

Установка и настройка pfSense - Академия Selectel

 selectel.ru/blog/tutorials/how-to-install-and-configure-pfsense

17 декабря 2021 г.

Введение

Что такое pfSense

Многофункциональный программный маршрутизатор-брандмауэр pfSense разработан компанией Netgate на базе ОС FreeBSD.

pfSense распространяется в нескольких редакциях: программный Community Edition (CE), в виде аппаратного appliance NetGate. Для Community Edition доступна коммерческая поддержка по цене от \$400 до \$800 в год. В 2021 году запущен pfSense Plus Software, в пользу которого предполагается сфокусировать основные усилия по разработке новых функций.

pfSense имеет модульную архитектуру и свой пакетный менеджер. Основные функции: маршрутизация, в т.ч. динамическая, межсетевое экранирование, NAT, DHCP-сервер, балансировка нагрузки, VPN (включая OpenVPN и L2TP), dDNS, PPPoE, IDS, проксирование и другое. Поддерживается построение отказоустойчивого кластера. Есть встроенный мониторинг, журналирование и построение отчетов.

Многие организации и домашние офисы используют pfSense для подключения к интернет-ресурсам. При этом часто используется бесплатная редакция Community Edition без техподдержки.

Продукт развивается с 2004 года, на текущий момент достиг высокой зрелости и стабильности. Во многих случаях это позволяет использовать его бесплатную редакцию Community Edition без техподдержки.

Аппаратные требования

CE можно установить как на bare metal, так и в виртуальной машине. Аппаратные требования диктуются необходимыми скоростями сетевых интерфейсов — от минимальных 500 МГц/512 МиБ для 10 Мб/с. до многоядерного 2+ ГГц/2 ГиБ для 1 Гб/с.

Использование дополнительных функций и модулей требует увеличения количества ядер ЦПУ и объема ОЗУ. Для часто используемого подключения со скоростью 100 Мб/с. рекомендуется 1 ГГц/1 ГБ. Для более высоких скоростей также необходима шина PCIe, т.к. в противном случае ее предшественница будет узким местом.

К размеру диска требования невысокие, но также зависят от используемых функций, минимальный размер — 8 ГБ. В остальном, pfSense построен на базе FreeBSD, поэтому список совместимого аппаратного обеспечения диктуется поддерживаемым во FreeBSD.

Установка pfSense CE

Продemonстрируем установку, настройку и работу pfSense на примере виртуальной машины в облаке Selectel. В качестве стенда создадим лабораторию из двух машин: на одной (с двумя интерфейсами — внешним и внутренним) будет работать pfSense, на другой (с одним внутренним) — десктопный клиент.

pfSense является кастомным решением для облачной платформы Selectel, поэтому есть ряд неочевидных нюансов.

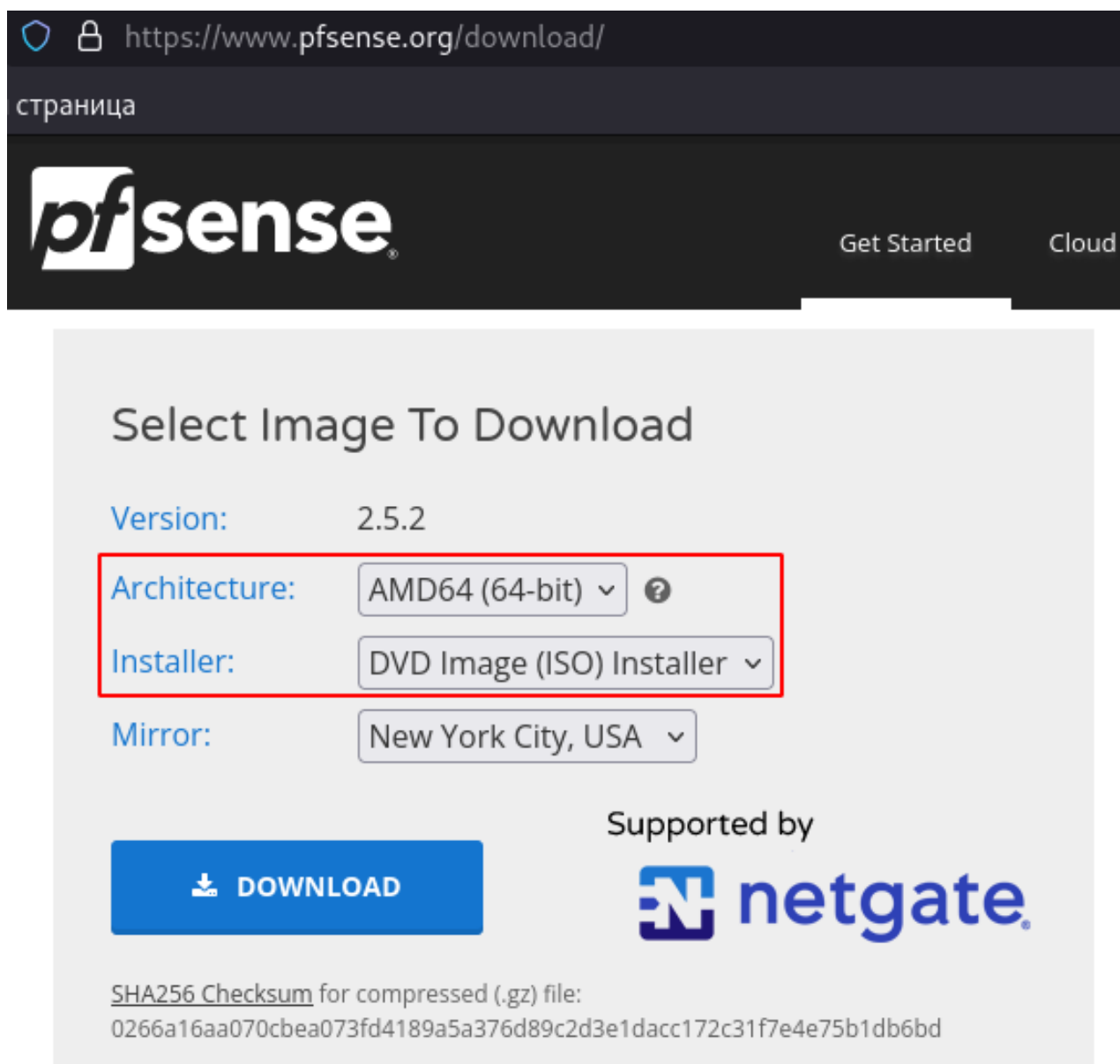
По состоянию на август 2021 года:

- В настройках установочного образа необходимо указывать Linux вместо «Другая» (в противном случае получим ошибку Internal error Invalid image metadata. Error: Field value other is invalid).
- Дистрибутив работает только с сетевыми дисками и не может установиться на сервер с локальным диском.
- Другой нюанс заключается в том, что невозможно совместить установку через образ в панели управления и выбор сразу двух сетевых интерфейсов.

Обходные пути — создание машины с двумя интерфейсами и подключение установочного ISO-образа через OpenStack CLI, либо установка с одним сетевым интерфейсом с последующим добавлением 2-го. Последний путь проще, им и пойдем.

Загрузка образа

На странице загрузки pfSense CE выбираем архитектуру *AMD64 (64-bit)* и тип образа *DVD Image (ISO)*.



Выполняем проверку целостности загруженного архива и распаковываем его:

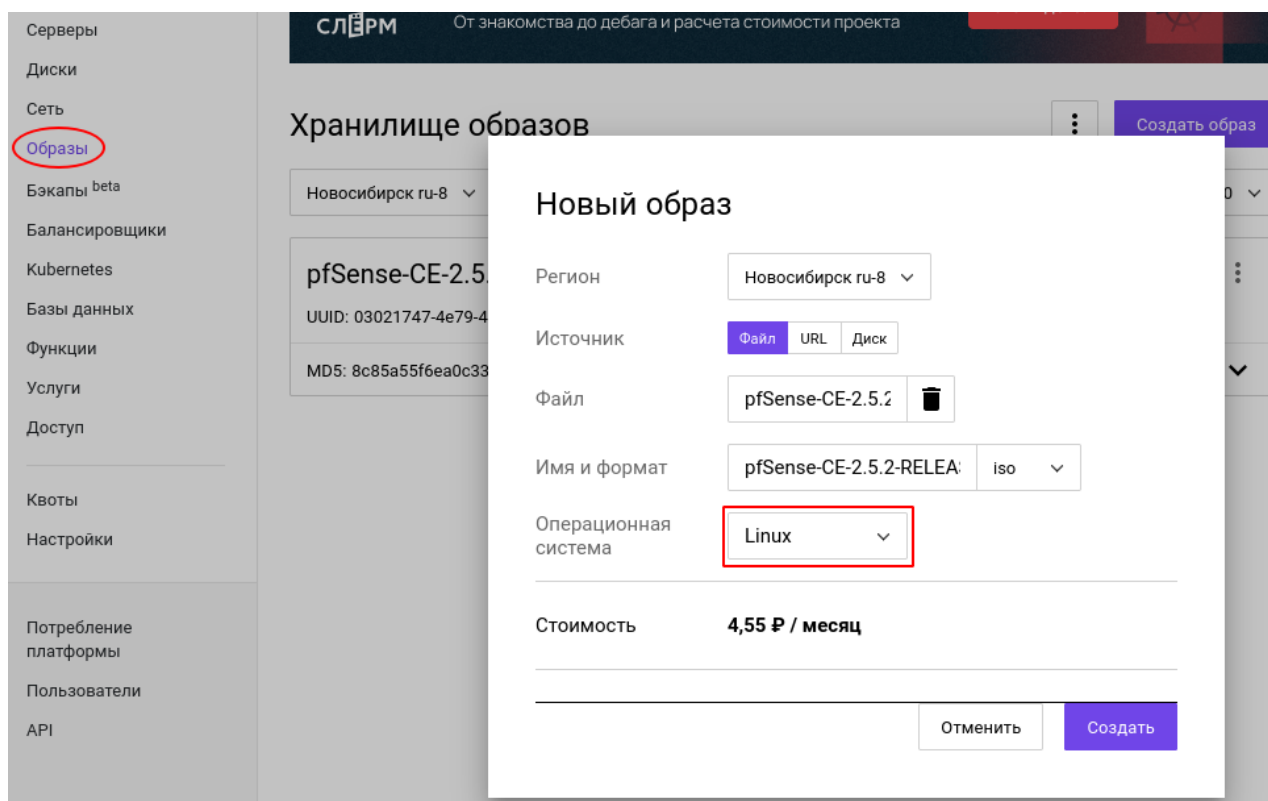
```
$ sha256sum=$(sha256sum Download/pfSense-CE-2.5.2-RELEASE-amd64.iso.gz) && [
"$sha256sum" == "0266a16aa070cbea073fd4189a5a376d89c2d3e1dacc172c31f7e4e75b1db6bd"
] && echo "Ok" || echo "Something wrong"
$ gunzip Download/pfSense-CE-2.5.2-RELEASE-amd64.iso.gz
```

Значение контрольной суммы sha256

0266a16aa070cbea073fd4189a5a376d89c2d3e1dacc172c31f7e4e75b1db6bd

смотрим на странице загрузки. В примере указана для актуальной на момент написания версии 2.5.2.

После этого создаем и загружаем образ в хранилище в панели управления, указав ОС Linux:



Установка и первоначальная настройка pfSense

В разделе серверы «Облачной платформы» нажимаем кнопку «Создать сервер» вверху справа (или в центре, если это 1-й). Выбираем минимальную произвольную конфигурацию (1 vCPU/512 МиБ RAM/5 ГиБ Storage, 17,82 Р/день по состоянию на август 2021) — в тестовых целях этого достаточно, для остальных случаев системные требования указаны выше.

My First Project

Серверы

Диски

Сеть

Образы

Бэкапы beta

Балансировщики

Kubernetes

Базы данных

Функции

Услуги

Доступ

Квоты

Настройки

Потребление платформы

Пользователи

API

Новый сервер

Имя и расположение

Имя

Регион

Зона

gw02

Новосибирск ru-8

ru-8a

Источник

pfSense-CE-2.5.2-RELEASE-amd64
1 ГБ Диск

Выбрать другой источник

{...}

Конфигурация

Фиксированные конфигурации
для решения конкретных задач

Произвольная конфигурация
по вашим требованиям

☐ Локальный диск
Загрузочный диск без сетевых задержек. Чтение 12800 IOPS / Запись 6400 IOPS.

vCPU
от 1 до 8 ядер

RAM
от 512 МБ до 64 ГБ

—

1

+

—

512

+

MB

GB

Сетевые диски

Тип диска

Размер диска

Универсальный диск

—

5

+

GB

TB

Удалить диск

Сеть на данном этапе оставляем как «**Новая приватная сеть**» — она будет у нас внутренней, адрес 192.168.1.0/24. Присвоим имя `int_net`, DHCP — выключим. Настройка шлюза в данном случае ни на что не влияет, но убрать его невозможно.

