contains the following fields:

Hostname:	<input type="text" value="pfSense"/> <small>EXAMPLE: myserver</small>
Domain:	<input type="text" value="localdomain"/> <small>EXAMPLE: mydomain.com</small>
<p>The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services &gt; DNS Resolver and enable DNS Query Forwarding after completing the wizard.</p>	
Primary DNS Server:	<input type="text" value="8.8.8.8"/>
Secondary DNS Server:	<input type="text" value="8.8.4.4"/>
Override DNS:	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

A "Next" button is located at the bottom right of the form.

# การใช้งาน pfSense

Please enter the time, date and time zone.

Time Server Information	
Time server hostname:	<input type="text" value="time.navy.mi.th"/> <small>Enter the hostname (FQDN) of the time server.</small>
Timezone:	<input type="text" value="Asia/Bangkok"/>

Next



# การเข้าใช้งาน pfSense

เอาเครื่องหมายออก

On this screen we will configure the Wide Area Network information.

**Configure WAN Interface**

Selected Type: Static

**General configuration**

MAC Address:

MTU:

MSS:

**Static IP Configuration**

IP Address:  / 24

Upstream Gateway:

**DHCP client configuration**

DHCP Hostname:

**PPPoE configuration**

PPPoE Username:

PPPoE Password:

PPPoE Service name:

PPPoE Dial on demand: ☐

PPPoE Idle timeout:

**PPTP configuration**

PPTP Username:

PPTP Password:

PPTP Local IP Address:  / 1

PPTP Remote IP Address:

PPTP Dial on demand: ☐

PPTP Idle timeout:

**RFC1918 Networks**

Block RFC1918 Private Networks: ☐

**Block bogon networks**

Block bogon networks: ☐

Next

**RFC1918 Networks**

Block RFC1918 Private Networks: ☐

**Block bogon networks**

Block bogon networks: ☐

Next

# การใช้งาน pfSense

On this screen we will configure the Local Area Network information.

**Configure LAN Interface**

LAN IP Address:   
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

Next

On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

**Set Admin WebGUI Password**

Admin Password:

Admin Password AGAIN:

Next

Click 'Reload' to reload pfSense with new changes.

Reload

Congratulations! pfSense is now configured.  
Please consider contributing back to the project!  
Click [here](#) to purchase services offered by the pfSense team and find other ways to contribute.  
Click [here](#) to continue on to pfSense webConfigurator.

Wizard completed.

# การเข้าใช้งาน pfSense

pfSense.localdomain - Stat... x +

https://172.17.12.151

pfSense.localdomain

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

## Status: Dashboard

### System Information

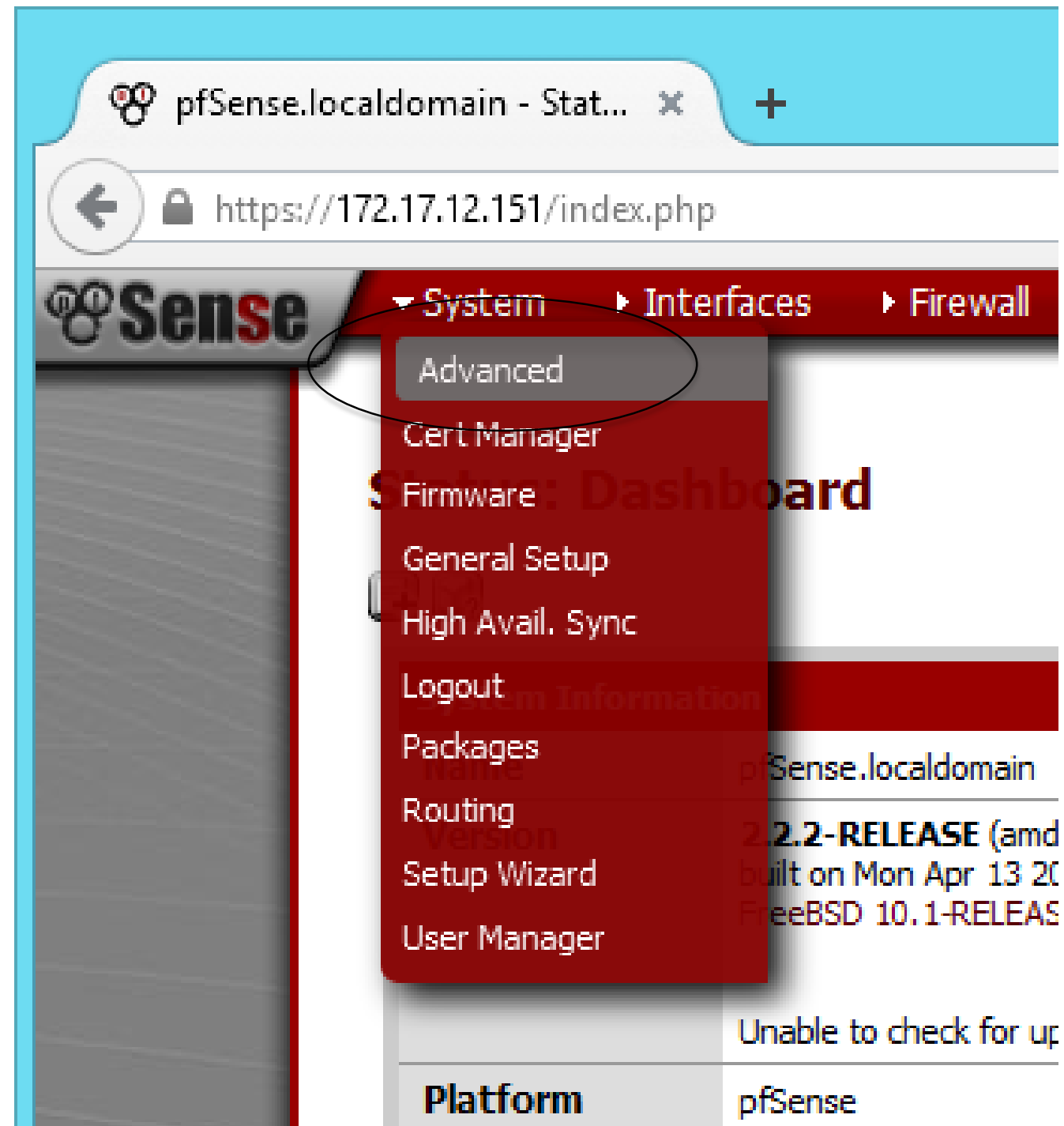
Name	pfSense.localdomain
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9  Unable to check for updates.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz Current: 333 MHz, Max: 2666 MHz 2 CPUs: 1 package(s) x 2 core(s)
Uptime	00 Hour 32 Minutes 07 Seconds
Current date/time	Sat May 16 17:28:56 ICT 2015
DNS server(s)	127.0.0.1 8.8.8.8 8.8.4.4
Last config change	Sat May 16 17:25:32 ICT 2015
State table size	0% (114/98000) <a href="#">Show states</a>
MBUF Usage	4% (1016/26584)
Load average	0.07, 0.04, 0.00
CPU usage	0%
Memory usage	12% of 989 MB
SWAP usage	0% of 2047 MB
Disk usage	/ (ufs): 5% of 5.8G /var/run (ufs in RAM): 3% of 3.4M

### Interfaces

WAN	↑	1000baseT <full-duplex> 123.242.1.2
LAN	↑	1000baseT <full-duplex> 172.17.12.151

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

# การเปลี่ยน Management port (TCP/443 --> TCP/8443)



# การเปลี่ยน Management port (TCP/443 --> TCP/8443)

## System: Advanced: Admin Access



Admin Access Firewall / NAT Networking Miscellaneous System Tunables Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

### webConfigurator

Protocol ☐ HTTP ☒ HTTPS

SSL Certificate webConfigurator default (55570eee93664)

TCP port   
Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes   
Enter the number of webConfigurator processes you want to run. This defaults to 2. It allows multiple users/browsers to access the GUI concurrently.

