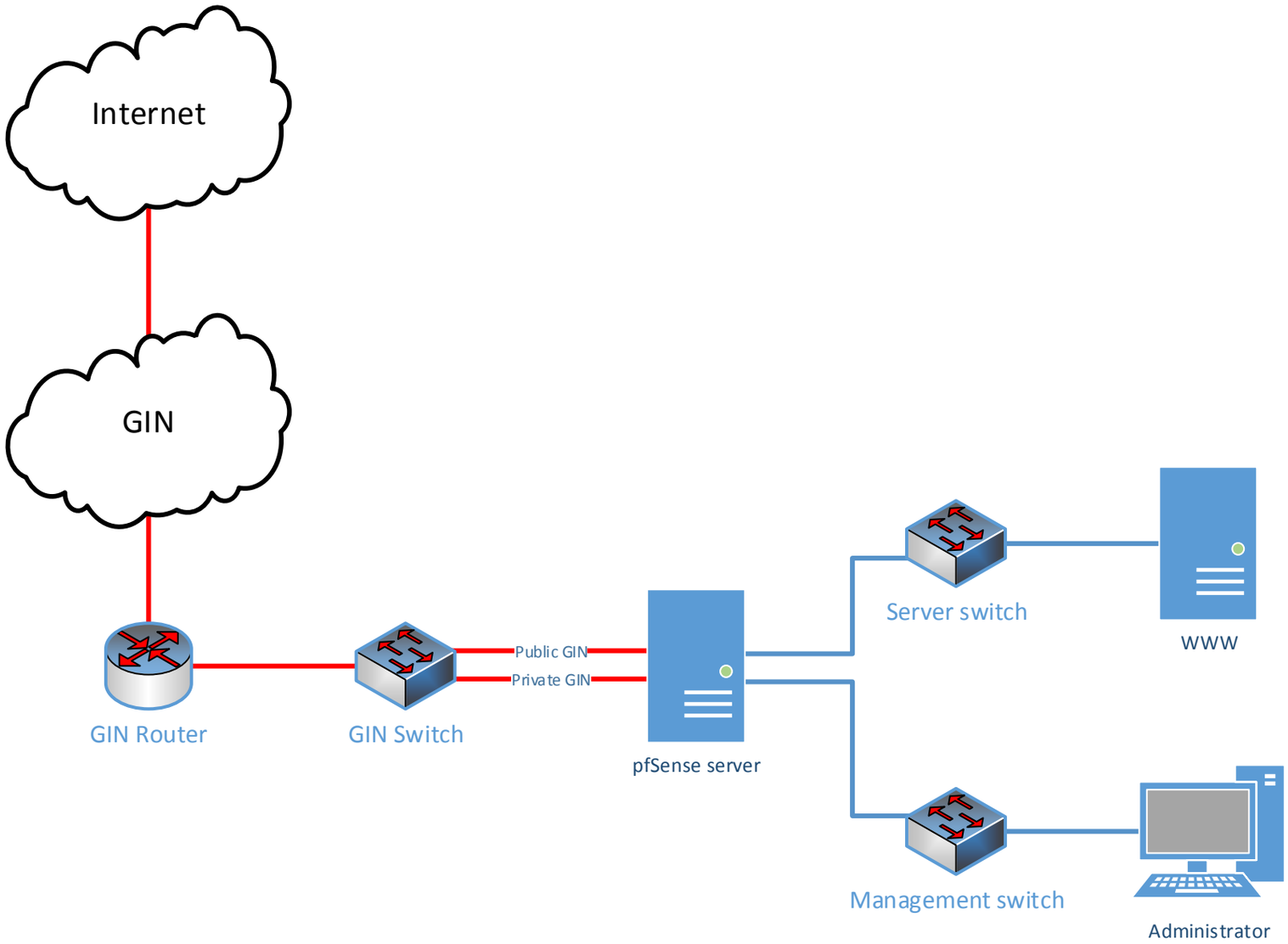
# การใช้งาน pfSense
# ร่วมกับระบบเครือข่าย GIN

**คมกริช คำสวัสดิ์**
วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

EGA e-Government Agency

G-CERT by EGA

# ผังการเชื่อมต่อระบบเครือข่าย GIN



# การติดตั้ง pfSense

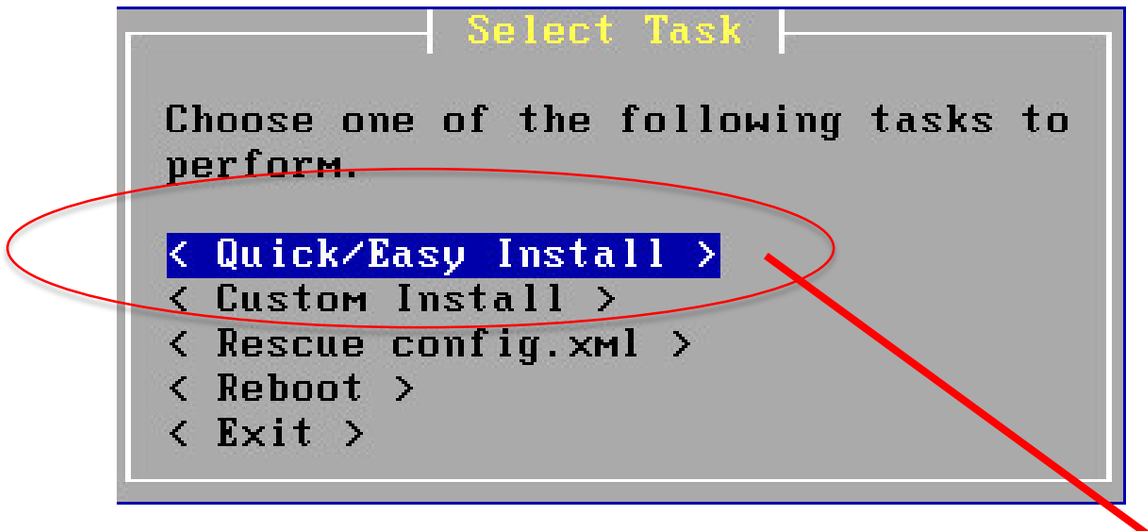
# การติดตั้ง pfSense

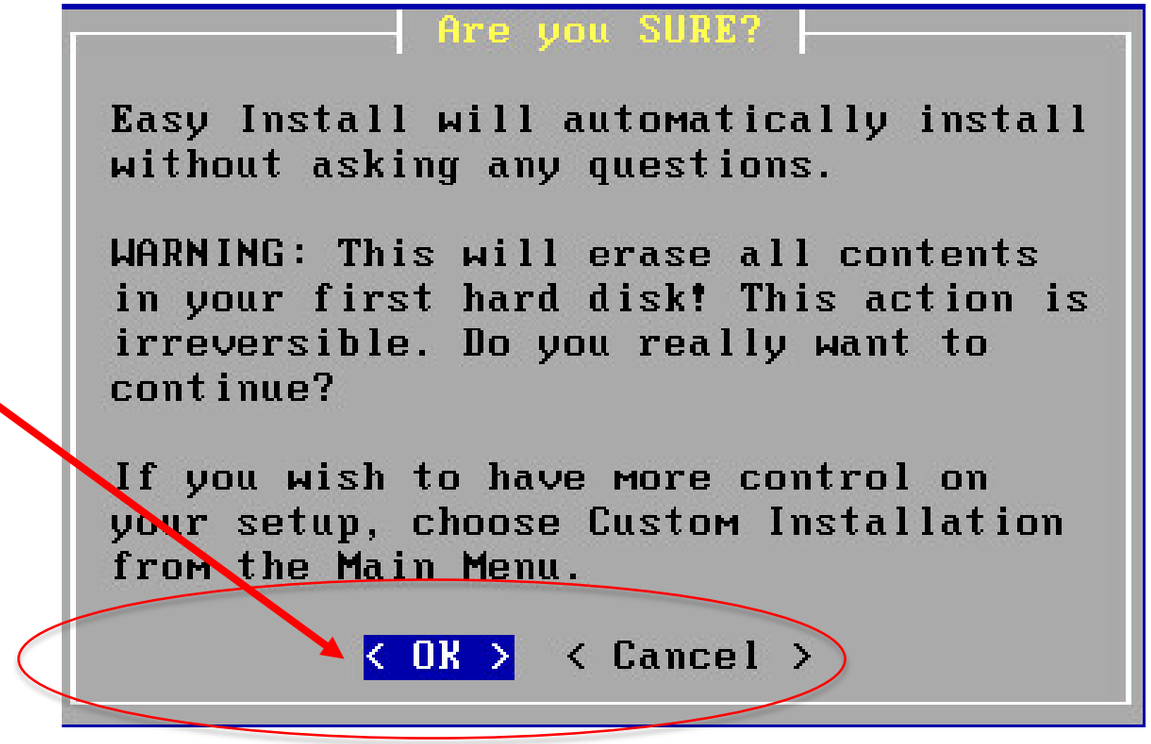
```
32-bit compatibility ldconfig path: /usr/lib32
done.
Launching the init system... done.
Initializing..................... done.
Starting device manager (devd)...done.

[ 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....
```

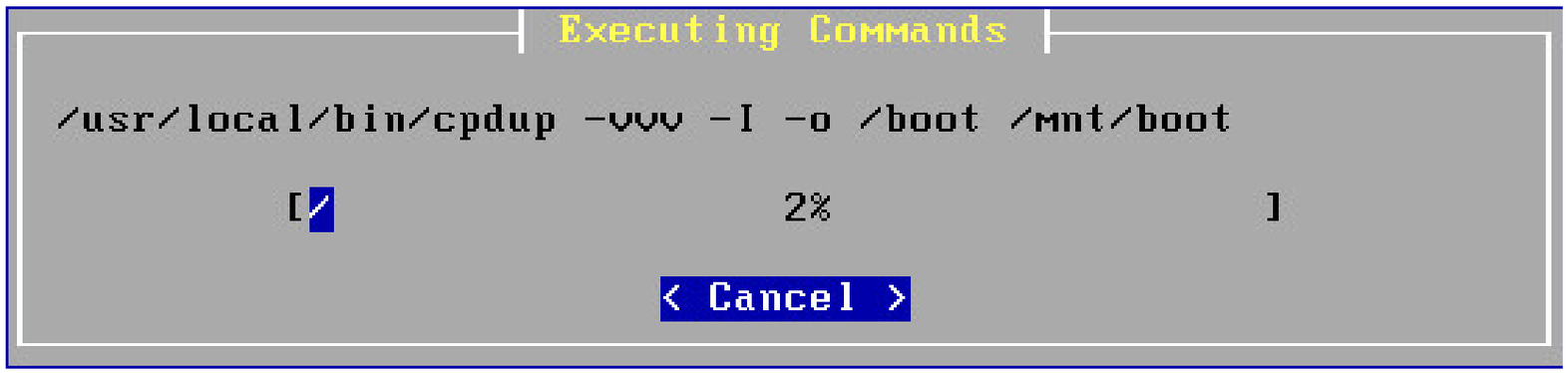
กด i

# การติดตั้ง pfSense

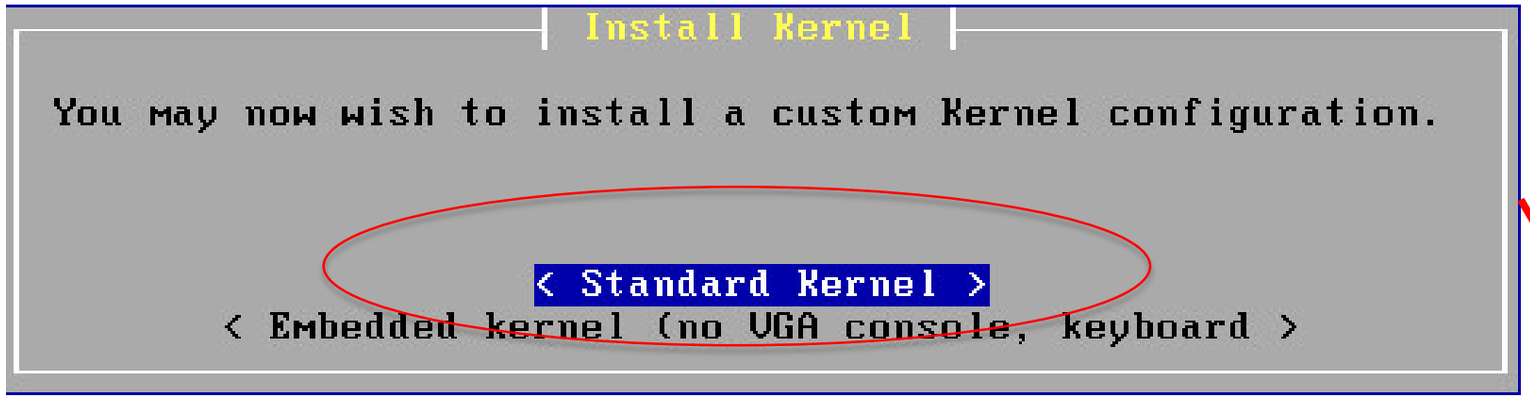
# การติดตั้ง pfSense

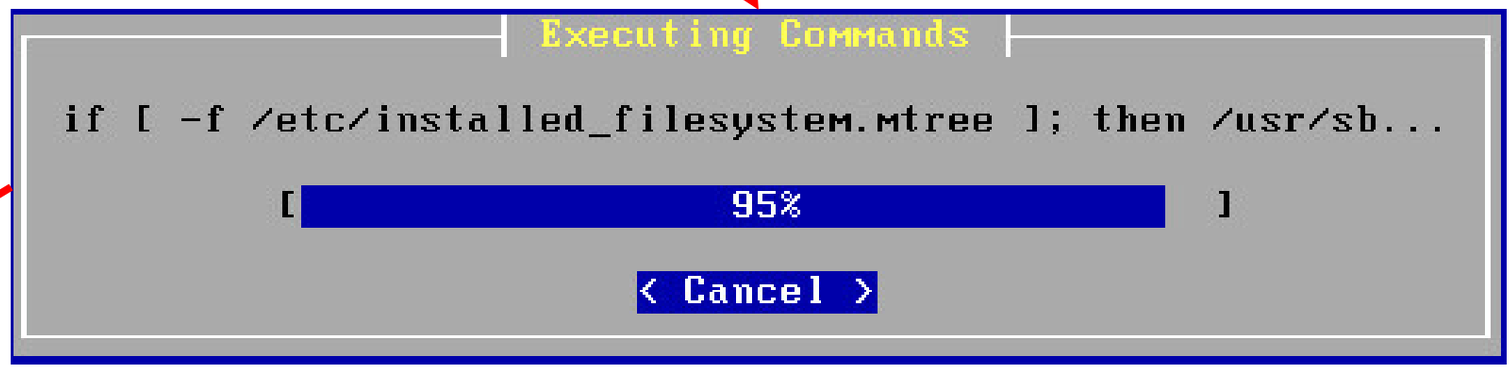


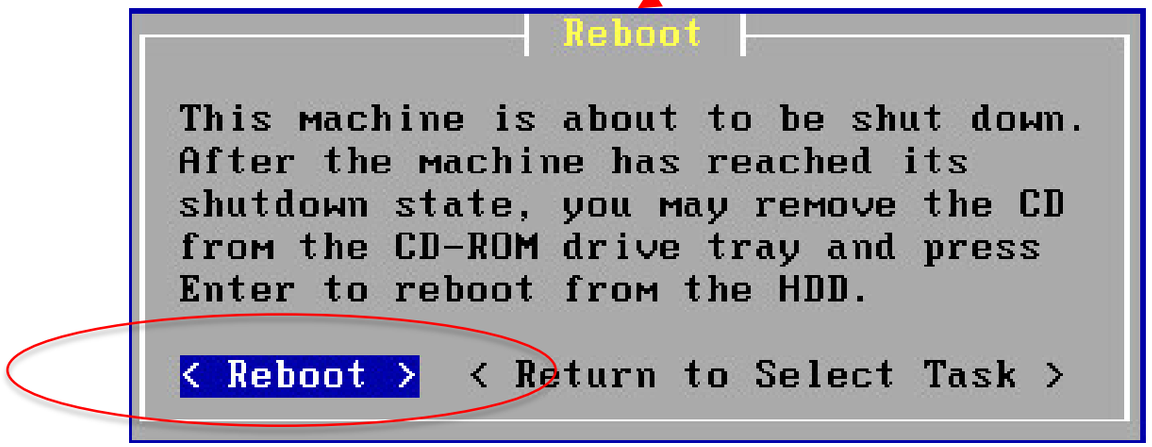



# การติดตั้ง pfSense



# 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:
>
```

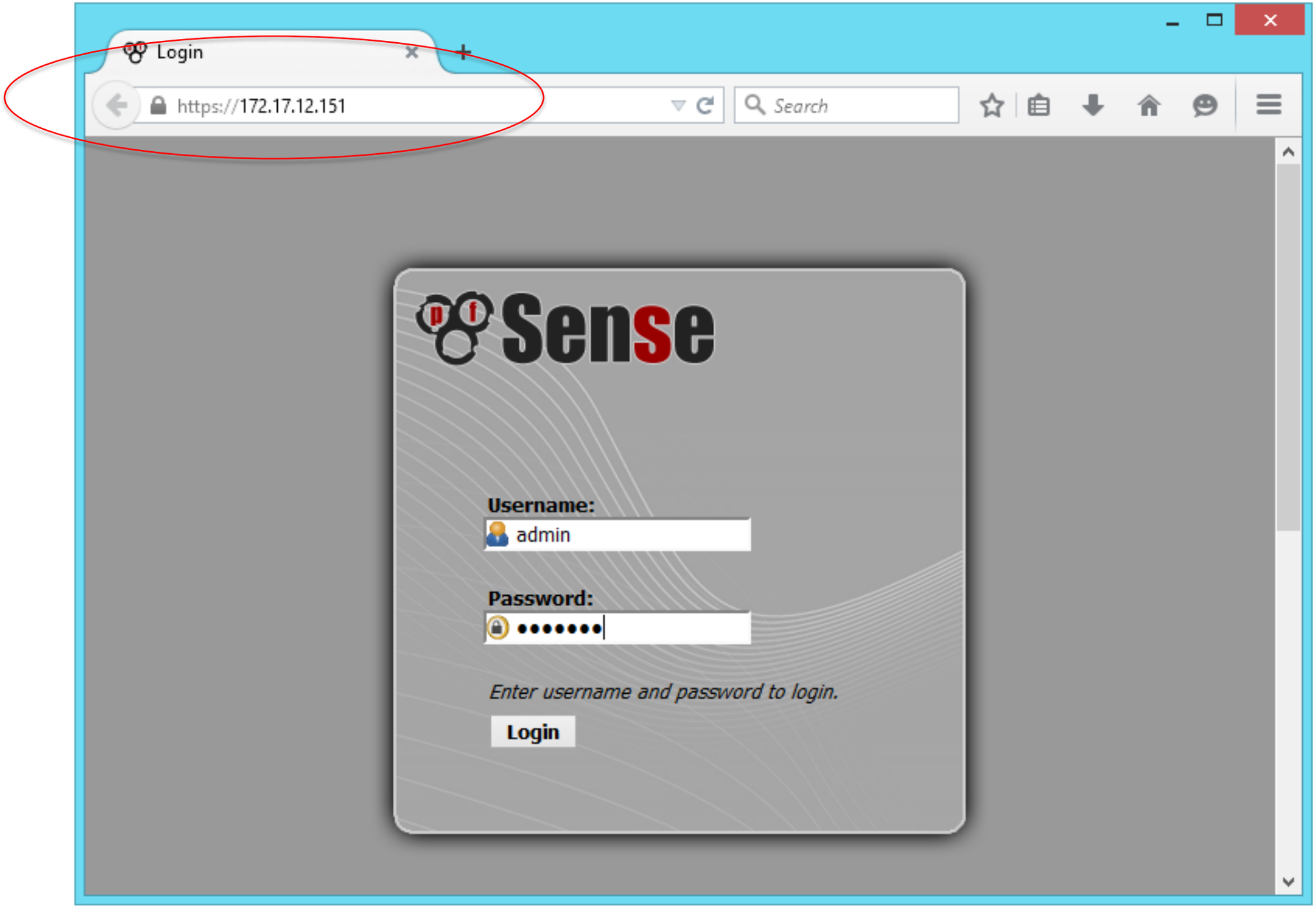
# การกำหนด IP address ให้ LAN Interface