Сеть

Подсеть

Новая приватная подсеть

CIDR подсети

DHCP

192.168.1.0/24

⏻

Шлюз: 192.168.1.1

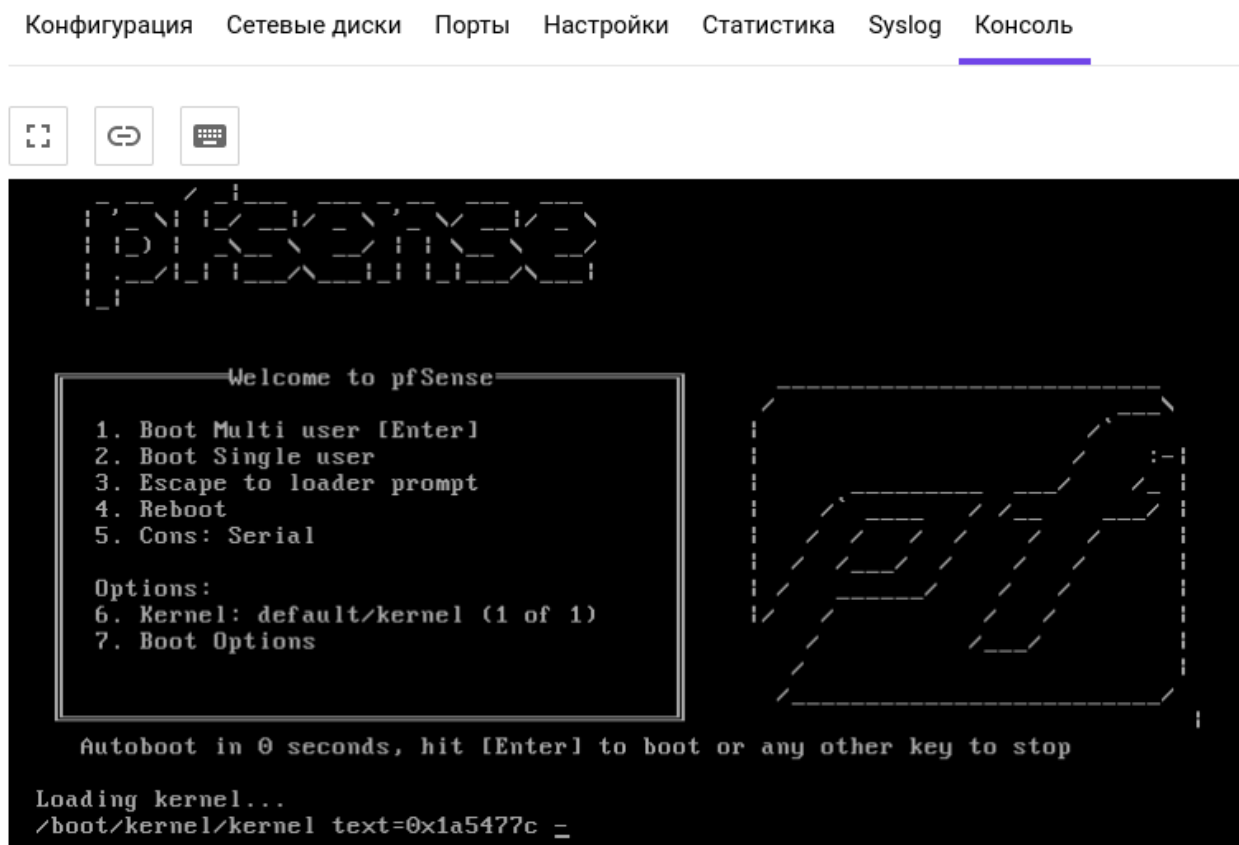
Подсеть будет создана в сети:

Имя новой сети

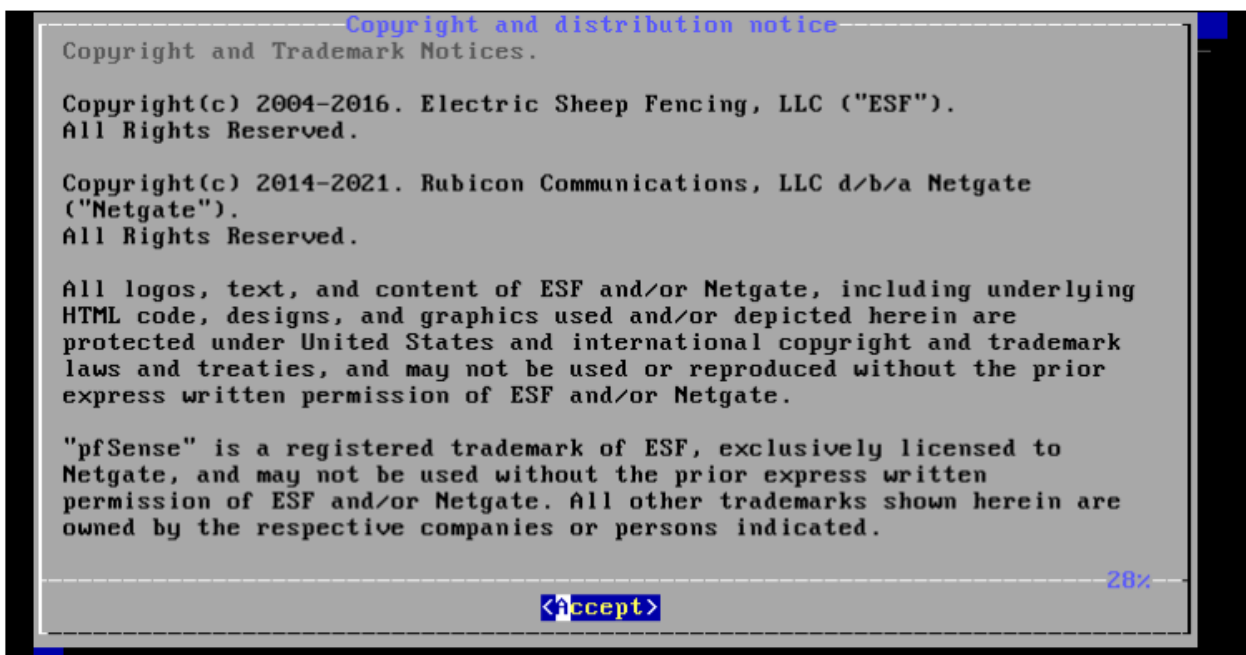
int_net

Приватный адрес будет присвоен серверу в про

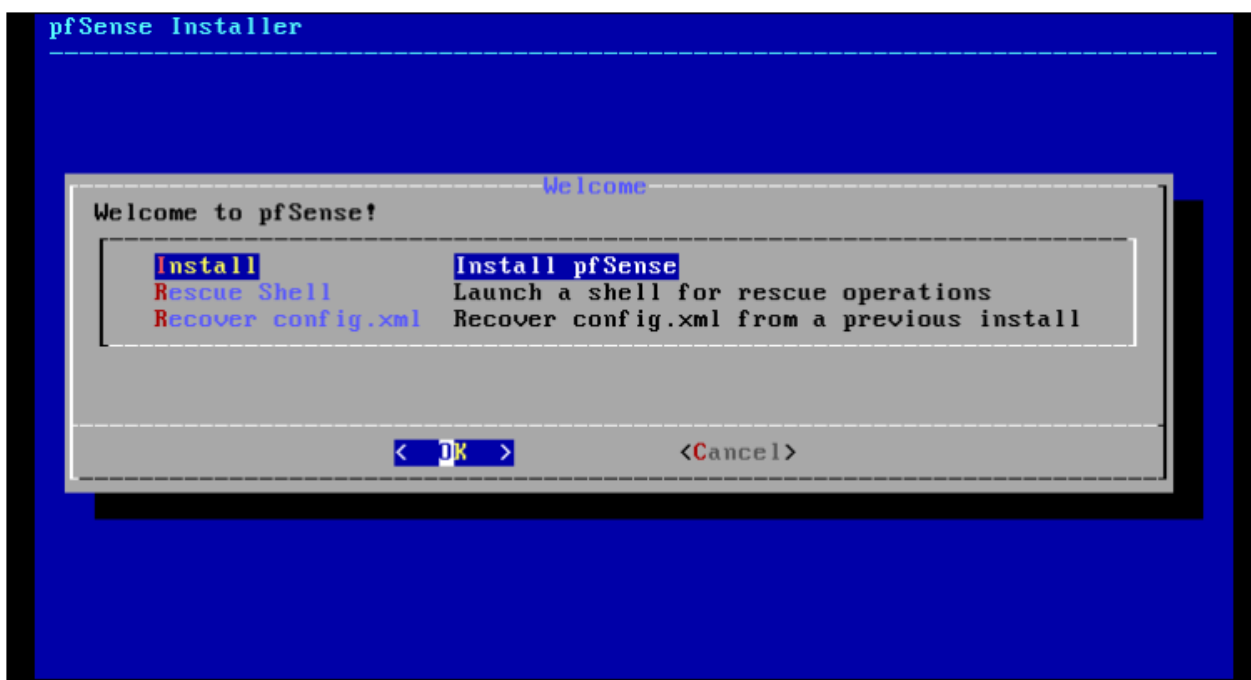
После указания необходимых параметров нажимаем кнопку **«Создать»**. Сервер конфигурируется и будет доступен через 30 секунд. Если вы случайно закрыли вкладку, где создавалась машина — не проблема, теперь сервер доступен в глобальном разделе **«Серверы»**. Для взаимодействия с консолью сервера мы переходим в его карточку на вкладке **«Серверы»**, далее открываем пункт **«Консоль»**.



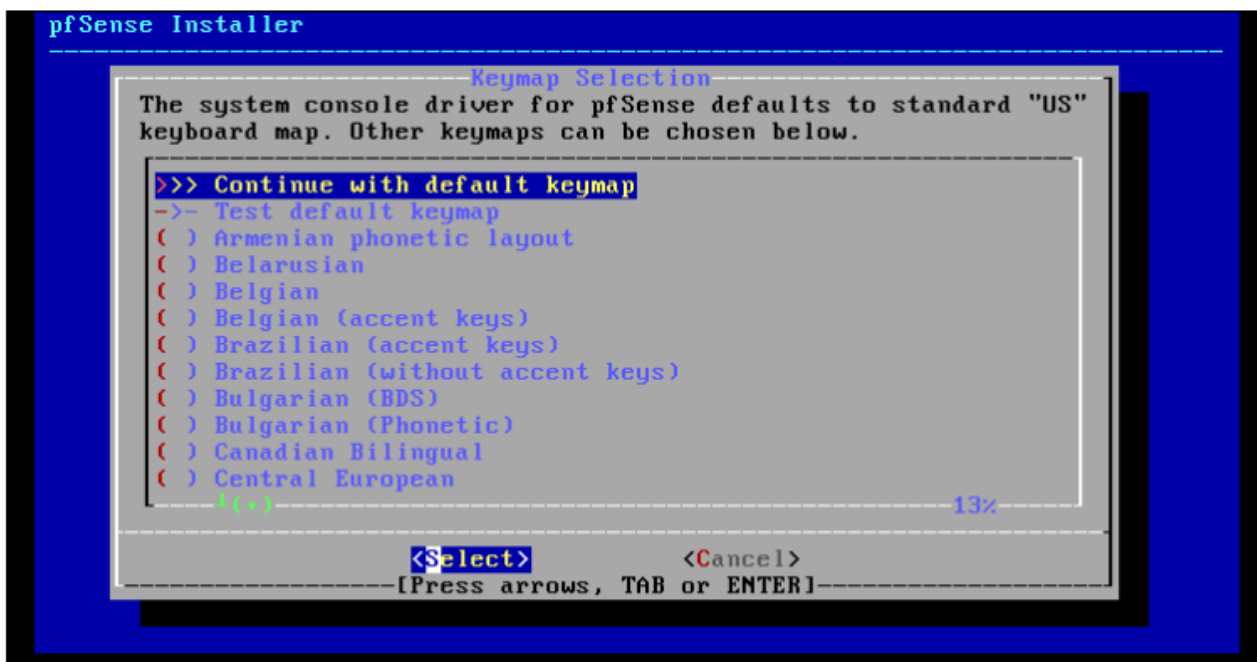
Читаем и соглашаемся с авторскими правами.



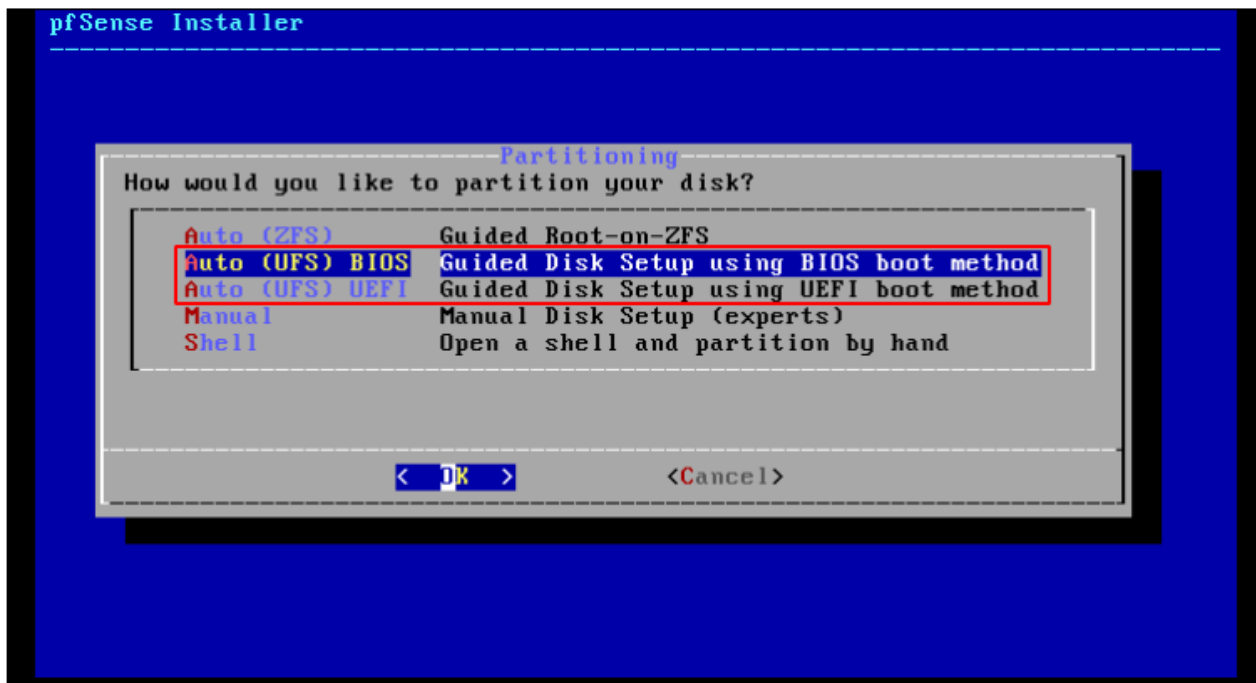
Выбор режима установки. На этом же этапе работы установщика можно задействовать и встроенный режим восстановления.



