

AAEON PfSense User Guild

Specification

Rev. 0.1

Contents

1.	Create PfSense Installation USB	3
2.	Install PfSense	5
3.	Set interface(s) IP address	10
4.	PfSense WebGUI	21
5.	Port Forward	29
6.	Traffic Shaper	31
7.	Install pfBlockerNG	37
8.	IPSEC	39
9.	AAEON PfSense SDK	50
10.	Purchase Netgate PfSense Support	50

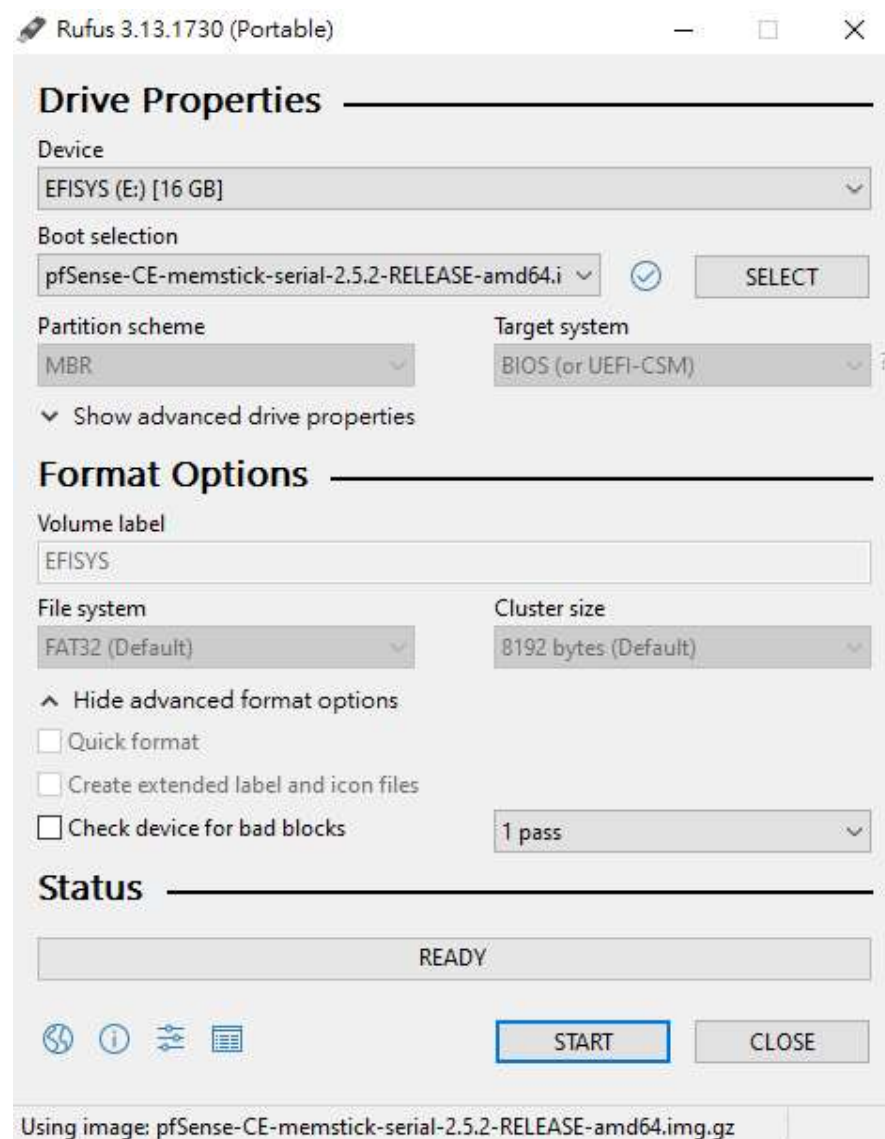
PfSense is an open source OS based on FreeBSD, customized for firewall and router functions. It can be easily deployed through WebUI as firewall, router, wireless access point, DHCP server, DNS server and VPN.

Necessary items:

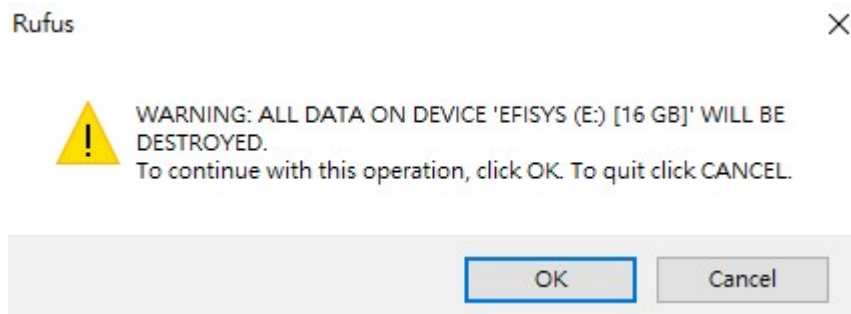
- PfSense ISO: pfSense-CE-memstick-serial-2.5.2-RELEASE-amd64.img
<https://www.pfsense.org/download/>
- Create bootable USB tool: Rufus
<https://rufus.ie/en/>

1. Create PfSense Installation USB

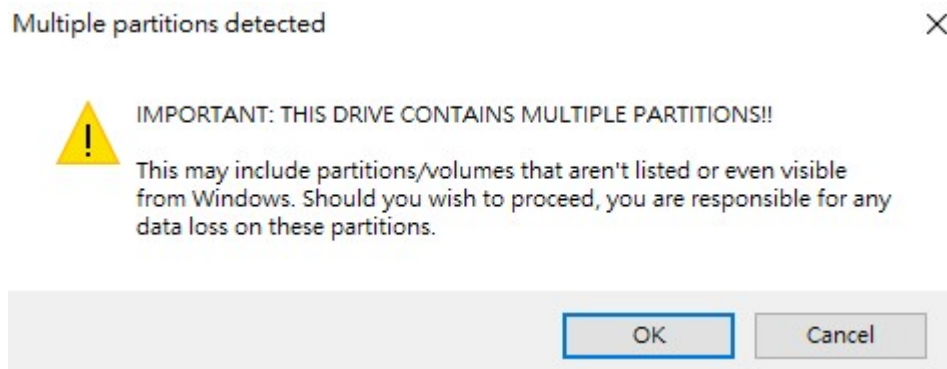
Step1. Click "SELECT" to choose image file and click "START" to create pfsense installation USB.



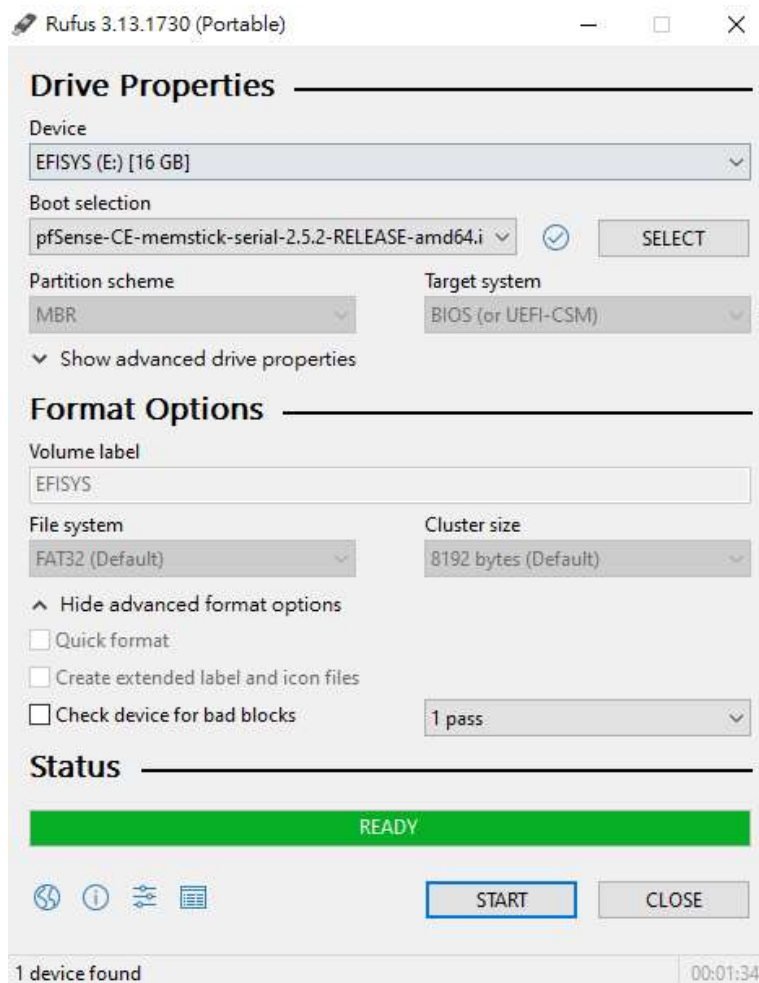
Step2. Click "OK" to the next.



Step3. Click "OK" to the next.



Step4. Finish.



Step9. Press “space” to choose the storage device you want to install and press “Enter” to the next.

```
pfSense Installer
lqqqqqqqqqqZFS Configurationqqqqqqqqqqqqqqk
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x[*] ada0 InnoDisk Corp. - mSATA 3ME3 x x
x x[ ] da0 JetFlash Transcend 32GB x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq x
x < OK > < Back > x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Step10. Choose “YES” and press “Enter” to the next.

```
pfSense Installer
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Last Chance! Are you sure you want to destroy x
x the current contents of the following disks: x
x x x x
x ada0 x
x x x
x tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq x
x < YES > < NO > x
mqqqqqqqqq[Press arrows, TAB or ENTER]qqqqqqqqqqj
```

Step11. Begin installing.

```
pfSense Installer
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x x x
x MANIFEST [ Done ] x
x base.txz [ 50% ] x
x x x
x Fetching distribution files... x
x x x
x lqOverall Progressqqqqqqqqqqqqqqqqqqqqk x
x x ██████████ 50% x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```


Step12. Choose "No" and press "Enter" to the next.

```
pfSense Installer
lqqqqqqqManual Configurationqqqqqqqqqqk
x The installation is now finished. x
x Before exiting the installer, would x
x you like to open a shell in the new x
x system to make any final manual x
x modifications? x
x < Yes > < No > x
```

Step13. Choose "Reboot" and press "Enter" to finish the installation.

※Remember to remove the USB after you press "Enter"

```
pfSense Installer
lqqqqqqqqqCompleteqqqqqqqqqqk
x Installation of pfSense x
x complete! Would you like x
x to reboot into the x
x installed system now? x
x < Reboot > < Shell > x
```

Step14. PfSense initial interface as shown below.

```
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyu0)
pfSense - Netgate Device ID: f5844f74919eab95a404

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan) -> igb0 ->
LAN (lan) -> igb1 -> 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) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update 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: █
```

3. Set interface(s) IP address

There are two modes for WAN settings, one is static IP and the other is DHCP.

Static IP:

Step1. Type "2" and press "Enter" to set interfaces IP address.

```
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyu0)

pfSense - Netgate Device ID: f5844f74919eab95a404

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      ->
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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
```

Step2. Type "1" and press "Enter" to set the WAN interfaces.

```
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      ->
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp, dhcp6)
2 - LAN (igb1 - static)

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

Step3. Type “n” and press “Enter” to the next.

```
WAN (wan)      -> igb0      ->
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp, dhcp6)
2 - LAN (igb1 - static)

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

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

Step4. Type your static IP and press “Enter” to the next.

```
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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp, dhcp6)
2 - LAN (igb1 - static)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1
```

Step5. Type "24" and press "Enter" to set the subnet masks.

```
7) Ping host          16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (igb0 - dhcp, dhcp6)
2 - LAN (igbl - static)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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
```

Step6. Type your gateway address and press "Enter".

```
Available interfaces:

1 - WAN (igb0 - dhcp, dhcp6)
2 - LAN (igbl - static)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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:
> 192.168.0.254
```

Step7. Type "n" and press "Enter".

```
1 - WAN (igb0 - dhcp, dhcp6)
2 - LAN (igb1 - static)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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:
> 192.168.0.254

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

Step8. Press "Enter" for none.

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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:
> 192.168.0.254

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

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

Step9. Type “n” and press “Enter”.

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.0.1

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:
> 192.168.0.254

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Step10. Press “Enter” to the next.