```
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.
```

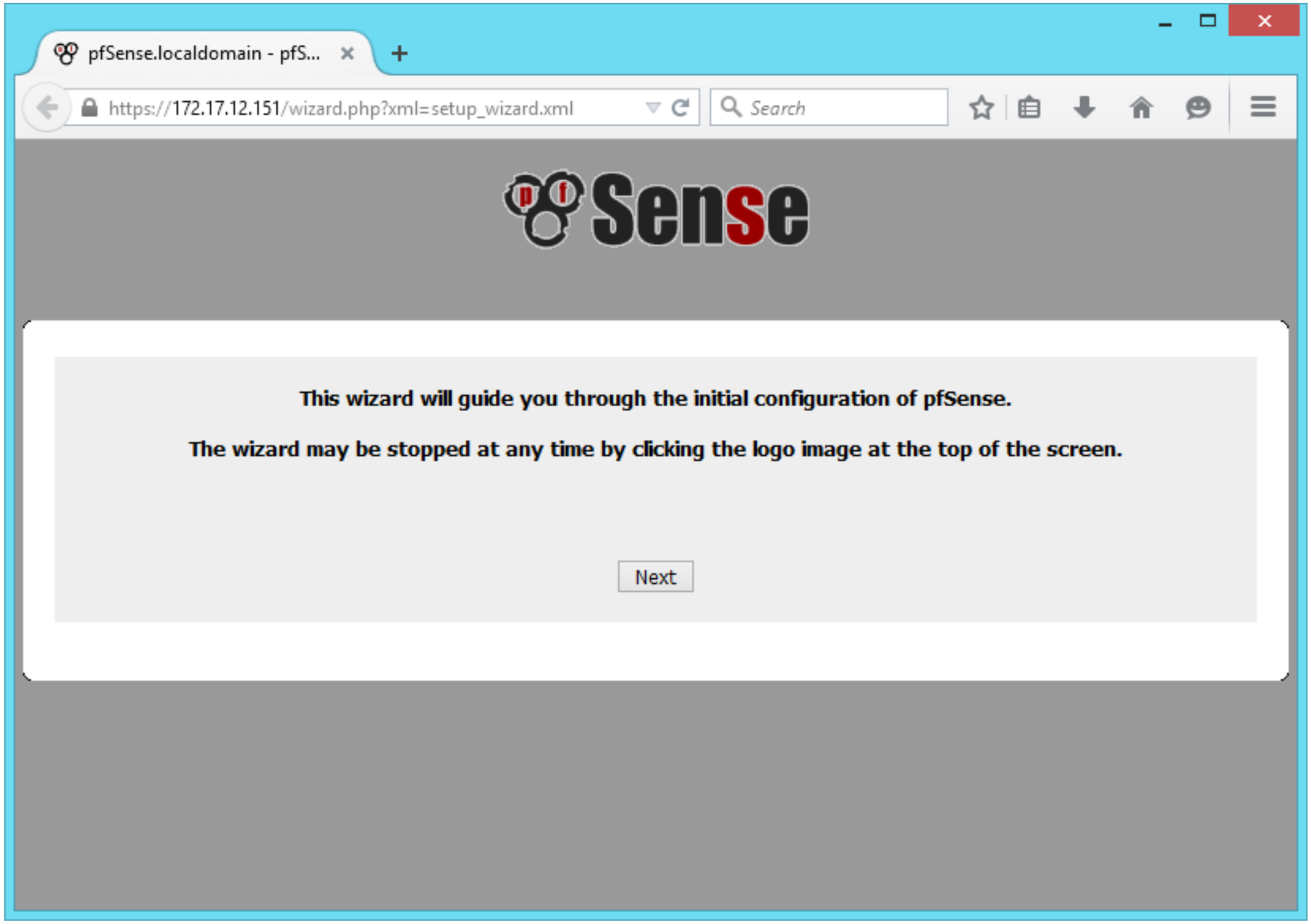
# การกำหนด IP address ให้ LAN Interface