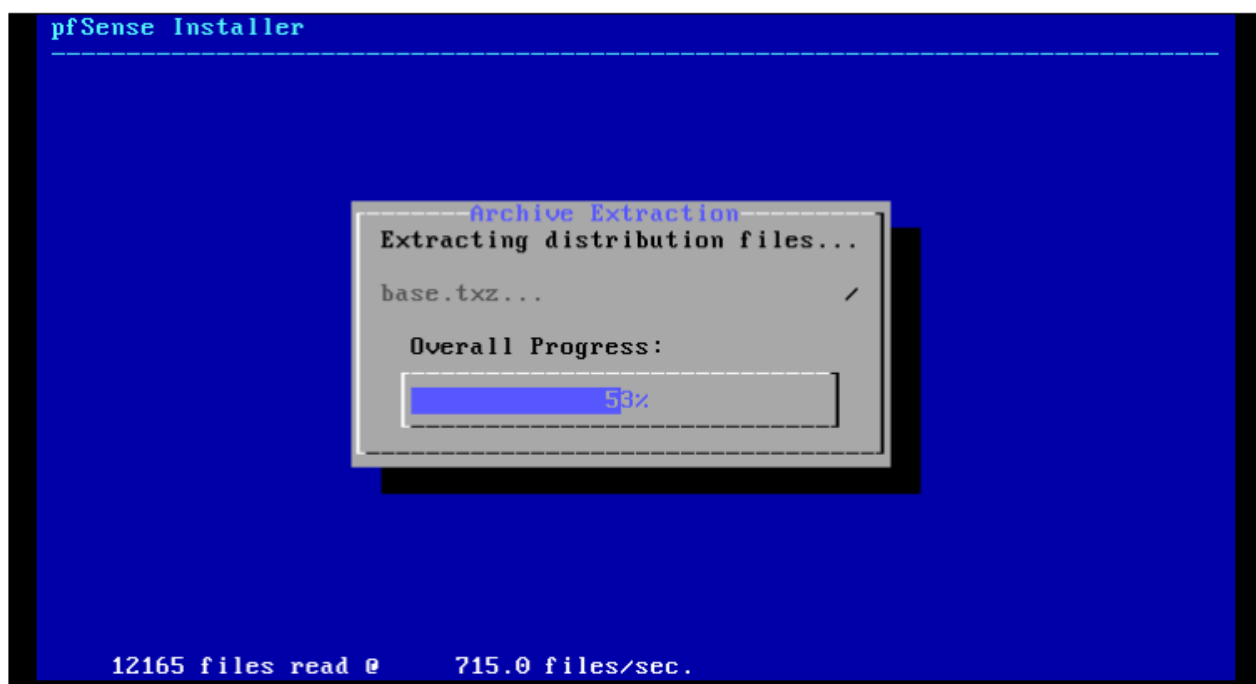
Консоль системы не будет видна рядовым пользователям, нет смысла менять локализацию — оставляем по умолчанию.



В зависимости от аппаратной архитектуры выбираем метод загрузки и разметки накопителя, для VM — BIOS.



Наблюдаем за процессом установки.



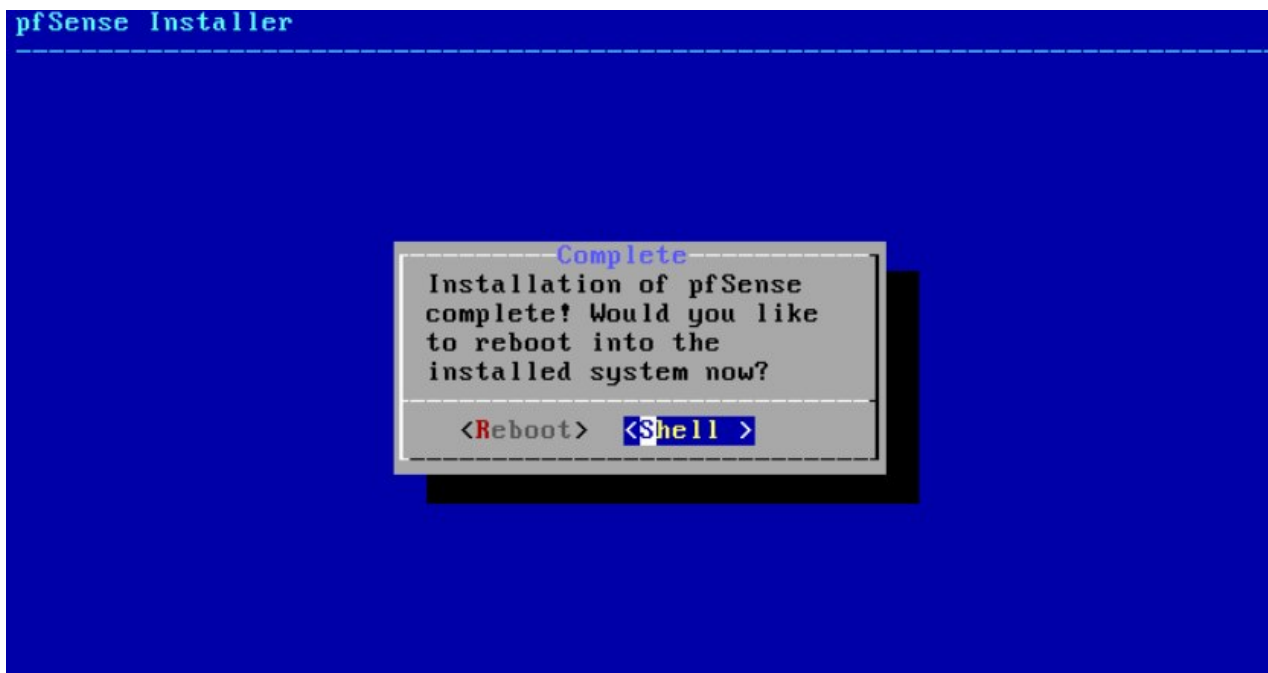
По окончании установки появится следующее окно.



Нажав кнопку **Yes**, мы попадем в оболочку (**Shell**). Здесь можно выполнить любые настройки системы вручную. После окончания настроек вернуться в программу установку можно, выполнив команду **exit**. Обычно на этом этапе ничего менять не требуется, нажимаем **No**.

Настройка сетей

Для нашей лаборатории понадобится одна внешняя и одна внутренняя сети — для этого нужно добавить второй интерфейс. Запускаем оболочку, нажав **Shell**.



И даем команду на выключение:

```
# poweroff
```

В реальной жизни при установке на своем сервере этот этап не потребуется.

На глобальной вкладке «**Серверы**» у виртуальной машины будет статус **SHUTOFF**.

Далее рассмотрим сценарий подключения к провайдеру по IP, где нам выдана сеть по маске /29 (минимально возможная на облачной платформе Selectel).

Переходим в глобальную панель «**Сеть**»->«**Публичные подсети**» и нажимаем «**Создать подсеть**».

В панели управления можно выбрать маски от /29 до /27. Если ваш провайдер предоставил сеть с маской /30, сценарий подключения и настройки будет аналогичным.

[Приватные сети](#) [Роутеры](#) [Публичные подсети](#) [Плавающие IP](#) [VRRP-подсети](#)

Публичные подсети

Создать подсеть

Санкт-Петербург ru-9 10

94.26.250.176/29

3306a3c7-b342-4214-9ea9-37af13ece320

94.26.250.176/29 0 портов

На этом этапе система выделит сеть (в примере — 94.26.250.176/29) и назначит шлюз по умолчанию (94.26.250.177). Он понадобится дальше при настройке WAN-интерфейса. В реальной жизни это будет адрес шлюза провайдера.

Добавим новую сеть к нашему серверу, «**Серверы**» -> «**Порты**» -> «**Добавить порт**» -> «**Выберите сеть**» -> «**Добавить порт**».

gw02

ru-9a • 6c72b453-30fb-40ca-9402-cf93992759ec

SHUTOFF



Конфигурация Сетевые диски **Порты** Настройки Статистика Syslog Консоль

Подсеть	IP-адрес	Плавающий IP ?	MAC
int_net	192.168.0.229	<input type="button" value="Подключить"/>	fa:16:3e:c8:5e:42

Подсеть	IP-адрес	<input type="button" value="Добавить порт"/>	<input type="button" value="X"/>
94.26.250.176/29	94.26.250.178		

При каждом изменении портов необходимо вручную дублировать изменения в файл конфигурации сети в сервере.

Система выделила адрес нашему серверу (94.26.250.178) — теперь у него, как и полагается настоящему интернет-шлюзу, два интерфейса — внешний, включенный в глобальную, и внутренний, включенный в нашу локальную сеть.

```

AMD Extended Feature Extensions ID EBX=0x1001000
UT-x: PAT,HLT,MTF,PAUSE,EPT,UG,UPID,UID,PostIntr
Hypervisor: Origin = "KVMKVMKVM"
Done.
.... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
vtnet0: link state changed to UP
vtnet1: link state changed to UP

Valid interfaces are:

vtnet0 fa:16:3e:c8:5e:42 (down) VirtIO Networking Adapter
vtnet1 fa:16:3e:28:25:6a (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? █

```

Поддержки VLAN в «Облачной платформе» Selectel нет, отказываемся и переходим к настройке интерфейсов.

Интерфейсом **vtnet0** наш сервер смотрит внутрь сети, **vtnet1** — наружу.

```

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet0 a or nothing if finished): vtnet0

The interfaces will be assigned as follows:

WAN   -> vtnet1
LAN   -> vtnet0

Do you want to proceed [y/n]? █

```

Для применения настроек и продолжения установки нажимаем клавишу у.

```

KVM Guest - Netgate Device ID: 14f8ce11aa150463fc52

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

WAN (wan)      -> vtnet1      ->
LAN (lan)      -> vtnet0      -> 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: █

```

В консоли pfSense присвоим выданный ранее внешний адрес (WAN-интерфейс).

```

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 (vtnet0 - static)
2 - LAN (vtnet1 - static)

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

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

```

Пункт 2-Set Iface IP -> 1-WAN -> DHCP -> N -> Enter IP-Address -> Enter mask -> Enter gateway.

```
2 - LAN (vtnet0 - 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:
> 94.26.250.178

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):
> 29

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 94.26.250.177

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

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

Следом система предложит изменить настройки IPv6. В нашем сценарии это не требуется, настройки не меняем.

Утвердительно отвечаем на вопрос «Do you want to revert to HTTP as the webConfigurator protocol?» и 3-4 секунды ожидаем применения конфигурации.

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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) y

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

The IPv4 WAN address has been set to 94.26.250.178/29

Press <ENTER> to continue.█
```

Проверяем доступность шлюза провайдера (эта возможность доступна в пункте 7).

```
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
```

```
Enter a host name or IP address: 94.26.250.177
```

```
PING 94.26.250.177 (94.26.250.177): 56 data bytes
64 bytes from 94.26.250.177: icmp_seq=0 ttl=64 time=0.660 ms
64 bytes from 94.26.250.177: icmp_seq=1 ttl=64 time=1.590 ms
64 bytes from 94.26.250.177: icmp_seq=2 ttl=64 time=3.756 ms
```

```
--- 94.26.250.177 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.660/2.002/3.756/1.297 ms
```

```
Press ENTER to continue.
```

После выбора пункта **Ping host** указываем адрес шлюза провайдера или, в нашей лаборатории, платформы.

Тестовый клиент

Следующим этапом добавим в нашу лабораторию тестовую машину (Ubuntu 18/1 vCPU/2 ГиБ RAM/8 ГиБ Storage). Она будет имитировать нашего пользователя и подключаться к интернет-ресурсам через pfSense. С нее же будем продолжать настройку pfSense.

От этой машины нам нужен только браузер. Возьмем готовый образ Ubuntu 18 и добавим туда графическую оболочку. Для доступа к репозиториям потребуется временно подключить машину ко внешней сети напрямую.

Новый сервер

Имя и расположение

Имя	Регион	Зона
<input type="text" value="clnt02"/>	<input type="text" value="Санкт-Петербург ru-9"/>	<input type="text" value="ru-9a"/>

Источник

 Ubuntu 18.04 LTS 64-bit 512 МБ RAM, 5 ГБ Диск	<input type="button" value="Выбрать другой источник"/>	<input data-bbox="1345 544 1390 577" type="button" value="{...}"/>
---------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------	--------------------------------------------------------------------

Конфигурация

<input type="radio"/> Фиксированные конфигурации выбор из готовых наборов ресурсов	<input checked="" type="radio"/> Произвольная конфигурация настройка каждого ресурса отдельно
---------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

☐ Локальный диск ⓘ
Загрузочный диск без сетевых задержек. Чтение **12800** IOPS / Запись **6400** IOPS.

vCPU от 1 до 8 ядер	RAM от 512 МБ до 64 ГБ
<input type="button" value="−"/> <input type="text" value="1"/> <input data-bbox="539 1014 566 1048" type="button" value="+"/>	<input type="button" value="−"/> <input type="text" value="2"/> <input data-bbox="826 1014 853 1048" type="button" value="+"/> <input type="text" value="MB"/> <input type="button" value="GB"/>

Процессоры 2,2–2,4 ГГц.

Сетевые диски

Тип диска	Размер диска
<input type="text" value="Универсальный диск"/>	<input type="button" value="−"/> <input type="text" value="8"/> <input data-bbox="826 1272 853 1305" type="button" value="+"/> <input type="text" value="GB"/> <input type="text" value="TB"/>

Сеть

Подсеть
<input type="text" value="94.26.250.176/29"/>
Публичный IP
<input type="text" value="94.26.250.179"/>

Нажимаем кнопку **«Создать»**, секунд 15-20 ожидаем рождения сервера и подключаемся к его консоли.

Если при создании машины была использована внутренняя сеть (int_net), можно либо пересоздать машину полностью, либо удалить этот сетевой интерфейс и добавить внешний, после чего выполнить на машине.

```
# ip link set eth0 down
# ip addr add 94.26.250.179/29 dev eth0
# ip link set eth0 up
# ip route add default via 94.26.250.177 dev eth0
# ping 94.26.250.177
# ping ya.ru
```

Обновление ОС

Хоть это и тестовая машина, первым делом обновляем ее:

```
# apt-get update -y && apt-get upgrade -y
```

Если обновилось ядро, машину следует перезагрузить.