แก้เป็น 8443

### Console Options

Console menu ☐ Password protect the console menu

Save

## System: Advanced: Admin Access



The changes have been applied successfully.  
One moment...redirecting to [https://172.17.12.151:8443/system\\_advanced\\_admin.php](https://172.17.12.151:8443/system_advanced_admin.php) in 20 seconds.

Close

Admin Access Firewall / NAT Networking Miscellaneous System Tunables Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

### webConfigurator

Protocol ☐ HTTP ☒ HTTPS

SSL Certificate webConfigurator default (55570eee93664)

TCP port   
Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.



# การกำหนด Network Interface

The screenshot shows the pfSense web interface at `https://172.17.12.151:8443/index.php`. The navigation menu includes System, Interfaces, Firewall, and Services. The 'Interfaces' menu is expanded, showing options like (assign), LAN, and WAN. The main content area is titled 'Interfaces: Assign network ports' and features tabs for Interface assignments, Interface Groups, Wireless, VLANs, QinQs, PPPs, GRE, GIF, Bridges, and LAGG. The 'Interface assignments' tab is active, displaying a table with columns 'Interface' and 'Network port'. The table lists WAN assigned to em0 (00:0c:29:2a:1b:54) and LAN assigned to em2 (00:0c:29:2a:1b:68). Below the table, 'Available network ports' lists em1 (00:0c:29:2a:1b:5e). A red notification bar at the bottom states 'Interface has been added.' with a 'Close' button. An arrow points from the '+' icon in the available ports list to the updated table below.

Interface	Network port
<a href="#">WAN</a>	em0 (00:0c:29:2a:1b:54) ▼
<a href="#">LAN</a>	em2 (00:0c:29:2a:1b:68) ▼

Available network ports:

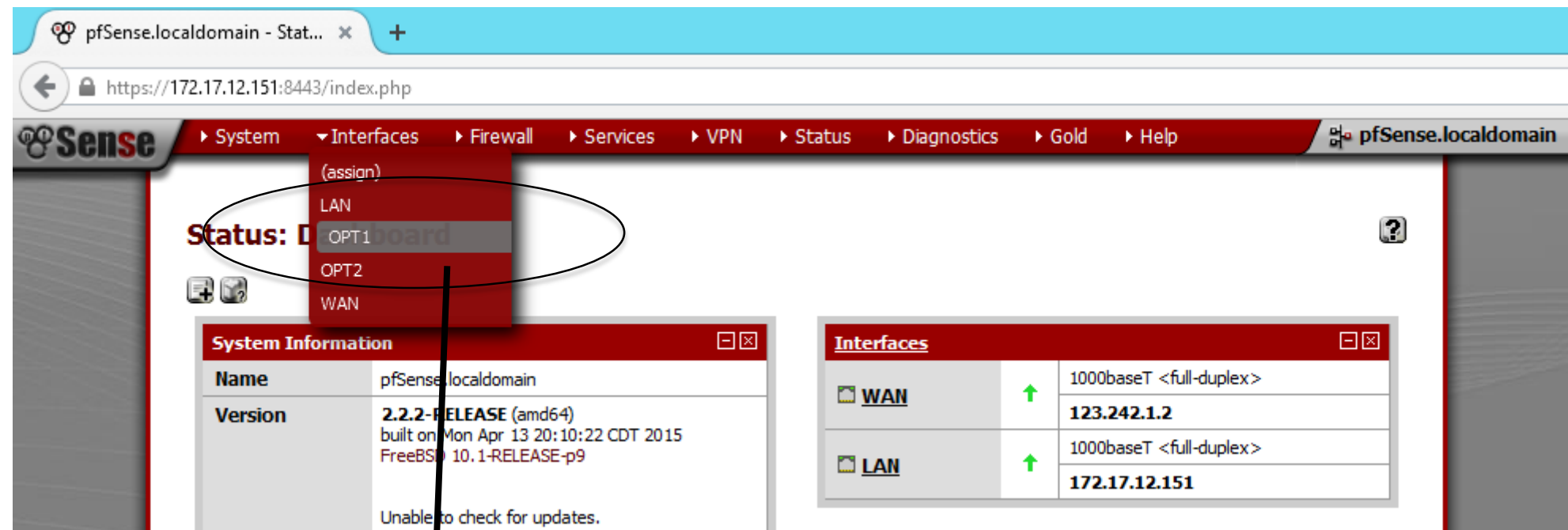
Network port
em1 (00:0c:29:2a:1b:5e) ▼

Interface has been added. [Close]

Interface	Network port
<a href="#">WAN</a>	em0 (00:0c:29:2a:1b:54) ▼
<a href="#">LAN</a>	em2 (00:0c:29:2a:1b:68) ▼
<a href="#">OPT1</a>	em1 (00:0c:29:2a:1b:5e) ▼
<a href="#">OPT2</a>	em3 (00:0c:29:2a:1b:72) ▼



# การเปลี่ยนชื่อ Interface (Network Zone) และการตั้งค่าให้ Interface



## Interfaces: OPT1

**General configuration**

Enable ☐ Enable Interface

Save Cancel

# การเปลี่ยนชื่อ Interface (Network Zone) และการตั้งค่าให้ Interface

## Interfaces: OPT1



### General configuration

Enable	<input checked="" type="checkbox"/> <b>Enable Interface</b>
Description	<input type="text" value="GIN_Private"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4 ▾
IPv6 Configuration Type	None ▾
MAC address	<input type="text"/> <small>Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank</small>
MTU	<input type="text"/> <small>If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.</small>
Speed and duplex	Advanced - Show advanced option

### Static IPv4 configuration

IPv4 address	<input type="text" value="10.0.1.1"/> / 24 ▾
IPv4 Upstream Gateway	None ▾ - or <b>add a new one.</b> <small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above. On local LANs the upstream gateway should be "none".</small>

### Private networks

<input type="checkbox"/> <b>Block private networks</b> <small>When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.</small>
<input type="checkbox"/> <b>Block bogon networks</b> <small>When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.</small>
<small>Note: The update frequency can be changed under System-&gt;Advanced Firewall/NAT settings.</small>



# การเปลี่ยนชื่อ Interface (Network Zone) และการตั้งค่าให้ Interface

## Interfaces: GIN\_Private



The GIN\_Private configuration has been changed.

You must apply the changes in order for them to take effect.

Don't forget to adjust the DHCP Server range if needed after applying.

Apply changes

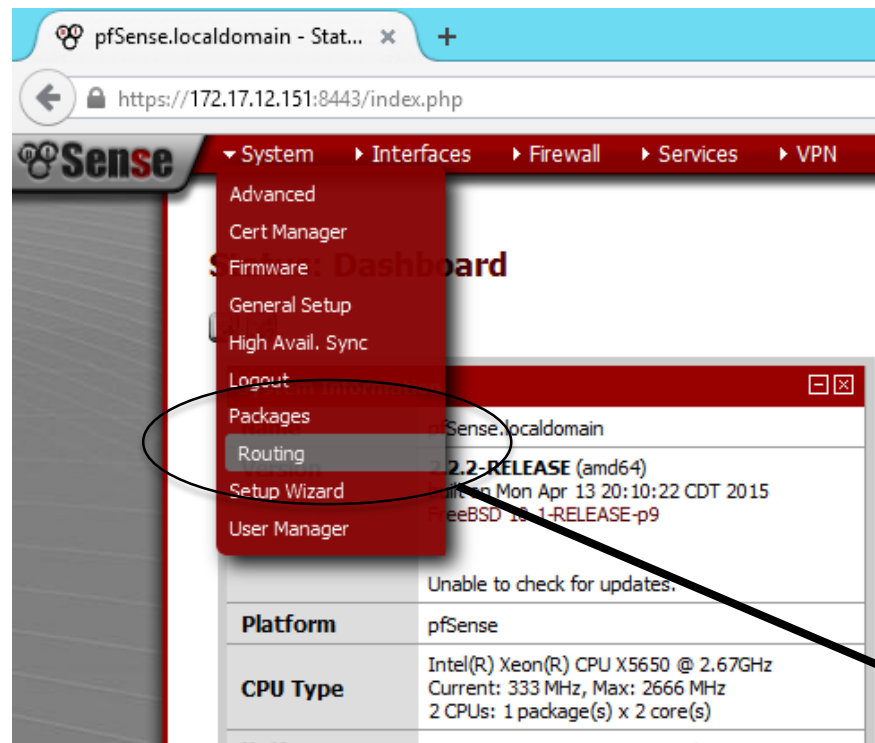
## Status: Dashboard



System Information	
Name	pfSense.localdomain
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9  Obtaining update status ...
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz Current: 333 MHz, Max: 2666 MHz 2 CPUs: 1 package(s) x 2 core(s)