```
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       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:
```

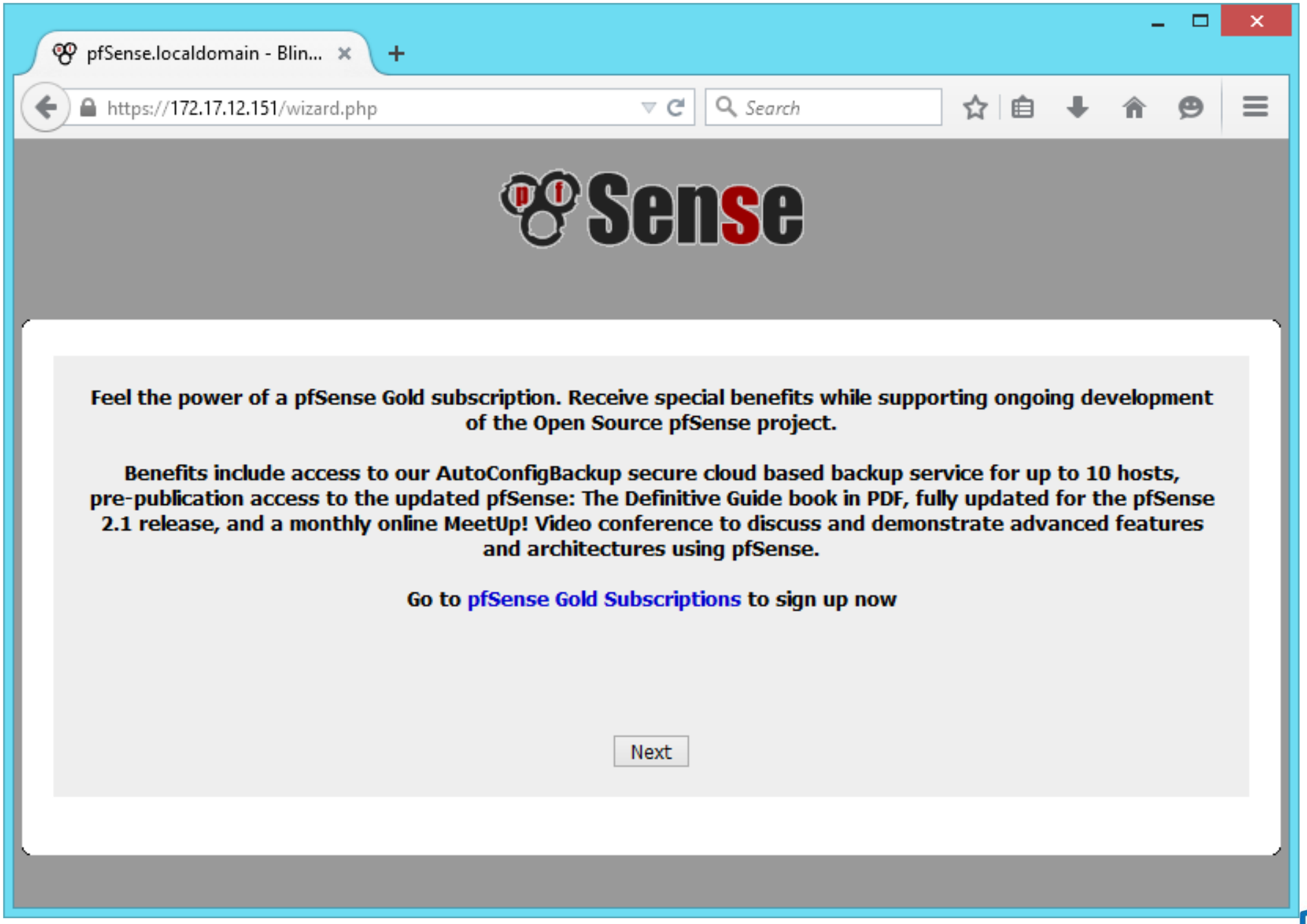
# การเข้าใช้งาน pfSense



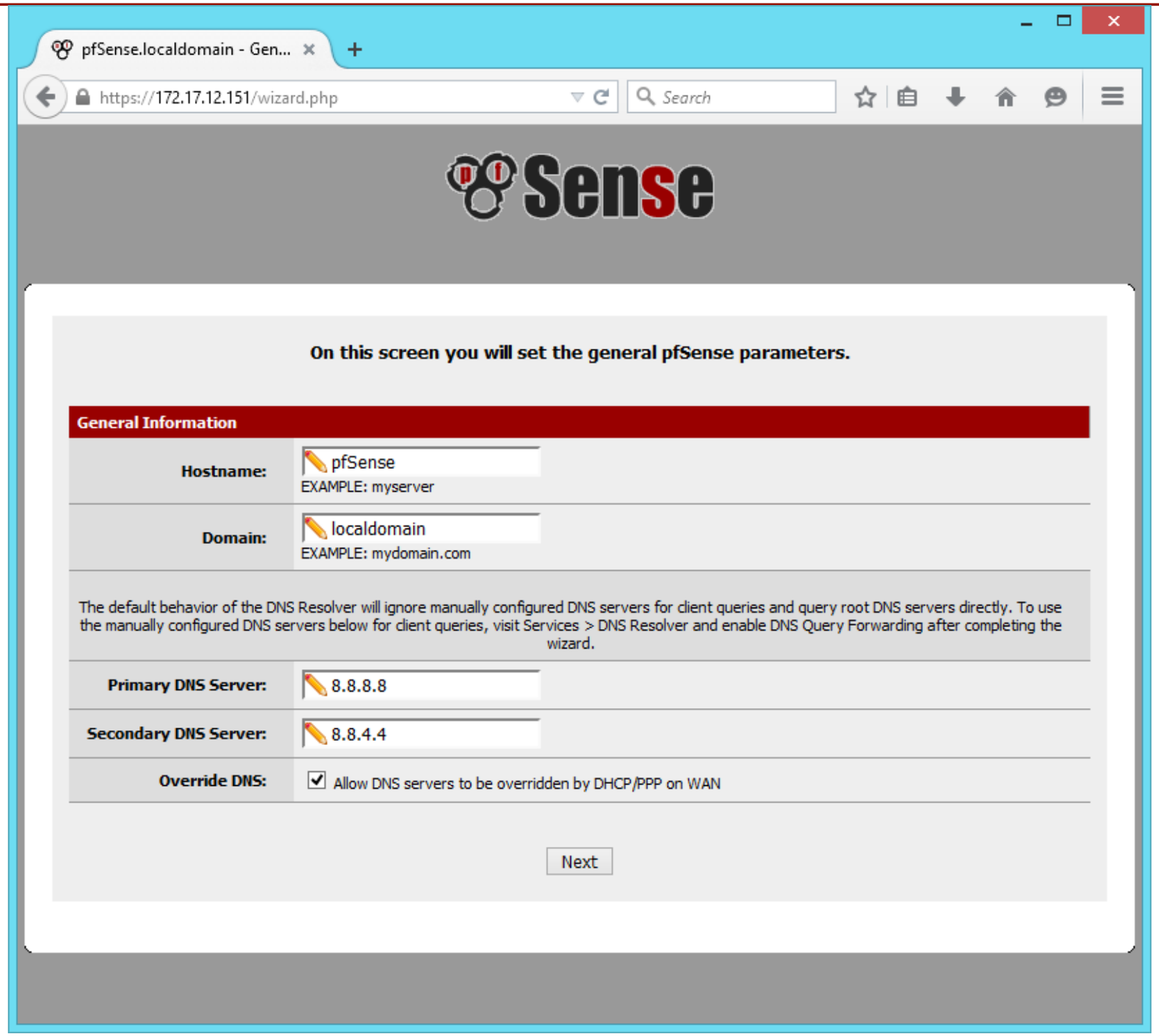
# การเข้าใช้งาน pfSense



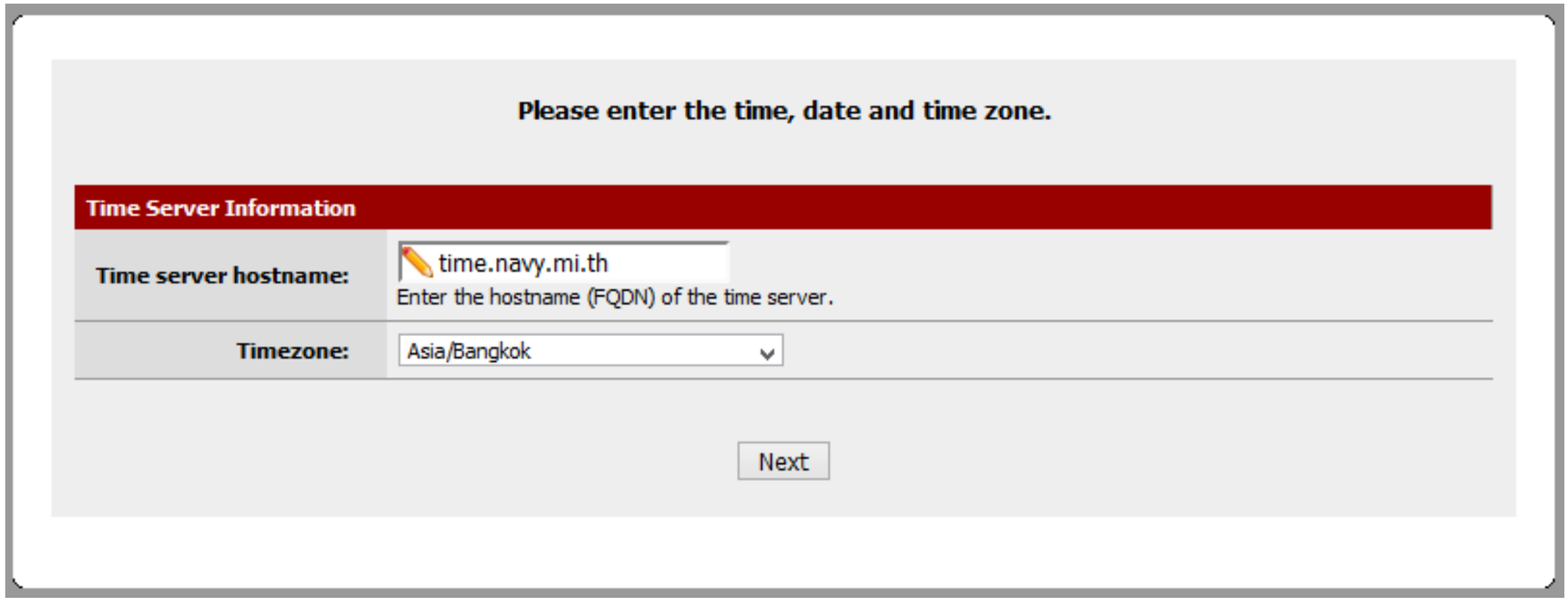
# การเข้าใช้งาน pfSense



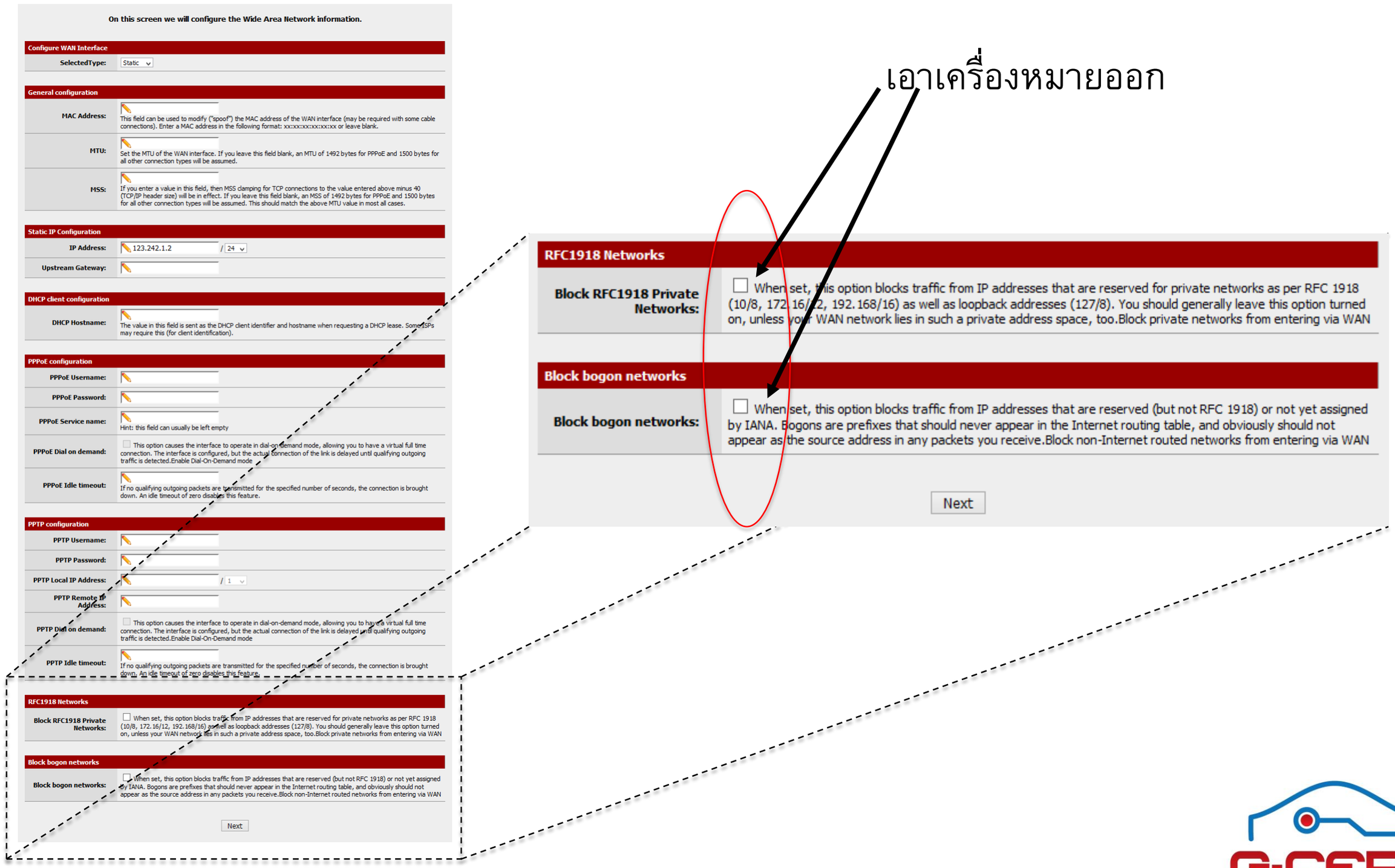
# การเข้าใช้งาน pfSense



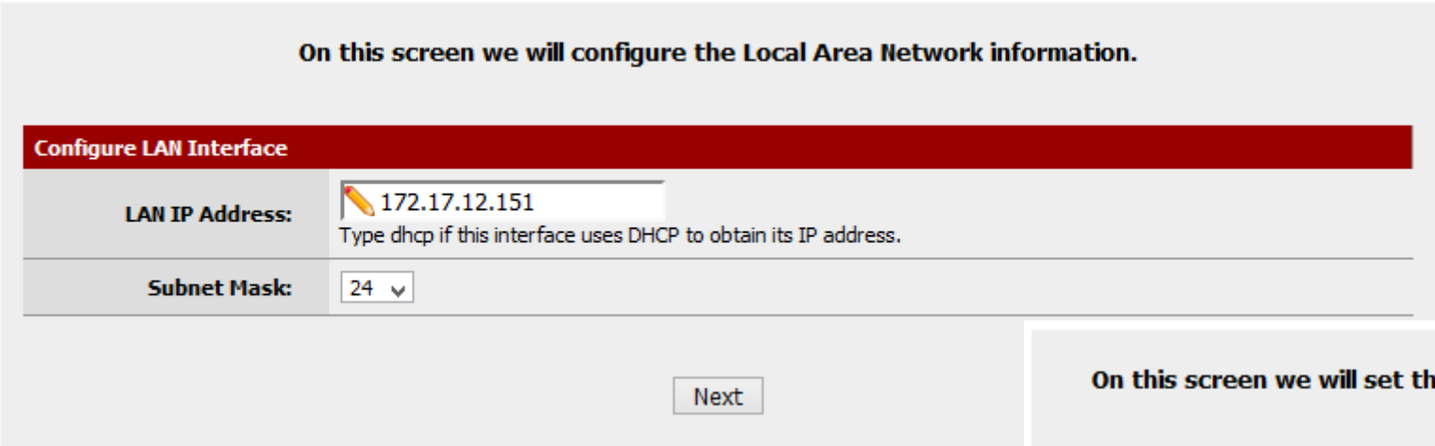
# การเข้าใช้งาน pfSense

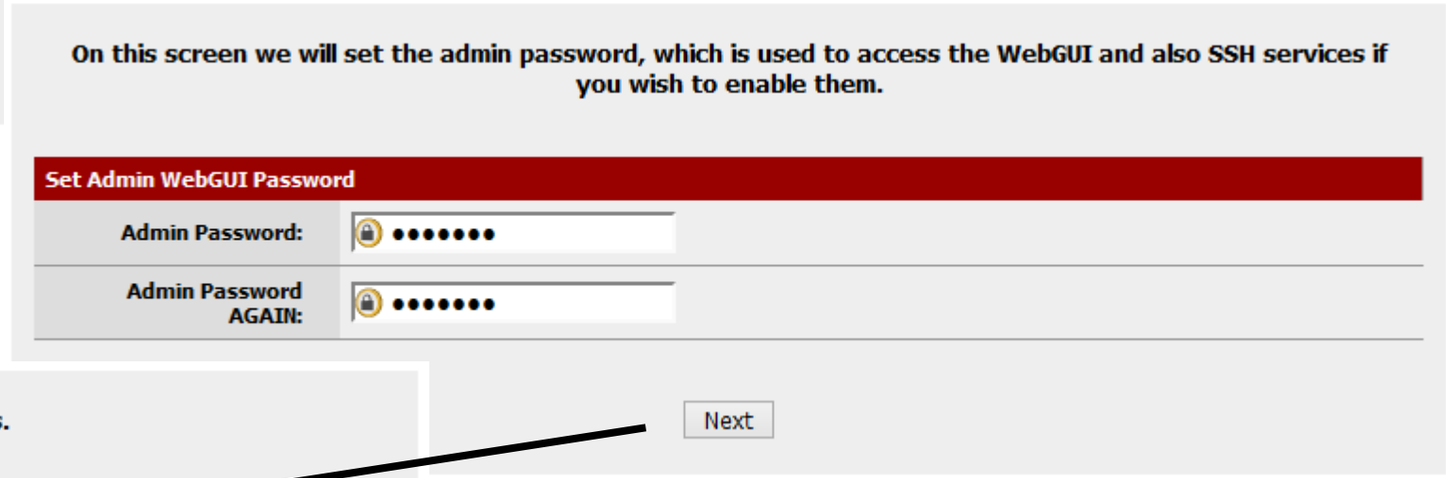


# การเข้าใช้งาน pfSense

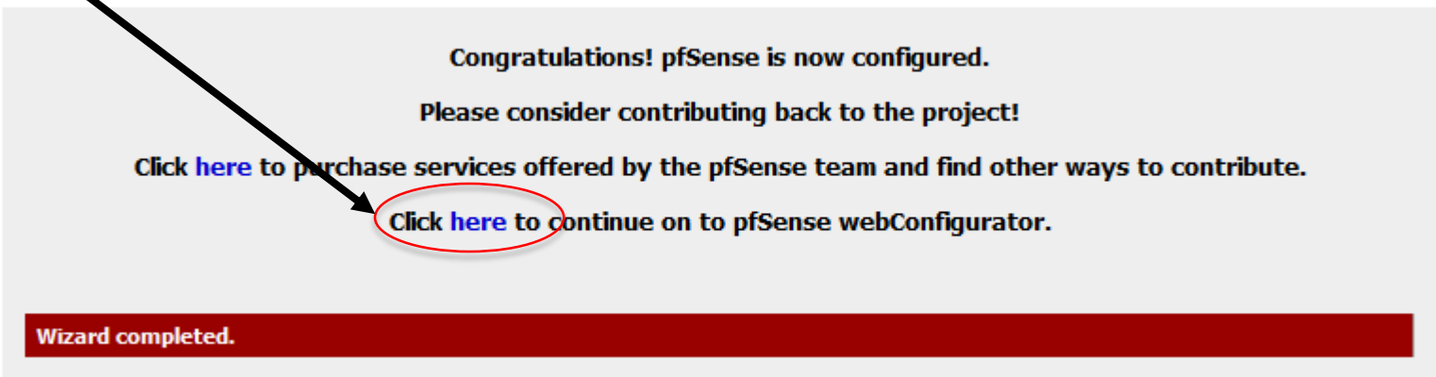


# การเข้าใช้งาน pfSense

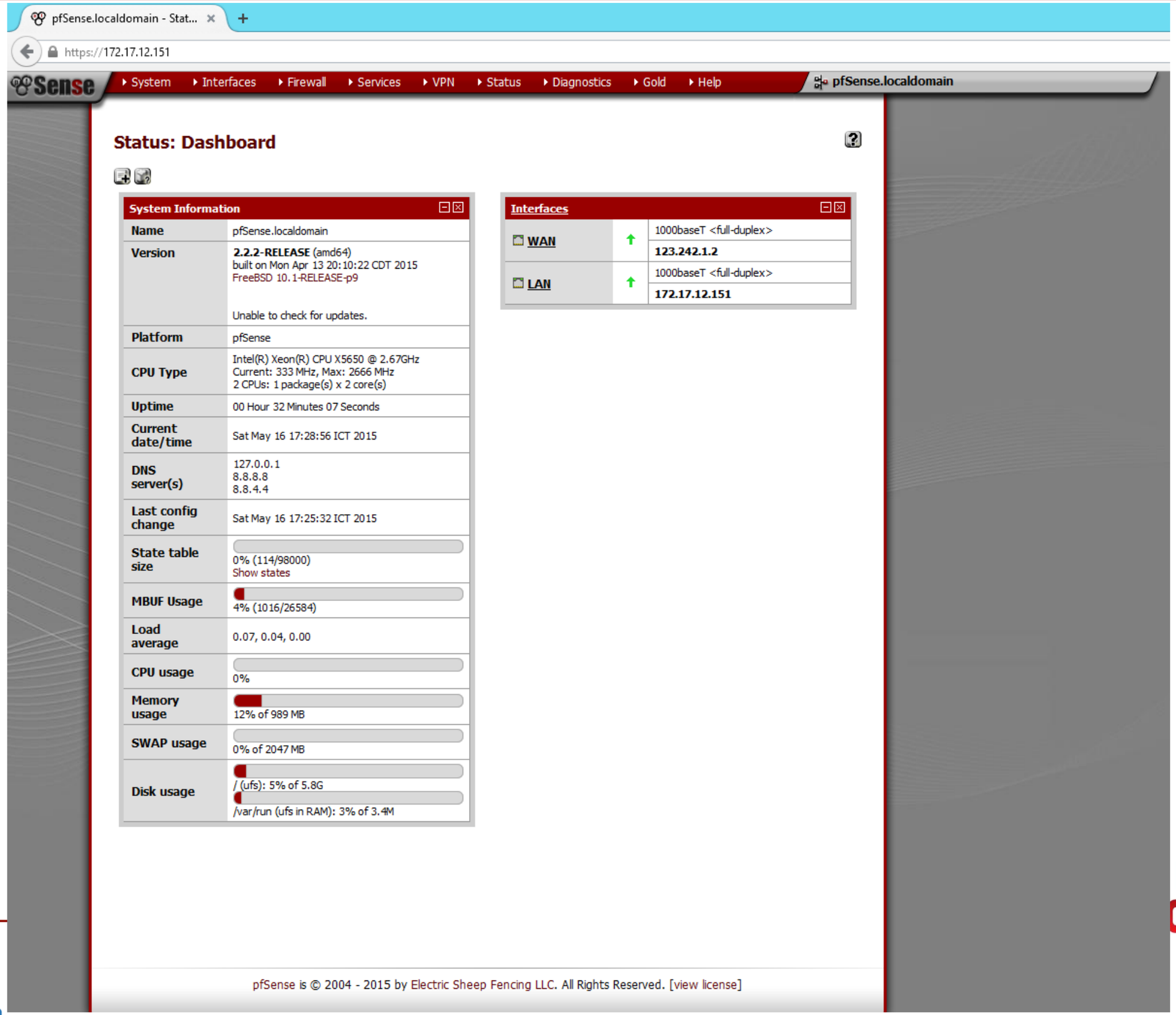


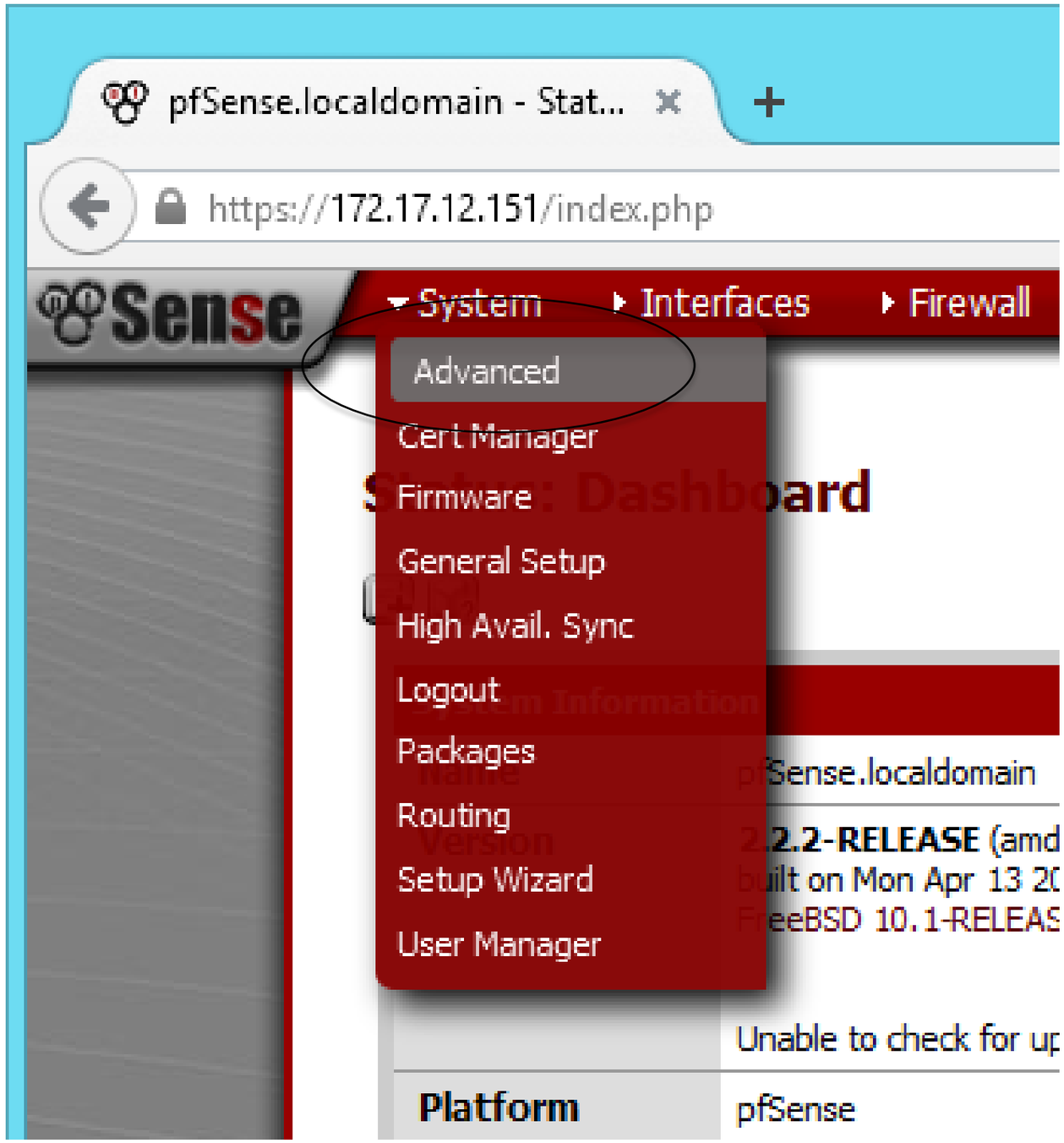




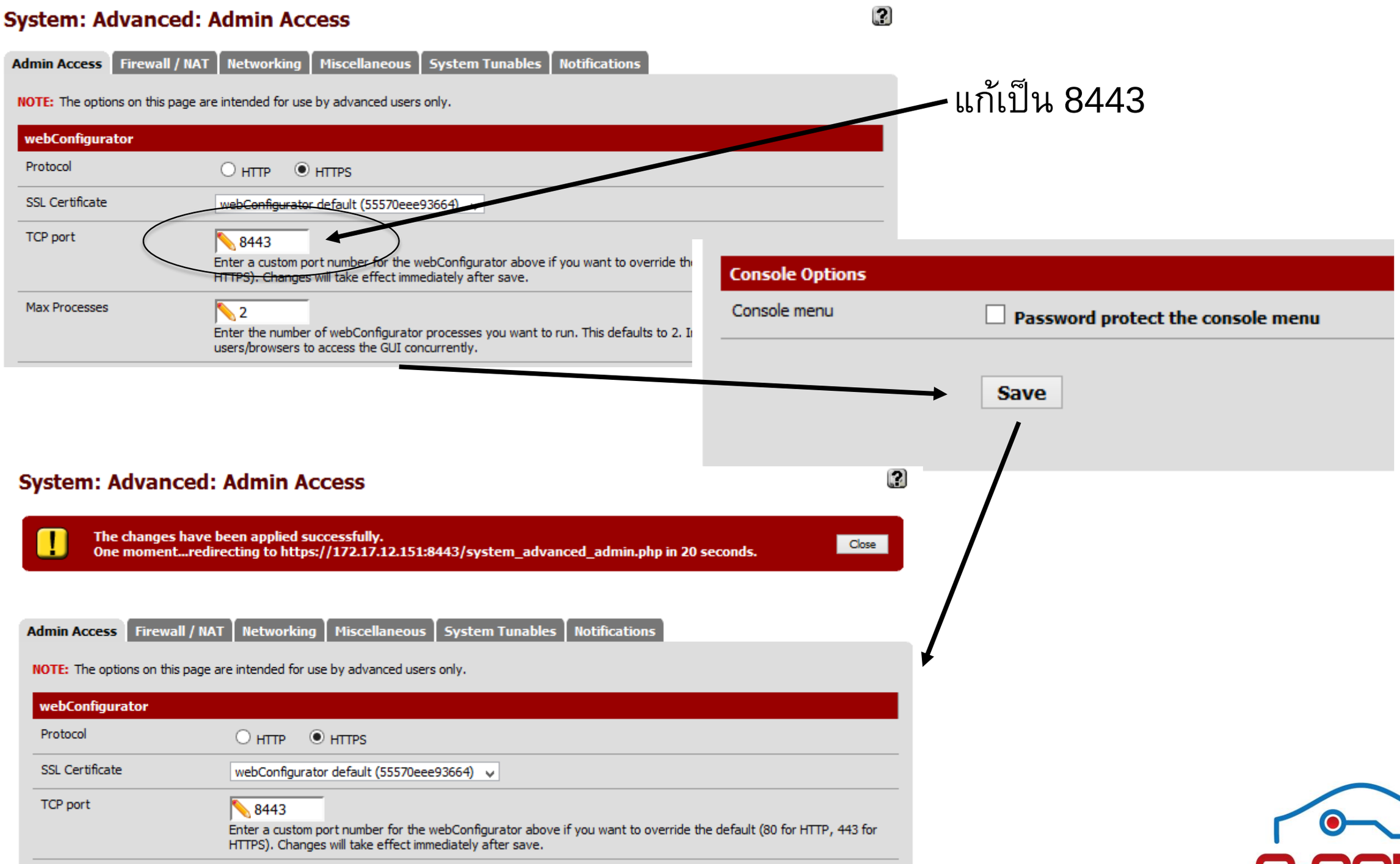
# การเข้าใช้งาน pfSense



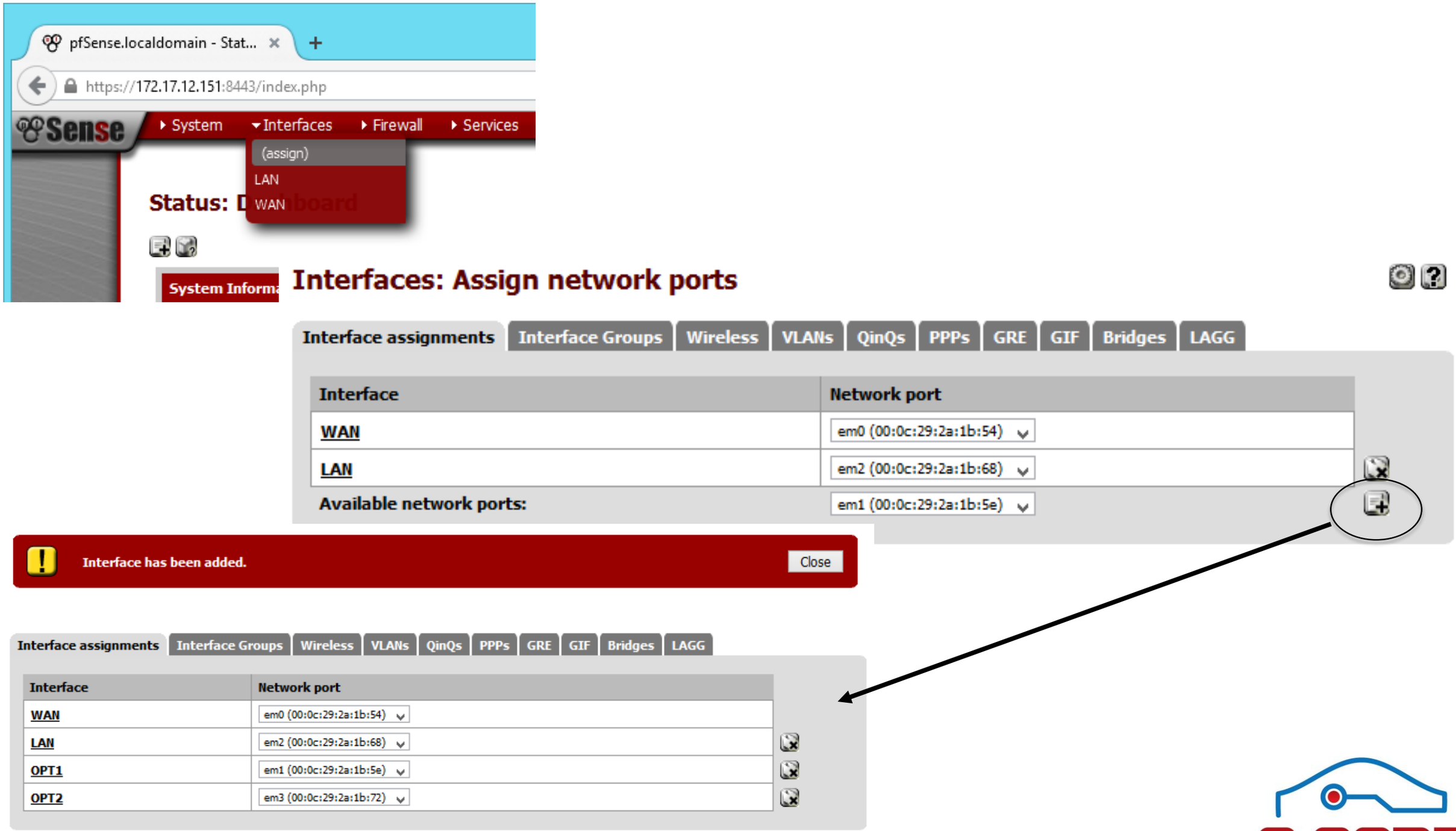
# การเปลี่ยน Management port (TCP/443 --> TCP/8443)



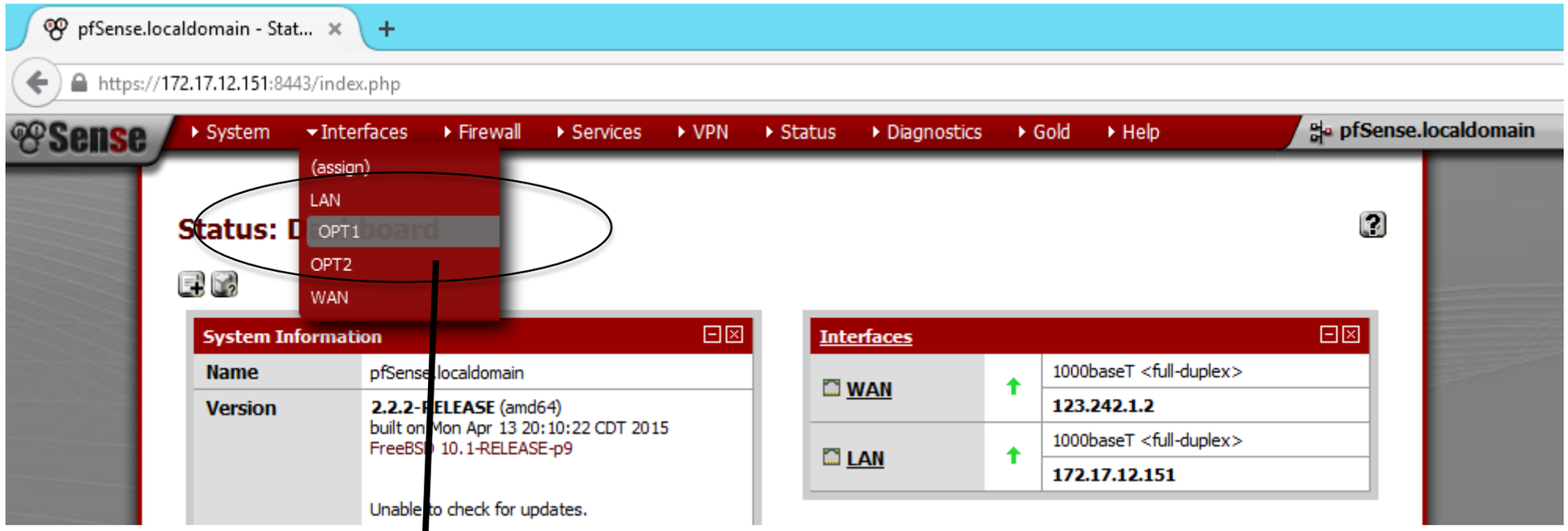
# การเปลี่ยน Management port (TCP/443 --> TCP/8443)



# การกำหนด Network Interface



# การเปลี่ยนชื่อ Interface (Network Zone) และการตั้งค่าให้ Interface




# การเปลี่ยนชื่อ Interface (Network Zone) และการตั้งค่าให้ Interface

**Interfaces: OPT1**

**General configuration**

| | |
|---|---|
| Enable | ☑ **Enable Interface** |
| Description | GIN_Private<br>Enter a description (name) for the interface here. |
| **IPv4 Configuration Type** | Static IPv4 |
| **IPv6 Configuration Type** | None |
| MAC address | Insert my local MAC address<br>This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)<br>Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank |
| MTU | 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. |
| MSS | 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. |
| Speed and duplex | Advanced - Show advanced option |

**Static IPv4 configuration**

| | |
|---|---|
| **IPv4 address** | 10.0.1.1 / 24 |
| IPv4 Upstream Gateway | None - or **add a new one.**<br>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.<br>On local LANs the upstream gateway should be "none". |

**Private networks**

☐ **Block private networks**
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.

☐ **Block bogon networks**
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.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

**Save** **Cancel**

# 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.

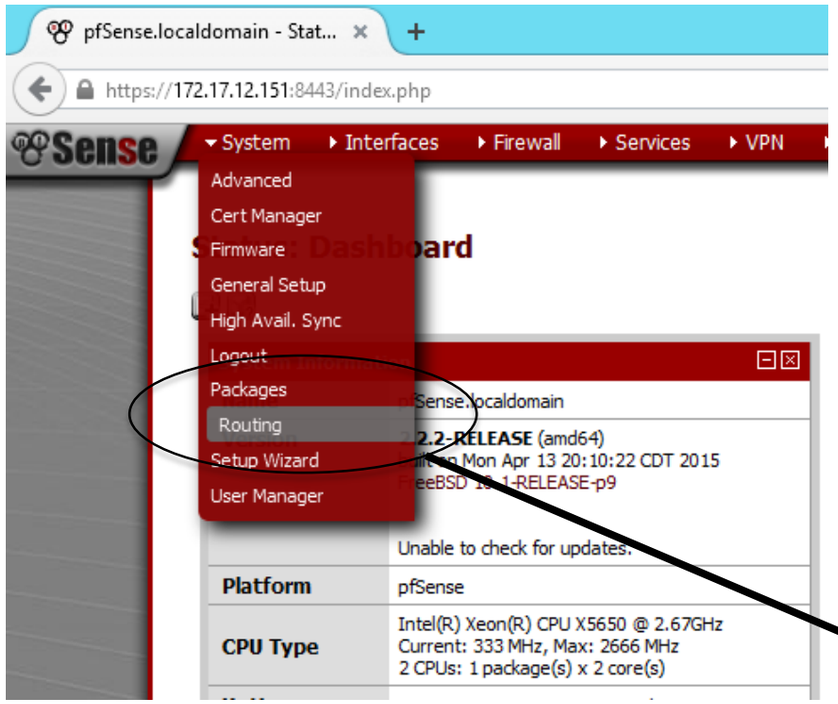
Apply changes

## Status: Dashboard

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

| Interfaces | | |
|---|---|---|