Установка GUI

Настройка графики выходит за рамки статьи, подробнее о ней можно найти на тематических сайтах, перечень команд может быть таким.

```
# apt install tasksel slim -y
# tasksel install ubuntu-desktop
# adduser myuser
# systemctl start slim
```

По графической части: на платформе Selectel для переключения между консолями ВМ можно использовать сочетание **Alt+left/right arrow** или **F1**, привычное **Ctrl+Alt+Fn** может не сработать.

Здесь же создается рядовой пользователь, дабы исключить дальнейшую работу под root'ом.

Переключение сетевого интерфейса

После запуска графического интерфейса переносим наш десктоп во внутреннюю сеть, для чего на вкладке «**Порты**» сервера удаляем внешний интерфейс и подключаем внутреннюю сеть — int_net (это лучше делать на выключенной машине — systemctl poweroff).

Поскольку образ взят из репозитория Selectel, он заточен под взаимодействие с этой платформой и получает от нее сетевую конфигурацию.

В нашей лаборатории это не нужно, наш DHCP работает на pfSense и именно он должен задавать сетевые параметры клиента. Поведение гостевой машины меняется командой.

```
$ sudo touch /etc/cloud/cloud-init.disabled
```


Netplan в облачной платформе использоваться не должен, поэтому для включения DHCP на интерфейсе машины редактируем файл.

```
/etc/network/interfaces.d/50-cloud-init.cfg
```

Приводим к виду:

```
# network: {config: disabled}
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Проверка:

Посмотреть текущий ip-адрес можно командой `ip a[ddress]`, а проверить настройки, полученные от DHCP-сервера командой.

```
less /var/lib/dhcp/dhclient.<iface>.leases
```

Адрес DHCP-сервера можно узнать так:

```
myuser@clnt02:~$ grep ident /var/lib/dhcp/dhclient.eth0.leases |tail -n 1
option dhcp-server-identifier 192.168.1.1;
```

Если по какой-то причине при создании машины в сети `int_net` был включен DHCP, на этапе перед выключением или перезагрузкой машины DHCP в этой сети необходимо выключить, в противном случае адреса будет раздавать хост 192.168.1.2 или .3. После этого приводим настройки `cloud-init` и сетевого интерфейса как указано выше.

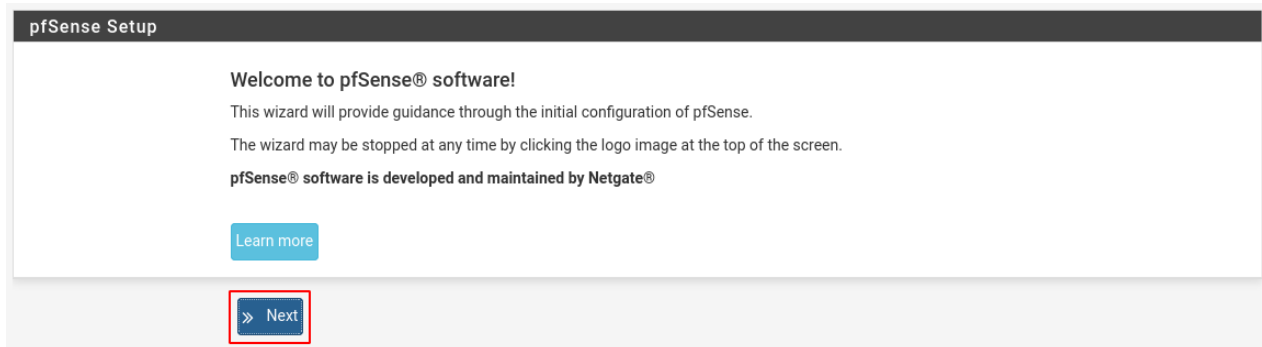
9 шагов мастера настройки pfSense

Запускаем браузер, переходим по адресу 192.168.1.1 — мы оказываемся в веб-интерфейсе pfSense. Вводим имя/пароль по умолчанию (`admin/pfsense`), запускается мастер настройки, состоящий из 9 шагов. При базовой настройке необходимо поменять только небольшое количество настроек.

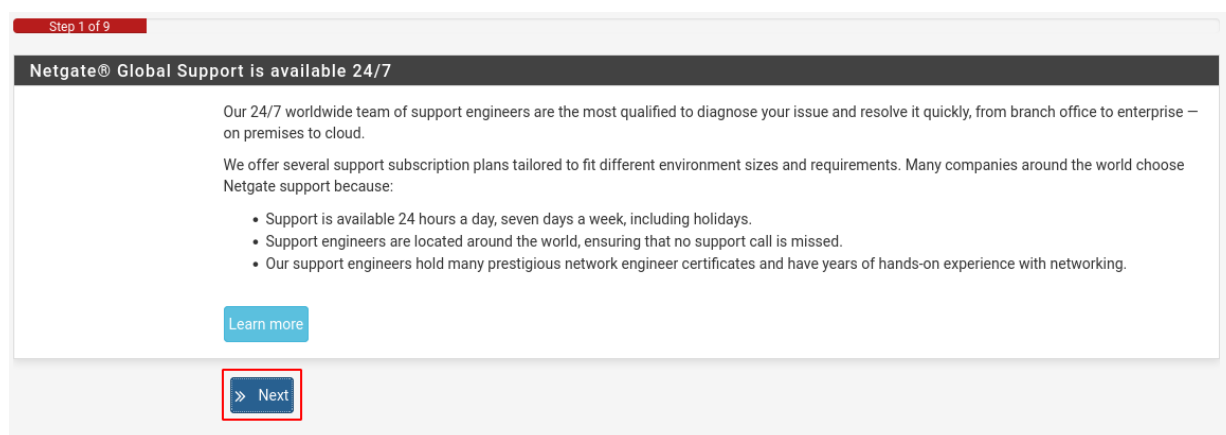
Баннер вверху напоминает о необходимости изменить пароль по умолчанию на свой. На 6-м шаге мастер настройки предложит поменять пароль, поэтому сейчас можно баннер проигнорировать.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Видим приветствие мастера настройки.



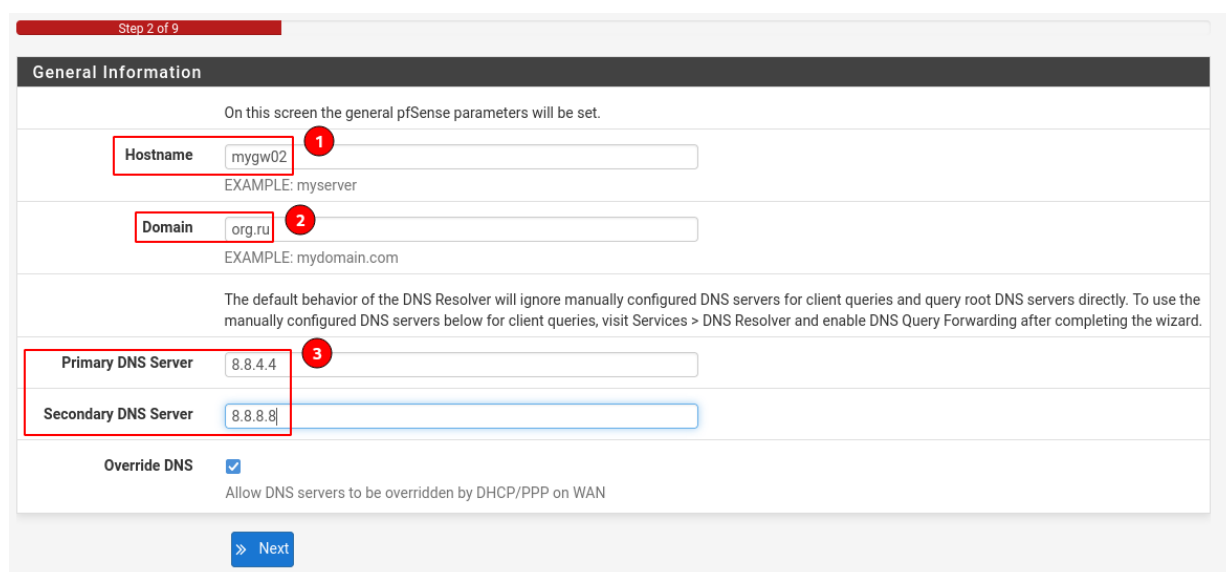
Шаг 1. Начало настройки



Шаг 2. Указание имени и домена шлюза

В мастере указываем имя и домен нашего шлюза (шаг 2, например, mygw02 & myorg.ru), DNS-серверы (напр., dns.google — 8.8.4.4 & 8.8.8.8).

Предостережение! В РФ планируют заблокировать DNS от Google, Cloudflare и DoH — учитывайте при настройке DNS.



Шаг 3. Настройка синхронизации времени

Настраиваем синхронизацию времени по NTP и часовой пояс: сервер можно оставить предложенный по умолчанию, либо выбрать по своим предпочтениям с подходящим **stratum** (достаточно и уровня 3).

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)

Шаг 4. Настройка PPPoE

На этом шаге, как правило, ничего менять не приходится. В дополнение к внешнему адресу указываем upstream gateway — вышестоящий (провайдерский) шлюз, если он не был задан ранее. Здесь же указываются настройки PPPoE, если их требует провайдер. Некоторые операторы требуют подключение только с конкретного MAC-адреса, его также можно указать на этом шаге.

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

MAC Address

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.

Шаг 5. Настройка внутреннего интерфейса

Относится к настройке внутреннего интерфейса. У нас он уже настроен, переходим к следующему шагу.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

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

Subnet Mask

[» Next](#)

Шаг 6. Пароль администратора

На этом шаге система потребует изменить пароль администратора:

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[» Next](#)

Проверка соответствия предыдущему (в том числе установленному по умолчанию) паролю не производится. Технически можно повторить, но из соображений безопасности следует установить стойкий пароль.

Шаг 7. Применение настроек

И затем предложит применить настройки.

Wizard / pfSense Setup / Reload configuration

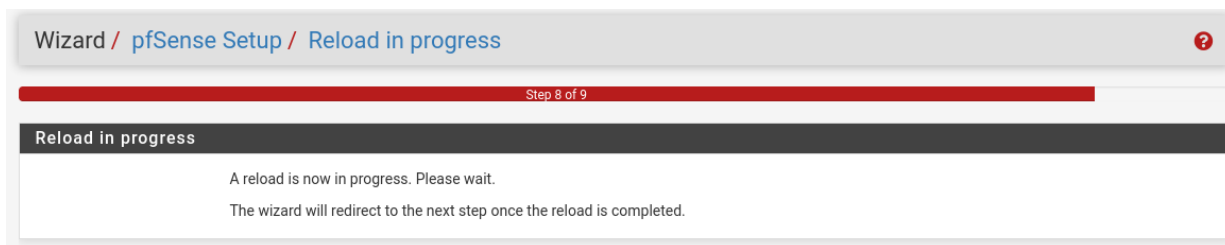
Step 7 of 9

Reload configuration

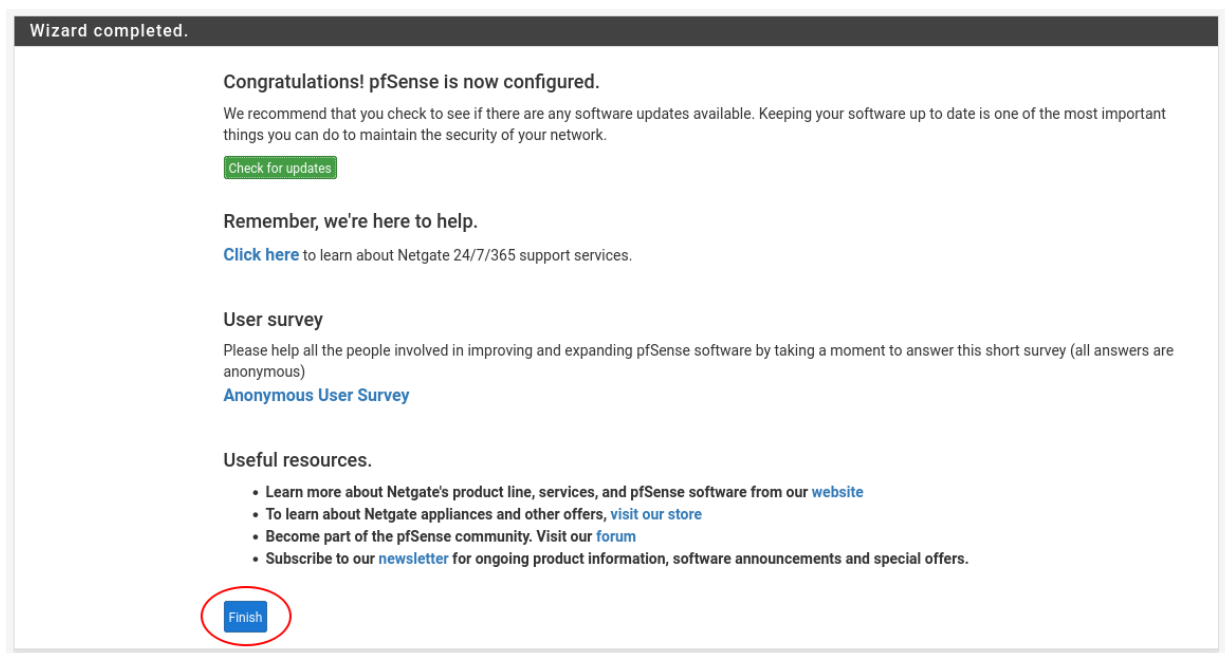
Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

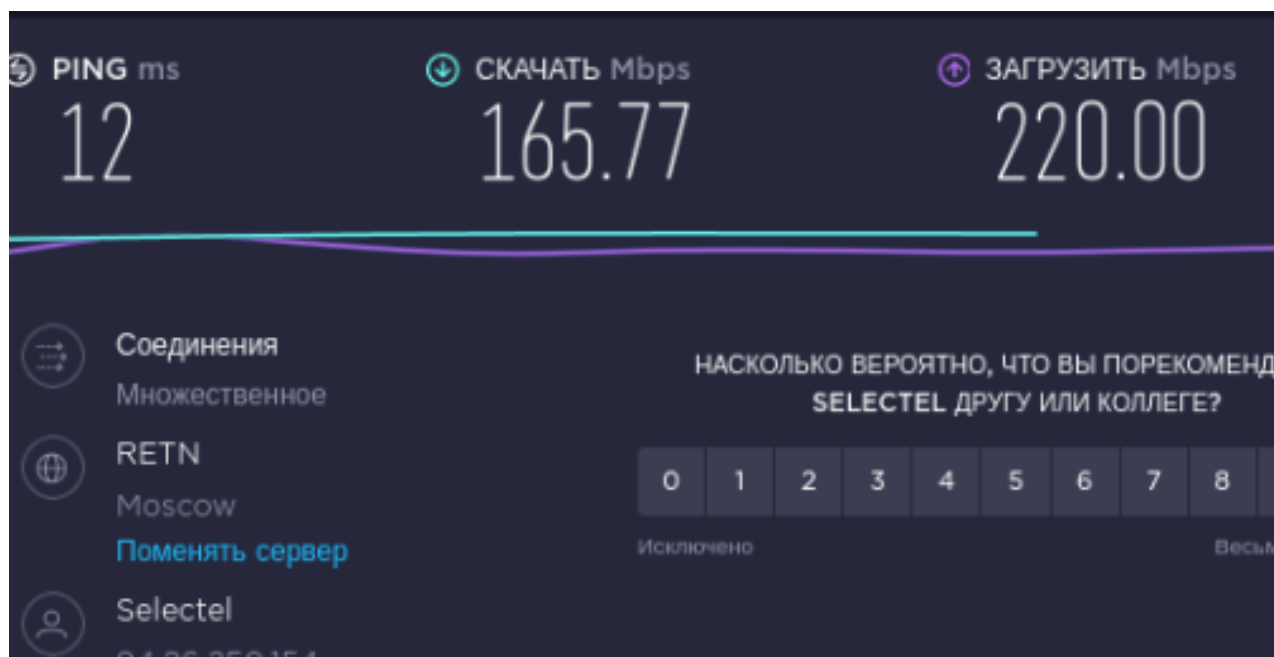
Шаг 8. Продолжение применения настроек



Шаг 9. Настройка завершена



Нажимаем кнопку Finish — мастер настройки успешно завершил работу. На этом этапе наш pfSense уже готов выполнять базовые функции интернет-шлюза — можем в браузере зайти в поисковик и запустить сетевой спидометр.



В дальнейшем (например, после сброса к заводским настройкам: **Diagnostics -> Factory Defaults**), мастер можно запустить из меню **System -> Setup Wizard**.

Интерфейс pfSense

При подключении к маршрутизатору первым делом отображается дашборд, который может выглядеть следующим образом:



Его отрисовка занимает некоторое время, экран открывается не мгновенно.

Дашборд гибко настраивается — можно добавлять новые элементы, удалять неиспользуемые, настраивать имеющиеся.

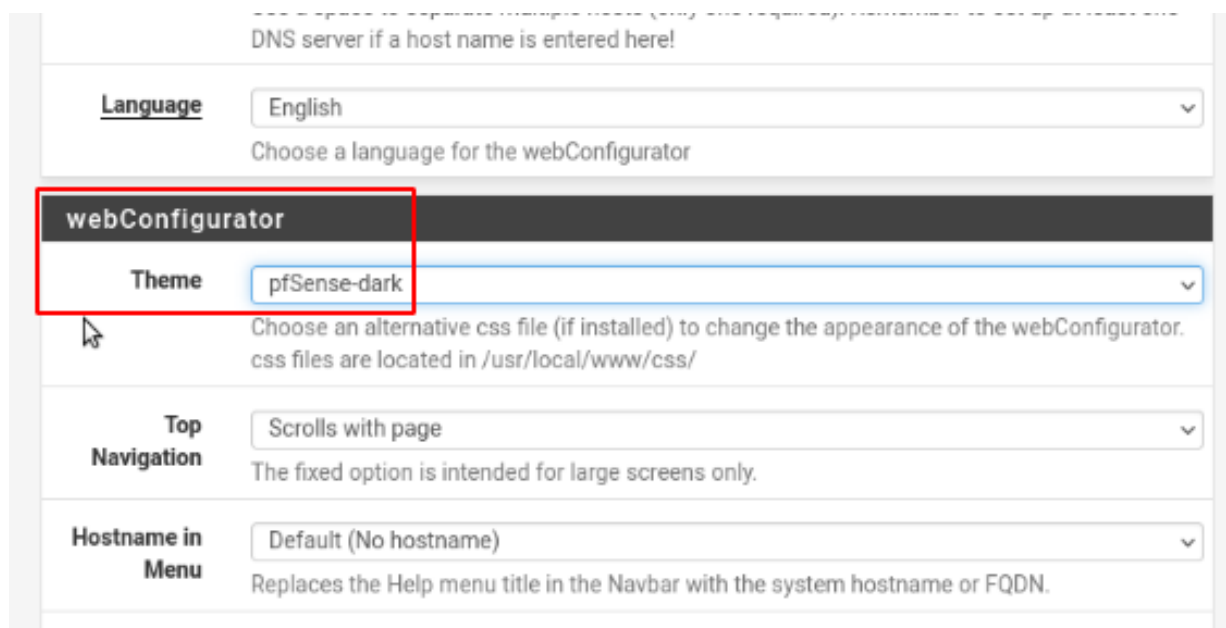
Структура меню

Функций pfSense выполняет множество, настройки сгруппированы:

- Кнопка с логотипом pfSense — переход на дашборд.
- System — общие системные настройки; управление маршрутизацией, сертификатами, обновлением; пакетный менеджер.
- Interfaces — маппинг и настройка интерфейсов.
- Firewall — файерволлинг — настройка NAT и правил брандмауэра; здесь же настраивается шейпинг.
- Services — дополнительные функции, запущенные отдельными демонами (DHCP Server/Relay, DNS; NTP, SNMP, etc), в т.ч. установленными из менеджера пакетов (Squid, Snort, Nagios (NRPE) и Zabbix агенты).
- VPN — настройки служб удаленного доступа (IPsec, L2TP, OpenVPN) вынесены сюда.
- Status — текущее состояние компонентов — счетчики, значения и состояние реального времени, а также графики мониторинга и системные журналы.
- Diagnostics — различные диагностические инструменты (архивация/восстановление, выключение/перезапуск, ping/traceroute/DNS lookup и много чего еще).
- Mygw02.myorg.ru — что-то вроде кнопки help/about.

Изменение темы

Многим нравятся «темные» темы, они есть в pfSense, меню **System -> General Setup**, раздел **webConfigurator**:



В статье будет чередоваться темная и светлая тема, используемая по умолчанию.

Локализация

Раздел **System -> General Setup**, секция **Localization**, параметр **Language**, позволяют переключать язык веб-интерфейса.

Пример интерфейса на русском языке:

Система
Интерфейсы
Межсетевой экран
Сервисы
VPN
Статус
Диагностика
Помощь

Статус / Приборная панель

Информация Системы

Имя

mygw02.org.ru

Пользователь

admin@192.168.1.2 (Local Database)

Система

KVM Guest
Идентификатор Устройства Netgate:
fdd668184930b7796df4

SMART

Производитель: SeaBIOS
Версия: 1.11.0-2.el7
Дата Релиза: Tue Apr 1 2014

Версия

2.5.2-RELEASE (amd64)
сделан Fri Jul 02 15:33:00 EDT 2021
FreeBSD 12.2-STABLE

Система работает на последней версии.
Информация о версии обновлена в Fri Dec 17 18:38:55 +05 2021

Тип Процессора

Intel Xeon Processor (Skylake)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No

Аппаратное шифрование

Ядро PTI

Включен

MDS Mitigation

Inactive

Аптайм

00 Hour 35 Minutes 53 Seconds

Статус NTP

Время Сервера

19:14:19 +05

Синхронизация Источника

212.13.97.58 (Страта 2)

Статистика Интерфейсов

	WAN	LAN
Входящие Пакеты	13504	2566
Исходящие Пакеты	13344	4445
Входящие Байты	9.37 MiB	325 KiB
Исходящие Байты	682 KiB	4.07 MiB
Входящие Ошибки	0	0
Исходящие Ошибки	0	0
Коллизии	0	0

Диагностика

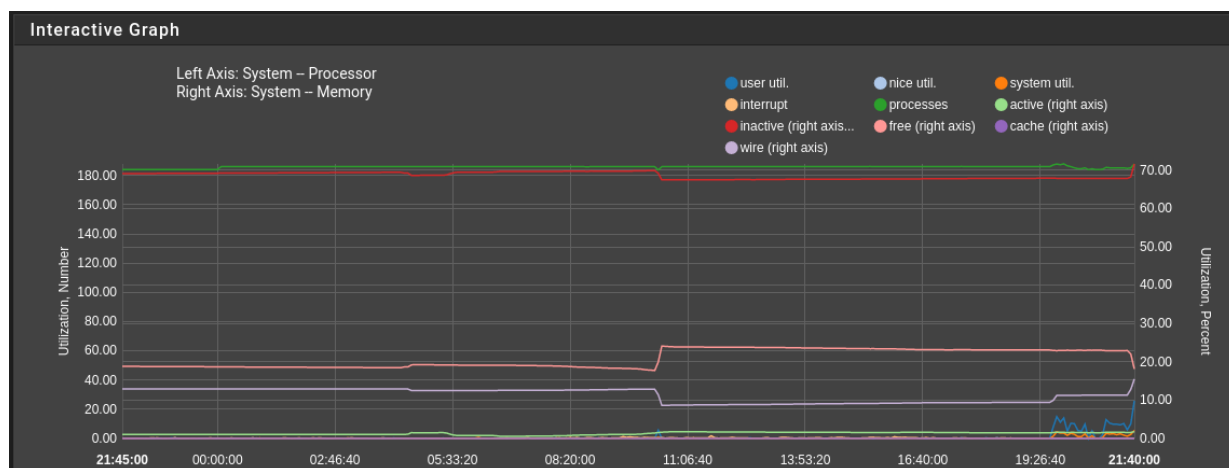
Первичная диагностика обычно начинается с анализа журналов работы системы и компонентов, после чего полезно проанализировать историческую загрузку системы на определенном интервале, например, в течение последних суток или часа.

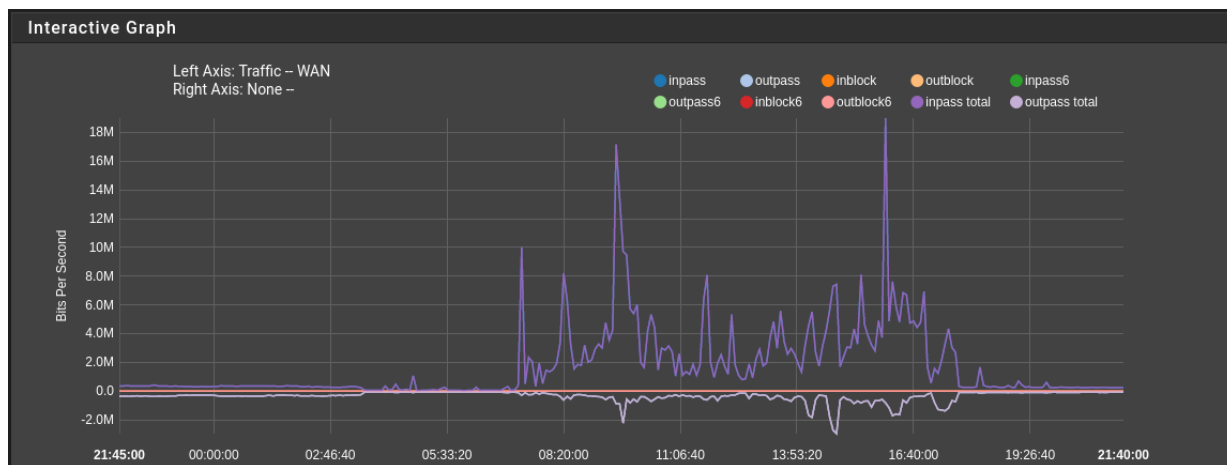
Системные журналы

Доступны на вкладке **Status -> System Logs**. Журналов много, но они разделены по категориям. В первую очередь будут интересны журналы **Status/System Logs/System/General** и **Status/System Logs/Firewall**.

Графики нагрузки

Оценить нагрузку на систему удобно в графическом виде в разделе **Status/Monitoring**.





Последующая диагностика заключается во внимательном анализе значений в счетчиках на вкладке «**Статусы**» и использовании диагностических инструментов на вкладке «**Диагностика**».

Сброс пароля

Если пароль от pfSense потерялся, в консоли его можно сбросить до значения по умолчанию в пункте 3 (Reset webConfigurator password):

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

Enter an option: 3

The webConfigurator admin password and privileges will be reset to the default (
which is "pfsense").
Do you want to proceed [y/n]?
```