```
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:
> 192.168.0.254

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

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

The IPv4 WAN address has been set to 192.168.0.1/24

Press <ENTER> to continue.
```

Step11. Now you can see the static IP of the WAN has been set. Type "7" and press "Enter" to check the network is connected.

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

The IPv4 WAN address has been set to 192.168.0.1/24

Press <ENTER> to continue.
pfSense - Netgate Device ID: f5844f74919eab95a404

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      -> v4: 192.168.0.1/24
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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: 7
```

Step12. Type "8.8.8.8" and press "Enter" to test network connection.

```
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update 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: 7

Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=55 time=4.983 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=7.728 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=5.567 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.983/6.092/7.728/1.181 ms

Press ENTER to continue.
```

DHCP:

Step1. Type "2" and press "Enter" to set interfaces IP address.

```
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyu0)
pfSense - Netgate Device ID: f5844f74919eab95a404

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      ->
LAN (lan)      -> igbl      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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
```

Step2. Type "1" and press "Enter" to set the WAN interfaces.

```
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      ->
LAN (lan)      -> igbl      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp, dhcp6)
2 - LAN (igbl - static)

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


Step3. Type "y" and press "Enter" to configure DHCP.

```
WAN (wan)      -> igb0      ->
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp)
2 - LAN (igb1 - static)

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

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

Step4. Type "n" and press "Enter" to the next.

```
LAN (lan)      -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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 (igb0 - dhcp)
2 - LAN (igb1 - static)

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

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

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

Step5. Press "Enter" for none to the next.

```
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update 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 (igb0 - dhcp)
2 - LAN (igb1 - static)

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

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

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

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

Step6. Type "n" and press "Enter" to the next.

```
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 (igb0 - dhcp)
2 - LAN (igb1 - static)

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

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

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Step7. Press "Enter" to the next.

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

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

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...route: writing to routing socket: Network is
unreachable

DHCPD...

The IPv4 WAN address has been set to dhcp
Press <ENTER> to continue.
```

Step8. Now you can see the DHCP of the WAN has been set. Type "7" and press "Enter" to check the network is connected.

```
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.115/6.984/8.069/1.327 ms

Press ENTER to continue.

pfSense - Netgate Device ID: f5844f74919eab95a404

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> igb0      -> v4/DHCP4: 192.168.50.174/24
LAN (lan)     -> igb1      -> 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) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update 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: 7
```

Step9. Type "8.8.8.8" and press "Enter" to test network connection.

```
2) Set interface(s) IP address      11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell + pfSense tools
4) Reset to factory defaults       13) Update 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: 7

Enter a host name or IP address: 8.8.8.8

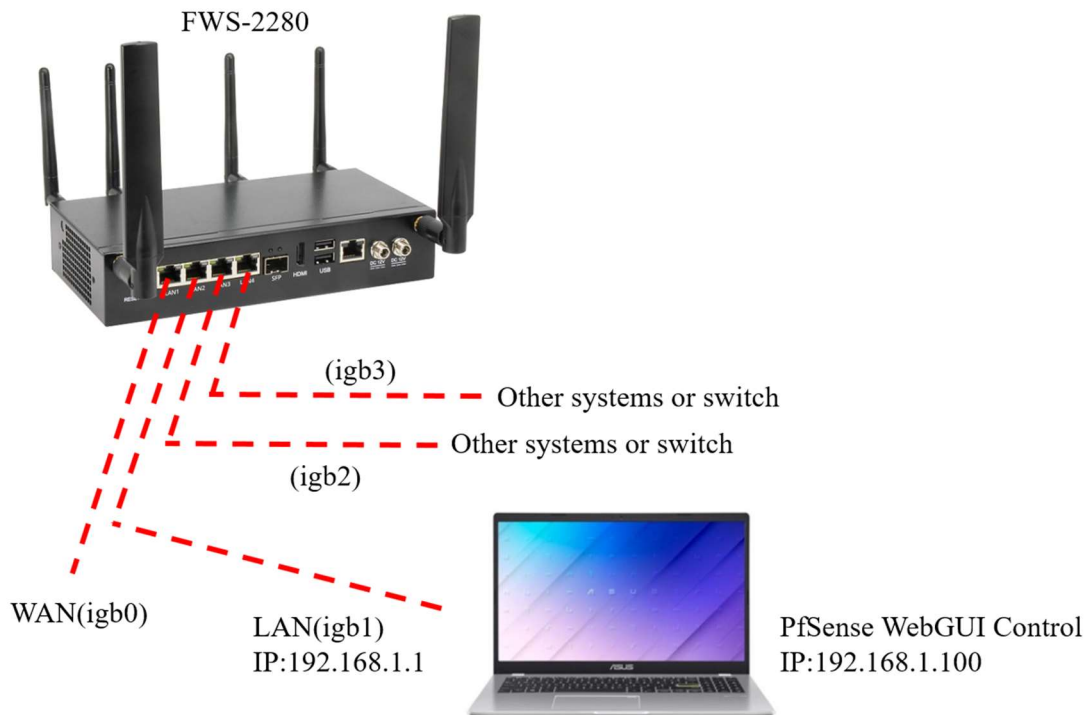
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=55 time=8.539 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=7.726 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=9.505 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.726/8.590/9.505/0.727 ms

Press ENTER to continue.
```

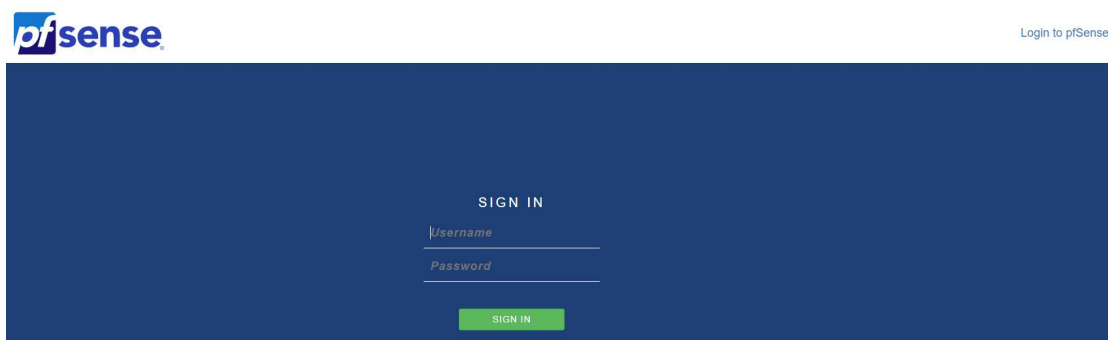
4. PfSense WebGUI

The following picture is the pfsense firewall framework example. You can configure it through pfsense WebGUI to make the system have functions like port forward, traffic shaper, IPSEC etc.



Step1. You can see the default igb1 IP of pfsense is 192.168.1.1, so you must set the laptop IP to the same domain, such as 192.168.1.100. Then type 192.168.1.1 on the browser to enter the pfsense WebGUI.

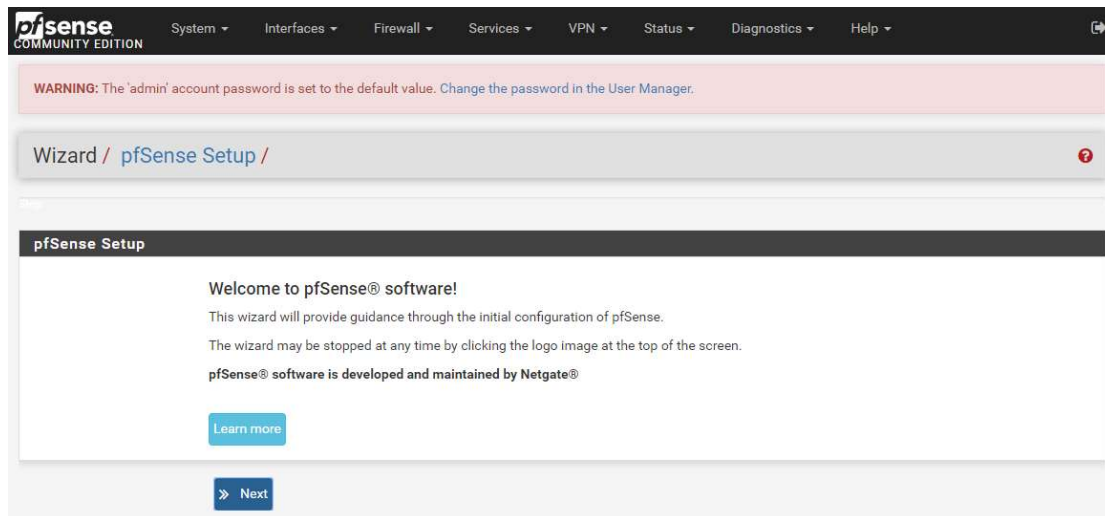
```
LAN (lan)      -> igb1      -> v4: 192.168.1.1/24
```



Default Username: **admin**

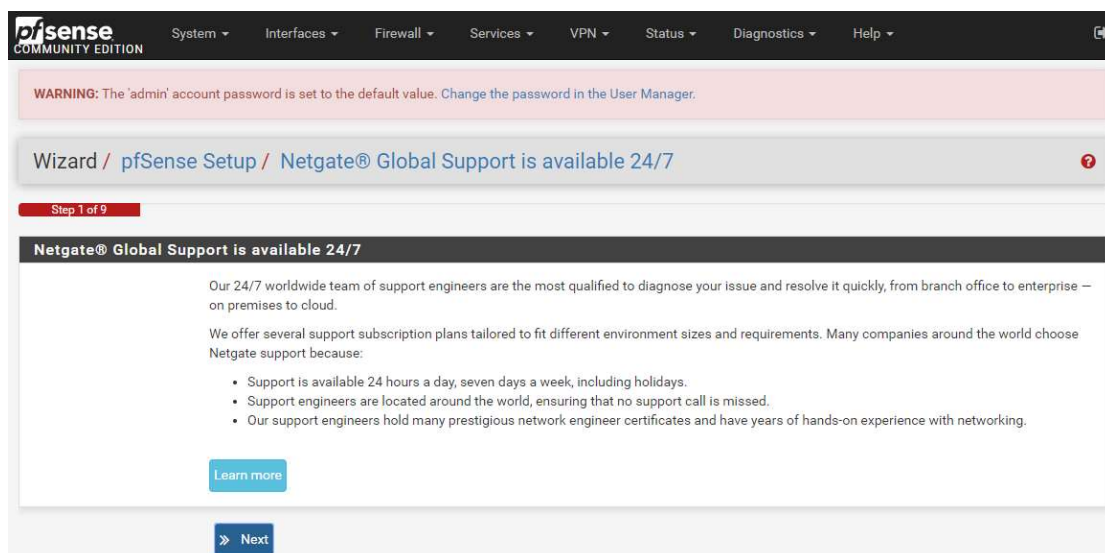
Default Password: **pfsense**

Step2. Click “Next” to the next pfsense setup.



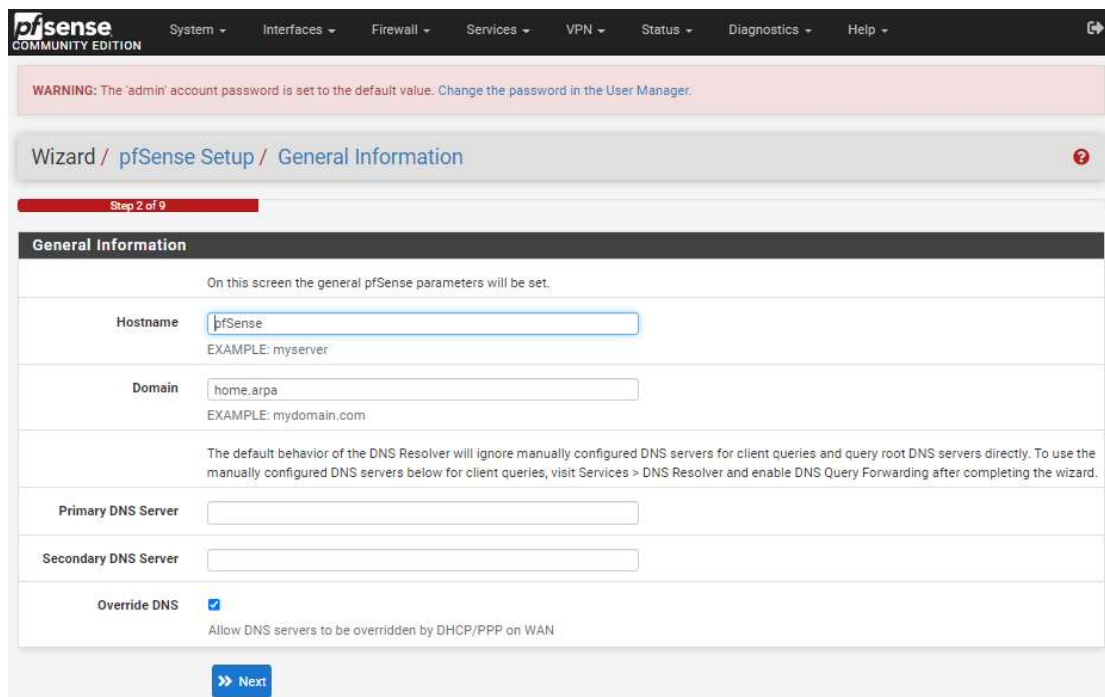
The screenshot shows the pfSense Setup Wizard. At the top, there is a navigation menu with items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu is a warning banner: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail reads "Wizard / pfSense Setup /". The main content area is titled "pfSense Setup" and contains the following text: "Welcome to pfSense® software! This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen. pfSense® software is developed and maintained by Netgate®". There are two buttons: a blue "Learn more" button and a dark blue "Next" button with a right-pointing arrow.