Interfaces		
WAN	↑	1000baseT <full-duplex> <b>123.242.1.2</b>
LAN	↑	1000baseT <full-duplex> <b>172.17.12.151</b>
GIN_PRIVATE	↑	1000baseT <full-duplex> <b>10.0.1.1</b>

# การกำหนด Routing table สำหรับ Private GIN




## System: Gateways



Gateways

Routes

Groups

Name	Interface	Gateway	Monitor IP	Description
<input type="checkbox"/>  GW_WAN (default)	GIN_PUBLIC	123.242.1.1	123.242.1.1	Interface wan Gateway



# การกำหนด Routing table สำหรับ Private GIN

## System: Gateways: Edit gateway



Edit gateway	
Disabled	<input type="checkbox"/> <b>Disable this gateway</b> Set this option to disable this gateway without removing it from the list.
Interface	<input type="text" value="GIN_PRIVATE"/> Choose which interface this gateway applies to.
Address Family	<input type="text" value="IPv4"/> Choose the Internet Protocol this gateway uses.
Name	<input type="text" value="GIN_Private_GW"/> Gateway name
Gateway	<input type="text" value="10.0.1.254"/> Gateway IP address
Default Gateway	<input type="checkbox"/> <b>Default Gateway</b> This will select the above gateway as the default gateway
Disable Gateway Monitoring	<input type="checkbox"/> <b>Disable Gateway Monitoring</b> This will consider this gateway as always being up
Monitor IP	<input type="text"/> <b>Alternative monitor IP</b> Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Mark Gateway as Down	<input type="checkbox"/> <b>Mark Gateway as Down</b> This will force this gateway to be considered Down
Advanced	<input type="button" value="Advanced"/> - Show advanced option
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

# การกำหนด Routing table สำหรับ Private GIN

## System: Gateways



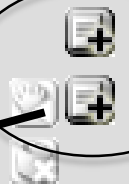
The gateway configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes

### Gateways Routes Groups

	Name	Interface	Gateway	Monitor IP	Description	
<input type="checkbox"/>	<input checked="" type="checkbox"/> GW_WAN (default)	GIN_PUBLIC	123.242.1.1	123.242.1.1	Interface wan Gateway	     
<input type="checkbox"/>	<input checked="" type="checkbox"/> GIN_Private_GW	GIN_PRIVATE	10.0.1.254	10.0.1.254		  


# การกำหนด Routing table สำหรับ Private GIN

Gateways Routes Groups			
Network	Gateway	Interface	Description
			

## System: Static Routes: Edit route

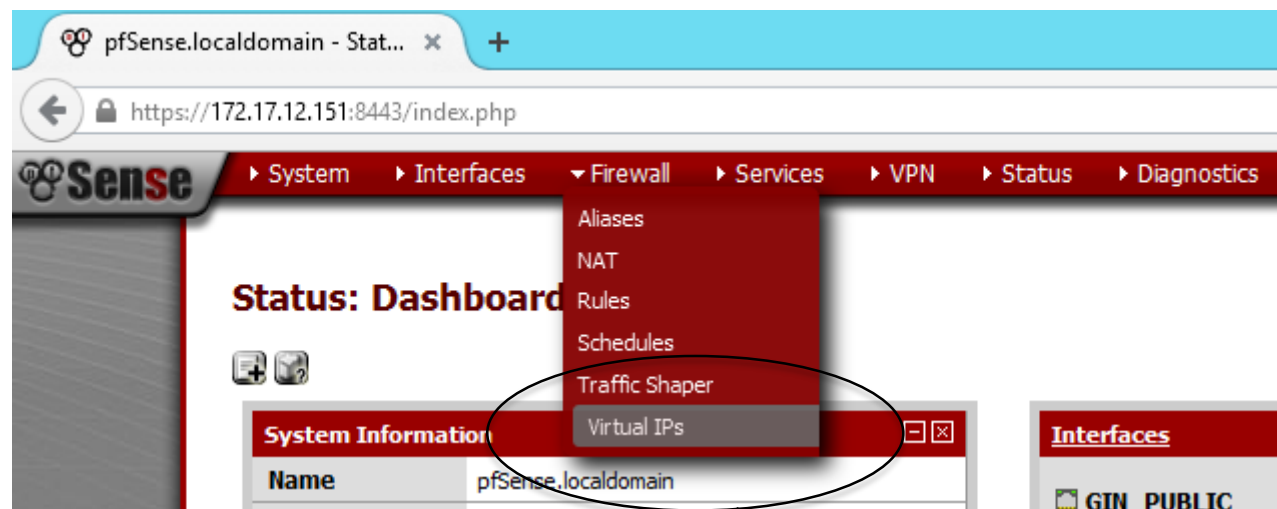
### Edit route entry

Destination network	<input type="text" value="10.0.0.0"/> / <input type="text" value="8"/>
Destination network for this static route	
Gateway	<input type="text" value="GIN_Private_GW - 10.0.1.254"/>
Choose which gateway this route applies to or add a new one.	
Disabled	<input type="checkbox"/> <b>Disable this static route</b> Set this option to disable this static route without removing it from the list.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

 The static route configuration has been changed.  
You must apply the changes in order for them to take effect.

Gateways Routes Groups			
	Network	Gateway	Interface
<input type="checkbox"/>	10.0.0.0/8	GIN_Private_GW - 10.0.1.254	GIN_PRIVATE

# การกำหนด Virtual IP ที่ได้รับมาจาก GIN



## Firewall: Virtual IP Addresses



### Virtual IPs

### CARP Settings

Virtual IP address	Interface	Type	Description
--------------------	-----------	------	-------------



#### Note:

The virtual IP addresses defined on this page may be used in NAT mappings.  
You can check the status of your CARP Virtual IPs and interfaces [here](#).

# การกำหนด Virtual IP ที่ได้รับมาจาก GIN

## Firewall: Virtual IP Address: Edit



Edit Virtual IP	
Type	<input type="radio"/> IP Alias <input type="radio"/> CARP <input checked="" type="radio"/> Proxy ARP <input type="radio"/> Other
Interface	GIN_PUBLIC
IP Address(es)	Type: Network Address: 123.242.1.0 / 28 <small>This is a CIDR block of proxy ARP addresses.</small> Expansion: <input type="checkbox"/> Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.)
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	1 Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 Skew: 0  The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

### Note:

Proxy ARP and Other type Virtual IPs cannot be bound to by anything running on the firewall, such as IPsec, OpenVPN, etc. Use a CARP or IP Alias type address for these cases.

For more information on CARP and the above values, visit the [OpenBSD CARP FAQ](#).