| WAN | ↑ | 1000baseT <full-duplex><br>**123.242.1.2** |
| LAN | ↑ | 1000baseT <full-duplex><br>**172.17.12.151** |
| GIN_PRIVATE | ↑ | 1000baseT <full-duplex><br>**10.0.1.1** |

# การกำหนด Routing table สำหรับ Private GIN




## System: Gateways

Gateways | Routes | Groups

| Name | Interface | Gateway | Monitor IP | Description |
|---|---|---|---|---|
| GW_WAN (default) | GIN_PUBLIC | 123.242.1.1 | 123.242.1.1 | Interface wan Gateway |

# การกำหนด Routing table สำหรับ Private GIN

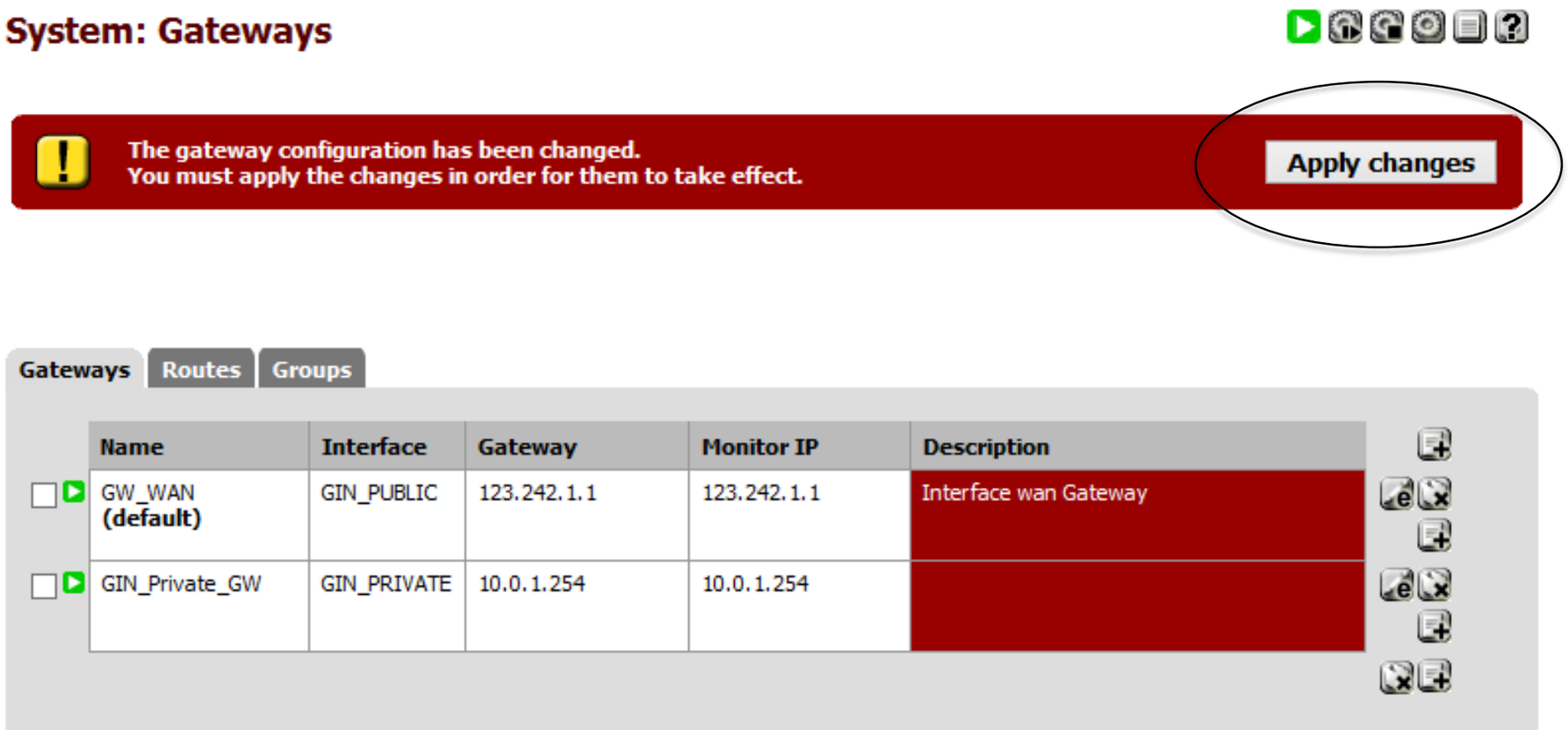
## System: Gateways: Edit gateway

**Edit gateway**

| | |
|---|---|
| **Disabled** | ☐ **Disable this gateway**<br>Set this option to disable this gateway without removing it from the list. |
| **Interface** | GIN_PRIVATE<br>Choose which interface this gateway applies to. |
| **Address Family** | IPv4<br>Choose the Internet Protocol this gateway uses. |
| **Name** | GIN_Private_GW<br>Gateway name |
| **Gateway** | 10.0.1.254<br>Gateway IP address |
| Default Gateway | ☐ **Default Gateway**<br>This will select the above gateway as the default gateway |
| Disable Gateway Monitoring | ☐ **Disable Gateway Monitoring**<br>This will consider this gateway as always being up |
| Monitor IP | **Alternative monitor IP**<br>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 | ☐ **Mark Gateway as Down**<br>This will force this gateway to be considered Down |
| Advanced | Advanced - Show advanced option |
| Description | You may enter a description here for your reference (not parsed). |

**Save** **Cancel**

# การกำหนด Routing table สำหรับ Private GIN



# การกำหนด Routing table สำหรับ Private GIN

Gateways | Routes | Groups

| Network | Gateway | Interface | Description |
|---|---|---|---|

## System: Static Routes: Edit route

**Edit route entry**

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

Save | Cancel

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

Apply changes

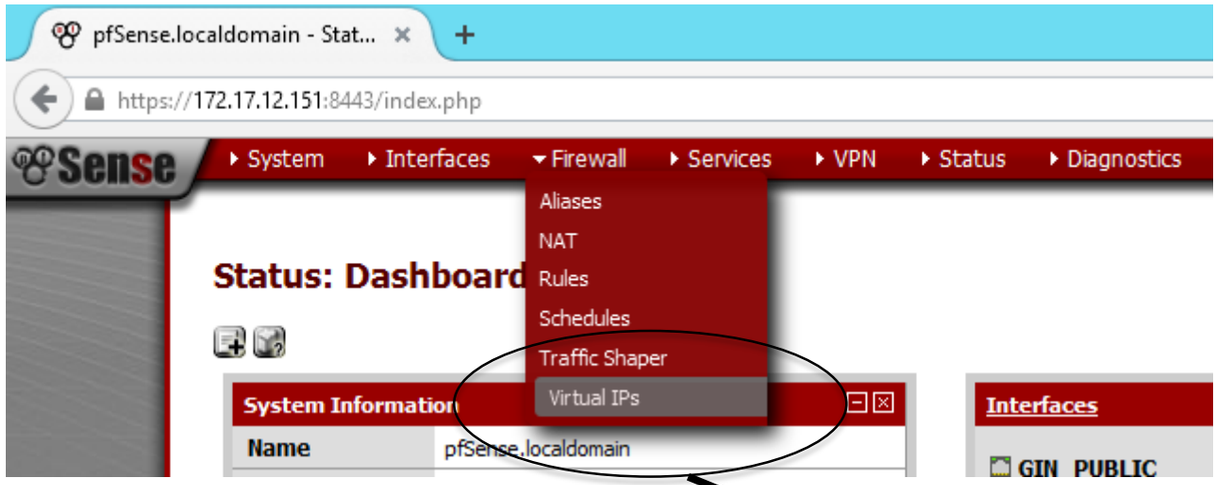
Gateways | Routes | Groups

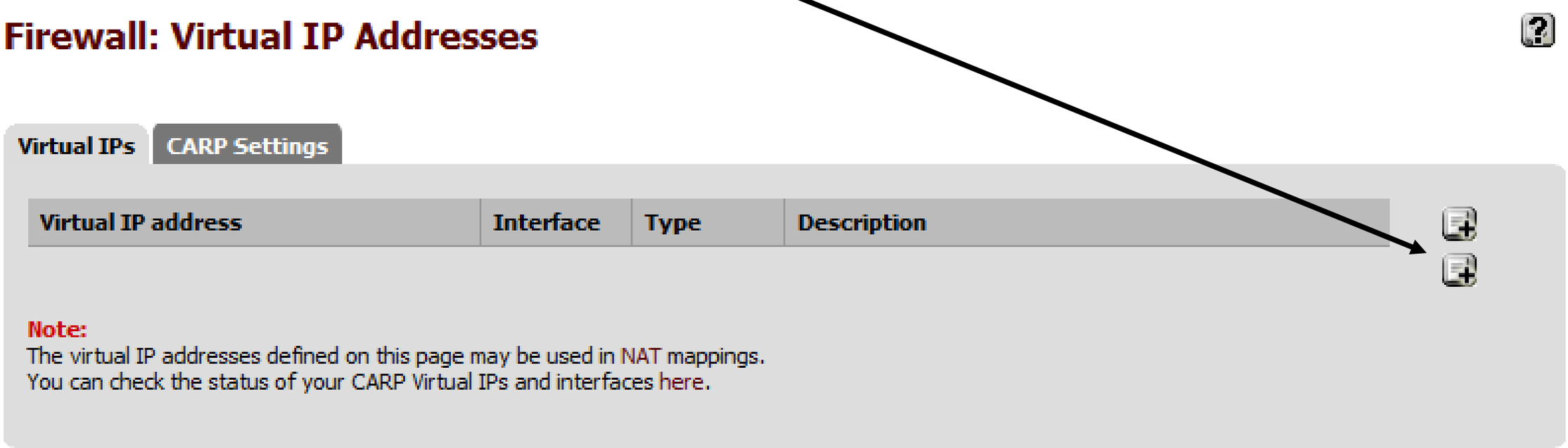
| Network | Gateway | Interface | Description |
|---|---|---|---|
| 10.0.0.0/8 | GIN_Private_GW - 10.0.1.254 | GIN_PRIVATE | |

EGA e-Government Agency

CERT by EGA

# การกำหนด Virtual IP ที่ได้รับมาจาก GIN



# การกำหนด Virtual IP ที่ได้รับมาจาก GIN

## Firewall: Virtual IP Address: Edit

**Edit Virtual IP**

| | |
|---|---|
| **Type** | ○ IP Alias ○ CARP ◉ Proxy ARP ○ Other |
| **Interface** | GIN_PUBLIC |