Step3. Click “Next” to the next pfsense setup.



The screenshot shows the second step of the pfSense Setup Wizard. The navigation menu and warning banner are identical to the previous step. The breadcrumb trail now includes the current step: "Wizard / pfSense Setup / Netgate® Global Support is available 24/7". A red progress bar indicates "Step 1 of 9". The main content area is titled "Netgate® Global Support is available 24/7" and contains the following text: "Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud. We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:" followed by a bulleted list: "• Support is available 24 hours a day, seven days a week, including holidays. • Support engineers are located around the world, ensuring that no support call is missed. • Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking." There are two buttons: a blue "Learn more" button and a dark blue "Next" button with a right-pointing arrow.

Step4. Type the hostname, domain and DNS or use default value and click “Next”.

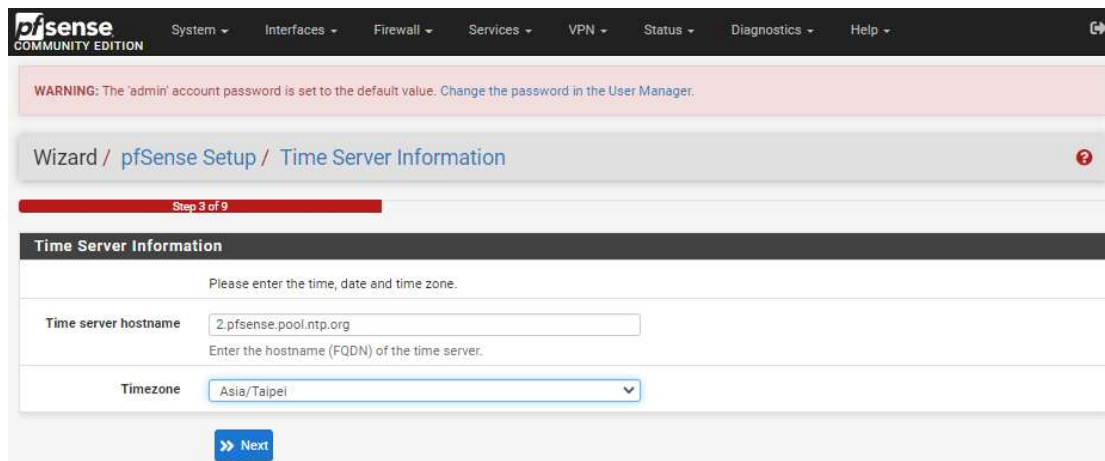


The screenshot shows the pfSense Setup Wizard at Step 2 of 9, titled "General Information". At the top, there is a navigation menu with "System", "Interfaces", "Firewall", "Services", "VPN", "Status", "Diagnostics", and "Help". A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb "Wizard / pfSense Setup / General Information" is visible. The main content area is titled "General Information" and contains the following fields:

- Hostname:** A text input field containing "pfSense". Below it, the text "EXAMPLE: myserver" is displayed.
- Domain:** A text input field containing "home.arpa". Below it, the text "EXAMPLE: mydomain.com" is displayed.
- Primary DNS Server:** An empty text input field.
- Secondary DNS Server:** An empty text input field.
- Override DNS:** A checked checkbox with the label "Override DNS". Below it, the text "Allow DNS servers to be overridden by DHCP/PPP on WAN" is displayed.

At the bottom of the form, there is a blue button labeled "Next" with a right-pointing arrow.

Step5. Choose your time zone and click “Next”.



The screenshot shows the pfSense Setup Wizard at Step 3 of 9, titled "Time Server Information". The navigation menu and warning message are identical to the previous screen. The breadcrumb is "Wizard / pfSense Setup / Time Server Information". The main content area is titled "Time Server Information" and contains the following fields:

- Time server hostname:** A text input field containing "2.pfsense.pool.ntp.org". Below it, the text "Enter the hostname (FQDN) of the time server." is displayed.
- Timezone:** A dropdown menu with "Asia/Taipei" selected.

At the bottom of the form, there is a blue button labeled "Next" with a right-pointing arrow.

Step6. Configure your WAN Interface, PPPoE, PPTP and click “Next” to the next.

The screenshot shows the pfSense Setup Wizard at Step 4 of 9, titled "Configure WAN Interface". At the top, there is a navigation menu with "System", "Interfaces", "Firewall", "Services", "VPN", "Status", "Diagnostics", and "Help". A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb trail is "Wizard / pfSense Setup / Configure WAN Interface". A progress bar indicates "Step 4 of 9".

The main heading is "Configure WAN Interface". Below it, a sub-heading reads: "On this screen the Wide Area Network information will be configured." The "SelectedType" dropdown menu is set to "DHCP".

The "General configuration" section includes three input fields: "MAC Address" (with a note: "This field can be used to modify ('spoof') the MAC address of the WAN 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."), "MTU" (with a note: "Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed."), and "MSS" (with a note: "If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.").

The "Static IP Configuration" section has an "IP Address" input field.

Step7. Configure your LAN Interface and click “Next” to the next.

The screenshot shows the pfSense Setup Wizard at Step 5 of 9, titled "Configure LAN Interface". The navigation menu and warning message are identical to Step 4. The breadcrumb trail is "Wizard / pfSense Setup / Configure LAN Interface". The progress bar indicates "Step 5 of 9".

The main heading is "Configure LAN Interface". Below it, a sub-heading reads: "On this screen the Local Area Network information will be configured." The "LAN IP Address" input field contains "192.168.1.1" (with a note: "Type dhcp if this interface uses DHCP to obtain its IP address."). The "Subnet Mask" dropdown menu is set to "24".

At the bottom of the form, there is a blue "Next" button with a right-pointing arrow.

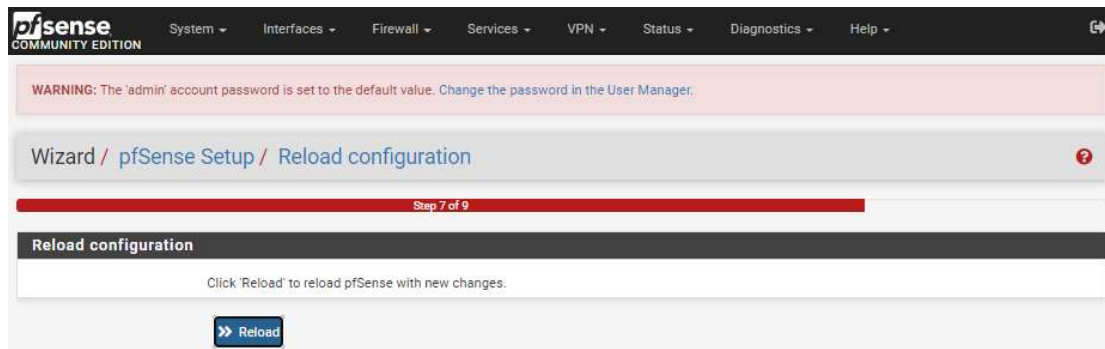
Step8. Set your admin password and click “Next” to the next.

The screenshot shows the pfSense Setup Wizard at Step 6 of 9, titled "Set Admin WebGUI Password". The navigation menu and warning message are identical to previous steps. The breadcrumb trail is "Wizard / pfSense Setup / Set Admin WebGUI Password". The progress bar indicates "Step 6 of 9".

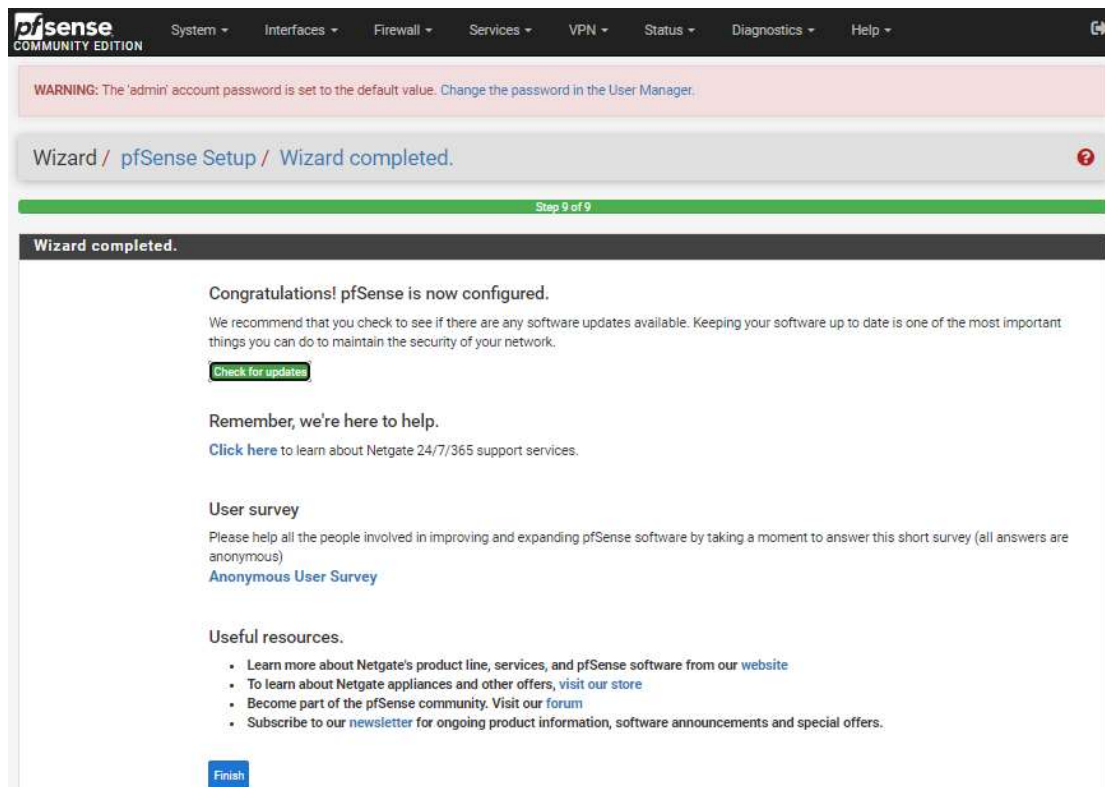
The main heading is "Set Admin WebGUI Password". Below it, a sub-heading reads: "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." There are two input fields: "Admin Password" and "Admin Password AGAIN".

At the bottom of the form, there is a blue "Next" button with a right-pointing arrow.

Step9. Click “Reload” to reload pfsense with new changes.



Step10. Click “Finish” to complete the configuration.



Step11. Click “Accept” to accept copyright and trademark notices.

Copyright and Trademark Notices.

Copyright© 2004-2016. Electric Sheep Fencing, LLC (“ESF”). All Rights Reserved.

Copyright© 2014-2021. Rubicon Communications, LLC d/b/a Netgate (“Netgate”). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

“pfSense” is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.

Restricted Rights Legend.