# การกำหนด Virtual IP ที่ได้รับมาจาก GIN

**Virtual IPs** **CARP Settings**

Virtual IP address	Interface	Type	Description
123.242.1.0/28	GIN_PUBLIC	P ARP	

**Note:**  
The virtual IP addresses defined on this page may be used in NAT mappings.  
You can check the status of your CARP Virtual IPs and interfaces [here](#).

## Firewall: Virtual IP Addresses



The VIP configuration has been changed.  
You must apply the changes in order for them to take effect.

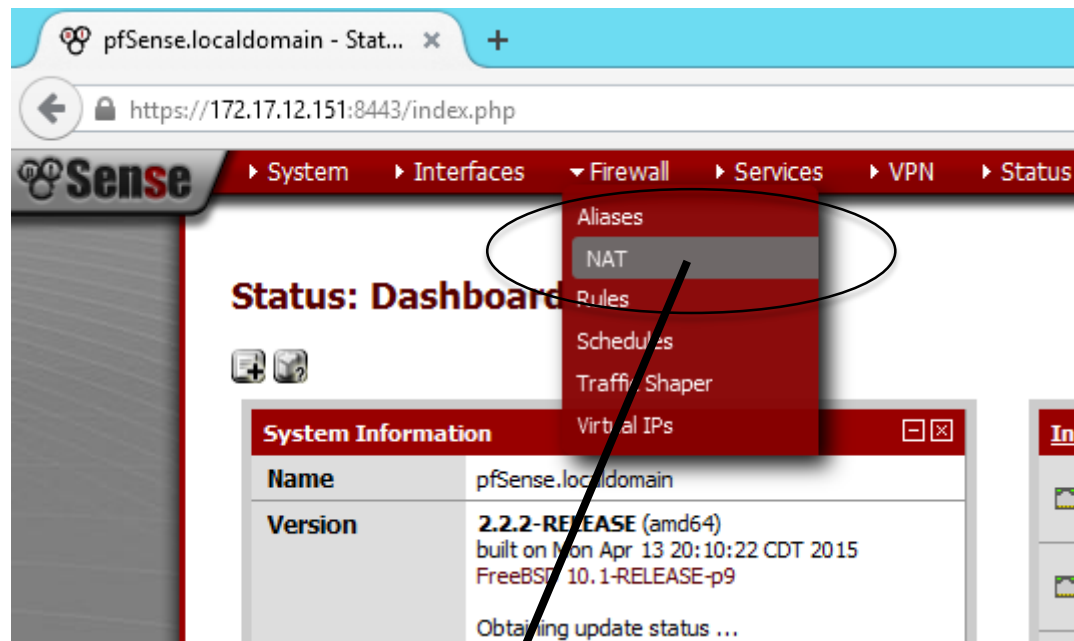
Apply changes

**Virtual IPs** **CARP Settings**

Virtual IP address	Interface	Type	Description
123.242.1.0/28	GIN_PUBLIC	P ARP	
10.0.1.0/24	GIN_PRIVATE	P ARP	



# การ NAT เพื่อใช้งาน Virtual IP กับ IP server



**Firewall: NAT: 1:1**



Port Forward   **1:1**   Outbound   NPT

Interface	External IP	Internal IP	Destination IP	Description
-----------	-------------	-------------	----------------	-------------

**Note:**  
Depending on the way your WAN connection is setup, you may also need a Virtual IP.  
If you add a 1:1 NAT entry for any of the interface IPs on this system, it will make this system inaccessible on that IP address. i.e. if you use your WAN IP address, any services on this system (IPsec, OpenVPN server, etc.) using the WAN IP address will no longer function.

# การ NAT เพื่อใช้งาน Virtual IP กับ IP server

## Firewall: NAT: 1:1: Edit



### Edit NAT 1:1 entry

Disabled	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
Interface	<div>GIN_PRIVATE ▾</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External subnet IP	<div> 10.0.1.3</div> <div>Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address. Hint: this is generally an address owned by the router itself on the selected interface.</div>
Internal IP	<div><input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.</div> <div>Type: <div>Single host ▾</div></div> <div>Address: <div>192.168.1.3</div> / <div>31 ▾</div></div> <div>Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.</div>
Destination	<div><input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.</div> <div>Type: <div>any ▾</div></div> <div>Address: <div></div> / <div>31 ▾</div></div> <div>The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually 'any'.</div>
Description	<div></div> <div>You may enter a description here for your reference (not parsed).</div>
NAT reflection	<div>use system default ▾</div>

Save

Cancel

# การ NAT เพื่อใช้งาน Virtual IP กับ IP server

## Firewall: NAT: 1:1



The NAT configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes

Port Forward 1:1 Outbound NPT

	Interface	External IP	Internal IP	Destination IP	Description
<input type="checkbox"/> <input checked="" type="checkbox"/>	GIN_PRIVATE	10.0.1.3	192.168.1.3	*	

## Firewall: NAT: 1:1



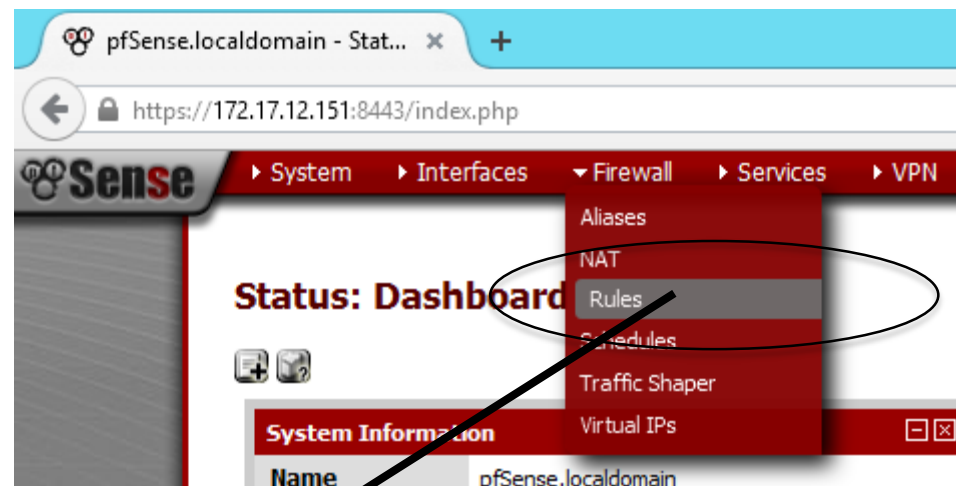
The NAT configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes

Port Forward 1:1 Outbound NPT


	Interface	External IP	Internal IP	Destination IP	Description
<input type="checkbox"/> <input checked="" type="checkbox"/>	GIN_PRIVATE	10.0.1.3	192.168.1.3	*	
<input type="checkbox"/> <input checked="" type="checkbox"/>	GIN_PUBLIC	123.242.1.3	192.168.1.3	*	

# การกำหนด Firewall rules เบื้องต้น













## Firewall: Rules

**Floating** | GIN\_PUBLIC | LAN | GIN\_PRIVATE | SERVER

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
No floating rules are currently defined. Click the  button to add a new rule.									