| **IP Address(es)** | Type: Network<br>Address: 123.242.1.0 / 28 *This is a CIDR block of proxy ARP addresses.*<br>Expansion: ☐ Disable expansion of this entry into IPs on NAT lists (e.g. 192.168.1.0/24 expands to 256 entries.) |
| **Virtual IP Password** | Enter the VHID group password. |
| **VHID Group** | 1<br>Enter the VHID group that the machines will share |
| **Advertising Frequency** | Base: 1 Skew: 0<br>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 | You may enter a description here for your reference (not parsed). |

**Save** **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.

EGA e-Government Agency

G-CERT by EGA

# 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

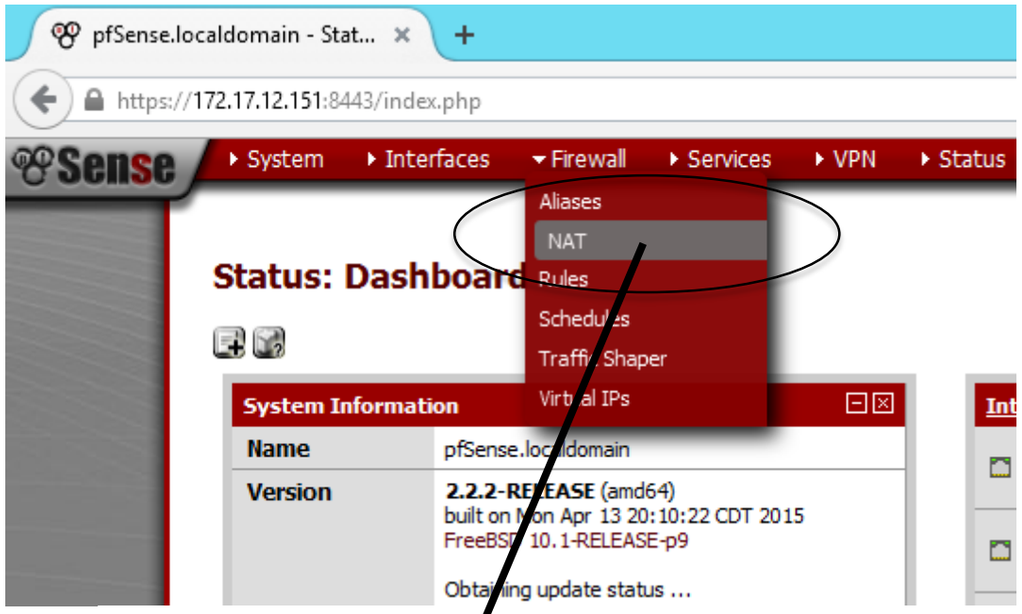
The VIP configuration has been changed.
You must apply the changes in order for them to take effect.

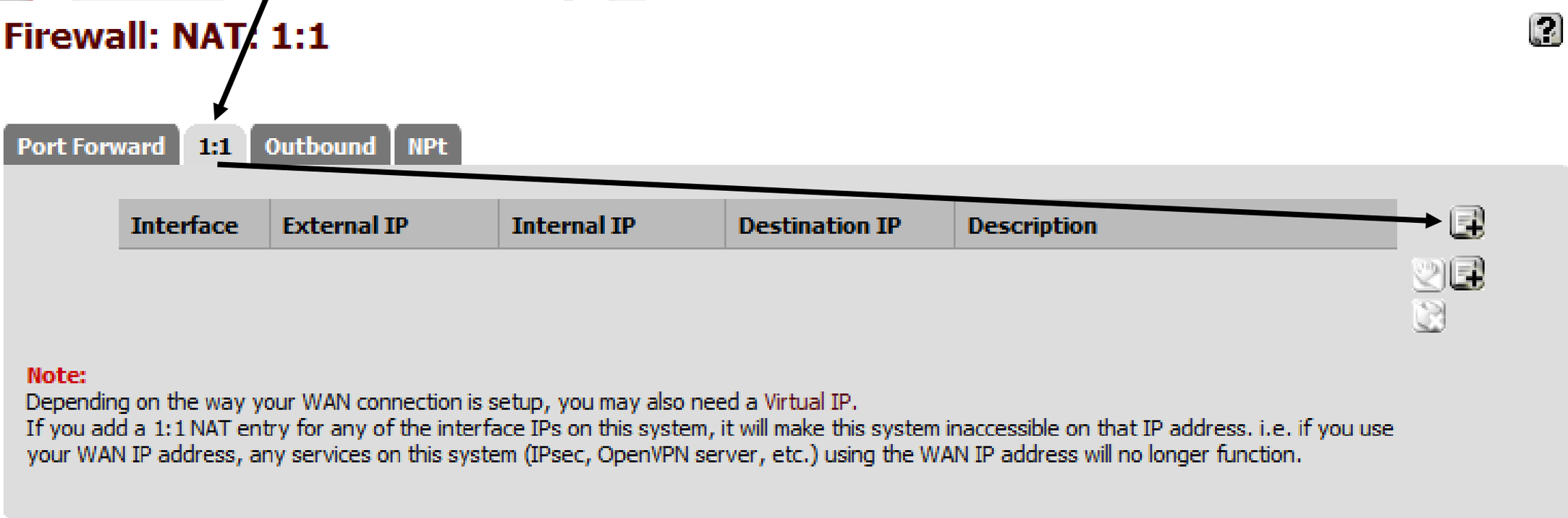
Apply changes

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



# การ NAT เพื่อใช้งาน Virtual IP กับ IP server

## Firewall: NAT: 1:1: Edit

**Edit NAT 1:1 entry**

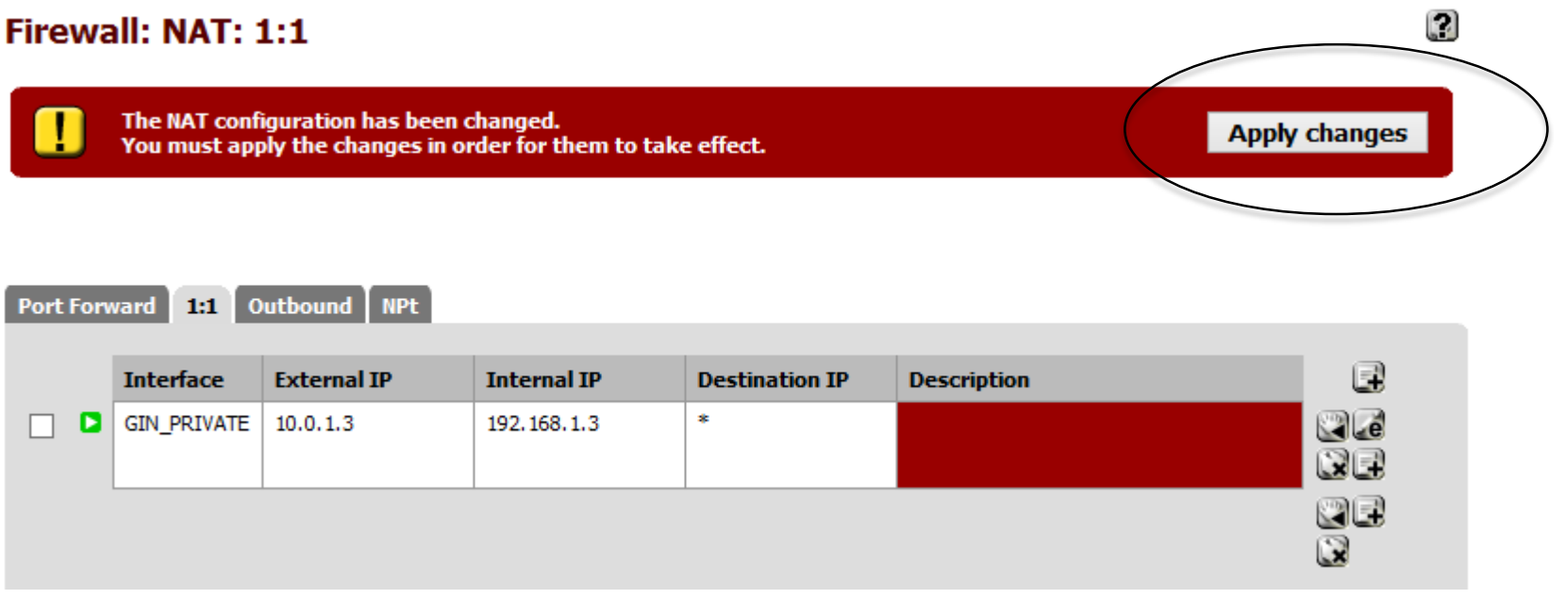
| | |
|---|---|
| **Disabled** | ☐ **Disable this rule**<br>Set this option to disable this rule without removing it from the list. |
| **Interface** | GIN_PRIVATE<br>Choose which interface this rule applies to.<br>Hint: in most cases, you'll want to use WAN here. |
| **External subnet IP** | 10.0.1.3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

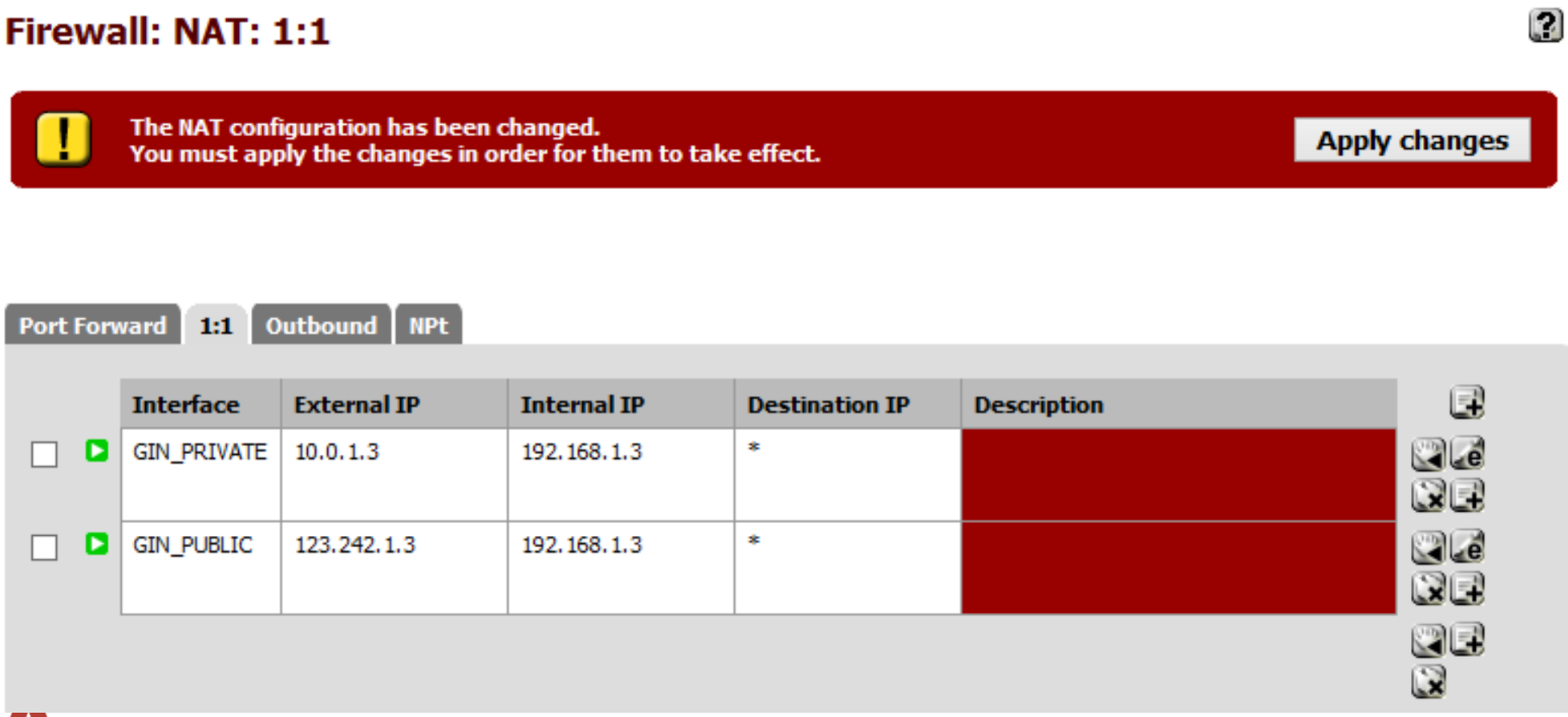
**Save** **Cancel**

EGA e-Government Agency

G-CERT by EGA

# การ NAT เพื่อใช้งาน Virtual IP กับ IP server

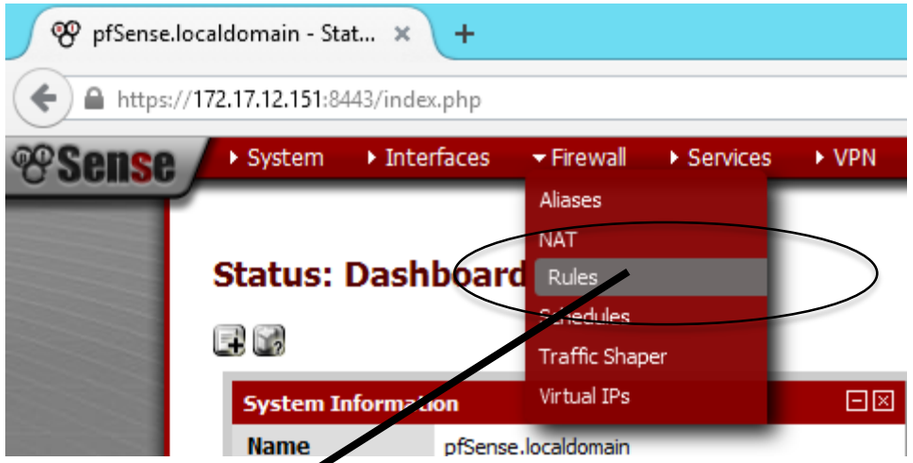


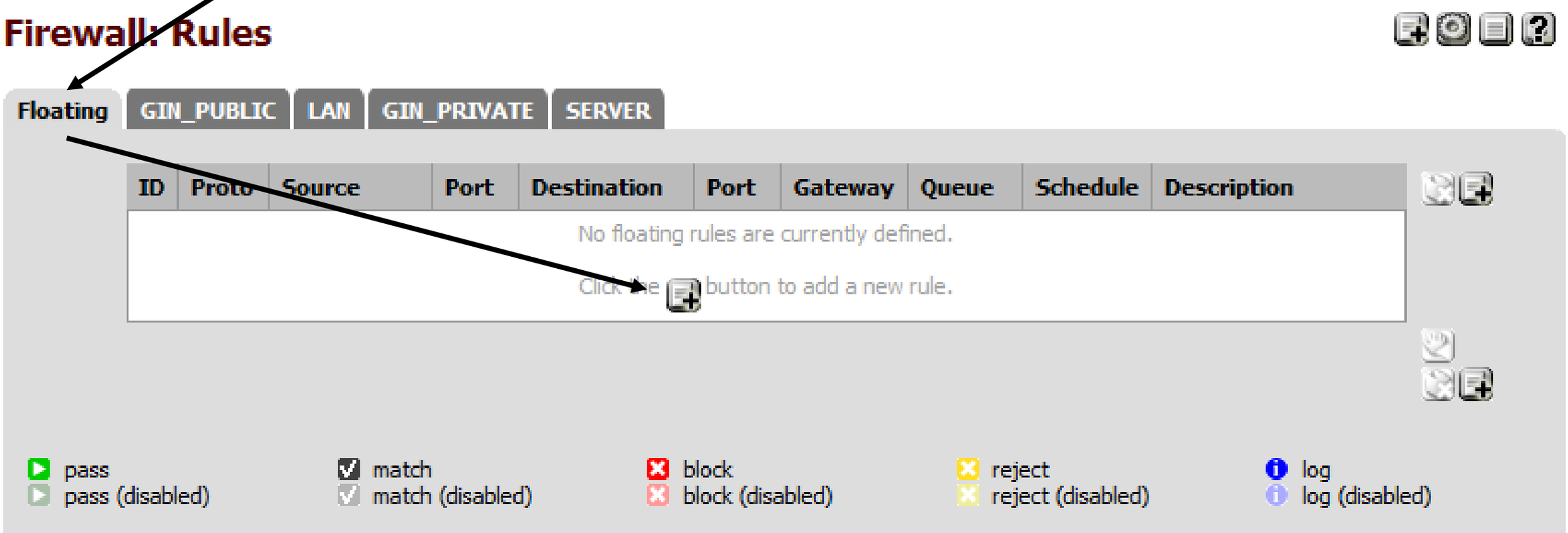




EGA e-Government Agency

G-CERT by EGA

# การกำหนด Firewall rules เบื้องต้น



# การกำหนด Firewall rules เบื้องต้น

## Firewall: Rules: Edit

**Edit Firewall rule**

| | |
|---|---|
| **Action** | Pass<br>Choose what to do with packets that match the criteria specified below.<br>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. |
| **Disabled** | ☐ **Disable this rule**<br>Set this option to disable this rule without removing it from the list. |
| **Quick** | ☐ **Apply the action immediately on match.**<br>Set this option if you need to apply this action to traffic that matches this rule immediately. |
| **Interface** | GIN_PUBLIC<br>LAN<br>GIN_PRIVATE<br>SERVER<br>Choose the interface(s) for this rule. |
| **Direction** | any |
| **TCP/IP Version** | IPv4 **Select the Internet Protocol version this rule applies to** |