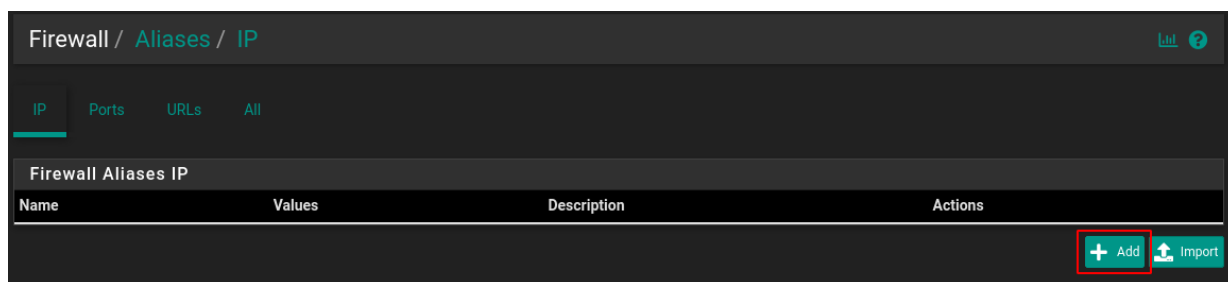
Расширенные настройки

Правила брандмауэра

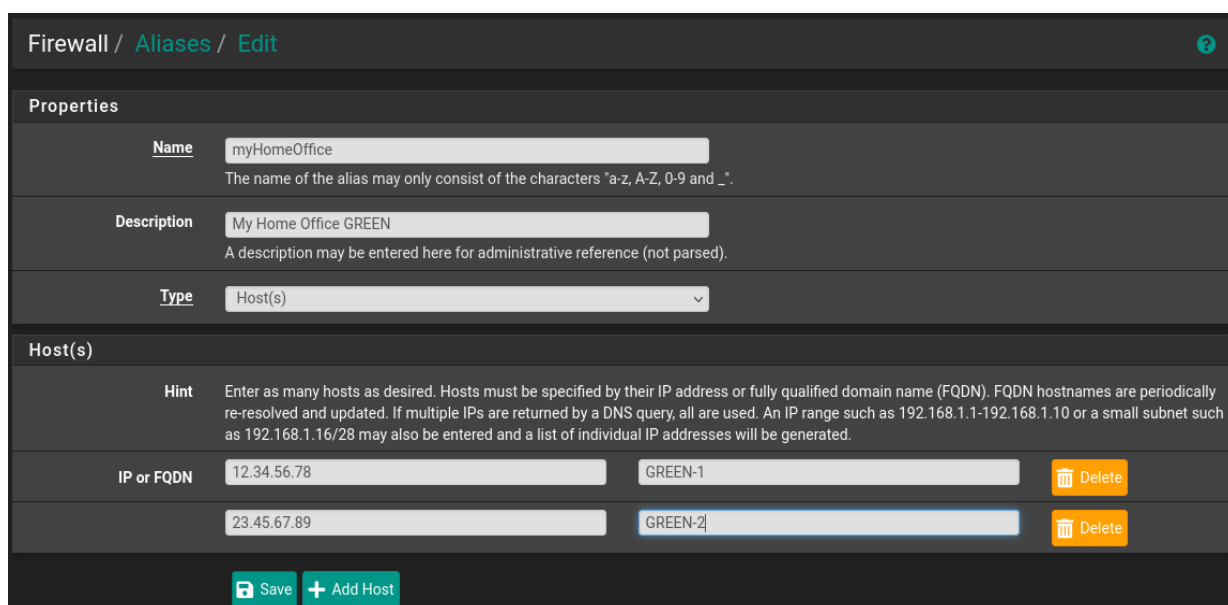
Настройки по умолчанию запрещают подключение к pfSense из глобальной сети и разрешают доступ клиентов наружу с использованием трансляции адресов NAT (точнее, наиболее частый вариант динамической NAT — NAPT по RFC 2663, она же NAT overload, маскардинг или PAT — здесь и далее будем говорить только об этом типе).

Для примера создадим разрешающее правило для подключения к pfSense из дома (правило задается на интерфейсе WAN), затем ограничим подключения пользователей только серфингом (правило задается на интерфейсе LAN).

В pfSense есть удобный механизм описания переменных через псевдонимы, создадим такой для нашего домашнего офиса и портов tcp:80/443, включим регистрацию пакетов. В пункте Aliases меню Firewall на вкладке IP, открывающейся по умолчанию, нажмем кнопку **+Add**:

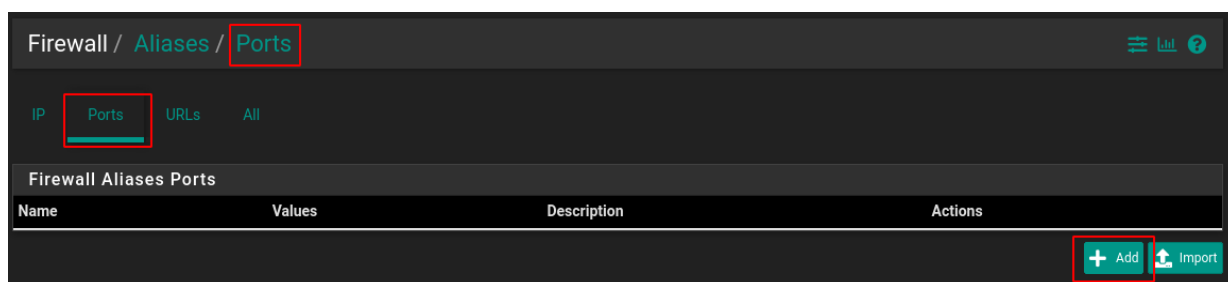


Откроется редактор псевдонимов для IP-адресов:



В редакторе присвоим имя псевдониму, укажем тип (Host(s)) и добавим IP-адреса.

На вкладке Ports аналогичным образом создаем правило для служб:



Указываем понятное имя, даем описание, добавляем один или несколько портов:

Properties

Name

mySerfing

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

HTTP(S)

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

Type

Port(s)

Port(s)

Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port

80

Description

443

Description

Delete

Delete

Save

+ Add Port

В подсказке указан удобный способ создания псевдонима для диапазона портов.

Для настройки того-то, переходим **Firewall/Rules/**.

Теперь при создании или редактировании существующих правил мы можем использовать псевдонимы. Это особенно удобно, когда какая-то настройка повторяется в нескольких правилах и иногда меняется.

В этом случае достаточно скорректировать только один псевдоним.

27/46

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

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

Protocol TCP
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Single host or alias myHomeOffice /
Display Advanced
 The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match any Destination Address /
Destination Port Range (other) mySerfing (other)
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs Settings](#) page).

Description Access to my pfSense GW from home
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

На примере выше для адреса источника и портов назначения мы выбрали заданные ранее псевдонимы.

После настройки не забываем нажимать **Apply Changes**. Теперь можно проверять подключение.

Аналогично на интерфейсе **LAN** создаем правило для серфинга:

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

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN net

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

(other)

mySerfing

(other)

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Allow only serfing

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

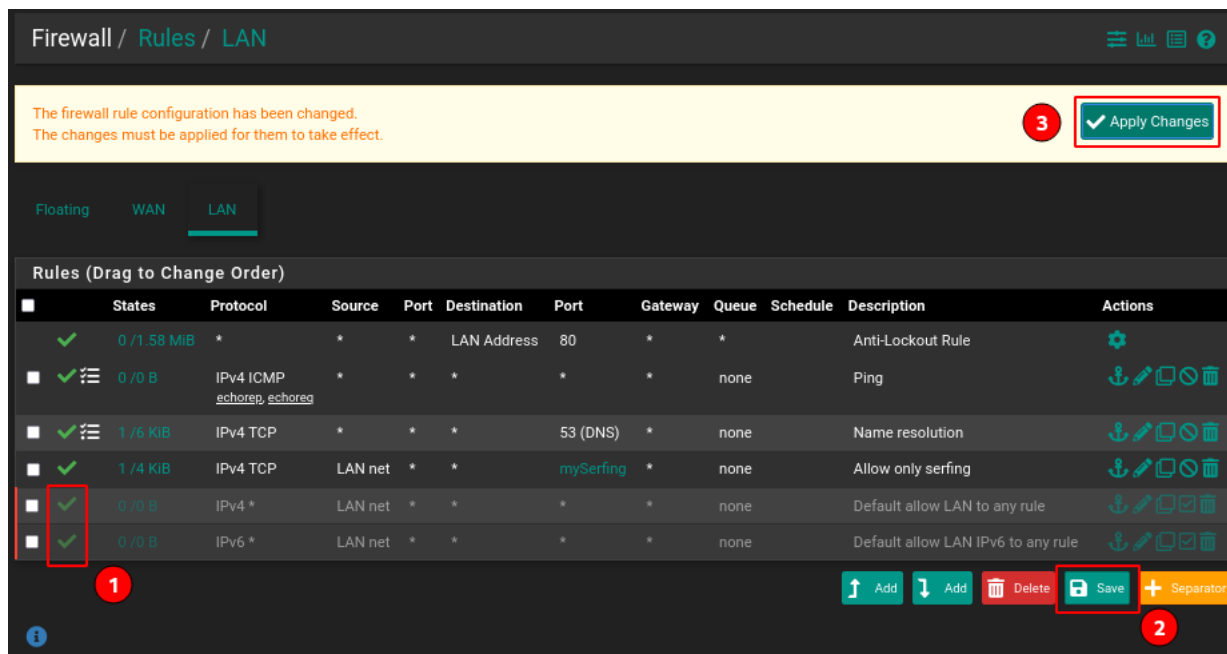
Advanced Options

Display Advanced

Далее на этом же интерфейсе создаем правила для DNS (udp:53) и (необязательно, облегчает диагностику) ICMP (достаточно echo request, echo reply).

Теперь отключаем правила по умолчанию, нажав на зеленую галочку(1), **Save** (2, если менялся порядок правил) и **Apply Changes** (3):

29/46



Проверяем доступ к web-сайтам, затем к нестандартным портам, используя ресурс portquiz.net:

Пинг работает, имена сайтов разрешаются, http по tcp/80 открыт, а на нестандартный порт tcp/8080 соединение не проходит:

```

myuser@clnt02 (192.168.1.3) - byobu
File Edit View Search Terminal Help
myuser@clnt02:~$ ping -c 2 ya.ru
PING ya.ru (87.250.250.242) 56(84) bytes of data.
64 bytes from ya.ru (87.250.250.242): icmp_seq=1 ttl=55 time=15.9 ms
64 bytes from ya.ru (87.250.250.242): icmp_seq=2 ttl=55 time=15.8 ms

--- ya.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 8048ms
rtt min/avg/max/mdev = 15.889/15.913/15.938/0.128 ms
myuser@clnt02:~$ telnet portquiz.net 80
Trying 52.47.209.216...
Connected to portquiz.net.
Escape character is '^]'.
^]
telnet> Connection closed
myuser@clnt02:~$ telnet portquiz.net 8080
Trying 52.47.209.216...
telnet: Unable to connect to remote host: Connection timed out

```

О чем также видим записи в журнале:

Status / System Logs / Firewall / Normal View

System

Firewall

DHCP

Authentication

IPsec

PPP

PPPoE/L2TP Server

OpenVPN

NTP

Packages

Settings

Normal View

Dynamic View

Summary View

Advanced Log Filter

192.168.

Source IP Address

Destination IP Address

Pass

Time

Block

Interface

Source Port

8080

Destination Port

Protocol

Protocol Flags

Quantity

500

Rule Tracker ID

Apply Filter

Regular expression reference Precede with exclamation (!) to exclude match.

7 Matched Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Sep 26 21:34:37	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:34:38	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:34:40	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:34:44	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:34:52	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:35:08	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S
✗	Sep 26 21:35:42	LAN	Default deny rule IPv4 (1000000103)	192.168.1.3:43278	52.47.209.216:8080	TCP:S

Таким образом мы решили поставленную задачу по организации доступа к веб-ресурсам и ограничению нежелательных ресурсов, работающих на других портах.

Трансляция портов

Частая задача — публикация какого-либо сервиса, размещенного в локальной сети — например, почтового или веб-сервера.

Тестовый веб-сервер

Тема не относится к pfSense, но в нашей лаборатории пока нет никакого ресурса для публикации, создадим его.

```
apt install apache2 php libapache2-mod-php
```

В каталоге /var/www/html создадим файл demo.php следующего содержания:

```
<?php
phpinfo();

?>
```

На этом создание тестового сервера завершено, осталось убедиться, что веб-сервер запущен:

```
systemctl status apache2
```

Настройка NAT на pfSense

Производится в меню в Firewall. Ранее мы использовали стандартный http-порт для удаленного подключения к pfSense, поэтому настройку трансляции продемонстрируем для другого порта (tcp:8080) и с заменой его номера.

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address / Address/mask
Type

Destination port range Other 8080 Other 8080
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host 192.168.1.3
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port HTTP
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

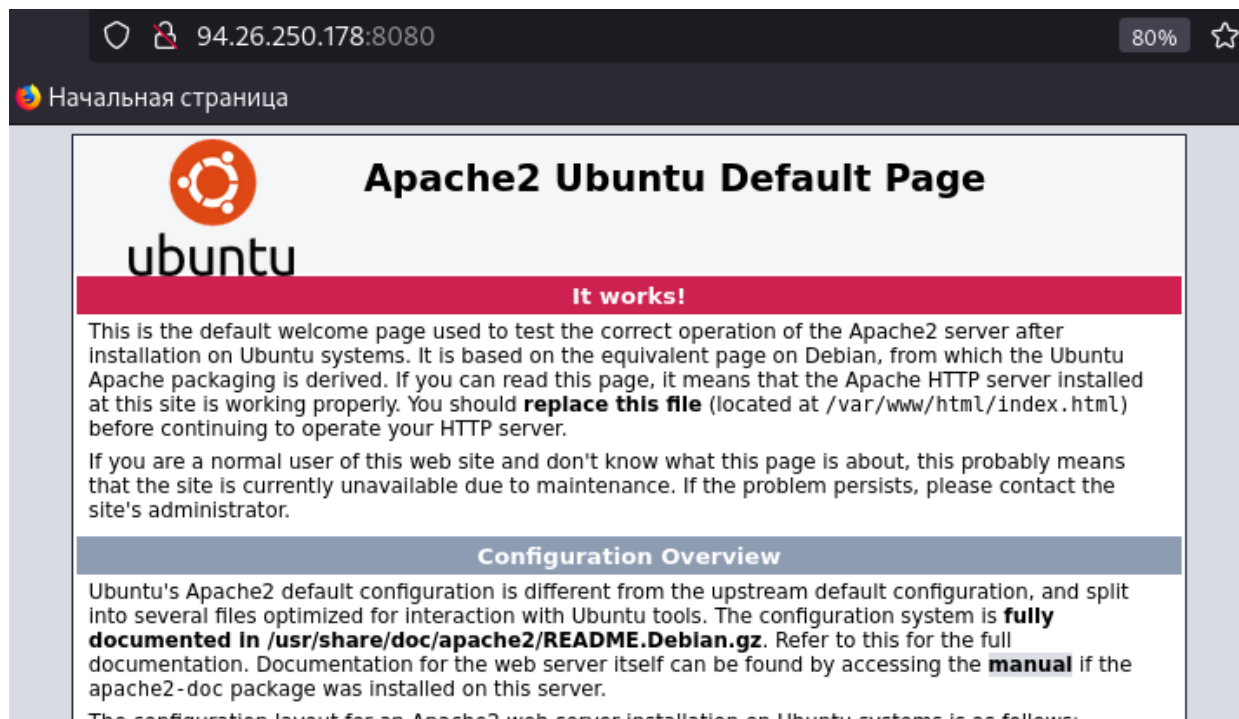
Description myWebSrv
A description may be entered here for administrative reference (not parsed).