Legend:

-  pass
-  pass (disabled)
-  match
-  match (disabled)
-  block
-  block (disabled)
-  reject
-  reject (disabled)
-  log
-  log (disabled)

# การกำหนด Firewall rules เบื้องต้น

## Firewall: Rules: Edit



Edit Firewall rule	
Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Quick	<div><input type="checkbox"/> Apply the action immediately on match.</div> <div>Set this option if you need to apply this action to traffic that matches this rule immediately.</div>
Interface	<div>GIN_PUBLIC LAN GIN_PRIVATE SERVER</div> <div>Choose the interface(s) for this rule.</div>
Direction	<div>any</div>
TCP/IP Version	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to</div>
Protocol	<div>ICMP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</div>
ICMP type	<div>any</div> <div>If you selected ICMP for the protocol above, you may specify an ICMP type here.</div>
Source	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: / 127</div>
Destination	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: Single host or alias</div> <div>Address: 192.168.1.3 / 31</div>
Log	<div><input checked="" type="checkbox"/> Log packets that are handled by this rule</div> <div>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</div>
Description	<div></div> <div>You may enter a description here for your reference.</div>

Save Cancel

# การกำหนด Firewall rules เบื้องต้น

## Firewall: Rules



The firewall rule configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes

Floating

GIN\_PUBLIC

LAN

GIN\_PRIVATE

SERVER

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 ICMP	*	*	192.168.1.3	*	*	none		



pass



pass (disabled)



match



match (disabled)



block



block (disabled)



reject



reject (disabled)



log



log (disabled)

# การกำหนด Firewall rules เบื้องต้น

## Firewall: Rules: Edit



Edit Firewall rule	
Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Quick	<div><input type="checkbox"/> Apply the action immediately on match.</div> <div>Set this option if you need to apply this action to traffic that matches this rule immediately.</div>
Interface	<div>GIN_PUBLIC LAN GIN_PRIVATE SERVER</div> <div>Choose the interface(s) for this rule.</div>
Direction	<div>any</div>
TCP/IP Version	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to</div>
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</div>
Source	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: any</div> <div>Address: / 127</div> <div>Advanced - Show source port range</div>
Destination	<div><input type="checkbox"/> not</div> <div>Use this option to invert the sense of the match.</div> <div>Type: Single host or alias</div> <div>Address: 192.168.1.3 / 31</div>
Destination port range	<div>from: HTTP (80)</div> <div>to: HTTP (80)</div> <div>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</div>
Log	<div><input checked="" type="checkbox"/> Log packets that are handled by this rule</div> <div>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</div>
Description	<div></div> <div>You may enter a description here for your reference.</div>

Save Cancel



# การกำหนด Firewall rules เบื้องต้น

## Firewall: Rules



The firewall rule configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes









Floating



GIN\_PUBLIC

LAN



GIN\_PRIVATE



SERVER



	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>		IPv4 ICMP	*	*	192.168.1.3	*	*	none			 
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.1.3	80 (HTTP)	*	none			 
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.1.3	443 (HTTPS)	*	none			 
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.1.3	3389 (MS RDP)	*	none			 

 pass  
 pass (disabled)

☒ match  
☐ match (disabled)

 block  
 block (disabled)

 reject  
 reject (disabled)

 log  
 log (disabled)







# การกำหนด Firewall rules เบื้องต้น



## Firewall: Rules







Floating GIN\_PUBLIC LAN GIN\_PRIVATE SERVER



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	 								
	IPv4+6 *	*	*	*	*	*	none		allow servers to any.

 pass  
 pass (disabled)

 match  
 match (disabled)

 block  
 block (disabled)

 reject  
 reject (disabled)

 log  
 log (disabled)

# การตรวจสอบ Network logs

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The 'Status' menu is expanded, showing options like CARP (failover), Dashboard, DHCP Leases, DHCPv6 Leases, Filter Reload, Gateways, Interfaces, IPsec, Load Balancer, NTP, OpenVPN, Package Logs, Queues, RRD Graphs, **System Logs** (highlighted with a red circle), Traffic Graph, and UPnP & NAT-PMP.

**Status: Dashboard**

**System Information**

Name	fw_A.ega.or.th
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9  Unable to check for updates.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz Current: 333 MHz, Max: 2666 MHz
Uptime	00 Hour 08 Minutes 42 Seconds
Current date/time	Sat May 16 21:05:44 ICT 2015
DNS server(s)	127.0.0.1 10.10.44.14
Last config change	Sat May 16 21:04:24 ICT 2015
State table size	0% (63/98000) <a href="#">Show states</a>
MBUF Usage	5% (1266/26584)
Load average	0.01, 0.08, 0.07
CPU usage	0%
Memory usage	14% of 989 MB
SWAP usage	0% of 2047 MB
Disk usage	/ (ufs): 7% of 5.8G /var/run (ufs in RAM): 3% of 3.4M

**Gateways**

Interfaces	1000baseT <full-duplex>
IPsec	123.242.1.2
Load Balancer	1000baseT <full-duplex>
NTP	172.17.12.151
OpenVPN	1000baseT <full-duplex>
Package Logs	10.0.1.1
Queues	1000baseT <full-duplex>
RRD Graphs	192.168.1.1

# การตรวจสอบ Network logs

Status: System logs: Firewall



System **Firewall** DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View **Dynamic View** Summary View

Action	Time	Source IP Address	Source Port	Protocol	Quantity
<input type="checkbox"/> Pass	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Block	Interface	Destination IP Address	Destination Port	Protocol Flags	
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<b>Filter</b>

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

Last 10 firewall log entries.Max(50)

Act	Time	If	Source	Destination	Proto
	May 16 21:05:03	SERVER	192.168.2.3:138	192.168.2.255:138	UDP
	May 16 21:04:59	SERVER	192.168.1.3:138	192.168.1.255:138	UDP
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:49162	192.168.1.3:3389	TCP:SEC
	May 16 21:02:00	SERVER	192.168.1.3:137	192.168.1.255:137	UDP

Clear log

# การตรวจสอบ Network logs

Status: System logs: Firewall



System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View Dynamic View Summary View

Filtering options for Firewall logs:

Action	Time	Source IP Address	Source Port	Protocol	Quantity
<input type="checkbox"/> Pass	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Block	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

Destination Port:  Protocol Flags:

**Filter**

3 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49165	192.168.1.3:80	TCP:SEC
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49164	192.168.1.3:80	TCP:SEC
	May 16 21:08:08	GIN_PRIVATE	10.0.2.3:49163	192.168.1.3:80	TCP:SEC

Clear log

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR

# การตรวจสอบ Network logs

Status: System logs: Firewall



System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View Dynamic View Summary View

Action: ☐ Pass ☐ Block

Time:

Interface:

Source IP Address:

Destination IP Address:

Source Port:

Destination Port:

Protocol:

Protocol Flags:

Quantity:

Filter

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

9 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49165	192.168.1.3:80	TCP:SEC
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49164	192.168.1.3:80	TCP:SEC
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:49162	192.168.1.3:3389	TCP:SEC

Clear log

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR

# การตรวจสอบ Network logs

**Status: System logs: Firewall**

System

Firewall

DHCP

Portal Auth

IPsec

PPP

VPN

Load Balancer

OpenVPN

NTP

Settings

Normal View

Dynamic View

Summary View

Action

☐ Pass

☐ Block

Time

Source IP Address

123.242.2.3

Source Port

Protocol

Quantity

Interface

Destination IP Address

Destination Port

80

Protocol Flags

Filter

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

2 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49165	192.168.1.3:80	TCP:SEC
	May 16 21:08:19	GIN_PUBLIC	123.242.2.3:49164	192.168.1.3:80	TCP:SEC

Clear log

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR

# การตรวจสอบ Network logs

Status: System logs: Firewall



System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View Dynamic View Summary View

Filter configuration interface with the following fields:

- Action: ☐ Pass, ☐ Block
- Time: [Search icon] [Input field]
- Source IP Address: [Search icon] **!123.242.2.3**
- Interface: [Search icon] [Input field]
- Destination IP Address: [Search icon] [Input field]
- Source Port: [Search icon] [Input field]
- Destination Port: [Search icon] [Input field]
- Protocol: [Search icon] [Input field]
- Protocol Flags: [Search icon] [Input field]
- Quantity: [Input field]
- Filter button

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

5 matched log entries. Max(50)

Act	Time	If	Source	Destination	Proto
	May 16 21:09:32	SERVER	192.168.2.3:137	192.168.2.255:137	UDP
	May 16 21:08:08	GIN_PRIVATE	10.0.2.3:49163	192.168.1.3:80	TCP:SEC
	May 16 21:05:03	SERVER	192.168.2.3:138	192.168.2.255:138	UDP
	May 16 21:04:59	SERVER	192.168.1.3:138	192.168.1.255:138	UDP
	May 16 21:02:00	SERVER	192.168.1.3:137	192.168.1.255:137	UDP

Clear log

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR



# การตรวจสอบ Network logs

Status: System logs: Firewall



System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View Dynamic View Summary View

Filter

Action  
☐ Pass  
☒ Block

Time Source IP Address Source Port Protocol Quantity  
Interface Destination IP Address Destination Port Protocol Flags

Matches regular expression. Precede with exclamation (!) as first character to exclude match.