No part of ESF and/or Netgate’s information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government’s Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Accept

Step 12. The left block shows some system information, such as CPU information, CPU usage, memory usage, disk usage etc. And the right block shows the connection status of WAN and LAN interfaces. In addition, you can also click the "+" in the upper right corner to add different display blocks.

Status / Dashboard + ?

Available Widgets -

+ Captive Portal Status	+ CARP Status	+ Dynamic DNS Status	+ Firewall Logs
+ Gateways	+ GEOM Mirror Status	+ Installed Packages	+ Interface Statistics
+ Interfaces	+ IPsec	+ NTP Status	+ OpenVPN
+ Picture	+ RSS	+ S.M.A.R.T. Status	+ Services Status
+ System Information	+ Thermal Sensors	+ Traffic Graphs	+ Wake-on-Lan

Other dashboard settings are available from the General Setup page.

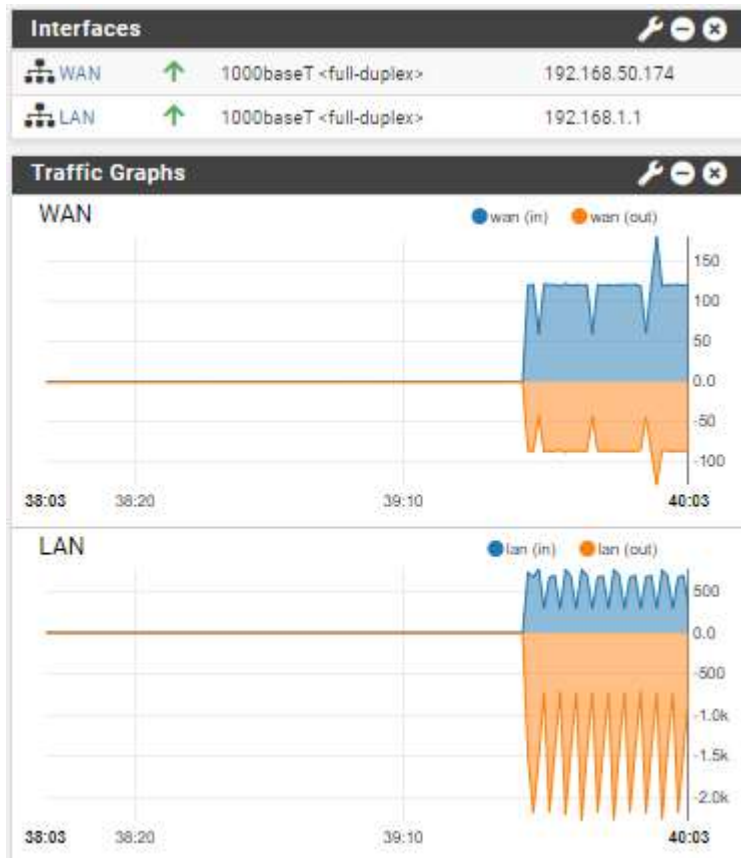
pfSense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard + ?

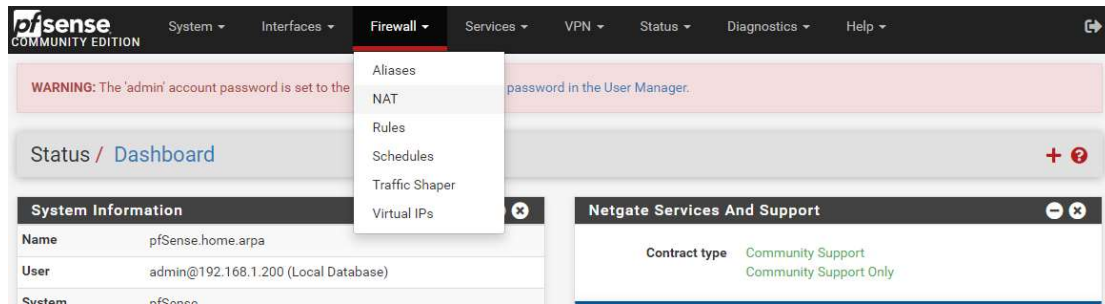
System Information	Netgate Services And Support																										
<table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <tr><td>Name</td><td>pfSense.home.arpa</td></tr> <tr><td>User</td><td>admin@192.168.1.200 (Local Database)</td></tr> <tr><td>System</td><td>pfSense Netgate Device ID: f5844f74919eab95a404</td></tr> <tr><td>BIOS</td><td>Vendor: American Megatrends International, LLC. Version: K228AM10 Release Date: Wed Jun 30 2021</td></tr> <tr><td>Version</td><td>2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Thu Feb 10 13:27:27 CST 2022</td></tr> <tr><td>CPU Type</td><td>Intel(R) Celeron(R) J6412 @ 2.00GHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No</td></tr> <tr><td>Hardware crypto</td><td></td></tr> <tr><td>Kernel PTI</td><td>Disabled</td></tr> <tr><td>MDS Mitigation</td><td>Inactive</td></tr> <tr><td>Uptime</td><td>02 Hours 08 Minutes 03 Seconds</td></tr> <tr><td>Current date/time</td><td>Thu Feb 10 13:30:25 CST 2022</td></tr> <tr><td>DNS server(s)</td><td> <ul style="list-style-type: none"> • 127.0.0.1 • 192.168.50.1 </td></tr> <tr><td>Last config change</td><td>Thu Feb 10 13:26:25 CST 2022</td></tr> </table>	Name	pfSense.home.arpa	User	admin@192.168.1.200 (Local Database)	System	pfSense Netgate Device ID: f5844f74919eab95a404	BIOS	Vendor: American Megatrends International, LLC. Version: K228AM10 Release Date: Wed Jun 30 2021	Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Thu Feb 10 13:27:27 CST 2022	CPU Type	Intel(R) Celeron(R) J6412 @ 2.00GHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	Hardware crypto		Kernel PTI	Disabled	MDS Mitigation	Inactive	Uptime	02 Hours 08 Minutes 03 Seconds	Current date/time	Thu Feb 10 13:30:25 CST 2022	DNS server(s)	<ul style="list-style-type: none"> • 127.0.0.1 • 192.168.50.1 	Last config change	Thu Feb 10 13:26:25 CST 2022	<p>Contract type Community Support Community Support Only</p> <hr/> <p style="text-align: center; background-color: #e1f5fe; padding: 5px; font-weight: bold; font-size: small;">NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES</p> <p style="font-size: x-small;">If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.</p> <p style="font-size: x-small;">You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.</p> <ul style="list-style-type: none"> • Upgrade Your Support • Community Support Resources • Netgate Global Support FAQ • Official pfSense Training by Netgate • Netgate Professional Services • Visit Netgate.com <div style="background-color: #ffe0b2; padding: 10px; font-size: x-small; margin-top: 10px;"> <p>If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support here.</p> </div>
Name	pfSense.home.arpa																										
User	admin@192.168.1.200 (Local Database)																										
System	pfSense Netgate Device ID: f5844f74919eab95a404																										
BIOS	Vendor: American Megatrends International, LLC. Version: K228AM10 Release Date: Wed Jun 30 2021																										
Version	2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Thu Feb 10 13:27:27 CST 2022																										
CPU Type	Intel(R) Celeron(R) J6412 @ 2.00GHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No																										
Hardware crypto																											
Kernel PTI	Disabled																										
MDS Mitigation	Inactive																										
Uptime	02 Hours 08 Minutes 03 Seconds																										
Current date/time	Thu Feb 10 13:30:25 CST 2022																										
DNS server(s)	<ul style="list-style-type: none"> • 127.0.0.1 • 192.168.50.1 																										
Last config change	Thu Feb 10 13:26:25 CST 2022																										
Interfaces																											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;"></td> <td style="width: 10%; text-align: center;">↑</td> <td style="width: 60%;">1000baseT <full-duplex></td> <td style="width: 15%; text-align: right;">192.168.50.174</td> </tr> <tr> <td></td> <td style="text-align: center;">↑</td> <td>1000baseT <full-duplex></td> <td style="text-align: right;">192.168.1.1</td> </tr> </table>		↑	1000baseT <full-duplex>	192.168.50.174		↑	1000baseT <full-duplex>	192.168.1.1																			
	↑	1000baseT <full-duplex>	192.168.50.174																								
	↑	1000baseT <full-duplex>	192.168.1.1																								

Assuming you added "Traffic graphs", you can see the dynamic WAN and LAN in/out situation in the lower right corner of the homepage.

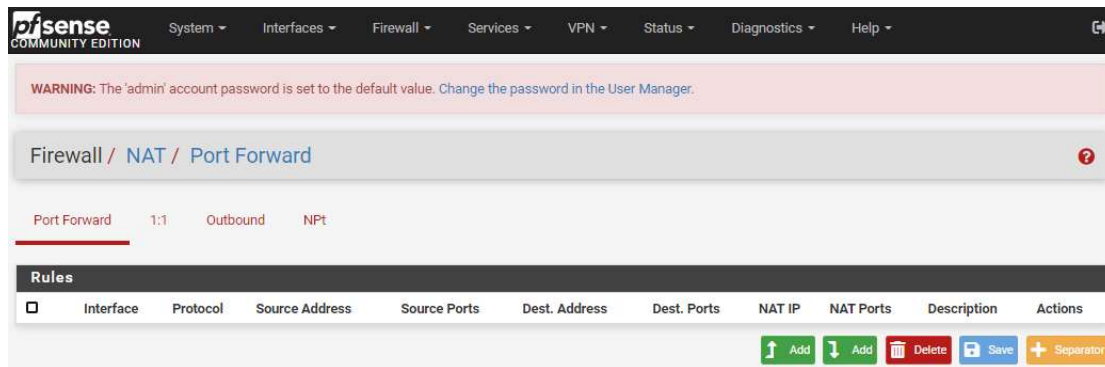


5. Port Forward

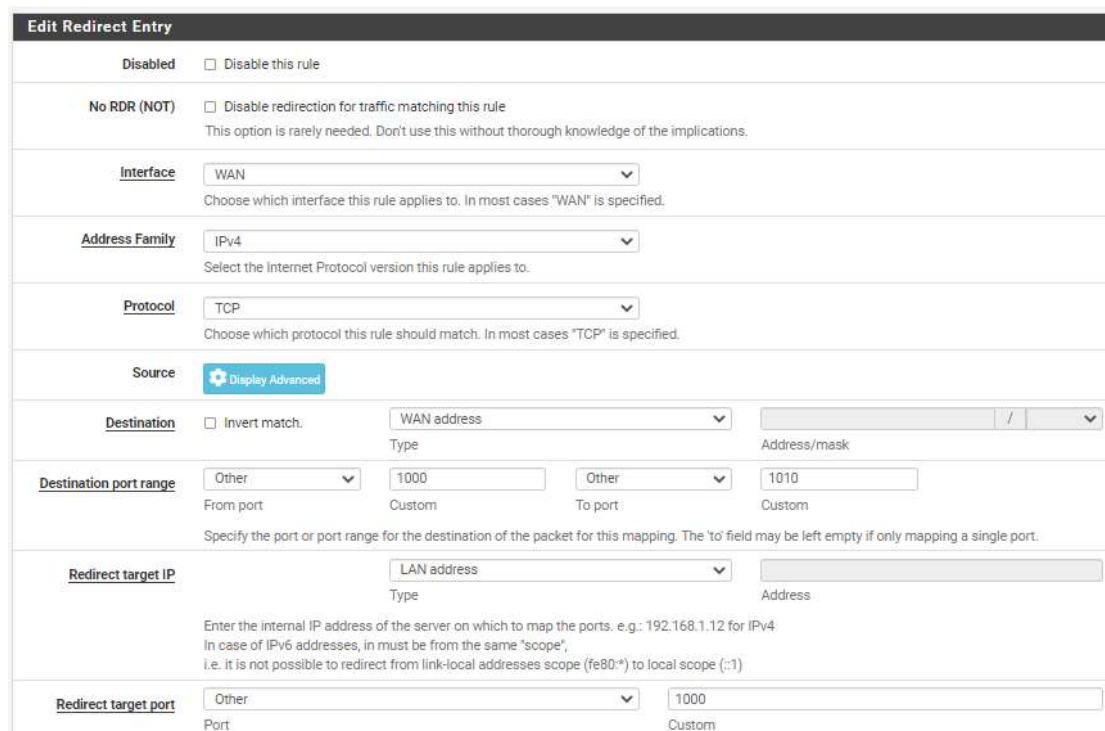
Step1. Choose Firewall and click "NAT".