| **Protocol** | ICMP<br>Choose which IP protocol this rule should match.<br>Hint: in most cases, you should specify *TCP* here. |
| ICMP type | any<br>If you selected ICMP for the protocol above, you may specify an ICMP type here. |
| **Source** | ☐ **not**<br>Use this option to invert the sense of the match.<br>Type: any<br>Address: / 127 |
| **Destination** | ☐ **not**<br>Use this option to invert the sense of the match.<br>Type: Single host or alias<br>Address: 192.168.1.3 / 31 |
| **Log** | ☑ **Log packets that are handled by this rule**<br>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). |
| Description | You may enter a description here for your reference. |

**Save** **Cancel**

EGA e-Government Agency

G-CERT by EGA

# 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** | Pass<br>Choose what to do with packets that match the criteria specified below.<br>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. |
| **Disabled** | ☐ **Disable this rule**<br>Set this option to disable this rule without removing it from the list. |
| **Quick** | ☐ **Apply the action immediately on match.**<br>Set this option if you need to apply this action to traffic that matches this rule immediately. |
| **Interface** | GIN_PUBLIC<br>LAN<br>GIN_PRIVATE<br>SERVER<br>Choose the interface(s) for this rule. |
| **Direction** | any |
| **TCP/IP Version** | IPv4 **Select the Internet Protocol version this rule applies to** |
| **Protocol** | TCP<br>Choose which IP protocol this rule should match.<br>Hint: in most cases, you should specify *TCP* here. |
| **Source** | ☐ **not**<br>Use this option to invert the sense of the match.<br>Type: any<br>Address: / 127<br>Advanced - Show source port range |
| **Destination** | ☐ **not**<br>Use this option to invert the sense of the match.<br>Type: Single host or alias<br>Address: 192.168.1.3 / 31 |
| **Destination port range** | from: HTTP (80)<br>to: HTTP (80)<br>Specify the port or port range for the destination of the packet for this rule.<br>Hint: you can leave the *'to'* field empty if you only want to filter a single port |
| **Log** | ☑ **Log packets that are handled by this rule**<br>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). |
| Description | You may enter a description here for your reference. |

**Save** **Cancel**

EGA e-Government Agency

G-CERT by EGA

# 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 | | |
| | IPv4 TCP | * | * | 192.168.1.3 | 80 (HTTP) | * | none | | |