12 matched log entries. Max(50)

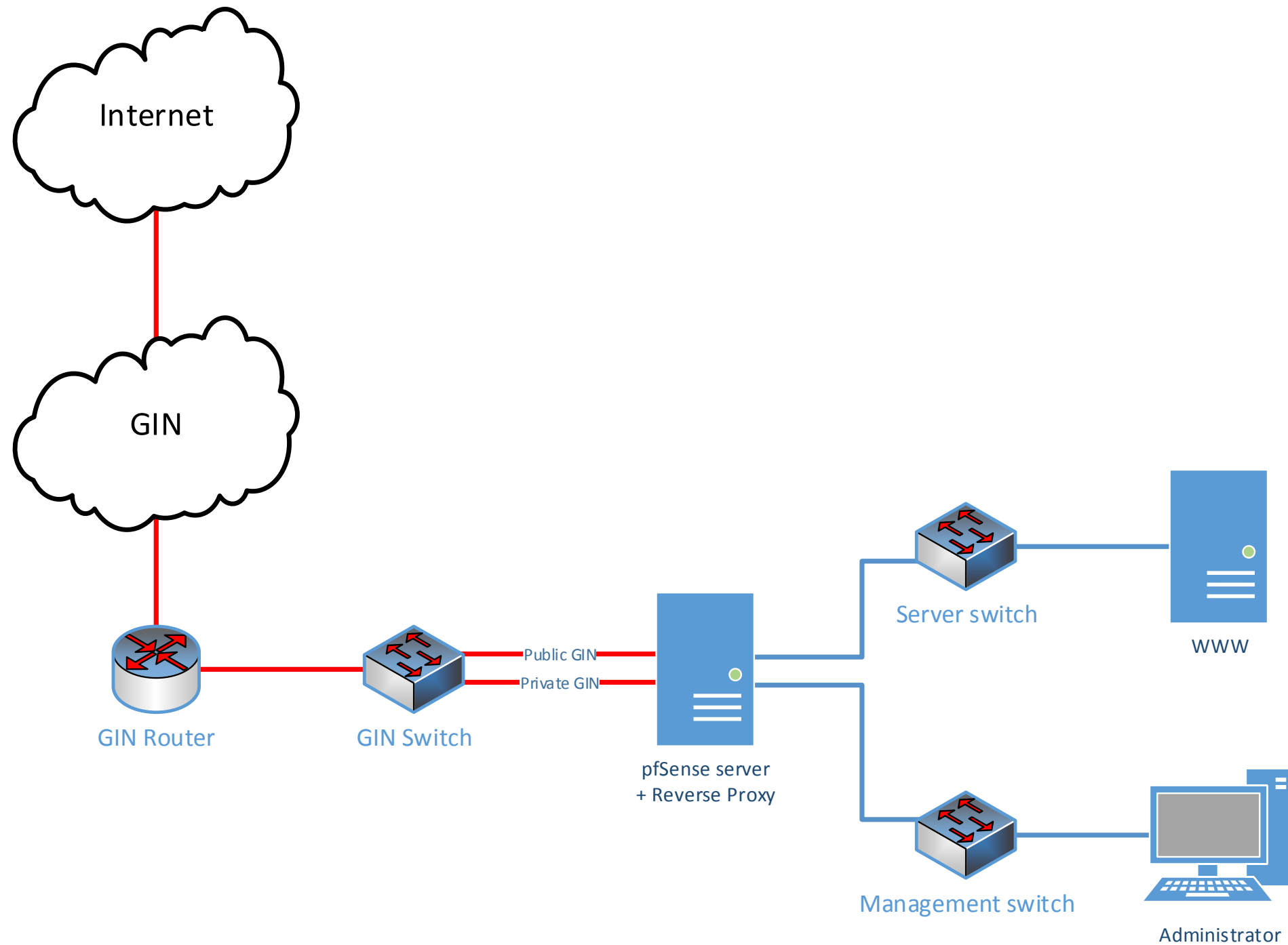
Act	Time	If	Source	Destination	Proto
	May 16 21:13:41	GIN_PUBLIC	123.242.2.3:49167	192.168.1.3:1000	TCP:S
	May 16 21:13:41	GIN_PUBLIC	123.242.2.3:49166	192.168.1.3:1000	TCP:S
	May 16 21:13:39	GIN_PUBLIC	123.242.2.3:49167	192.168.1.3:1000	TCP:SEC
	May 16 21:13:39	GIN_PUBLIC	123.242.2.3:49166	192.168.1.3:1000	TCP:SEC
	May 16 21:13:38	GIN_PUBLIC	123.242.2.3:49167	192.168.1.3:1000	TCP:SEC
	May 16 21:13:38	GIN_PUBLIC	123.242.2.3:49166	192.168.1.3:1000	TCP:SEC
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:09	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP
	May 16 21:02:06	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56170	192.168.1.3:3389	UDP
	May 16 21:02:04	GIN_PUBLIC	123.242.2.3:56169	192.168.1.3:3389	UDP

Clear log

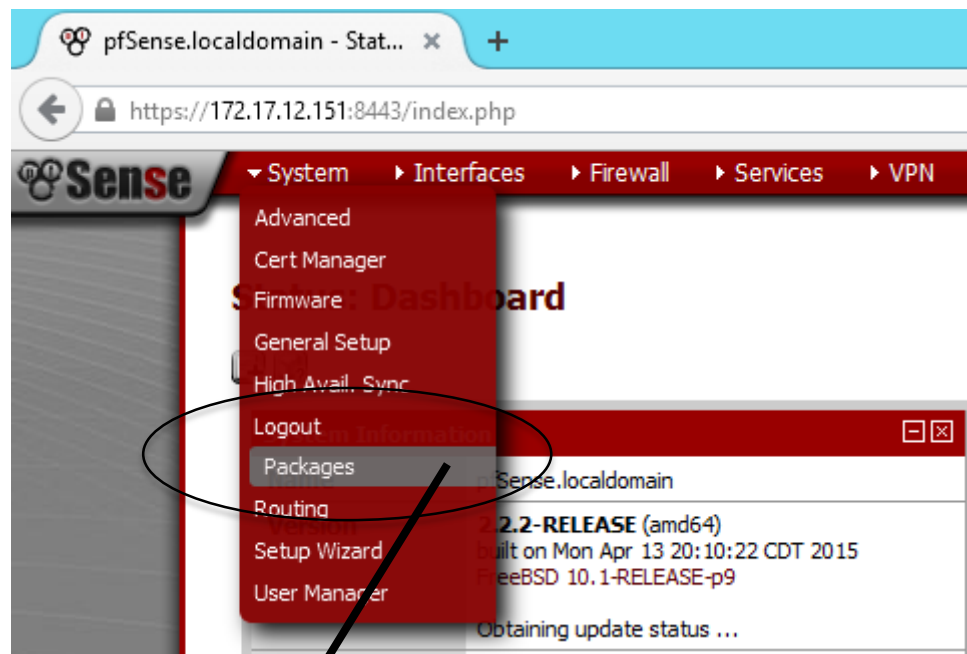
TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, W - CWR



# การใช้งาน pfSense เป็น Reverse Proxy



# การใช้งาน pfSense เป็น Reverse Proxy



## System: Package Manager



Available Packages

Installed Packages

Name	Category	Version	Description
------	----------	---------	-------------

There are no packages currently installed.