Step2. Click "Add".



Step3. Set the "destination port range" to "1000 to 1010", the "redirect target IP" to "LAN address", and "redirect target port" to "1000". Click "Save" to save the configuration.

A screenshot of the 'Edit Redirect Entry' form in pfSense. The form has several sections: 'Disabled' (checkbox), 'No RDR (NOT)' (checkbox), 'Interface' (dropdown menu set to 'WAN'), 'Address Family' (dropdown menu set to 'IPv4'), 'Protocol' (dropdown menu set to 'TCP'), 'Source' (button 'Display Advanced'), 'Destination' (checkbox 'Invert match.', dropdown 'WAN address', and input field for 'Address/mask'), 'Destination port range' (dropdown 'Other', input '1000', dropdown 'Other', input '1010'), 'Redirect target IP' (dropdown 'LAN address', and input field for 'Address'), and 'Redirect target port' (dropdown 'Other', input '1000').

Step4. Click “Apply Changes” to complete the configuration.

The screenshot shows the pfSense Community Edition web interface. At the top, there is a navigation menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb path is "Firewall / NAT / Port Forward". A yellow notification box says: "The NAT configuration has been changed. The changes must be applied for them to take effect." with an "Apply Changes" button. The current configuration is for "Port Forward" with a "1:1" ratio, "Outbound" direction, and "NAT" type. A table of rules is shown below:

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	1000 - 1010	LAN address	1000 - 1010		

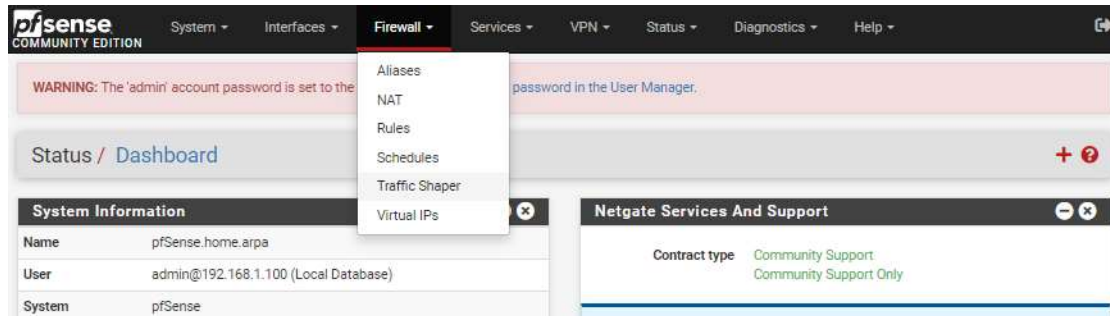
Below the table are buttons for "Add", "Add", "Delete", "Save", and "Separator". A legend indicates that a play icon means "Pass" and a crossed-out play icon means "Linked rule".

Step5. Now you can change your laptop connection mode to DHCP, and you can connect to Internet through port forward.

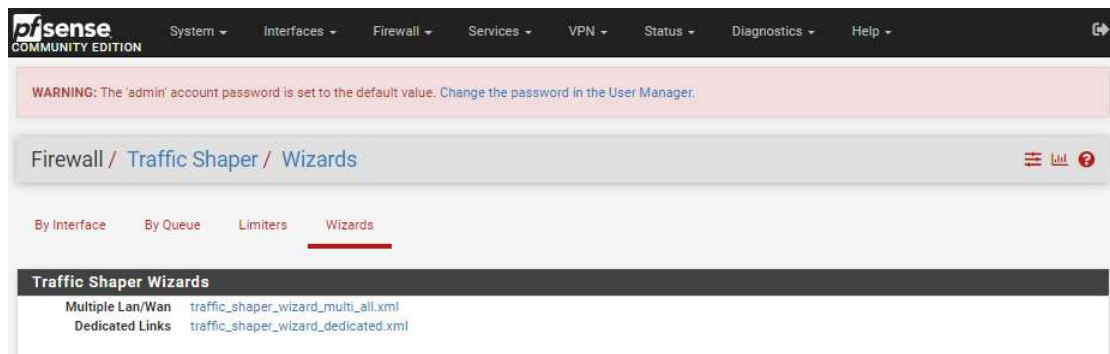
The advertisement for the Aeon FWS-7840 network switch features a central image of the device. To the left, it highlights the "intel INTEL XEON W PROCESSOR" and "intel Chipset i350AM4". The front panel of the switch is labeled with "RJ-45 Ports x 8", "SFP+ x 2", and "NIM Slots x 2". To the right, a grid of icons represents various features: Virtualization, QoS, SR-IOV, SD-WAN, NGFW, and UTM. The model number "FWS-7840" is prominently displayed. At the bottom, there is a "Learn More +" button and a "Get a Quote" button.

6. Traffic Shaper

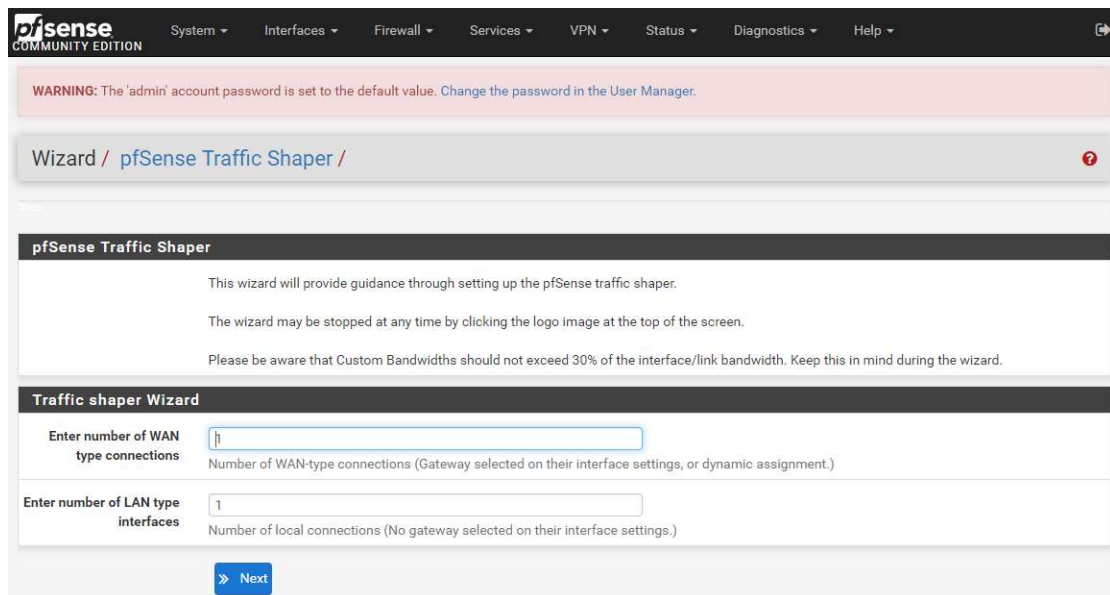
Step1. Choose “Firewall” and click “Traffic Shaper”.



Step2. Choose “Wizards” and click “traffic_shaper_wizard_multi_all.xml”.



Step3. Set your number of WAN/LAN type interfaces and click “Next”.



Step4. Click "Next".

The screenshot shows the pfSense Traffic Shaper configuration wizard at Step 1 of 8. At the top, there is a navigation menu with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is "Wizard / pfSense Traffic Shaper / Shaper configuration". The main heading is "Shaper configuration". Below this, there are two sections for configuring interfaces. The first section is "Setup connection speed and scheduler information for interface LAN #1", with "Interface & Scheduler" set to "LAN" and "Interface & Scheduler" set to "PRIQ". The second section is "Setup connection speed and scheduler information for interface WAN#1", with "Interface & Scheduler" set to "WAN" and "Interface & Scheduler" set to "PRIQ". Under the WAN section, there are input fields for "Upload" and "Download" speeds, each with a unit dropdown menu set to "Mbit/s". A blue "Next" button is located at the bottom of the form.

Step5. Click "Next".

The screenshot shows the pfSense Traffic Shaper configuration wizard at Step 2 of 8. The main heading is "Voice over IP". There is a checkbox labeled "enable" and a checkbox labeled "Prioritize Voice over IP traffic". Below this is the "VOIP specific settings" section, which includes a "Provider" dropdown menu set to "Generic (lowdelay)" and a text input field for "Upstream SIP Server". A note below the SIP server field states: "(Optional) If this is chosen, the provider field will be overridden. This allows providing the IP address of the remote PBX or SIP Trunk to prioritize. NOTE: A Firewall Alias can also be used in this location." The next section is "Connection WAN #1", with an input field for "Upload" speed and a unit dropdown menu set to "Kbit/s". The final section is "Connection LAN #1", with an input field for "Download" speed and a unit dropdown menu set to "Kbit/s". A blue "Next" button is located at the bottom of the form.

Step6. You can set an IP here and this will lower the priority of traffic from this IP. Then click “Next”.

Step 3 of 8

Penalty Box

Penalty Box

Enable Penalize IP or Alias
This will lower the priority of traffic from this IP or alias.

PenaltyBox specific settings

Address
This allows just providing the IP address of the computer(s) to penalize. NOTE: A Firewall Alias can also be used in this location.

Bandwidth

Bandwidth %
The desired limit to apply.

[» Next](#)

Step7. You can enable the lower priority of Peer-to-Peer traffic here. Then click “Next”.

Step 4 of 8

Peer to Peer networking

Peer to Peer networking

Enable Lower priority of Peer-to-Peer traffic
This will lower the priority of P2P traffic below all other traffic. Please check the items to prioritize lower than normal traffic.

p2p Catch all

p2pCatchAll When enabled, all uncategorized traffic is fed to the p2p queue.

Bandwidth

Bandwidth %
The desired limit to apply.

Enable/Disable specific P2P protocols

Aimster Aimster and other P2P using the Aimster protocol and ports

BitTorrent Bittorrent and other P2P using the Torrent protocol and ports

BuddyShare BuddyShare and other P2P using the BuddyShare protocol and ports

Step8. You can enable the priority of gaming traffic to higher than most traffic here. Then click “Next”.

Step 5 of 8

Network Games

Network Games

Enable Prioritize network gaming traffic
This will raise the priority of gaming traffic to higher than most traffic.

Enable/Disable specific game consoles and services

BattleNET Battle.net - Virtually every game from Blizzard publishing should match this. This includes the following game series: Starcraft, Diablo, Warcraft. Guild Wars also uses this port.

EAOrigin EA Origin Client - Some PC games by EA use this.

PlayStationConsoles PlayStation Consoles - This should cover all ports required for the Playstation 4, Playstation, PS Vita

Steam Steam Game Client (Includes: America's Army 3, Counter-Strike: Source, Counter-Strike: Global Offensive, Half-Life 2, COD: Black Ops Series, Borderlands 2, Natural Selection 2, Left 4 Dead Series, Portal 2 and many other games on the Steam)

WiiConsoles Wii Consoles - Wii, Wii U, DS and 3DS

XboxLive Xbox Live Services - Xbox 360, Xbox One, Windows 10 Store Games

GoogleStadia Google Stadia

Step9. You can enable the other networking protocols. This will help raise or lower the priority of other protocols higher than most traffic. Then click “Next”.

The screenshot shows the 'Step 6 of 8' configuration page for pfSense. The main heading is 'Raise or lower other Applications'. Below this, there is a section for 'Remote Service / Terminal emulation' with dropdown menus for AppleRemoteDesktop, MSRDP, PCAnywhere, and VNC, all set to 'Default priority'. Below that is a 'Messengers' section with dropdown menus for AIM, Facetime, ICQ, and IRC, also all set to 'Default priority'. There is an 'Enable' checkbox for 'Other networking protocols' which is currently unchecked. A note below it states: 'This will help raise or lower the priority of other protocols higher than most traffic.'