Как видим, все настраивается очень просто. pfSense слушает TCP порт 8080 и транслирует его в tcp:80 тестового хоста 192.168.1.3, на котором мы в предыдущем шаге настроили веб-сервер.

Настоятельно рекомендуется составлять описание всех правил, так как со временем их может стать много и разобраться в них будет сложно.

Проверка

Проверяем наши настройки, зайдя на WAN-адрес pfSense с указанием порта 8080.



Внутренний веб-сервер ответил на публичном адресе. Добавляем название демо-странички и видим, что она также успешно опубликована.

94.26.250.178:8080/demo.php

80%

Начальная страница

PHP Version 7.2.24-0ubuntu0.18.04.9

System	Linux clnt02 4.15.0-156-generic #163-Ubuntu SMP Thu Aug 19 23:31:58 UTC 2021 x86_64
Build Date	Aug 16 2021 05:46:32
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysmsg.ini, /etc/php/7.2/apache2/conf.d/20-syssem.ini, /etc/php/7.2/apache2/conf.d/20-sysshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.2.24-0ubuntu0.18.04.9, Copyright (c) 1999-2018, by Zend Technologies

Обновление

pfSense разработан не только как многофункциональный комбайн, разработчики уделили большое внимание простоте работы с ним. Обновление выполняется легко — в разделе **System Information** на дашборде либо в меню **System -> Update**.

mygw02.myorg.ru - St x +

192.168.1.1

pfSense
COMMUNITY EDITION

Status / Dashboard

System Information

Name	mygw02.myorg.ru
User	admin@192.168.1.3 (Local Database)
System	KVM Guest Netgate Device ID: e228d3dc41cd149226f1
BIOS	Vendor: SeaBIOS Version: 1.10.2-1ubuntu1 Release Date: Tue Apr 1 2014
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 Sun Sep 26 10:08:55 +07 2021

System / Update / System Update

System Update Update Settings

Confirmation Required to update pfSense system.

Branch	Latest stable version (2.5.x)
Please select the branch from which to update the system firmware. Use of the development version is at your own risk!	
Current Base System	2.5.2
Latest Base System	2.5.2
Status	Up to date.

Наша система установлена из свежего дистрибутива, а значит уже актуальна, обновление не требуется. Обновления выходят примерно раз в полгода.

Если готовы к экспериментам, можно обновиться до экспериментальной ветки.

Так выглядит процедура обновления с предыдущей версии (2.4.5):

Please wait while the system update completes.
This may take several minutes. Do not leave or refresh the page!

[System Update](#)[Update Settings](#)

Updating System

```
[8/164] Fetching strongswan-5.9.2_1.txz: ..... done
[9/164] Fetching sshguard-2.4.1_1.txz: ..... done
[10/164] Fetching ssh_tunnel_shell-0.2_1.txz: ..... done
[11/164] Fetching sqlite3-3.35.5_1_1.txz: ..... done
[12/164] Fetching smartmontools-7.2_1.txz: ..... done
[13/164] Fetching scponly-4.8.20110526_4.txz: ... done
[14/164] Fetching rrdtool-1.7.2_4.txz: ..... done
[15/164] Fetching readline-8.1.1.txz: ..... done
[16/164] Fetching rate-0.9_2.txz: ..... done
[17/164] Fetching radvd-2.19_2.txz: ..... done
[18/164] Fetching qstats-0.2.txz: . done
[19/164] Fetching pftop-0.7_9.txz: ..... done
[20/164] Fetching pfSense-rc-2.5.2.txz: .. done
[21/164] Fetching pfSense-kernel-pfSense-2.5.2.txz: ..... done
[22/164] Fetching pfSense-default-config-2.5.2.txz: . done
[23/164] Fetching pfSense-base-2.5.2.txz: .
```

По окончании процесса система автоматически перезагрузится:

[System Update](#)[Update Settings](#)

Rebooting

Page will automatically reload in 78 seconds

Updating System

```
The following 1 package(s) will be affected (0/0 checked):

Installed packages to be UPGRADED:
  pfSense-kernel-pfSense: 2.4.5_1 -> 2.5.2 [pfSense-core]

Number of packages to be upgraded: 1

The process will require 14 MiB more space.
[1/1] Upgrading pfSense-kernel-pfSense from 2.4.5_1 to 2.5.2...
[1/1] Extracting pfSense-kernel-pfSense-2.5.2: ..... done
====> Keeping a copy of current kernel in /boot/kernel.old
>>> Removing unnecessary packages... done.
System is going to be upgraded. Rebooting in 10 seconds.
>>> Unlocking package pkg... done.
Success
```

После перезагрузки в консоли наблюдаем распаковку и установку обновленных пакетов:

```
[1/1] Extracting pkg-1.16.3: ..... done
You may need to manually remove /usr/local/etc/pkg.conf if it is no longer needed.
>>> Upgrading necessary core packages...
Checking for upgrades (2 candidates): .. done
Processing candidates (2 candidates): .. done
Checking integrity... done (0 conflicting)
The following 2 package(s) will be affected (of 0 checked):

Installed packages to be UPGRADED:
  pfSense-base: 2.4.5_1 -> 2.5.2 [pfSense-core]
  pfSense-default-config: 2.4.5_1 -> 2.5.2 [pfSense-core]

Number of packages to be upgraded: 2

The process will require 32 MiB more space.
[1/2] Upgrading pfSense-default-config from 2.4.5_1 to 2.5.2...
[1/2] Extracting pfSense-default-config-2.5.2: . done
[2/2] Upgrading pfSense-base from 2.4.5_1 to 2.5.2...
[2/2] Extracting pfSense-base-2.5.2: .. done
==> Keeping a copy of current versionmtree
==> Removing schg flag from base files
==> Extracting new base tarball
```

Виртуализация

pfSense отлично работает в виртуальной среде. Надо понимать, что возможно незначительное снижение производительности, но заметным оно будет только на маломощной физической машине, к которой предъявляются требования не столько по ЦПУ/ОЗУ, сколько по шине и сетевым интерфейсам.

При запуске в среде ESXi/vSphere от VMware полезно установить гостевого агента. Предоставляется эта возможность пакетом Open-VM-Tools, устанавливаемым через пакетный менеджер в штатном репозитории.

В виртуальной среде может возникнуть проблема с низкой производительностью и/или искажением пакетов. Это происходит из-за того, pfSense пытается использовать аппаратное ускорение сетевого адаптера.

В Xen и KVM делать это не имеет смысла, поэтому функцию hardware checksum offload, настройка которой доступна в меню **System**, пункт **Advanced**, вкладка **Networking**, следует отключить и затем перезагрузить pfSense.

System / Advanced / Networking

Admin Access
Firewall & NAT
Networking
Miscellaneous
System Tunables
Notifications

IPv6 Options

Allow IPv6
☒

All IPv6 traffic will be blocked by the firewall unless this box is checked
NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

IPv6 over IPv4 Tunneling

☐ Enable IPv6 over IPv4 tunneling
These options create an RFC 2893 compatible mechanism for IPv4 NAT encapsulation of IPv6 packets, that can be used to tunnel IPv6 packets over IPv4 routing infrastructures. IPv6 firewall rules are [also required](#), to control and pass encapsulated traffic.

Prefer IPv4 over IPv6

☐ Prefer to use IPv4 even if IPv6 is available
By default, if IPv6 is configured and a hostname resolves IPv6 and IPv4 addresses, IPv6 will be used. If this option is selected, IPv4 will be preferred over IPv6.

IPv6 DNS entry

☐ Do not generate local IPv6 DNS entries for LAN interfaces
If a LAN interface's IPv6 configuration is set to Track, and the tracked interface loses connectivity, it can cause connections to this firewall that were established via hostname to fail. This can happen unintentionally when accessing the firewall by hostname, since by default both IPv4 and IPv6 entries are added to the system's DNS. Enabling this option prevents those IPv6 records from being created.

DHCP6 DUID

Raw DUID: As stored in DUID file or seen in firewall logs

A DHCPv6 Unique Identifier (DUID) is used by the firewall when requesting an IPv6 address.

By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall.

If the firewall is configured to use a RAM disk for /var, the best practice is to store a DUID here; otherwise, the DUID will change on each reboot.

Raw DUID

Copy DUID

You may use the Copy DUID button to copy the system detected DUID shown in the placeholder.

Network Interfaces

Hardware Checksum Offloading

☒ Disable hardware checksum offload
Checking this option will disable hardware checksum offloading.
Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.

Hardware TCP Segmentation Offloading

☒ Disable hardware TCP segmentation offload
Checking this option will disable hardware TCP segmentation offloading (TSO, TSQ, TSQ6). This offloading is broken in some hardware drivers, and

Hardware Checksum Offloading также рекомендовано отключать для адаптеров Realtek.

Внутренняя маршрутизация

Если внутренняя сеть сегментирована, нужно научить pfSense маршрутам в нее. «Из коробки» доступна статическая маршрутизация, конфигурируемая в меню **System -> Routing**.

Сперва на вкладке **System -> Routing -> Gateways** создается внутренний шлюз(ы), например, myIntGW, затем маршрут добавляется на вкладке **System -> Routing -> Static Routes**:

System / Routing / Static Routes / Edit

Edit Route Entry

Destination network 192.168.16.0 / 22
Destination network for this static route

Gateway myIntGW - 192.168.1.10
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 Campus 16-0
A description may be entered here for administrative reference (not parsed).

После внесения настроек не забываем нажимать кнопку **Apply changes**.

Для сценария динамической маршрутизации потребуется установка дополнительного пакета, например, frr (Free Range Routing aka FRRouting aka FRR), в котором реализована поддержка многих протоколов: GP, OSPF, RIP, IS-IS, PIM, LDP, BFD, Babel, PBR, OpenFabric и VRRP.

После установки пакета в меню Services добавляются разделы для настройки протоколов, например, FRR-OSPF:

Services / FRR / OSPF / OSPF

OSPF Areas Interfaces Neighbors [Global Settings] [BFD] [BGP] [OSPF6] Status

General Options

Enable ☒ Enable OSPF Routing

Log Adjacency ☐ If set to yes, adjacency changes will be written via syslog.

Перед настройкой динамической маршрутизации в Global Settings нужно включить FRR и задать обязательный мастер-пароль:

Services / FRR / Global Settings ?

Global Settings Access Lists Prefix Lists Route Maps Raw Config [BFD] [BGP] [OSPF]

[OSPF6] Status

General Options

Enable ☒ Enable FRR

Default Router ID

Specify the default Router ID. RID is the highest logical (loopback) IP address configured on a router.
For more information on router identifiers see [wikipedia](#).
Per-daemon configuration will take precedence over this setting.

Master Password

Password to access the management daemons. Required.

SSL

В пункте **Advanced** меню **System** производится переключение интерфейса управления между HTTP и HTTPS.

System / Advanced / Admin Access ?

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol ☐ HTTP ☒ HTTPS (SSL/TLS)

SSL/TLS Certificate

Certificates known to be incompatible with use for HTTPS are not included in this list.

TCP port

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

При установке генерируется самоподписанный сертификат на 13 месяцев.

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6148a771a77b2) Server Certificate CA: No Server: Yes	self-signed	<div> <div>O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6148a771a77b2</div> <div> <div>Serial: 4318047457030023770</div> <div>Signature Digest: RSA-SHA256</div> <div>SAN: DNS:pfSense-6148a771a77b2</div> <div>KU: Digital Signature, Key Encipherment</div> <div>EKU: TLS Web Server Authentication, TLS Web Client Authentication, IP Security</div> <div>IKE Intermediate</div> <div>Key Type: RSA</div> <div>Key Size: 2048</div> <div>DN: /O=pfSense webConfigurator Self-Signed Certificate/CN=pfSense-6148a771a77b2</div> <div>Hash: 26cc661b</div> <div>Subject Key ID: 91:AD:EF:96:17:B9:C7:78:62:A2:FF:6D:65:3B:9E:54:4E:48:F4:FC</div> <div>Authority Key ID: keyid:91:AD:EF:96:17:B9:C7:78:62:A2:FF:6D:65:3B:9E:54:4E:48:F4:FC</div> <div>DirName:/O=pfSense webConfigurator Self-Signed Certificate/CN=pfSense-6148a771a77b2</div> <div>serial:3B:EC:C9:48:BF:8D:AA:5A</div> </div> <div> <div>Total Lifetime: 398 days</div> <div>Lifetime Remaining: 388 days until expiration</div> </div> </div>	webConfigurator	

Valid From: Mon, 20 Sep 2021 22:23:29 +0700

Valid Until: Sun, 23 Oct 2022 22:23:29 +0700

В этом же меню кнопка **Add/Sign** позволяет сформировать запрос к корпоративному центру сертификации и затем установить полученный сертификат, либо перевыпустить самоподписанный сертификат на другой срок.

Обычно интерфейс pfSense оставляют доступным только из внутренней сети, не разрешая прямой доступ извне. Если по какой-то причине потребуется сделать наоборот, для LAN-интерфейса нужно будет отключить правило антиблокировки — **Anti-lockout rule**, расположенное в **System/Advanced/Admin Access/webConfigurator**.

Для подключения из глобальной сети потребуется ранее созданное правило на WAN-интерфейсе. Также удобно использовать сертификат, выпущенный публично доверенным центром сертификации, например, Let's encrypt. Так как срок действия такого сертификата только 90 дней, его нужно будет часто обновлять.

Для автоматизации перевыпуска в репозитории есть пакет асме:

Services / Acme / Certificate options: Edit

General settings Certificates **Account keys**

Edit Certificate options

Name myCert

Description

ACME Server Let's Encrypt Production ACME v2 (Applies rate limits to certificate r v
 The ACME server which will be used to issue certificates using this key.
 Use testing servers until certificate validation works, then switch to production.
 Let's Encrypt ACMEv1 servers no longer allow new registrations, and in June 2021 they will be completely disabled.