| | IPv4 TCP | * | * | 192.168.1.3 | 443 (HTTPS) | * | none | | |
| | IPv4 TCP | * | * | 192.168.1.3 | 3389 (MS RDP) | * | none | | |

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

fw_A.ega.or.th - Status: Da...

https://172.17.12.151:8443/index.php

pfSense | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | fw_A.ega.

- CARP (failover)
- Dashboard
- DHCP Leases
- DHCPv6 Leases
- Filter Reload
- Gateways
- Interfaces
- IPsec
- Load Balancer
- NTP
- OpenVPN
- Package Logs
- Queues
- RRD Graphs
- Services
- System Logs
- Traffic Graph
- UPnP & NAT-PMP

## Status: Dashboard

**System Information**

| | |
|---|---|
| Name | fw_A.ega.or.th |
| Version | **2.2.2-RELEASE** (amd64)<br>built on Mon Apr 13 20:10:22 CDT 2015<br>FreeBSD 10.1-RELEASE-p9<br><br>Unable to check for updates. |
| Platform | pfSense |
| CPU Type | Intel(R) Xeon(R) CPU X5650 @ 2.67GHz<br>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<br>10.10.44.14 |
| Last config change | Sat May 16 21:04:24 ICT 2015 |
| State table size | 0% (63/98000)<br>Show states |
| 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<br>/var/run (ufs in RAM): 3% of 3.4M |

| | |
|---|---|
| 1000baseT <full-duplex> | **123.242.1.2** |
| 1000baseT <full-duplex> | **172.17.12.151** |
| 1000baseT <full-duplex> | **10.0.1.1** |
| 1000baseT <full-duplex> | **192.168.1.1** |

EGA e-Government Agency

G-CERT by EGA

# 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 | Source Port | Protocol | Quantity

Interface | Destination IP Address | Destination Port | Protocol Flags | Filter

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

Action: Pass / Block

Time | Source IP Address | 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.

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

EGA e-Government Agency

G-CERT by EGA

# 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 | Protocol Flags | 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

EGA e-Government Agency

G-CERT by EGA

# 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 | Protocol Flags | Filter

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

EGA e-Government Agency

G-CERT by EGA

# 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 | Source Port | Protocol | Quantity

Interface | Destination IP Address | Destination Port | Protocol Flags | Filter

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 |

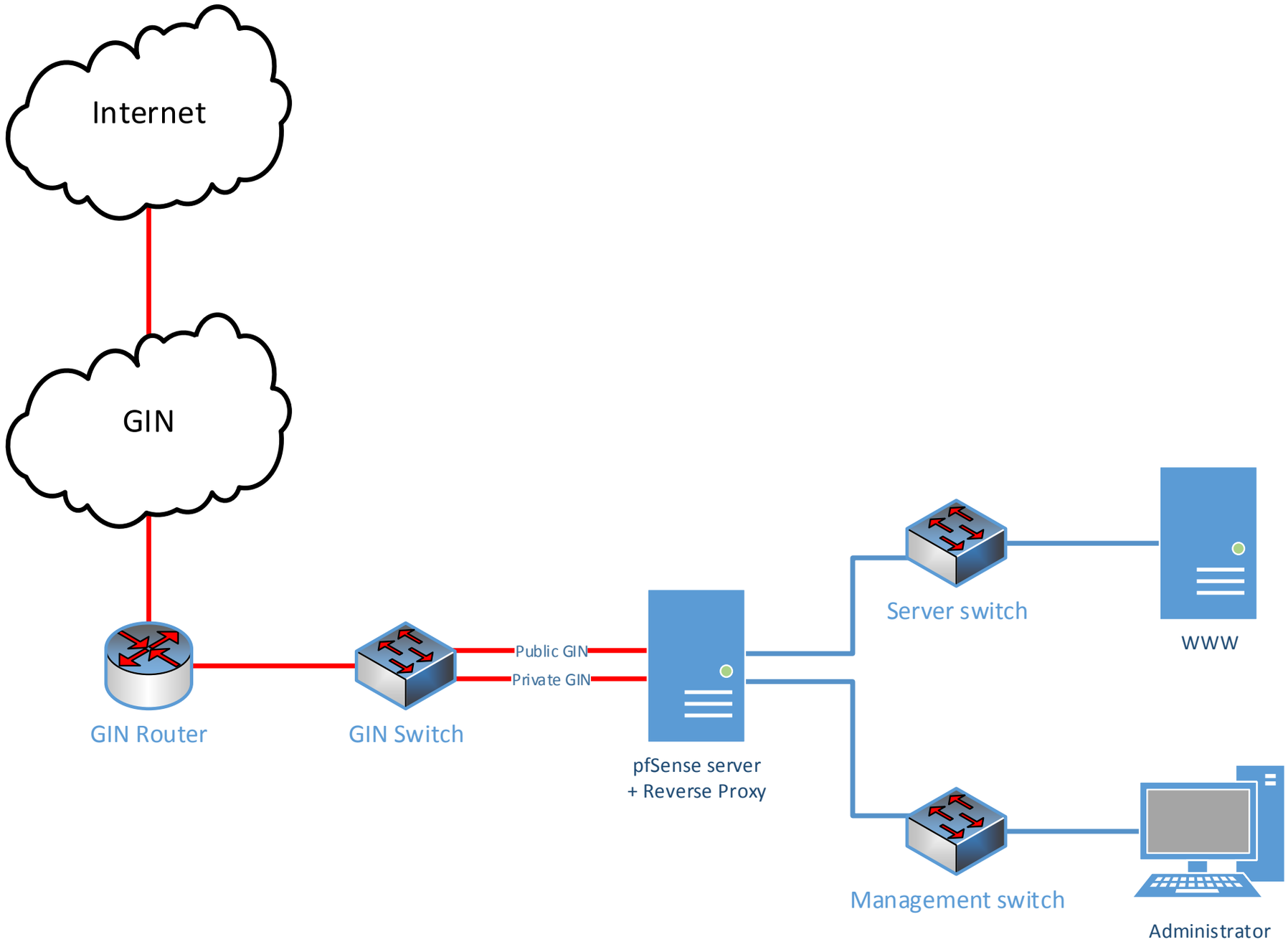
Clear log