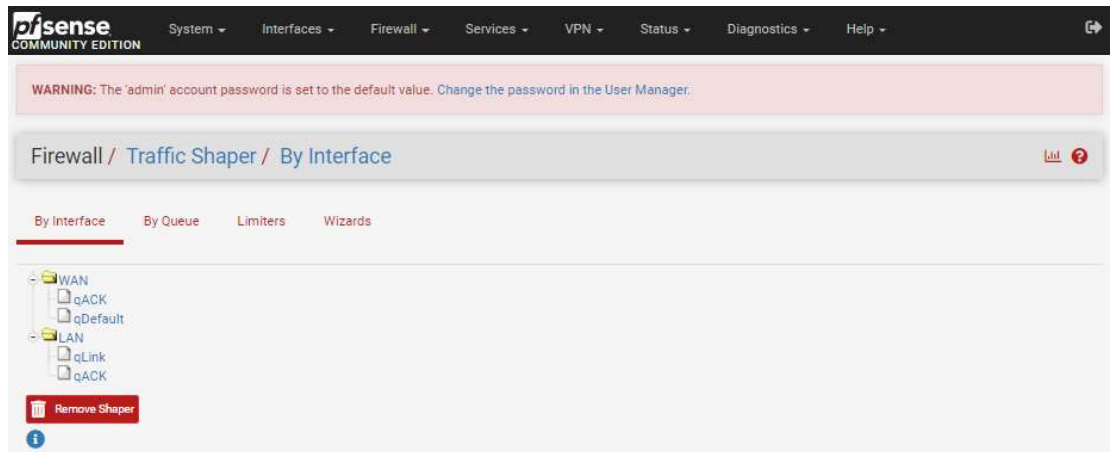
Step10. Click “Finish” to complete the configuration.

The screenshot shows the 'Step 7 of 8' configuration page for pfSense. The main heading is 'Reload Profile'. Below this, there is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below the warning, there is a breadcrumb trail: 'Wizard / pfSense Traffic Shaper / Reload Profile'. The main content area contains the following text: 'After pressing Finish the system will load the new profile. Please note that this may take a moment. Also note that the traffic shaper is stateful meaning that only new connections will be shaped. If this is an issue please reset the state table after loading the profile.' At the bottom of the page, there is a blue button with a right-pointing arrow and the text 'Finish'.

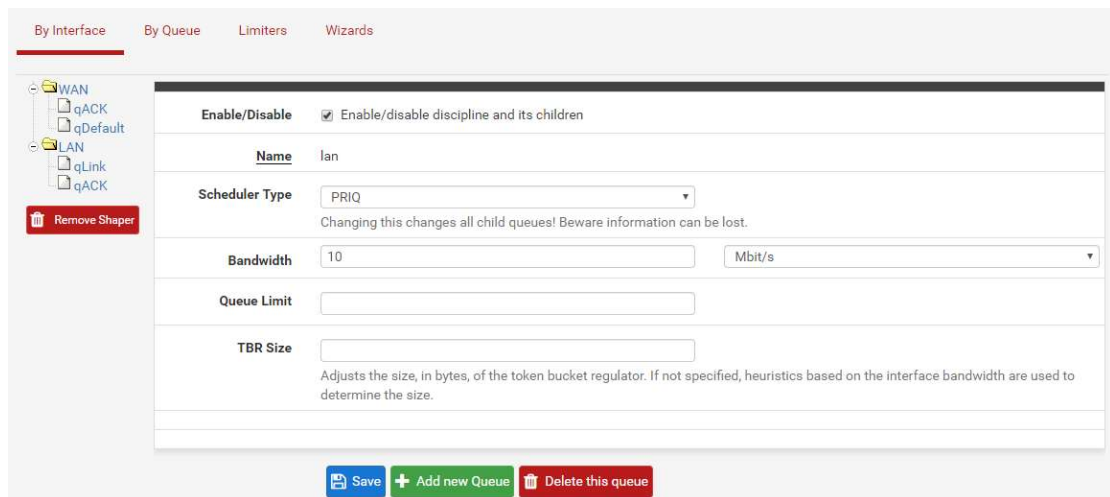
Step11. Choose “Firewall” and click “Traffic Shaper” again.

The screenshot shows the 'Filter Reload' configuration page for pfSense. The main heading is 'Filter Reload'. Below this, there is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below the warning, there is a breadcrumb trail: 'Status / Filter Reload'. The main content area contains a green button with a refresh icon and the text 'Reload Filter'. Below this, there is a section for 'Queue Status' and a 'Reload status' section. The 'Reload status' section contains the following text: 'Initializing', 'Creating aliases', 'Creating gateway group item...', 'Generating Limiter rules', 'Generating NAT rules', 'Creating I:1 rules...', and 'Creating I:1 rules...'. The 'Firewall' menu is open, showing options: Aliases, NAT, Rules, Schedules, Traffic Shaper, and Virtual IPs.

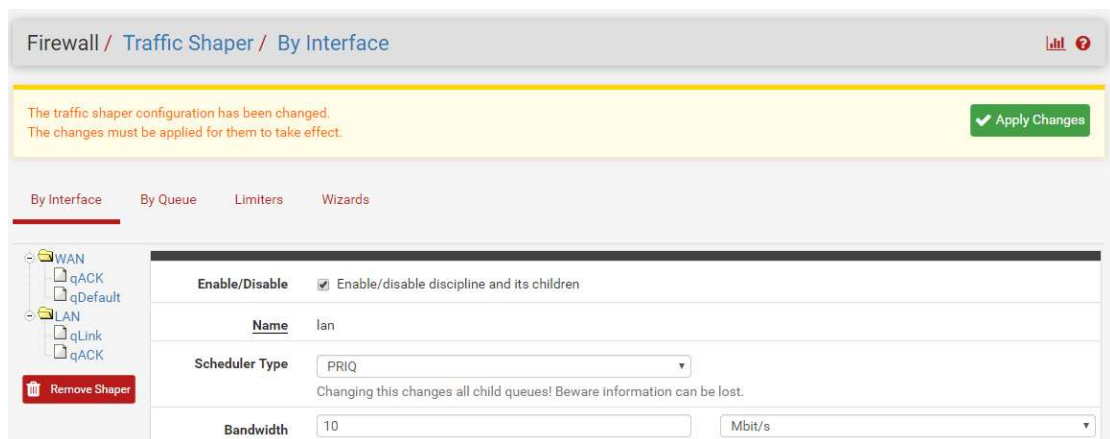
Step12. Click “LAN”.



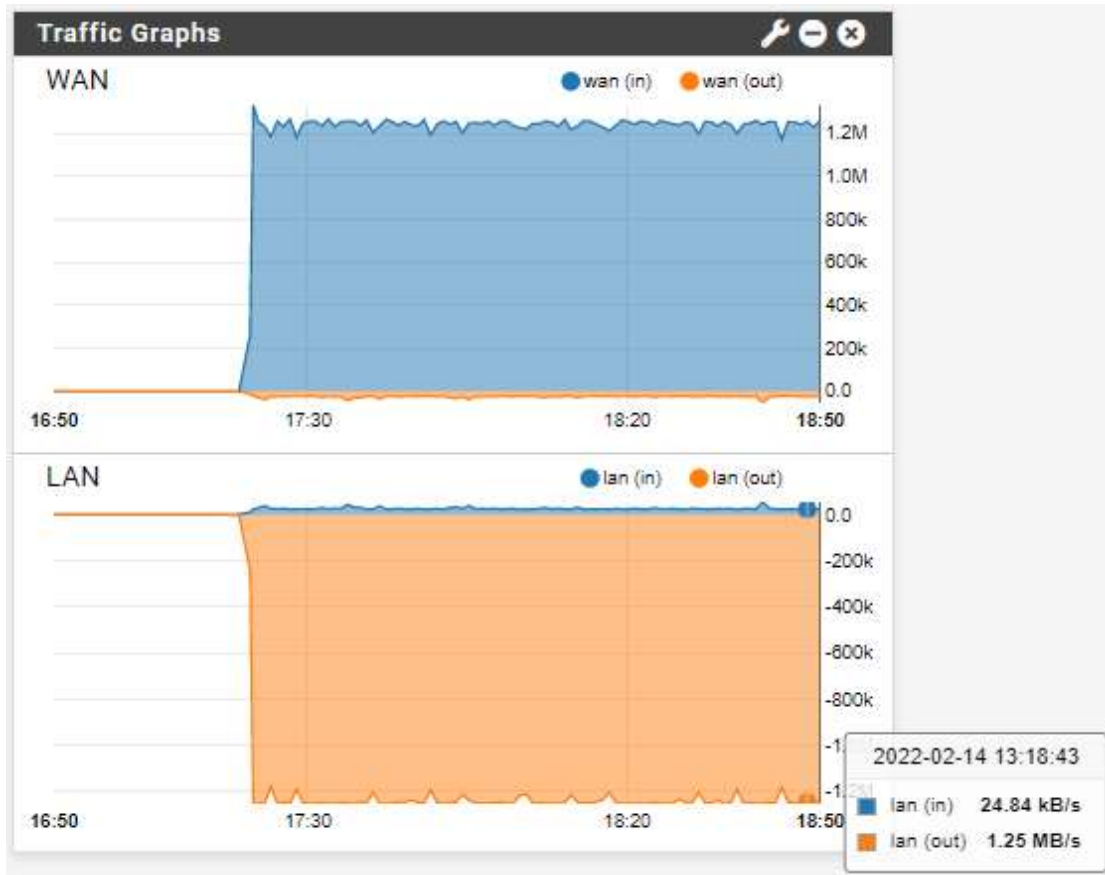
Step13. You can enable discipline and set the bandwidth here and click "Save". (For example, we set the bandwidth to 10Mbit/s)



Step14. Click “Apply Changes”.

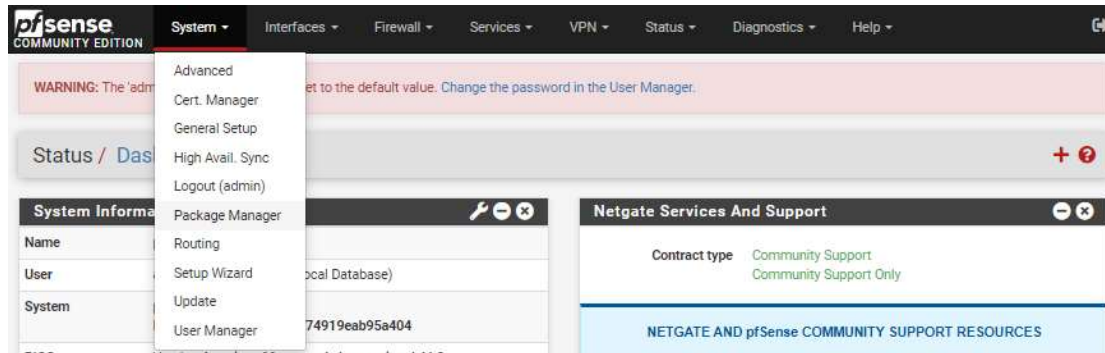


Step15. Please download a large file and go back to the home page. Then you can see the bandwidth of the LAN is keep on 1.25MB/s.

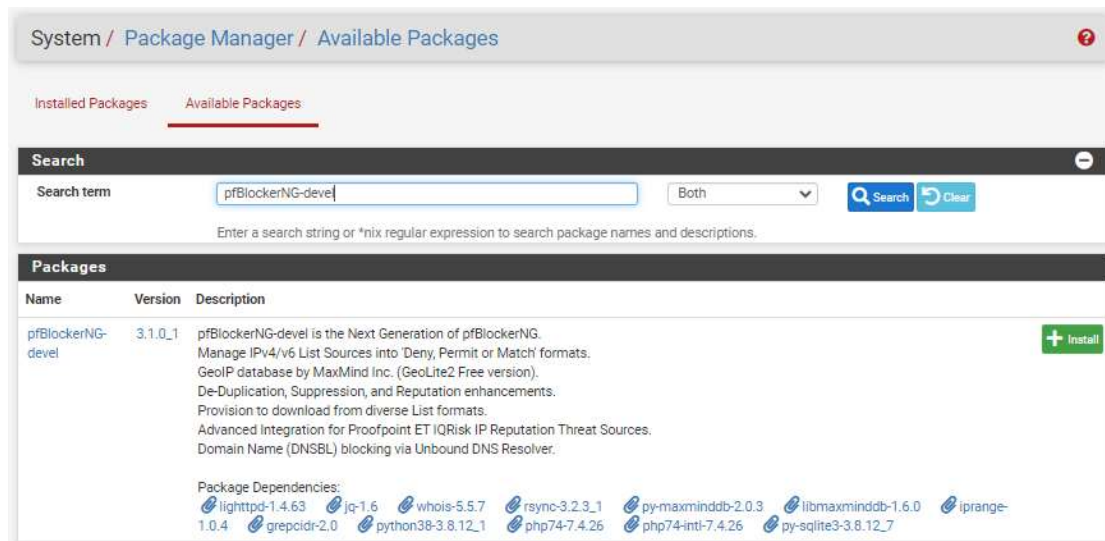


7. Install pfBlockerNG

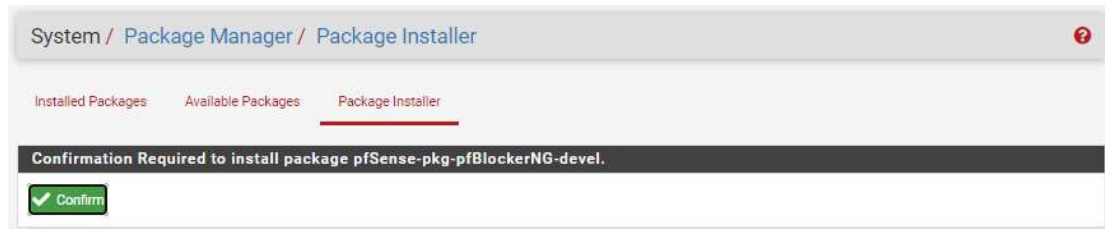
Step1. Choose "System" and click "Package Manager".