E-Mail Address myuser@mymailserver.ru
 The e-mail address to register for this key. This is used by Let's Encrypt to send automated certificate expiration notices.

Account key
 -----BEGIN RSA PRIVATE KEY-----
 MIIJKAIBAAKCAgEA1VGcpgg+fH8HRwHPJRwd/+s1Tuommd9ru4
 /z9MRXAMcnJax5LeIqebq7Ii1S10gqRUyCDikfqn+XQFJDfij
 vsjooC4zKq0s4N215qwu64Ds0dYfP3F0HQJxwj8TQV5rBs+Pyb
 LsHpJy/DnyGmErmsMFAP3KbywuFCA4dosMTsYhgI1idcsaA6QN

✓ Create new account key

ACME account registration Register ACME account key
 Before using an accountkey, it must first be registered with the chosen ACME Server.
 ✓ indicates a successful registration, ✗ indicates a failure.
 In the case of a failure, check /tmp/acme/_registerkey/acme_issuecert.log for more information.

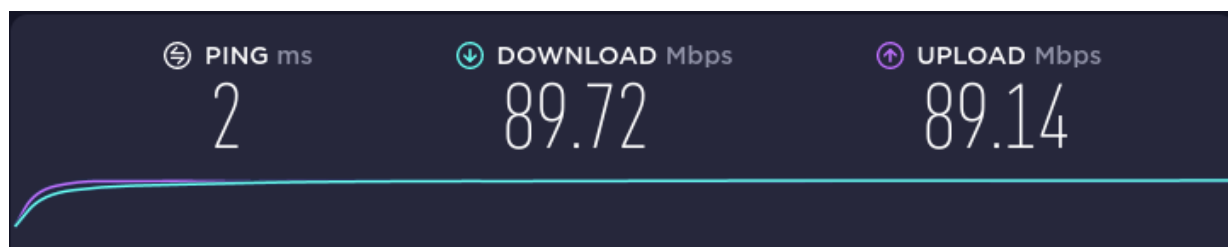
Save

Ограничение полосы

Часто в организации бывают пользователи, которым приходится разрешать неограниченные подключения к интернет-ресурсам. Это чревато забиванием всего канала и затруднением в работе остальных пользователей и сервисов. На помощь придет ограничение ширины канала. Шейпер имеет множество настроек, рассмотрим один из частых сценариев его использования.

Управляется в разделе **Firewall > Traffic Shaper** на вкладке **Limiters**.

Измерим текущую скорость.



Как указано выше, заходим в пункт Traffic Shapers меню Firewall, переходим на вкладку Limiters и создаем 2 ограничителя.

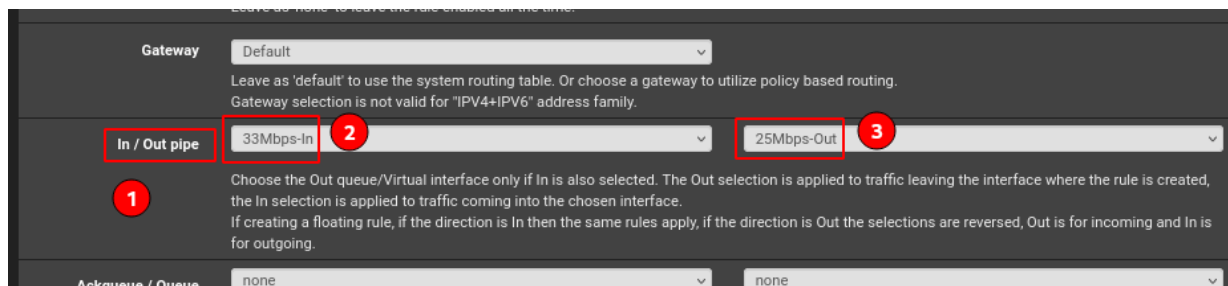
Включаем правило (1), присваиваем понятное имя (2), указываем ширину полосы (3). Для входящего и исходящего ограничения создаются отдельные правила (4).

Непосредственное включение шейпера выполняется в правилах брандмауэра (**Firewall** → **Rules**). Так как нас интересует ограничение со стороны наших внутренних клиентов, правила необходимо модифицировать/добавлять для интерфейса LAN. При этом лимиты рассматриваются со стороны интерфейса: **In** — входящий, **Out** — исходящий из интерфейса трафик. Таким образом, для ограничения трафика от клиента наружу используется правило **In**.

Таким образом, открываем пункт **Rules** меню **Firewall**, переходим на вкладку **LAN** и в секции **Extra Options** нужного (вновь созданного или существующего) правила включаем отображение расширенных настроек (кнопка **Display Advanced**):

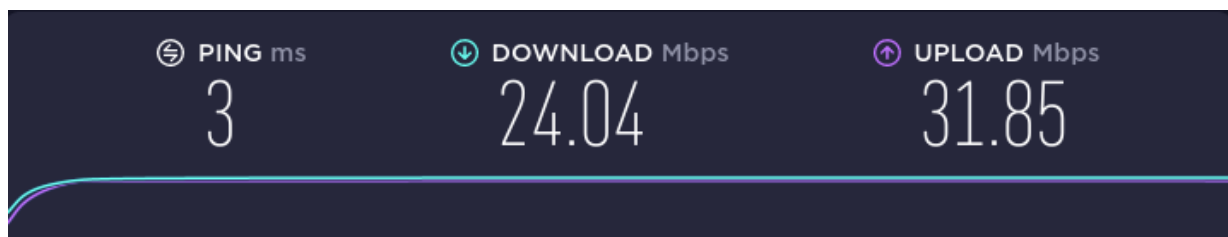
Примечание: в примере на картинке выше использовано существующее правило, разрешающее внутренним клиентам использовать подключение по https.

В предпоследней секции расширенных настроек (1, In/Out pipe) указываем правило для входящего в интерфейс (2) и исходящего из него трафика (3).



После сохранения и применения настроек pfSense сообщает о фоновой перезагрузке правил фильтрации и предлагает проверить статус на странице **Status/Filter Reload**.

После обновления правил выполним повторную проверку скорости.



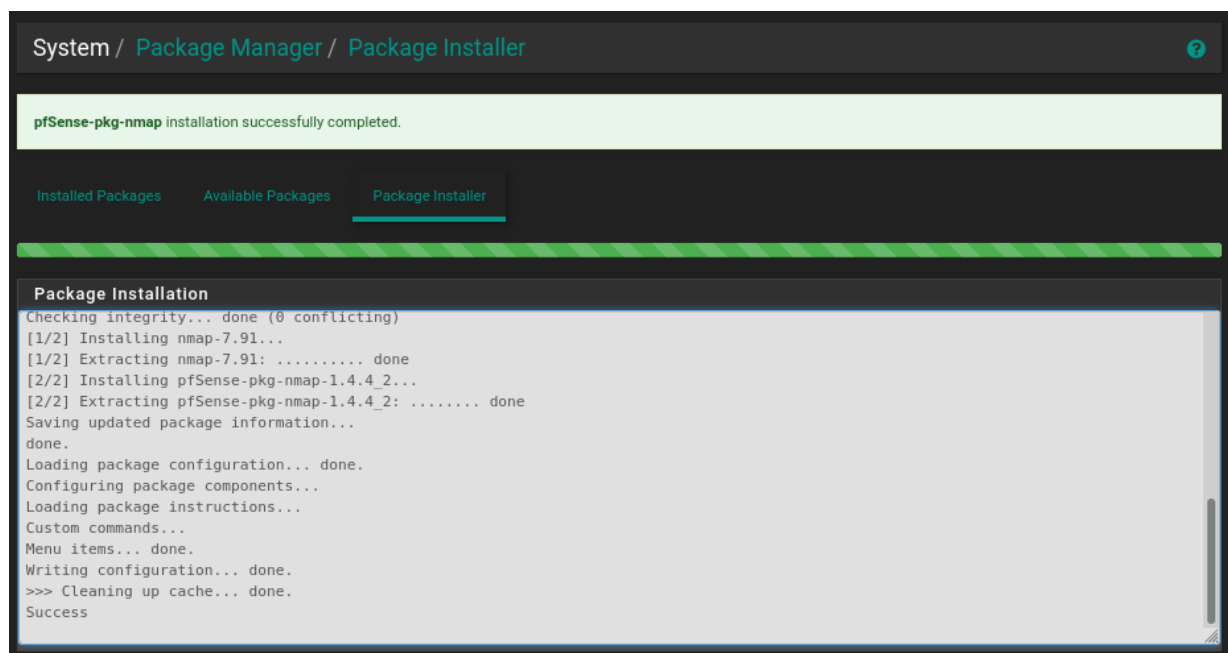
Дополнительные функции

Функциональность pfSense расширяется большим количеством пакетов, доступных через пакетный менеджер, их несколько десятков, вот лишь некоторые:

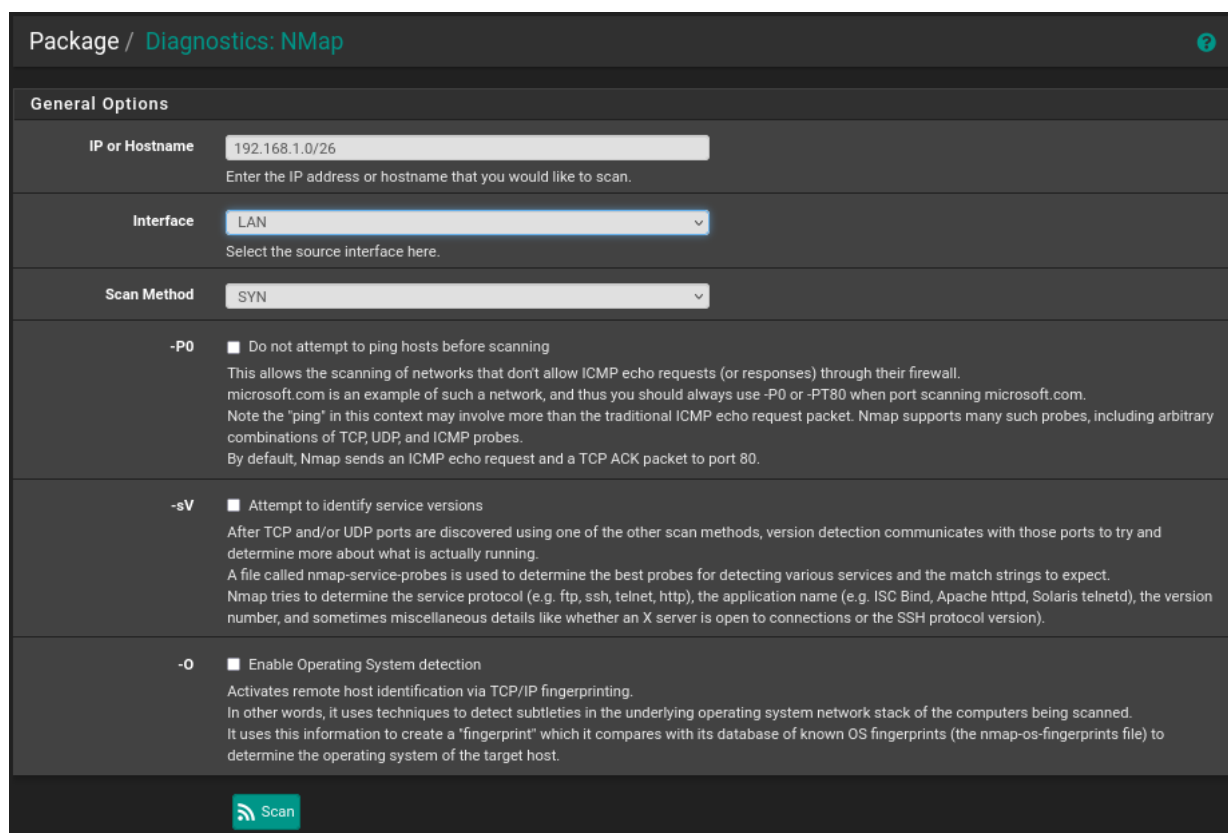
- arpsupsd — демон для связи с ИБП APC (ныне Schneider);
- arpwatch — мониторинг активности MAC/IP-адресов;
- cron — планировщик;
- filer — файловый менеджер;
- squid/lightsquid/squidGuard — прокси, генератор отчетов и фильтр;
- lldpd — предоставляет поддержку обнаружения по Link Layer Discovery Protocol, кроме того поддерживает проприетарные CDP, EDP, FDP, NDP;
- mailreport — рассылка отчета по почте;
- net-snmp — GUI для SNMP;
- nmap — nmap, классика сканирования сетей;
- snort/suricata/zeek — решения класса IDS/IPS.

Необходимо понимать, что за использование этих функций нужно заплатить повышением производительности оборудования. Интенсивное использование VPN может потребовать дополнительно одно или более ядер ЦПУ, а IDS/IPS также потребует дополнительно 1-2 ГиБ ОЗУ.

Проведем демонстрацию расширения функциональности на популярном сканере nmap. В меню **System** заходим в пункт **Package Manager**, вкладка **Available Packages**, рядом с пакетом NMap нажимаем на кнопку **Install**, ждем и получаем встроенный сканер:



В меню **Diagnostics** добавился пункт **NMap**, запускаем:



Во внутреннем сегменте нашей лаборатории только один хост, он был успешно обнаружен и просканирован:

```
Running: /usr/local/bin/nmap -sS -e vtnet1 '192.168.1.0/26'
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 21:51 +07
Nmap scan report for 192.168.1.3
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: FA:16:3E:2F:C0:99 (Unknown)

Nmap done: 64 IP addresses (1 host up) scanned in 2.62 seconds
```

[Back to NMap](#)

Заключение

В статье мы познакомились с решением для реализации производительного, надежного и функционального программного маршрутизатора — pfSense. Научились его устанавливать, настраивать, ограничивать скорости, добавлять новые функции, устанавливая пакеты расширения.

[Облачные серверы](#)[Сетевые технологии](#)