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

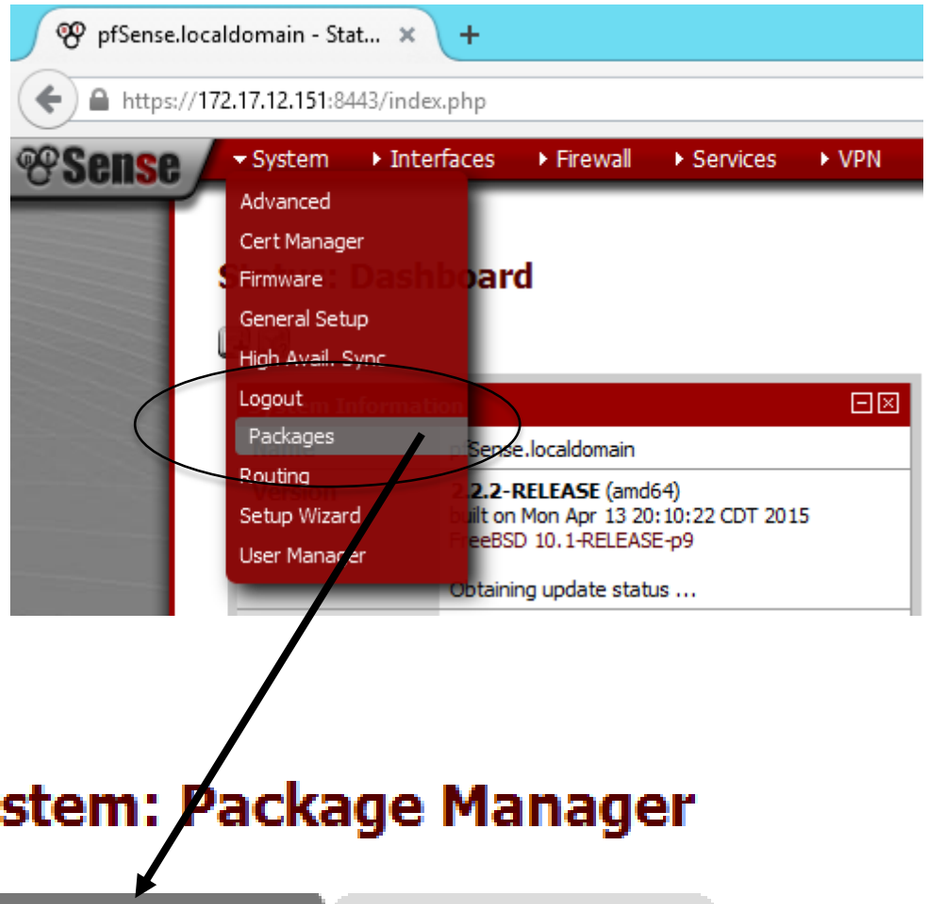
EGA e-Government Agency

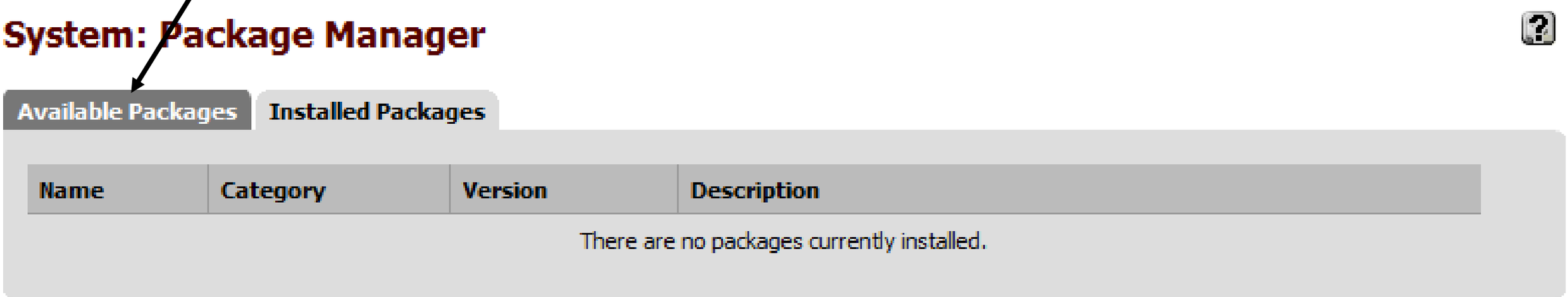
G-CERT by EGA

# การใช้งาน pfSense เป็น Reverse Proxy

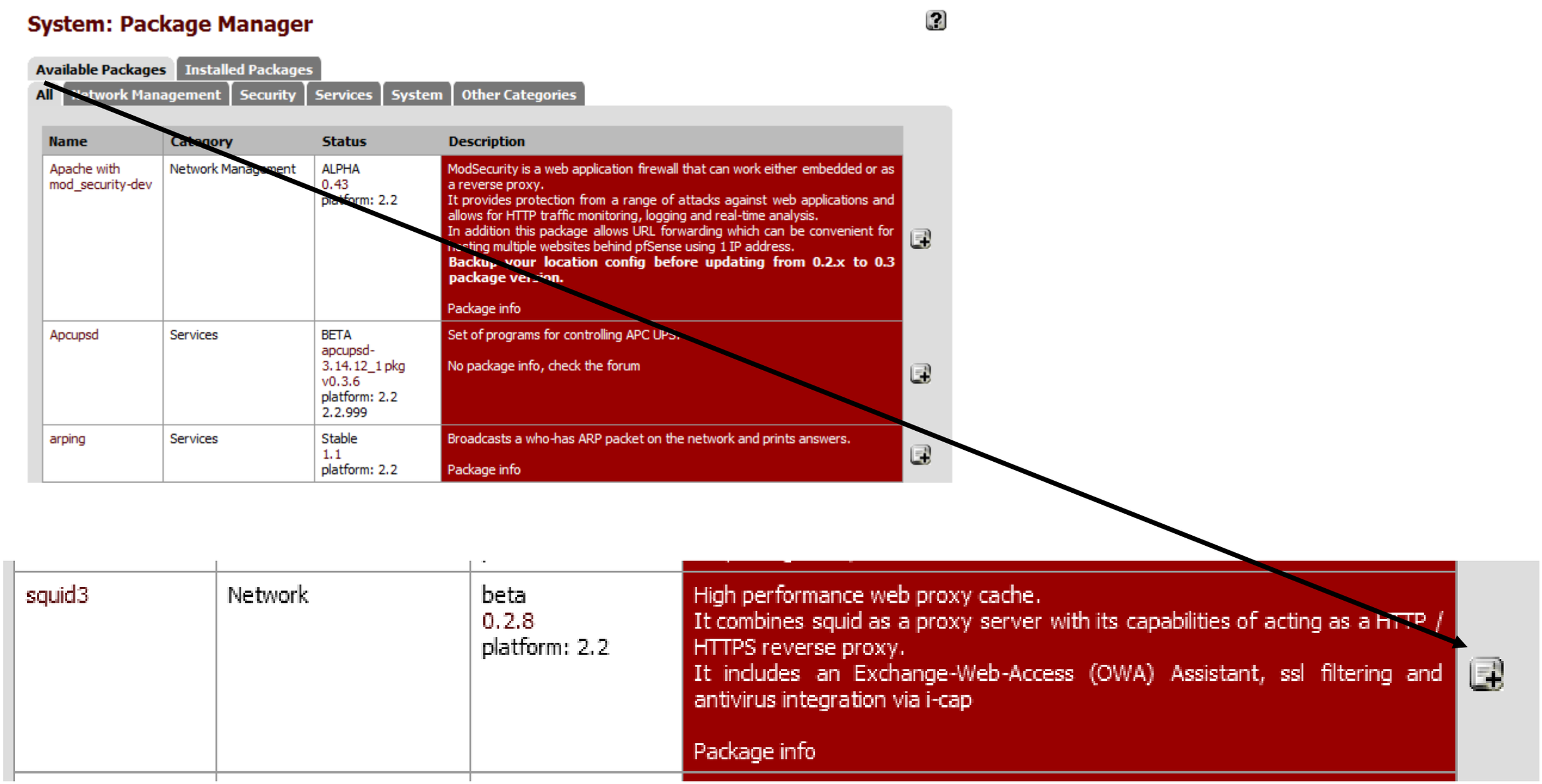


# การใช้งาน pfSense เป็น Reverse Proxy

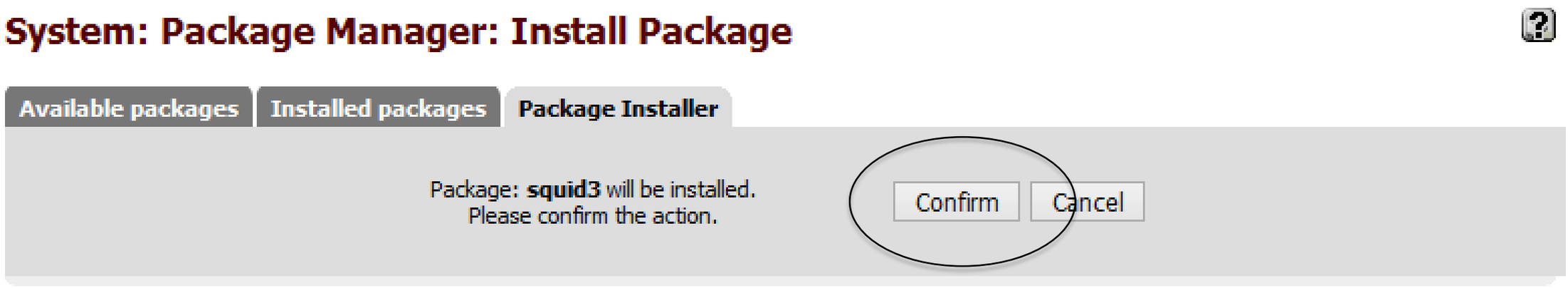


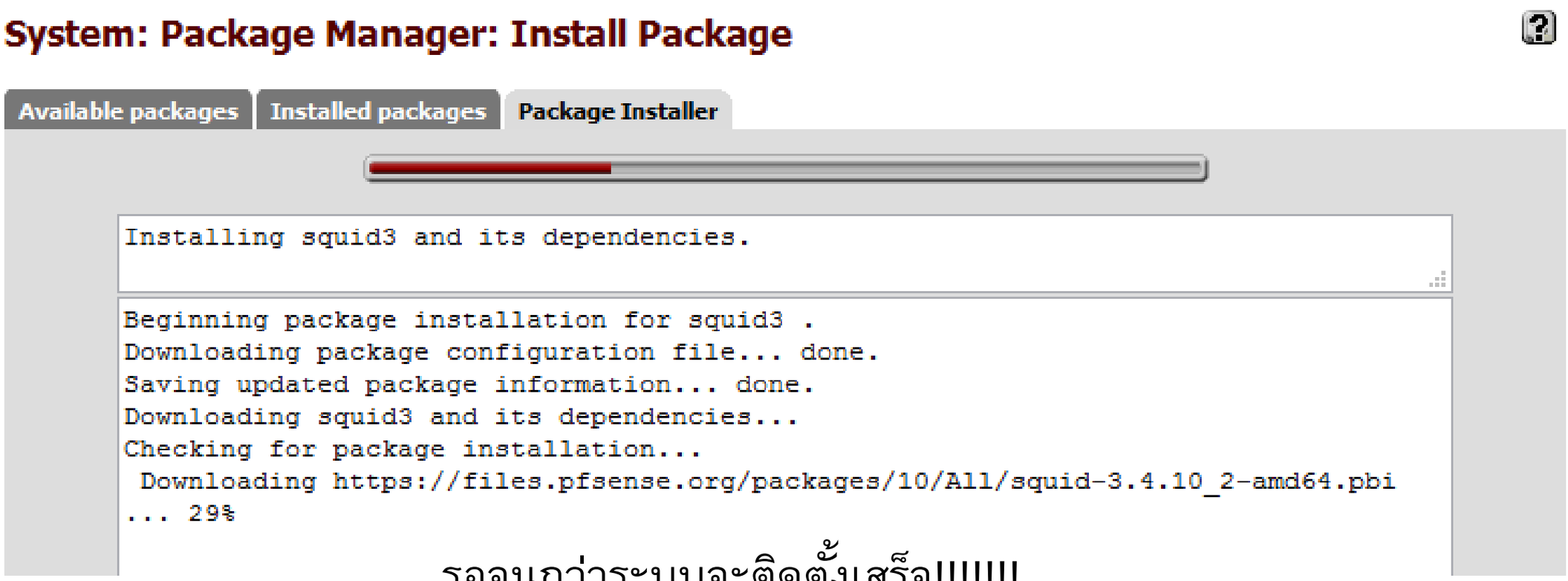



# การใช้งาน pfSense เป็น Reverse Proxy



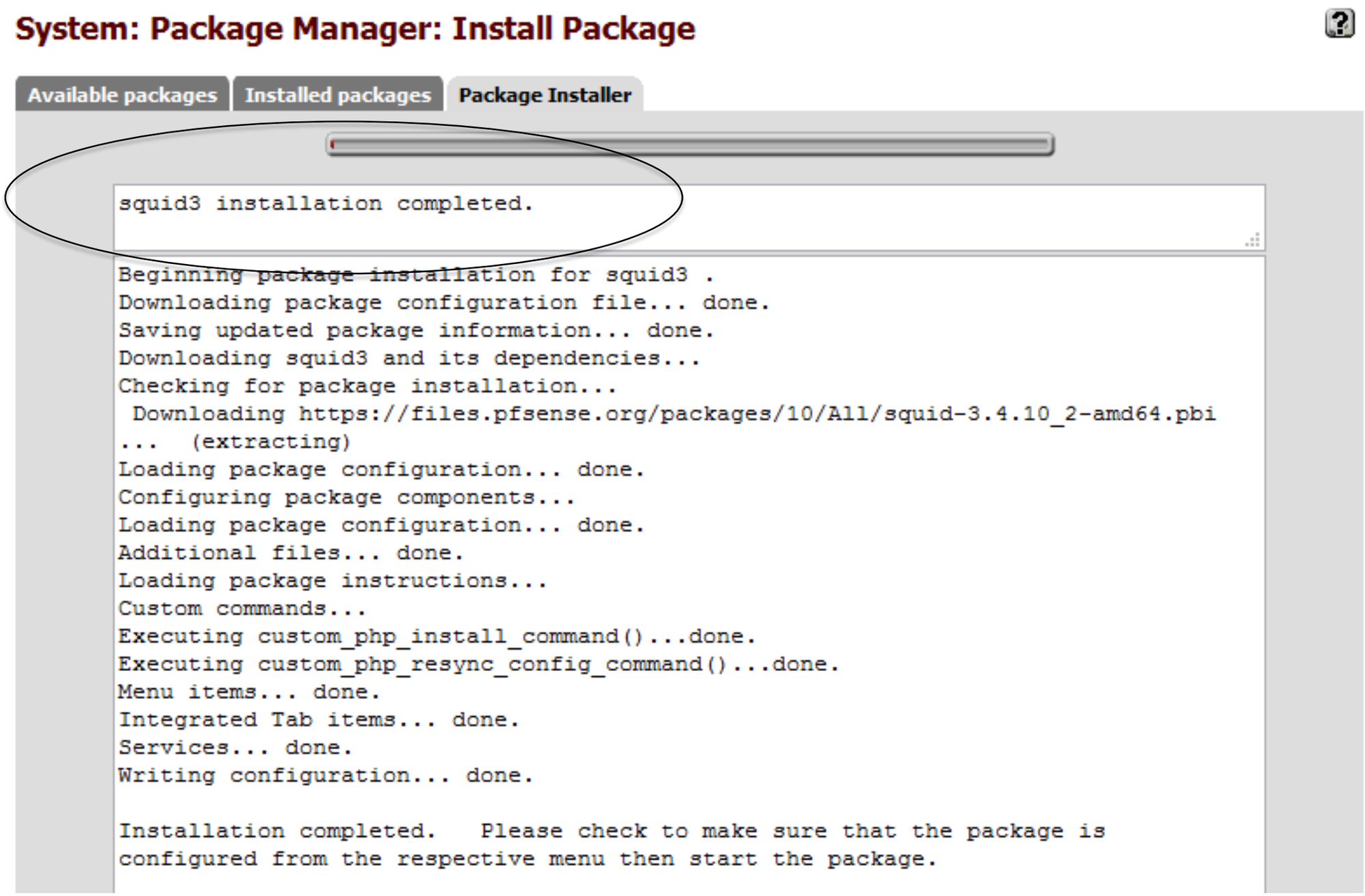
# การใช้งาน pfSense เป็น Reverse Proxy



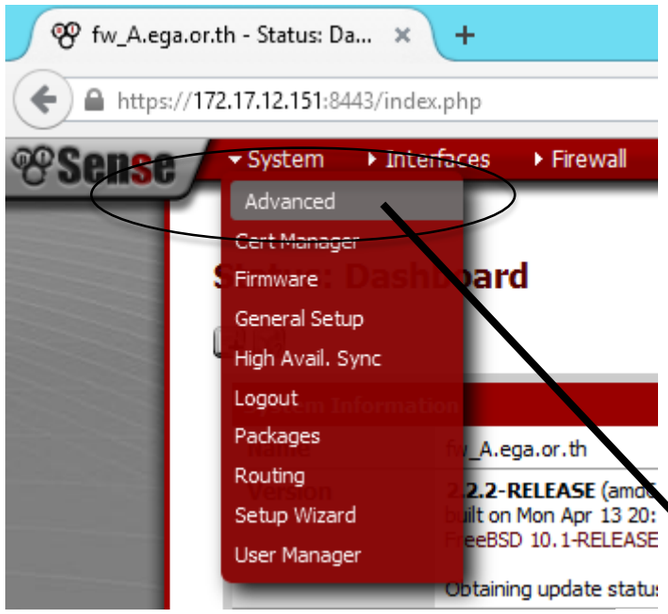



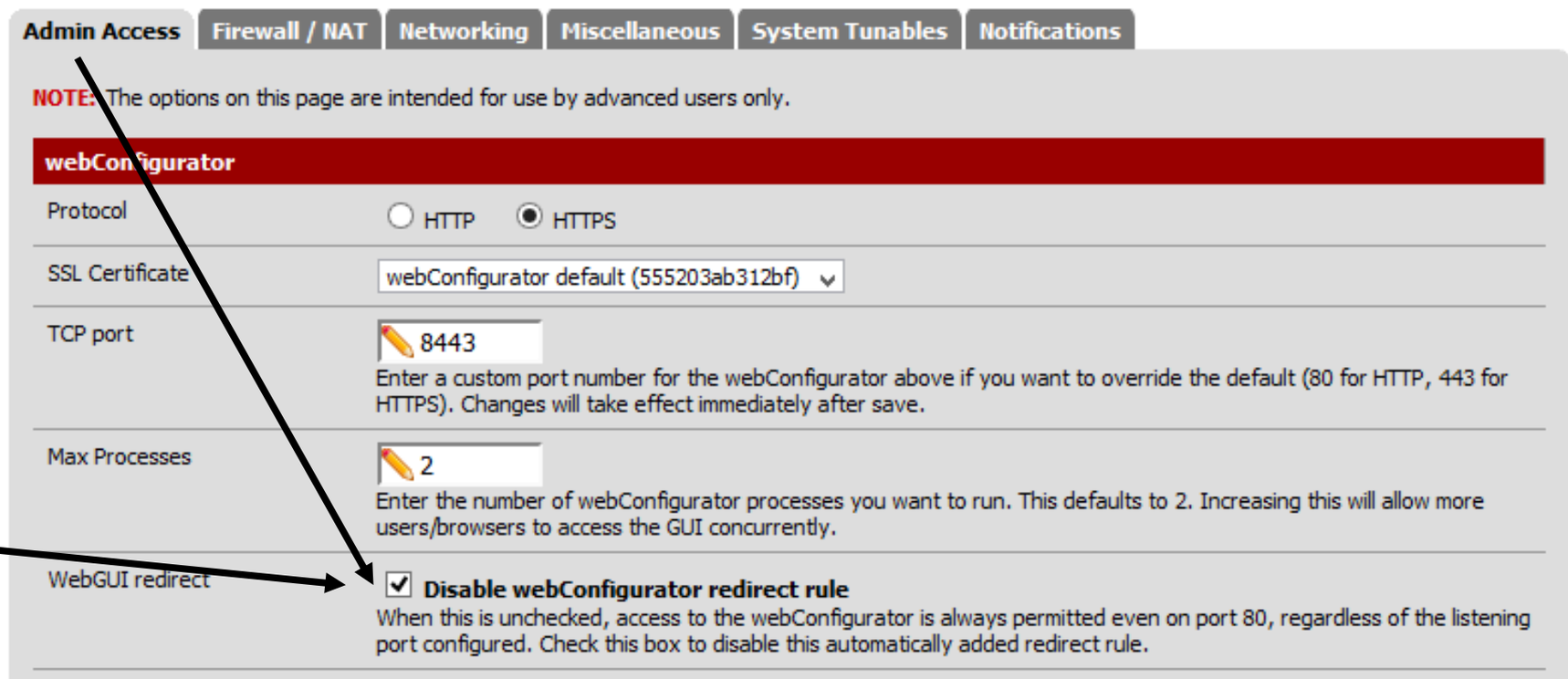

รอจนกว่าระบบจะติดตั้งเสร็จ!!!!!!!

# การใช้งาน pfSense เป็น Reverse Proxy



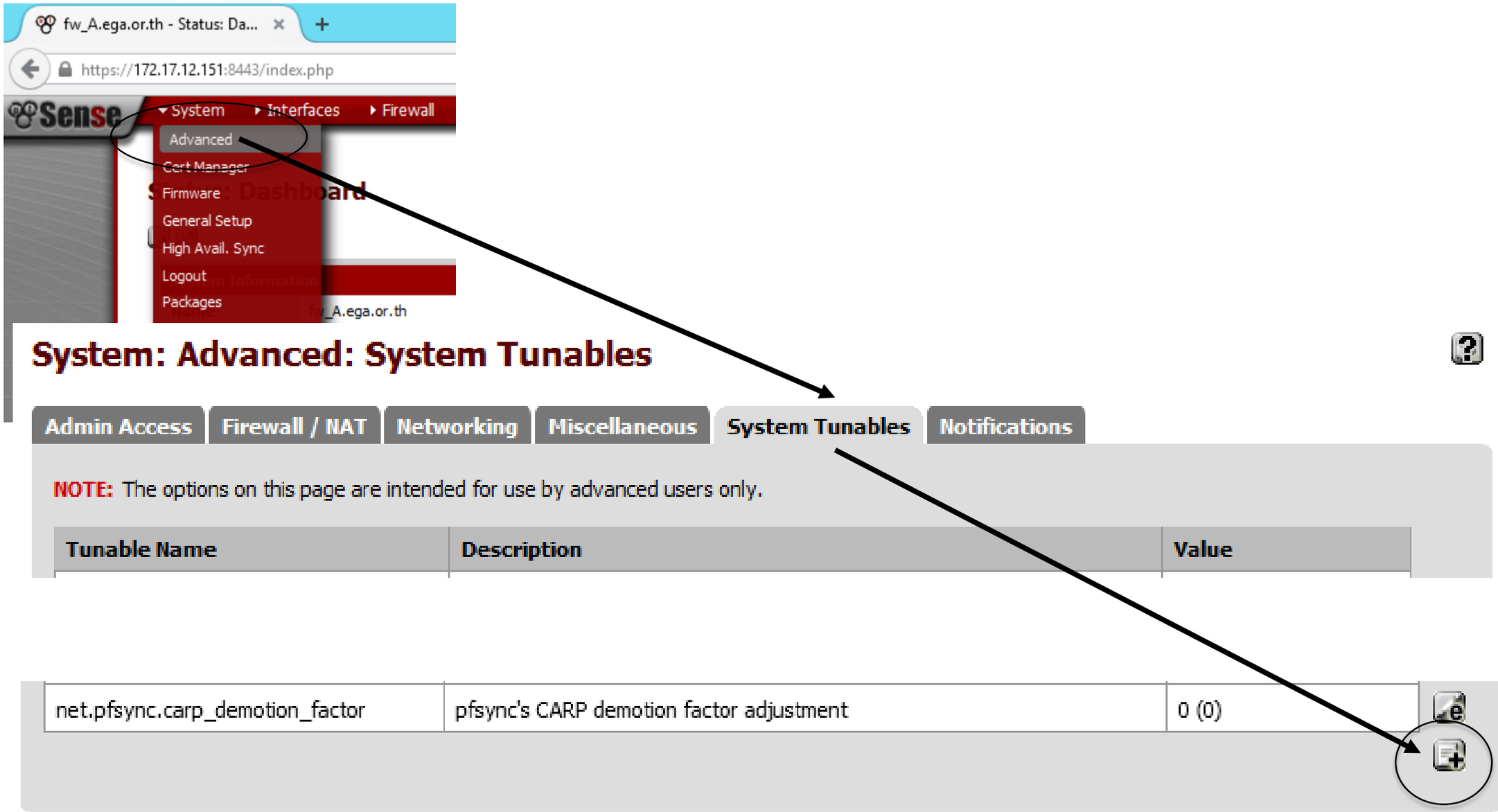
# การตั้งค่า Reverse Proxy



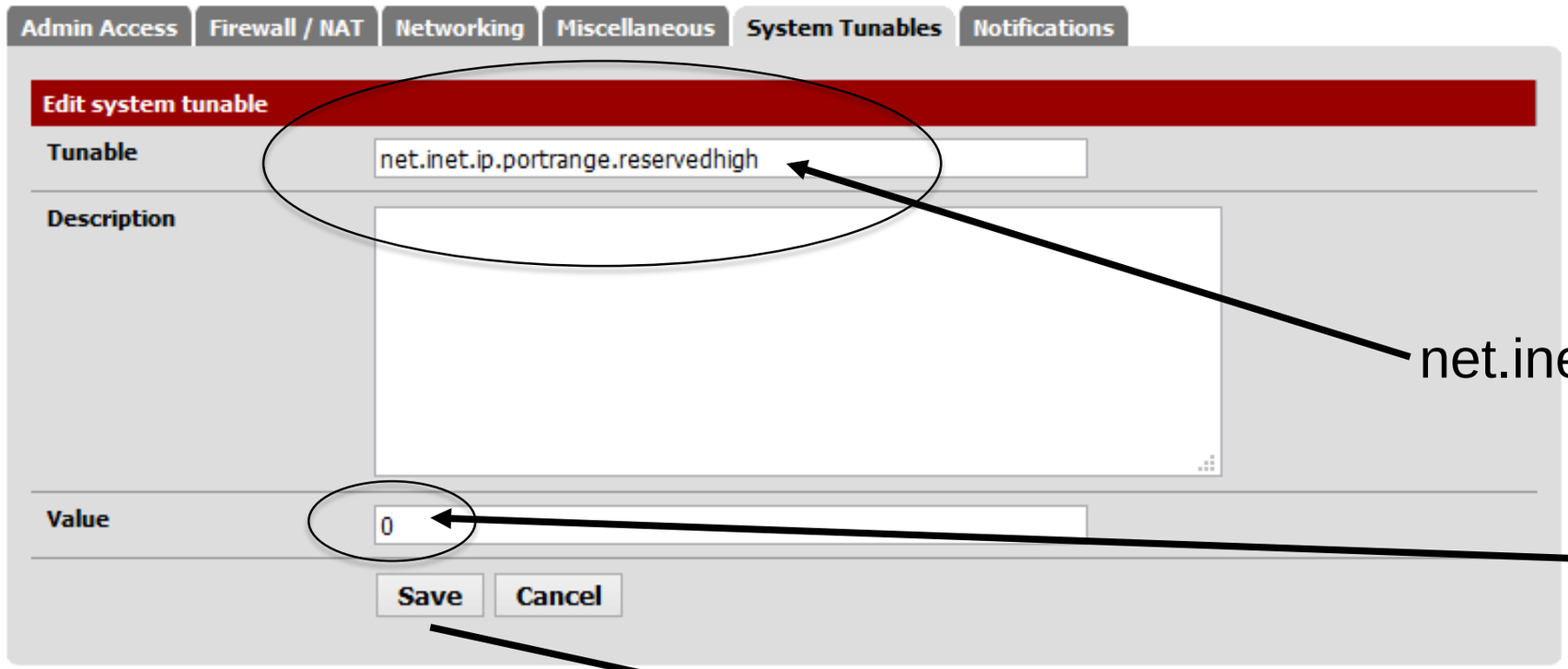




เลือก Disable….

# การตั้งค่า Reverse Proxy

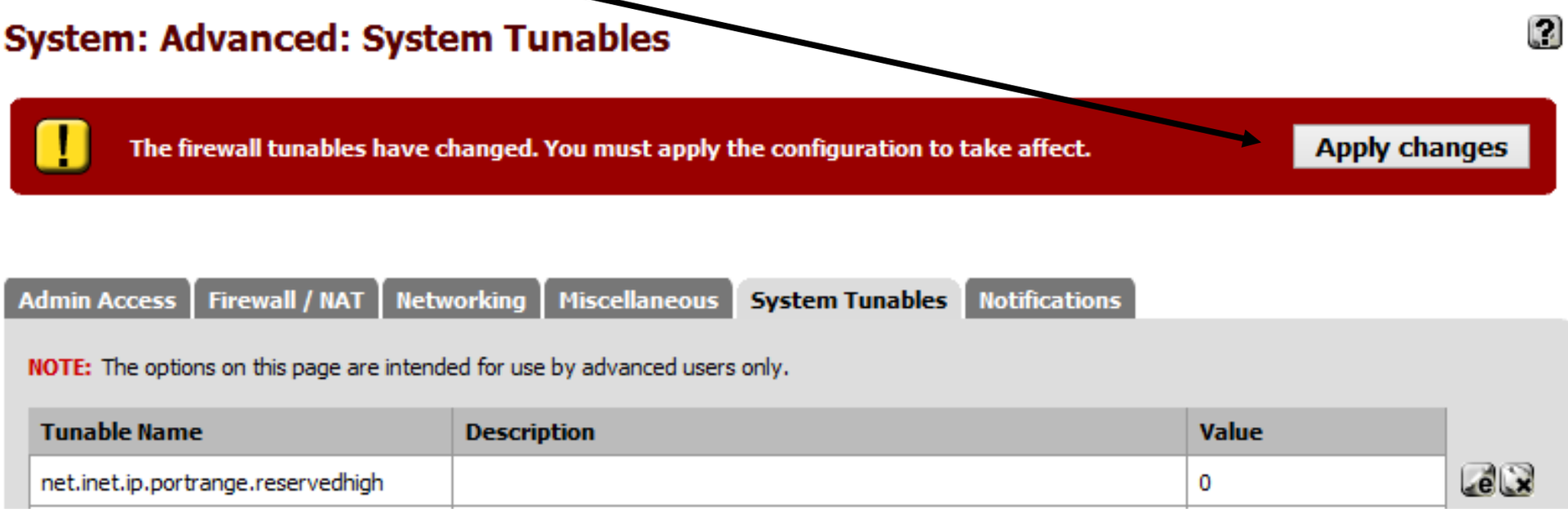


# การตั้งค่า Reverse Proxy

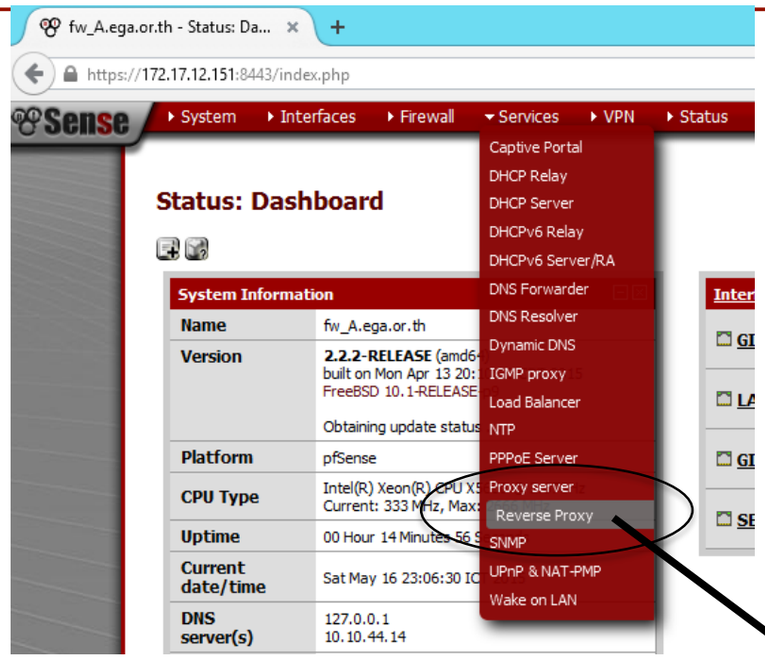


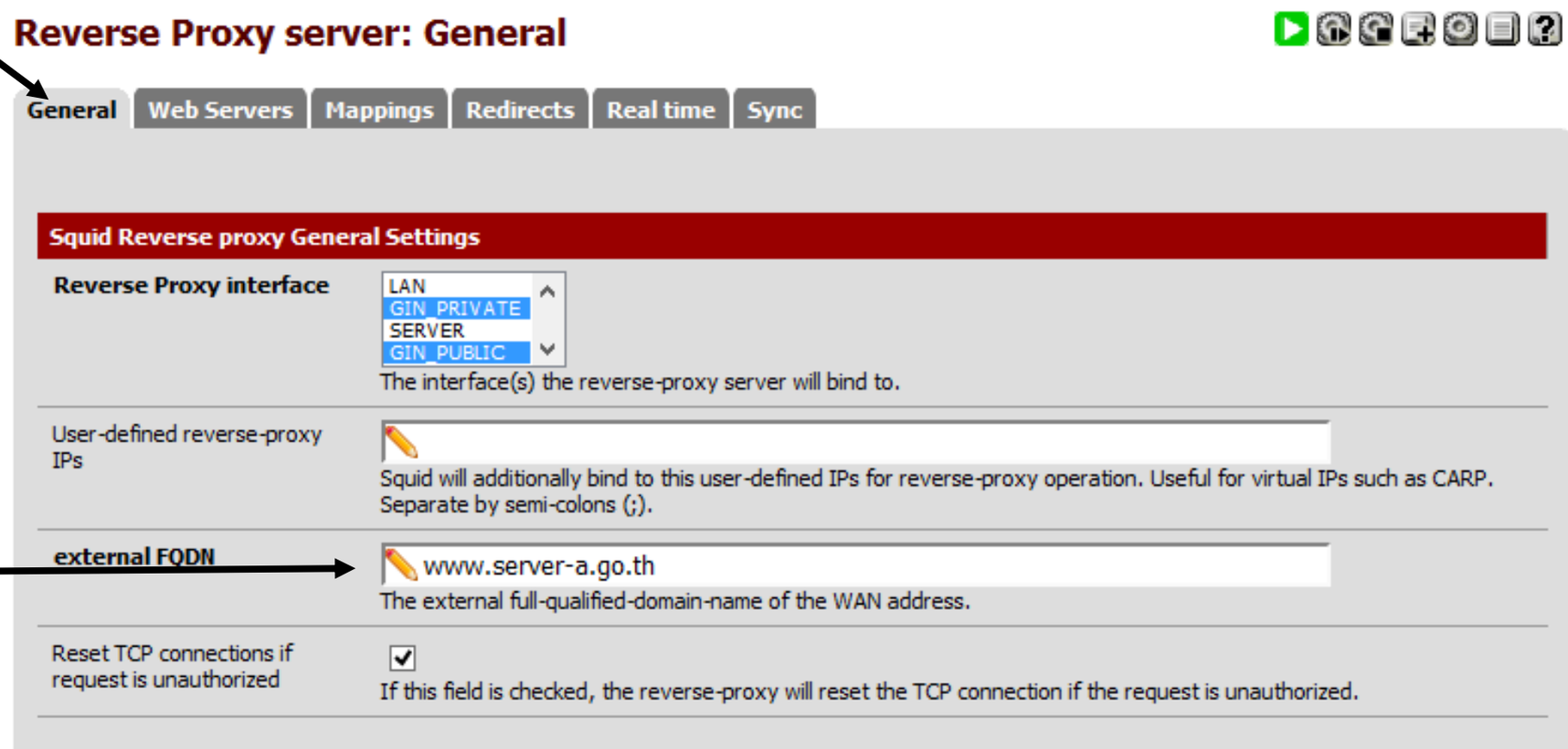

net.inet.ip.portrange.reservedhigh

0 (เลขศูนย์)



# การตั้งค่า Reverse Proxy




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 | 80 This is the port the HTTP reverse-proxy will listen on. (leave empty to use 80) |
| reverse HTTP default site | www.server-a.go.th This is the HTTP reverse default site. (leave empty to use the external fqdn) |

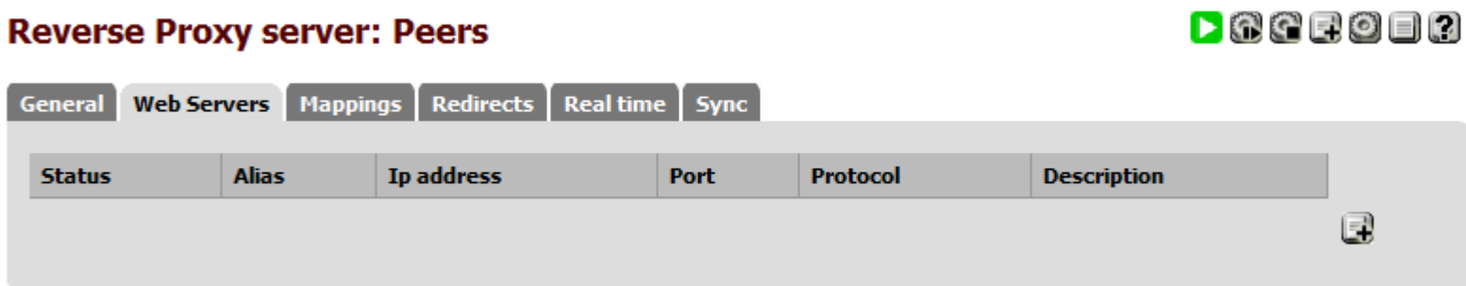
www.server-a.go.th

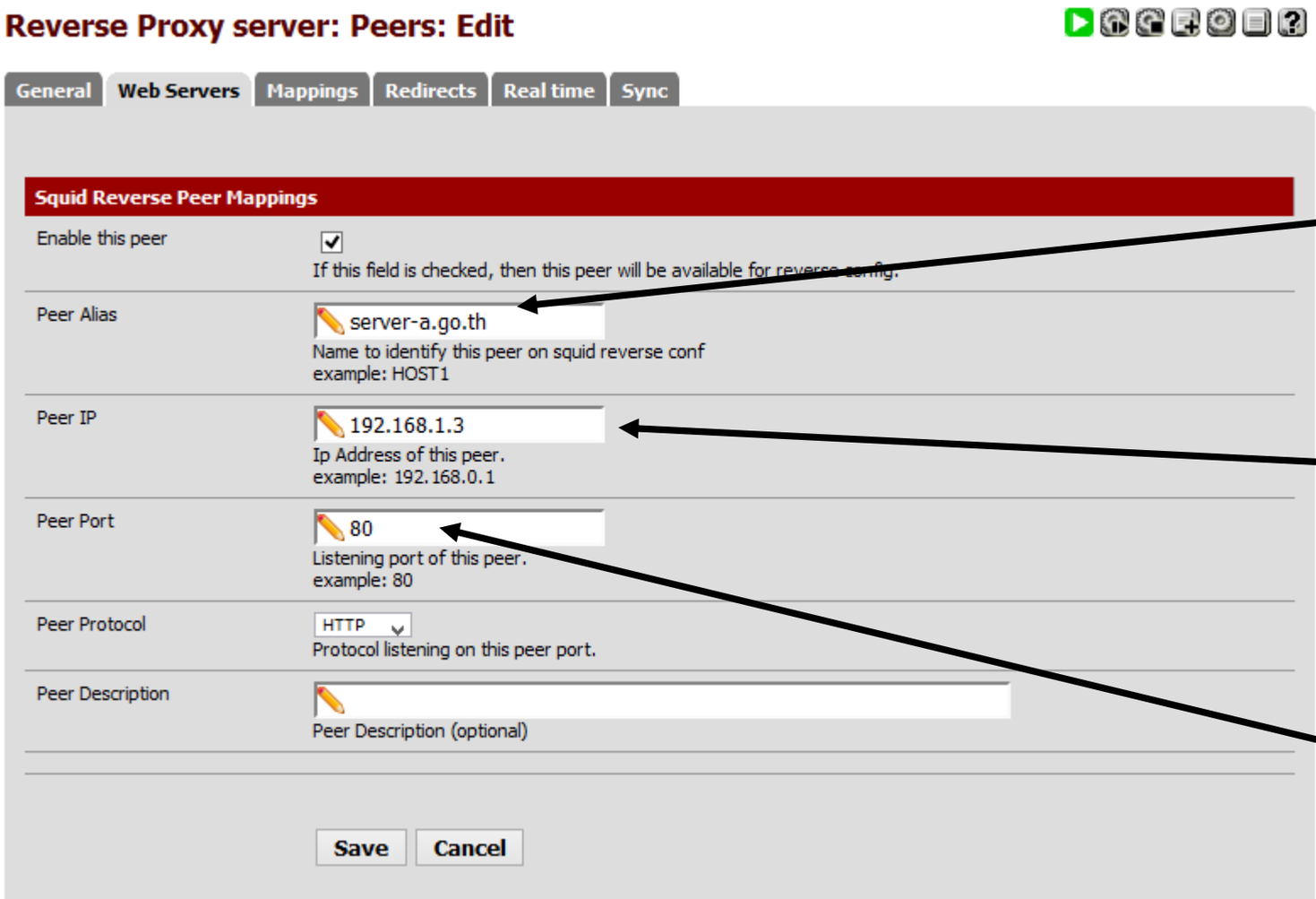
**Squid Reverse HTTPS Settings**

| | |
|---|---|
| **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 | 443 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 | webConfigurator default (555203ab312bf) 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**

# การตั้งค่า Reverse Proxy



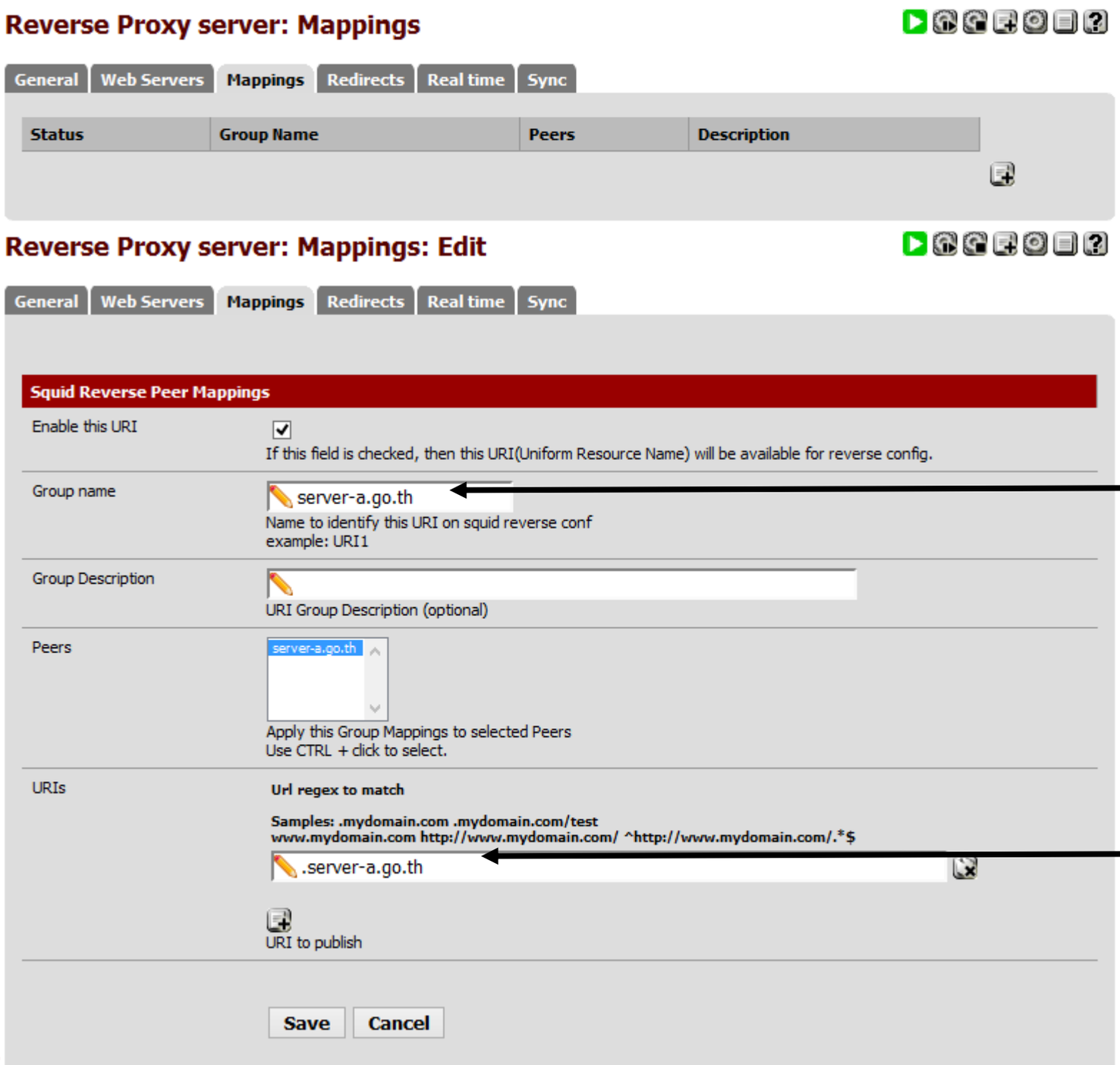




server-a.go.th

192.168.1.3
(IP ของเครื่อง Server เครื่องจริง)

80

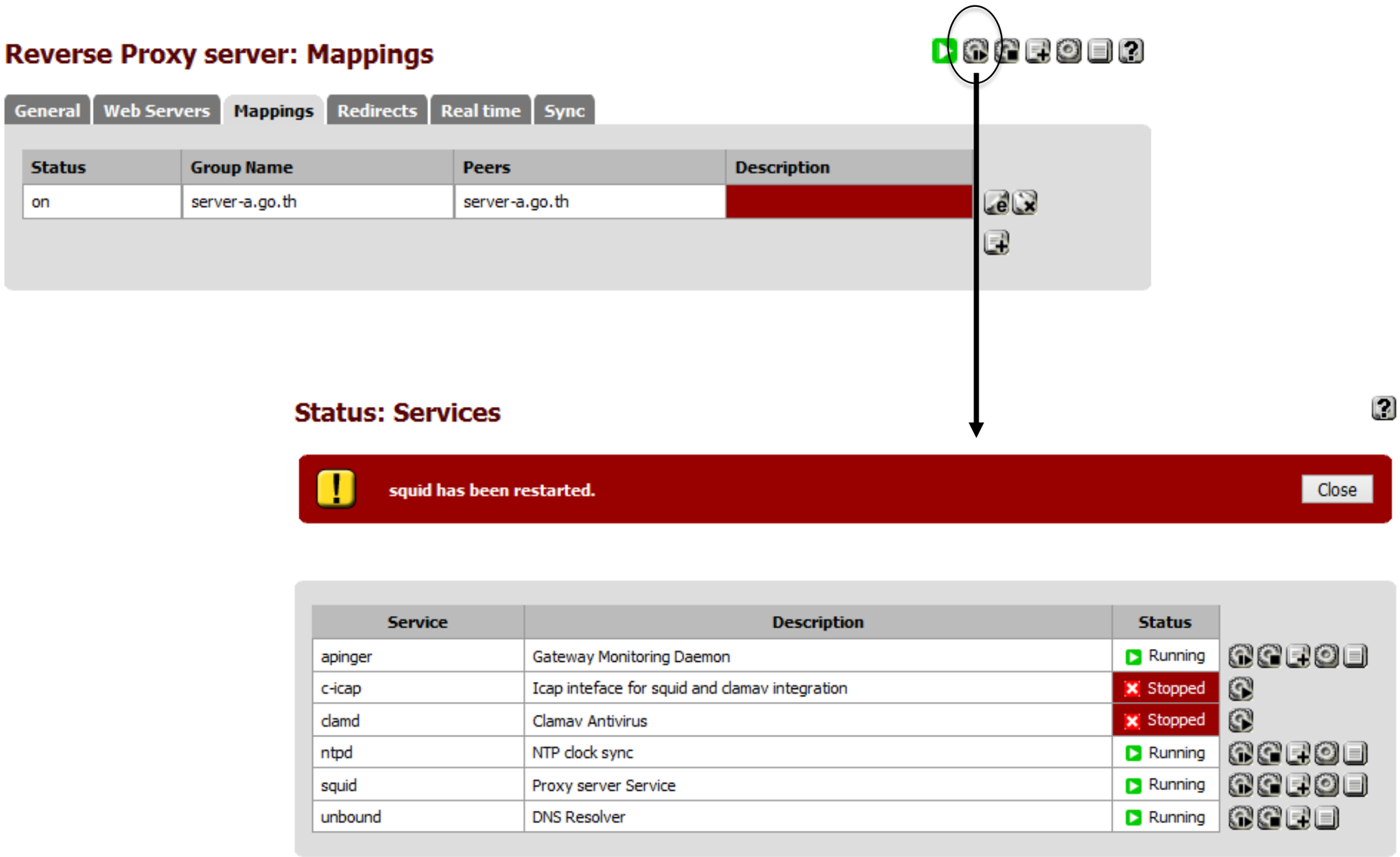
# การตั้งค่า Reverse Proxy



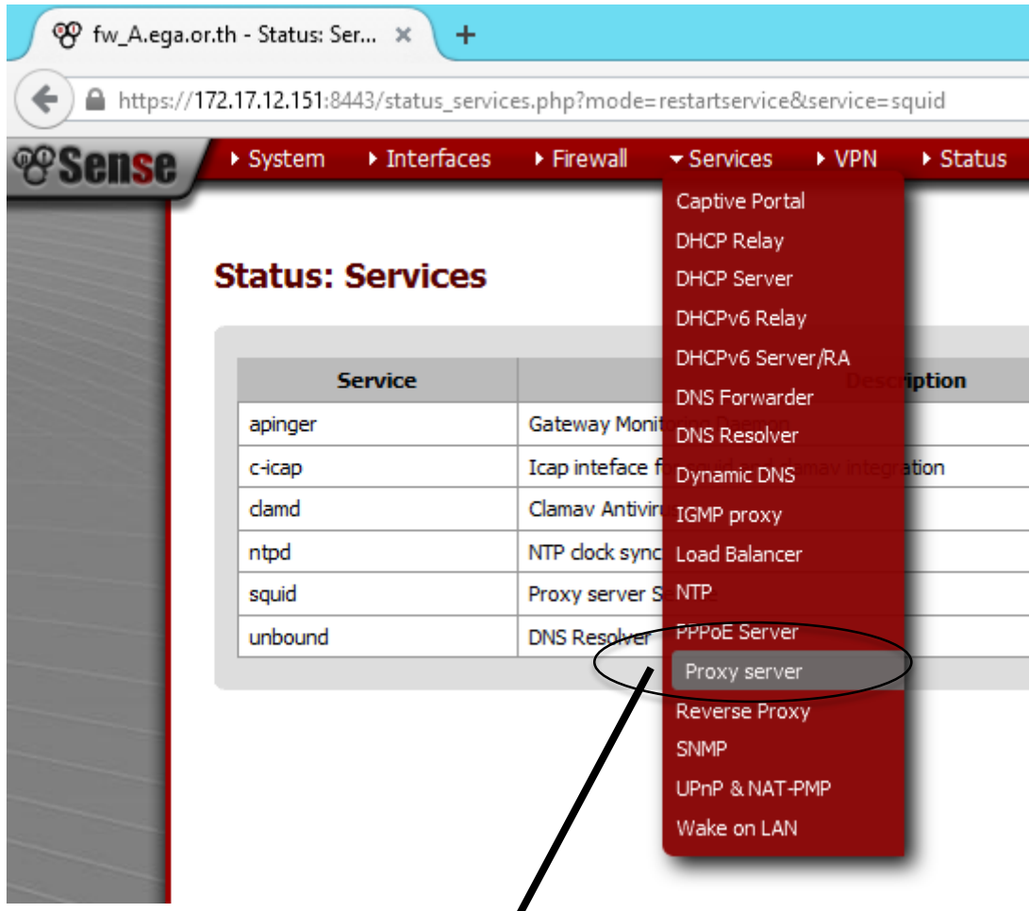

server-a.go.th

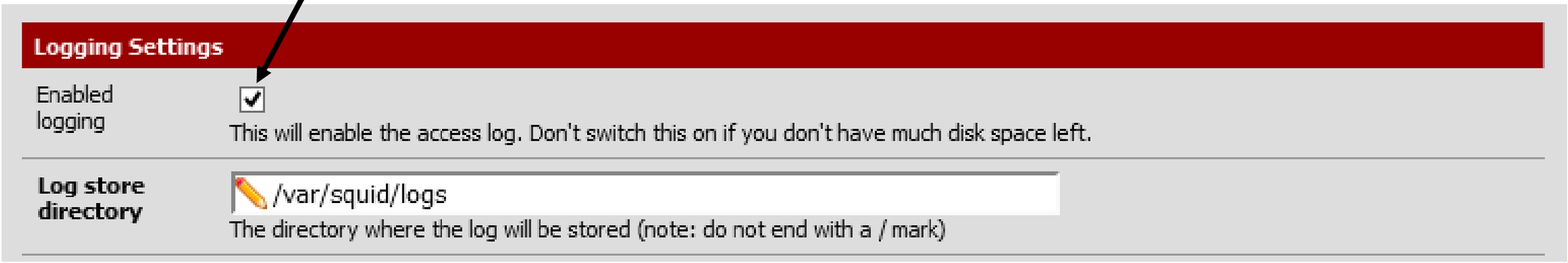
.server-a.go.th

# การตั้งค่า Reverse Proxy

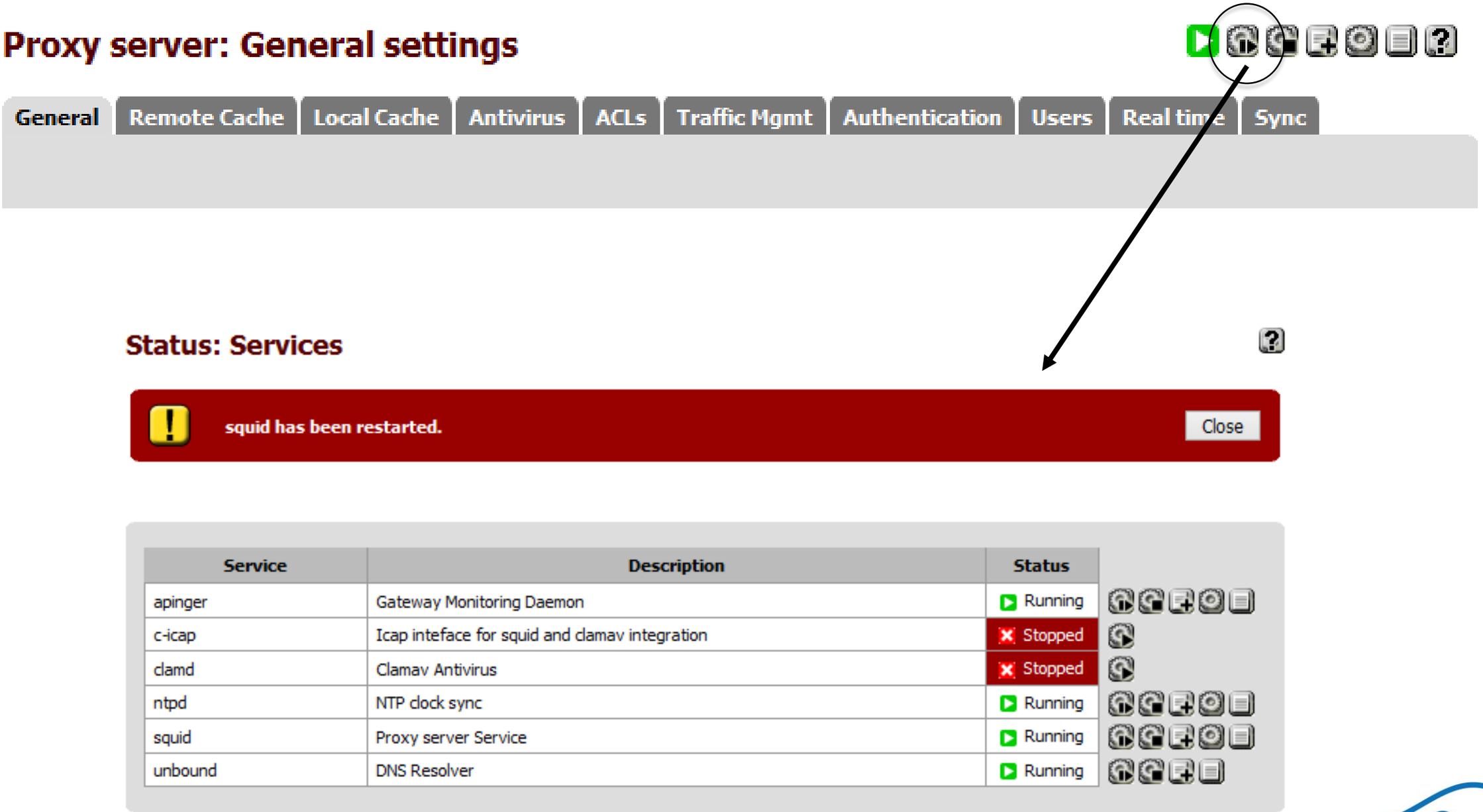


# การตั้งค่า Reverse Proxy Logs

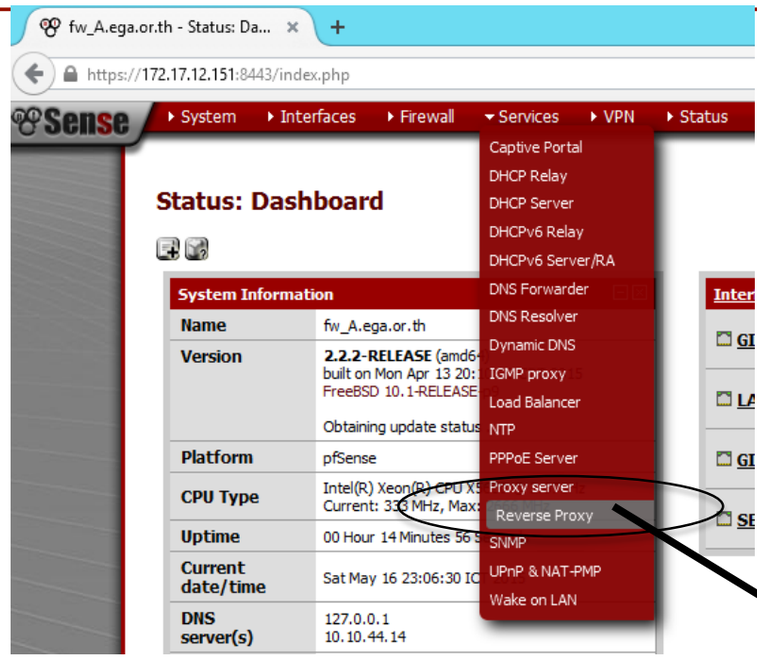



# การตั้งค่า Reverse Proxy Logs



# การตั้งค่า Reverse Proxy Logs




## 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 |

EGA e-Government Agency

G-CERT by EGA

# การใช้งาน pfSense
# ร่วมกับระบบเครือข่าย GIN

**คมกริช คำสวัสดิ์**
วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)