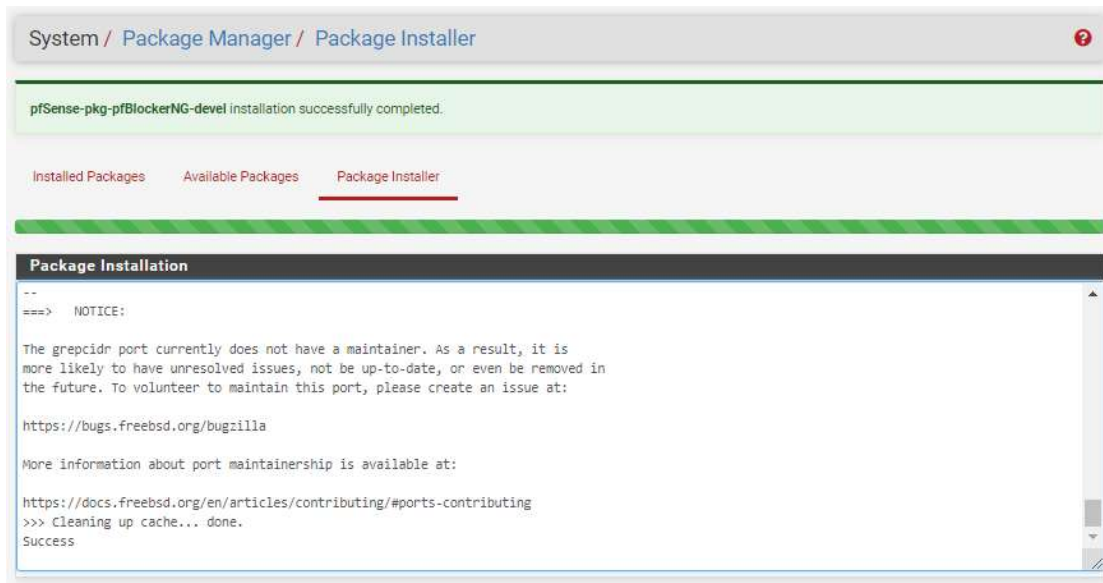
Step2. Click "Available Packages" and type "pfBlockerNG-devel" on the search term. Then click "Search" and "+Install".



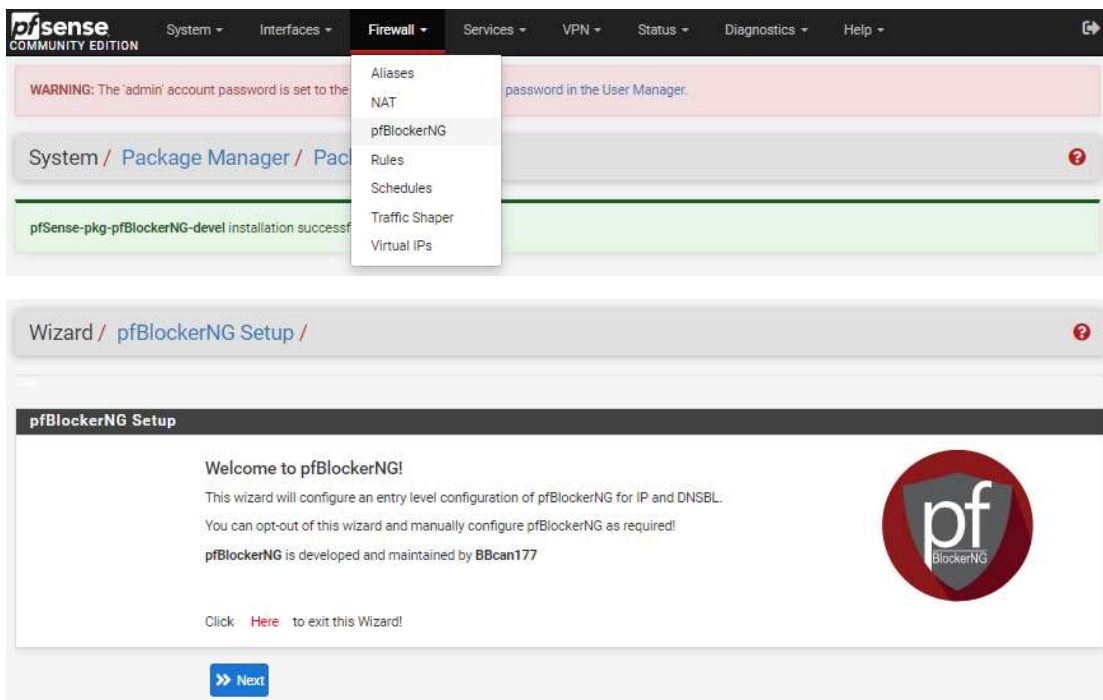
Step3. Click "Confirm".



Step4. When you see the word “Success” and it means the installation is complete.

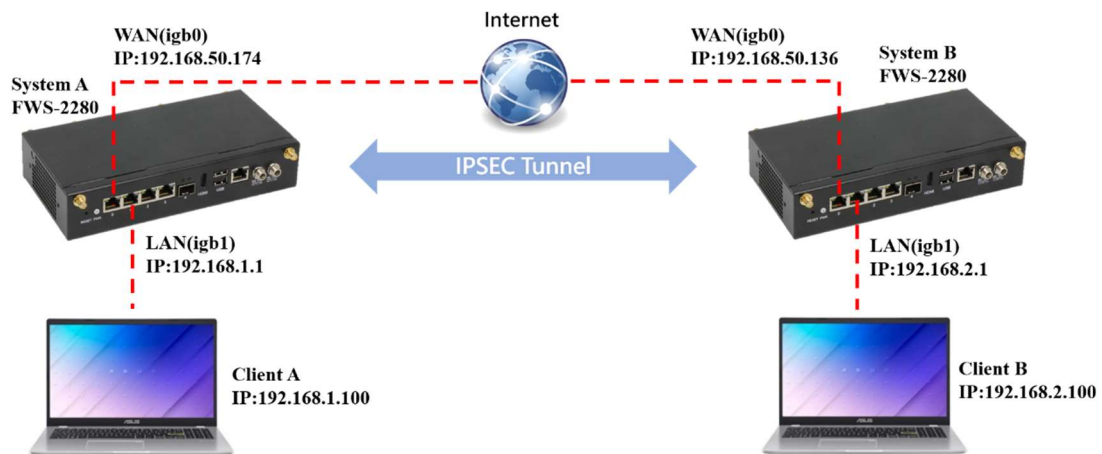


Step5. Now you can choose “Firewall” and click “pfBlockerNG” to start setting.



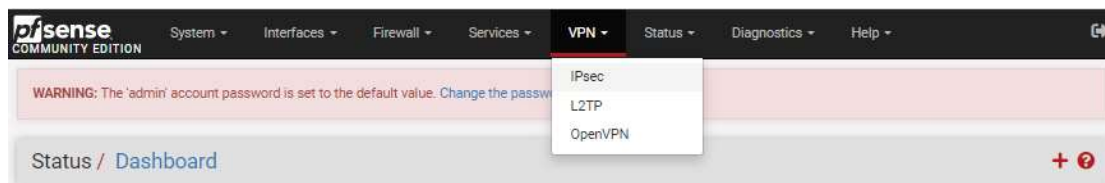
8. IPSEC

The following picture is the IPSEC framework example. You can refer to the following configuration to complete the IPSEC demonstration.

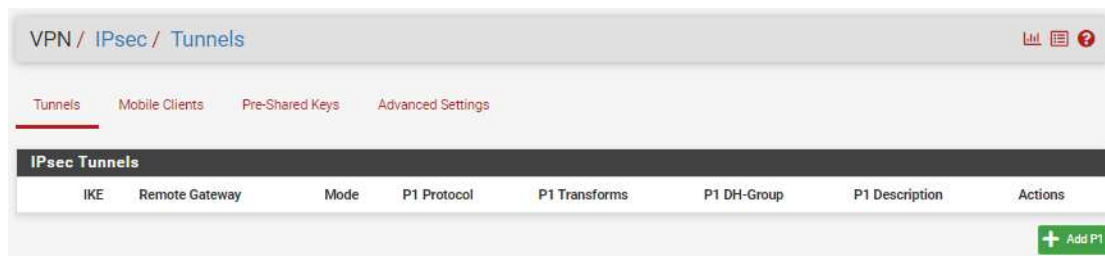


System A:

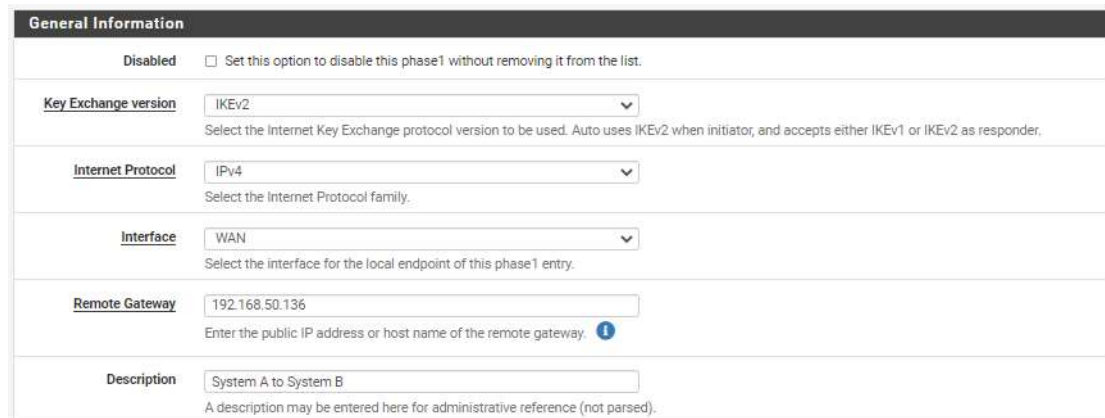
Step1. Choose “VPN” and click “IPsec”.



Step2. Click “Add P1”.



Step3. Type system B WAN IP on the “Remote Gateway”.



Step4. Click “Generate new Pre-Shared Key” and “Save” to finish Phase 1 configuration.

✂System B also needs to enter the same pre-shared key.

Phase 1 Proposal (Authentication)

Authentication Method
Must match the setting chosen on the remote side.

My identifier

Peer identifier

Pre-Shared Key
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
[Generate new Pre-Shared Key](#)

Step5. Click “Show Phase 2 Entries” and “Add P2”.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	V2	WAN 192.168.50.136		AES (128 bits)	SHA256	14 (2048 bit)	System A to System B	Edit Refresh Delete

[+ Show Phase 2 Entries \(0\)](#)

[+ Add P1](#) [Delete P1s](#)

Step6. Type System B subnet on “Remote Network”. For example, “192.168.2.0”. And click “Save” to finish Phase 2 configuration.

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled Disable this phase 2 entry without removing it from the list.

Mode

Local Network /
Type Address
Local network component of this IPsec security association.

NAT/BINAT translation /
Type Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network /
Type Address
Remote network component of this IPsec security association.