# การใช้งาน pfSense เป็น Reverse Proxy

## System: Package Manager

Available Packages

Installed Packages

All

Network Management

Security

Services

System

Other Categories

Name	Category	Status	Description
Apache with mod_security-dev	Network Management	ALPHA 0.43 platform: 2.2	ModSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pfSense using 1 IP address. <b>Backup your location config before updating from 0.2.x to 0.3 package version.</b>  Package info
Apcupsd	Services	BETA apcupsd-3.14.12_1 pkg v0.3.6 platform: 2.2 2.2.999	Set of programs for controlling APC UPS.  No package info, check the forum
arping	Services	Stable 1.1 platform: 2.2	Broadcasts a who-has ARP packet on the network and prints answers.  Package info

squid3	Network	beta 0.2.8 platform: 2.2	High performance web proxy cache. It combines squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, ssl filtering and antivirus integration via i-cap  Package info
--------	---------	--------------------------------	--

# การใช้งาน pfSense เป็น Reverse Proxy

## System: Package Manager: Install Package



Available packages

Installed packages

Package Installer

Package: **squid3** will be installed.  
Please confirm the action.

Confirm

Cancel

## System: Package Manager: Install Package



Available packages

Installed packages

Package Installer

Installing squid3 and its dependencies.

Beginning package installation for squid3 .

Downloading package configuration file... done.

Saving updated package information... done.

Downloading squid3 and its dependencies...

Checking for package installation...

Downloading [https://files.pfsense.org/packages/10/All/squid-3.4.10\\_2-amd64.pbi](https://files.pfsense.org/packages/10/All/squid-3.4.10_2-amd64.pbi)  
... 29%

รอกันกว่าระบบจะติดตั้งเสร็จ!!!!!!

# การใช้งาน pfSense เป็น Reverse Proxy

## System: Package Manager: Install Package



Available packages

Installed packages

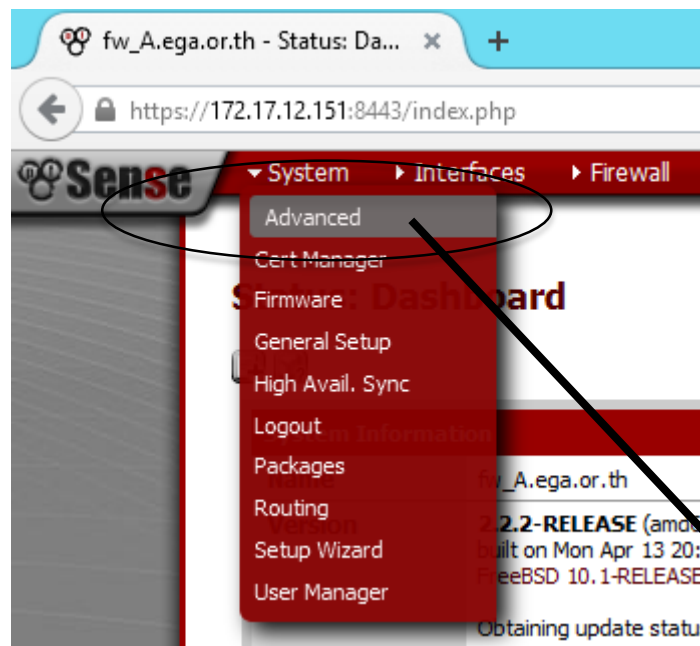
Package Installer

squid3 installation completed.

```
Beginning package installation for squid3 .
Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid3 and its dependencies...
Checking for package installation...
  Downloading https://files.pfsense.org/packages/10/All/squid-3.4.10_2-amd64.pbi
... (extracting)
Loading package configuration... done.
Configuring package components...
Loading package configuration... done.
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Integrated Tab items... done.
Services... done.
Writing configuration... done.

Installation completed. Please check to make sure that the package is
configured from the respective menu then start the package.
```

# การตั้งค่า Reverse Proxy



**Admin Access** | Firewall / NAT | Networking | Miscellaneous | System Tunables | Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

### webConfigurator

Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
SSL Certificate	webConfigurator default (555203ab312bf) ▼
TCP port	<input type="text" value="8443"/> Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Max Processes	<input type="text" value="2"/> Enter the number of webConfigurator processes you want to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
WebGUI redirect	<input checked="" type="checkbox"/> <b>Disable webConfigurator redirect rule</b> When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

เลือก Disable....

# การตั้งค่า Reverse Proxy

The screenshot shows the Sensei firewall configuration interface. The breadcrumb navigation path is **System > Advanced > System Tunables**. The **System Tunables** tab is selected, displaying a table of tunable parameters. A red note states: "NOTE: The options on this page are intended for use by advanced users only." The table has three columns: Tunable Name, Description, and Value. One entry is visible: `net.pfsync.carp_demotion_factor` with the description "pfsync's CARP demotion factor adjustment" and a value of "0 (0)". A black arrow points from the "Advanced" menu item to the "System Tunables" tab, and another black arrow points from the "+" icon in the bottom right of the table to the "Add" button in the bottom right corner of the page.

**System: Advanced: System Tunables**

NOTE: The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value
net.pfsync.carp_demotion_factor	pfsync's CARP demotion factor adjustment	0 (0)

# การตั้งค่า Reverse Proxy

Admin Access Firewall / NAT Networking Miscellaneous System Tunables Notifications

**Edit system tunable**

Tunable:

Description:

Value:

Save Cancel

net.inet.ip.portrange.reservedhigh

0 (เลขศูนย์)

## System: Advanced: System Tunables



The firewall tunables have changed. You must apply the configuration to take affect.

Apply changes

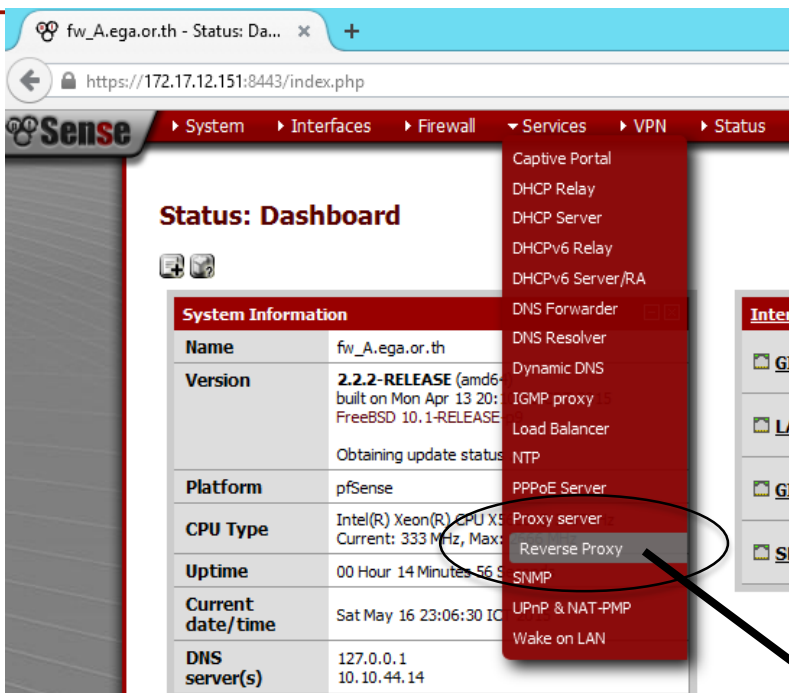
Admin Access Firewall / NAT Networking Miscellaneous System Tunables Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value
net.inet.ip.portrange.reservedhigh		0



# การตั้งค่า Reverse Proxy



## Reverse Proxy server: General

**Reverse Proxy server: General**

General Web Servers Mappings Redirects Real time Sync

**Squid Reverse proxy General Settings**

Reverse Proxy interface: LAN, GIN\_PRIVATE, SERVER, GIN\_PUBLIC  
The interface(s) the reverse-proxy server will bind to.

User-defined reverse-proxy IPs:   
Squid will additionally bind to this user-defined IPs for reverse-proxy operation. Useful for virtual IPs such as CARP. Separate by semi-colons (;).

external FQDN:   
The external full-qualified-domain-name of the WAN address.

Reset TCP connections if request is unauthorized: ☒   
If this field is checked, the reverse-proxy will reset the TCP connection if the request is unauthorized.

www.server-a.go.th

# การตั้งค่า Reverse Proxy

**Squid Reverse HTTP Settings**

**Enable HTTP reverse mode**

☒

If this field is checked, the proxy-server will act in HTTP reverse mode. (You have to add a rule with destination "WAN-address")

reverse HTTP port

This is the port the HTTP reverse-proxy will listen on. (leave empty to use 80)

reverse HTTP default site

This is the HTTP reverse default site. (leave empty to use the external fqdn)

**Squid Reverse HTTPS Settings**

**Enable HTTPS reverse proxy**

☒

If this field is checked, the proxy-server will act in HTTPS reverse mode. (You have to add a rule with destination "WAN-address")

reverse HTTPS port

This is the port the HTTPS reverse-proxy will listen on. (leave empty to use 443)

reverse HTTPS default site

This is the HTTPS reverse default site. (leave empty to use the external fqdn)

reverse SSL certificate

Choose the SSL Server Certificate here.

intermediate CA certificate (if needed)

Paste a signed certificate in X.509 PEM format here.

Ignore internal Certificate validation

☒

If this field is checked, internal certificate validation will be ignored.

Save

www.server-a.go.th

# การตั้งค่า Reverse Proxy

## Reverse Proxy server: Peers



General Web Servers Mappings Redirects Real time Sync

Status	Alias	Ip address	Port	Protocol	Description
--------	-------	------------	------	----------	-------------



## Reverse Proxy server: Peers: Edit



General Web Servers Mappings Redirects Real time Sync

### Squid Reverse Peer Mappings

Enable this peer



If this field is checked, then this peer will be available for reverse proxying.

Peer Alias

server-a.go.th

Name to identify this peer on squid reverse conf  
example: HOST1

Peer IP

192.168.1.3

Ip Address of this peer.  
example: 192.168.0.1

Peer Port

80

Listening port of this peer.  
example: 80

Peer Protocol

HTTP

Protocol listening on this peer port.

Peer Description



Peer Description (optional)

Save

Cancel

server-a.go.th

192.168.1.3

(IP ของเครื่อง Server เครื่องจริง)

80


# การตั้งค่า Reverse Proxy

## Reverse Proxy server: Mappings



General Web Servers Mappings Redirects Real time Sync

Status	Group Name	Peers	Description
--------	------------	-------	-------------



## Reverse Proxy server: Mappings: Edit



General Web Servers Mappings Redirects Real time Sync

**Squid Reverse Peer Mappings**

Enable this URI ☒  
If this field is checked, then this URI(Uniform Resource Name) will be available for reverse config.


Group name   
Name to identify this URI on squid reverse conf  
example: URI1

Group Description   
URI Group Description (optional)

Peers 

server-a.go.th

  
Apply this Group Mappings to selected Peers  
Use CTRL + click to select.

URIs  
Url regex to match  
Samples: .mydomain.com .mydomain.com/test  
www.mydomain.com http://www.mydomain.com/ ^http://www.mydomain.com/.\*\$  
  
  
URI to publish

Save Cancel

server-a.go.th

.server-a.go.th

# การตั้งค่า Reverse Proxy

## Reverse Proxy server: Mappings



General Web Servers Mappings Redirects Real time Sync

Status	Group Name	Peers	Description
on	server-a.go.th	server-a.go.th	

## Status: Services



squid has been restarted.

Close

Service	Description	Status
apinger	Gateway Monitoring Daemon	Running
c-icap	Icap interface for squid and clamav integration	Stopped
clamd	Clamav Antivirus	Stopped
ntpd	NTP clock sync	Running
squid	Proxy server Service	Running
unbound	DNS Resolver	Running

# การตั้งค่า Reverse Proxy Logs

fw\_A.ega.or.th - Status: Ser... x +

https://172.17.12.151:8443/status\_services.php?mode=restartservice&service=squid

**Sense** ▶ System ▶ Interfaces ▶ Firewall ▶ Services ▶ VPN ▶ Status


### Status: Services

Service	Description
apinger	Gateway Monitor
c-icap	Icap interface filter
clamd	Clamav Antivirus
ntpd	NTP clock sync
squid	Proxy server
unbound	DNS Resolver

- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server/RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP proxy
- Load Balancer
- NTP
- PPPoE Server
- Proxy server**
- Reverse Proxy
- SNMP
- UPnP & NAT-PMP
- Wake on LAN

### Logging Settings

Enabled logging ☒ This will enable the access log. Don't switch this on if you don't have much disk space left.

Log store directory  /var/squid/logs The directory where the log will be stored (note: do not end with a / mark)

Save

# การตั้งค่า Reverse Proxy Logs

## Proxy server: General settings

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real time Sync

## Status: Services



squid has been restarted.

Close

Service	Description	Status	
apinger	Gateway Monitoring Daemon	▶ Running	▶ ◀ + ⚙ 📄
c-icap	Icap interface for squid and clamav integration	✖ Stopped	▶
clamd	Clamav Antivirus	✖ Stopped	▶
ntpd	NTP clock sync	▶ Running	▶ ◀ + ⚙ 📄
squid	Proxy server Service	▶ Running	▶ ◀ + ⚙ 📄
unbound	DNS Resolver	▶ Running	▶ ◀ + 📄



# การตั้งค่า Reverse Proxy Logs

fw\_a.ega.or.th - Status: Da... x +

https://172.17.12.151:8443/index.php

Sense

System Interfaces Firewall Services VPN Status

**Status: Dashboard**

System Information

Name	fw_a.ega.or.th
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:00 UTC 2015 FreeBSD 10.1-RELEASE
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU X5650 Current: 3.33 MHz, Max: 3.33 MHz
Uptime	00 Hour 14 Minutes 56 Seconds
Current date/time	Sat May 16 23:06:30 ICT 2015
DNS server(s)	127.0.0.1 10.10.44.14

Services menu:

- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server/RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP proxy
- Load Balancer
- NTP
- PPPoE Server
- Proxy server
- Reverse Proxy
- SNMP
- UPnP & NAT-PMP
- Wake on LAN

## Status: Proxy Monitor

General Web Servers Mappings Redirects **Real time** Sync

Max lines: 10 lines  
Max. lines to be displayed.

String filter:

Enter a grep like string/pattern to filterlog.  
eg. username, ip addr, url.  
Use ! to invert the sense of matching, to select non-matching lines.

**Squid Logs**

Date	IP	Status	Address	User	Destination
16.05.2015 22:54:35	123.242.2.3	TCP_MISS/404	http://server-a.go.th/favicon.ico	-	192.168.1.3
16.05.2015 22:54:35	123.242.2.3	TCP_MISS/200	http://server-a.go.th/	-	192.168.1.3
16.05.2015 22:53:57	123.242.2.3	TCP_MISS/404	http://www.server-a.go.th/favicon.ico	-	192.168.1.3
16.05.2015 22:53:53	123.242.2.3	TCP_MISS/404	http://www.server-a.go.th/favicon.ico	-	192.168.1.3
16.05.2015 22:53:53	123.242.2.3	TCP_MISS/200	http://www.server-a.go.th/	-	192.168.1.3



# การใช้งาน pfSense ร่วมกับระบบเครือข่าย GIN

คมกริช คำสวัสดิ์

วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส  
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