Description
A description may be entered here for administrative reference (not parsed).

Step7. Click “Apply Changes”.

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
V2	WAN 192.168.50.136	tunnel	AES (128 bits)	SHA256	14 (2048 bit)	System A to System B	

Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions
tunnel	LAN	192.168.2.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	

Step8. Choose “Firewall” and click “Rules”.

Step9. Choose “IPsec” and click “Add”.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

Step10. Change “Address Family” to “IPv4+IPv6” and “Protocol” to “Any”. Then click “Save”.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
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.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface IPsec
Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Step11. Choose “System” and click “Routing”.

pfSense COMMUNITY EDITION

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

- Advanced
- Cert. Manager
- General Setup
- High Avail. Sync
- Logout (admin)
- Package Manager
- Routing**
- Setup Wizard
- Update
- User Manager

WARNING: The 'admin' password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

Floating WAN

Rules (Drag to Columns)

States	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	*	*	*	*	none			

Step12. Click “Add”.

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> WAN_DHCP		WAN	192.168.50.1	192.168.50.1	Interface WAN_DHCP Gateway	
<input checked="" type="checkbox"/> WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	

Step13. Type a gateway name and type system B WAN IP on the “Gateway”. Then click “Save”.

The screenshot shows the 'Edit Gateway' configuration page. The breadcrumb navigation is 'System / Routing / Gateways / Edit'. The page title is 'Edit Gateway'. There are several configuration fields:

- Disabled:** A checkbox labeled 'Disable this gateway' with a sub-note: 'Set this option to disable this gateway without removing it from the list.'
- Interface:** A dropdown menu set to 'WAN' with a sub-note: 'Choose which interface this gateway applies to.'
- Address Family:** A dropdown menu set to 'IPv4' with a sub-note: 'Choose the Internet Protocol this gateway uses.'
- Name:** A text input field containing 'GATEWAY_A' with a sub-note: 'Gateway name'.
- Gateway:** A text input field containing '192.168.50.136' with a sub-note: 'Gateway IP address'.

Step14. Change “Default gateway IPv4” to “GATEWAY_A” and click “Save”.

The screenshot shows the 'Default gateway' configuration page. The breadcrumb navigation is 'System / Routing / Gateways / Edit'. The page title is 'Default gateway'. There are two configuration fields:

- Default gateway IPv4:** A dropdown menu set to 'GATEWAY_A' with a sub-note: 'Select a gateway or failover gateway group to use as the default gateway.'
- Default gateway IPv6:** A dropdown menu set to 'Automatic' with a sub-note: 'Select a gateway or failover gateway group to use as the default gateway.'

At the bottom of the page, there is a blue 'Save' button.

Step15. Choose “Static Routes” and click “Add”.

The screenshot shows the 'Static Routes' configuration page. The breadcrumb navigation is 'System / Routing / Static Routes'. The page title is 'Static Routes'. There is a yellow notification bar at the top with the text: 'The static route configuration has been changed. The changes must be applied for them to take effect.' and a green 'Apply Changes' button. Below the notification bar, there are three tabs: 'Gateways', 'Static Routes' (which is selected), and 'Gateway Groups'. At the bottom right, there is a green '+ Add' button.

Step16. Type “0.0.0.0” and change mask to “/24” on “Destination network”. And choose “GATEWAY_A - 192.168.50.136” as “Gateway”. Then click “Save”.

The screenshot shows the 'Edit Route Entry' configuration page. The breadcrumb navigation is 'System / Routing / Static Routes / Edit'. The page title is 'Edit Route Entry'. There are several configuration fields:

- Destination network:** A text input field containing '0.0.0.0' and a dropdown menu set to '/ 24' with a sub-note: 'Destination network for this static route'.
- Gateway:** A dropdown menu set to 'GATEWAY_A - 192.168.50.136' with a sub-note: 'Choose which gateway this route applies to or add a new one first'.
- Disabled:** A checkbox labeled 'Disable this static route' with a sub-note: 'Set this option to disable this static route without removing it from the list.'
- Description:** A text input field with a sub-note: 'A description may be entered here for administrative reference (not parsed).'

At the bottom of the page, there is a blue 'Save' button.

Step17. Click “Apply Changes”.

System / Routing / Static Routes

The static route configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Gateways Static Routes Gateway Groups

Static Routes

Network	Gateway	Interface	Description	Actions
0.0.0.0/24	GATEWAY_A - 192.168.50.136	WAN		

Add

System B:

✂Please remember that the LAN port IP of System B should be set to “192.168.2.1”.
Please refer to “Step7” of “3. PfSense WebGUI”

Step1. Choose “VPN” and click “IPsec”.

pfSense COMMUNITY EDITION

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

WARNING: The 'admin' account password is set to the default value. Change the password.

IPsec
L2TP
OpenVPN

Status / Dashboard

Step2. Click “Add P1”.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
-----	----------------	------	-------------	---------------	-------------	----------------	---------

Add P1

Step3. Type system A WAN IP on the “Remote Gateway”.

General Information

Disabled Set this option to disable this phase1 without removing it from the list.

Key Exchange version IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol IPv4
Select the Internet Protocol family.

Interface WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway 192.168.50.174
Enter the public IP address or host name of the remote gateway.

Description System B to System A
A description may be entered here for administrative reference (not parsed).

Step4. Copy system A Pre-Shared Key to here and click “Save” to finish Phase 1 configuration.

Phase 1 Proposal (Authentication)

Authentication Method Mutual PSK
Must match the setting chosen on the remote side.

My identifier My IP address

Peer identifier Peer IP address

Pre-Shared Key 5d51895554772c59bc85c5a71f4ddc2f584c41ccacab12e570e449af
Enter the Pre-Shared Key string. This key must match on both peers.
 This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Generate new Pre-Shared Key

Step5. Click “Show Phase 2 Entries” and “Add P2”.

VPN / IPsec / Tunnels 🔍 📄 📑 ?

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
 The changes must be applied for them to take effect. ✔ Apply Changes

IPsec Tunnels								
	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	V2	WAN 192.168.50.174		AES (128 bits)	SHA256	14 (2048 bit)	System B to System A	🔧 📄 🗑

➕ Show Phase 2 Entries (1)

+ Add P1 🗑 Delete P1

Step6. Type System A subnet on “Remote Network”. For example, “192.168.1.0”. And click “Save” to finish Phase 2 configuration.

VPN / IPsec / Tunnels / Edit Phase 2 🔍 📄 📑 ?

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled Disable this phase 2 entry without removing it from the list.

Mode Tunnel IPv4

Local Network LAN subnet / 0
Type Address
 Local network component of this IPsec security association.

NAT/BINAT translation None / 0
Type Address
 If NAT/BINAT is required on this network specify the address to be translated

Remote Network Network 192.168.1.0 / 24
Type Address
 Remote network component of this IPsec security association.

Description IPSEC B
A description may be entered here for administrative reference (not parsed).

Step7. Click “Apply Changes”.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions	
<input type="checkbox"/>	Disable	V2	WAN	AES (128 bits)	SHA256	14 (2048 bit)	System B to System A		
			Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions
<input type="checkbox"/>	Disable	tunnel	LAN	192.168.1.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256		

+ Add P2

+ Add P1 Delete P1s

Step8. Choose “Firewall” and click “Rules”.

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the same password in the User Manager.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Step9. Choose “IPsec” and click “Add”.

Firewall / Rules / IPsec

Floating WAN LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--	--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Save Separator

Step10. Change “Address Family” to “IPv4+IPv6” and “Protocol” to “Any”. Then click “Save”.

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
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.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface IPsec
Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Step11. Choose “System” and click “Routing”.

pfSense COMMUNITY EDITION

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

- Advanced
- Cert. Manager
- General Setup
- High Avail. Sync
- Logout (admin)
- Package Manager
- Routing**
- Setup Wizard
- Update
- User Manager

WARNING: The 'adm... set to the default value. Change the password in the User Manager.

Firewall / Ru... Floating WAN... Rules (Drag to C... States 0/0 B...

Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
*	*	*	*	none			

Step12. Click “Add”.

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
WAN_DHCP		WAN	192.168.50.1	192.168.50.1	Interface WAN_DHCP Gateway	
WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	

Save + Add

Step13. Type a gateway name and type system A WAN IP on the “Gateway”. Then click “Save”.

System / Routing / Gateways / Edit

Edit Gateway

Disabled Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface WAN
Choose which interface this gateway applies to.

Address Family IPv4
Choose the Internet Protocol this gateway uses.

Name GATEWAY_B
Gateway name

Gateway 192.168.50.174
Gateway IP address

Save

Step14. Change “Default gateway IPv4” to “GATEWAY_B” and click “Save”.

System / Routing / Static Routes / Edit

Default gateway

Default gateway IPv4 GATEWAY_B
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6 Automatic
Select a gateway or failover gateway group to use as the default gateway.

Save

Step15. Choose “Static Routes” and click “Add”.

System / Routing / Static Routes

The static route configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Gateways Static Routes Gateway Groups

Static Routes

Network	Gateway	Interface	Description	Actions
---------	---------	-----------	-------------	---------

+ Add

Step16. Type “0.0.0.0” and change mask to “/24” on “Destination network”. And choose “GATEWAY_B - 192.168.50.174” as “Gateway”. Then click “Save”.

System / Routing / Static Routes / Edit

Edit Route Entry

Destination network 0.0.0.0 / 24
Destination network for this static route

Gateway GATEWAY_B - 192.168.50.174
Choose which gateway this route applies to or add a new one first

Disabled Disable this static route
Set this option to disable this static route without removing it from the list.

Description
A description may be entered here for administrative reference (not parsed).

Save

Step17. Click “Apply Changes”.

When both System A and System B are configured, please choose “Status” and click “IPsec”.

Click “Connect VPN”.

IPsec ID	Description	Local	Remote	Role	Timers	Algo	Status
	System A to System B	ID: 192.168.50.174 Host: 192.168.50.174	ID: 192.168.50.136 Host: 192.168.50.136				Disconnected Connect VPN

Please wait for a while, if you see a value in Bytes-in/out, it means that the tunnel can start to transmit.

IPsec ID	Description	Local	Remote	Role	Timers	Algo	Status
con100000: #11	System A to System B	ID: 192.168.50.174 Host: 192.168.50.174:500 SPI: 10b532b50d22f619	ID: 192.168.50.136 Host: 192.168.50.136:500 SPI: 59a0b2358e74492f	IKEv2 initiator	Rekey: 25013s (06:56:53) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 257 seconds (00:04:17) ago Disconnect

IPsec ID	Local subnets	Local SPI(s)	Remote subnets	Times	Algo	Stats
con100000: #14	192.168.1.0/24	Local: c6df87cc Remote: c875c3b4	192.168.2.0/24	Rekey: 2648 seconds (00:44:08) Life: 3343 seconds (00:55:43) Install: 257 seconds (00:04:17)	AES_GCM_16 (128) IPComp: none	Bytes-In: 480 (480 B) Packets-In: 6 Bytes-Out: 1,512 (1 KiB) Packets-Out: 12 Disconnect

In Client B, you can ping “192.168.1.100” to test the IPSEC.

```
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\NSD>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126
Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\NSD>
```

9. AAEON PfSense SDK

PfSense SDK from AAEON is a software development kit designed to help developers with controlling hardware on AAEON FWS series platforms.

AAEON PfSense SDK provides developers fast control on AAEON FWS series IO functions:

- Software Programmable Button Settings and Configuration
- Status LED Settings and Configuration
- DIO Settings and Configuration
- Lanbypass Settings and Configuration
- Watchdog Settings and Configuration
- Liquid Crystal Display Module (LCM) Settings and Configuration

10. Purchase Netgate PfSense Support

If you need pfsense support services (such as setup assistance), you can refer to the following website: <https://www.netgate.com/support>

Netgate TAC Support Options	TAC LITE	TAC PRO	TAC ENTERPRISE
For Netgate appliances, AWS/Azure pfSense cloud instances, or 3rd party hardware	FREE*	\$399 /per year	\$799 /per year
Zero-to-Ping**	✓	✓	✓
TAC Support Hours	—	24/7	24/7
Target Initial Response SLA	—	24 Hours	4 Hours
Email / Support Portal	—	✓	✓
Telephone Support	—	—	✓

[Buy TAC Pro](#) [Buy TAC Enterprise](#)