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

Продемонстрируем 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.

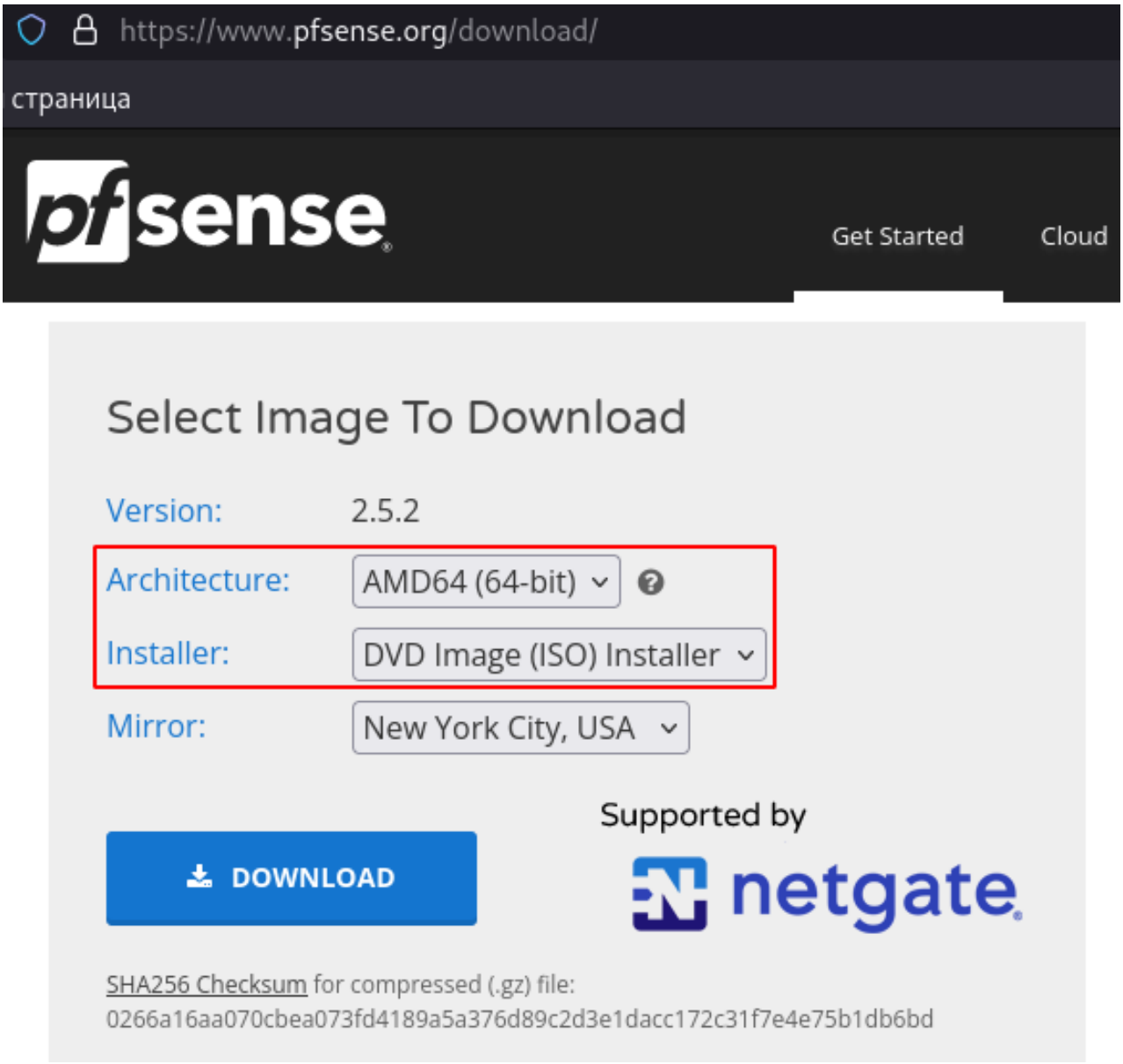
По состоянию на август 2021 года:

- 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)*.

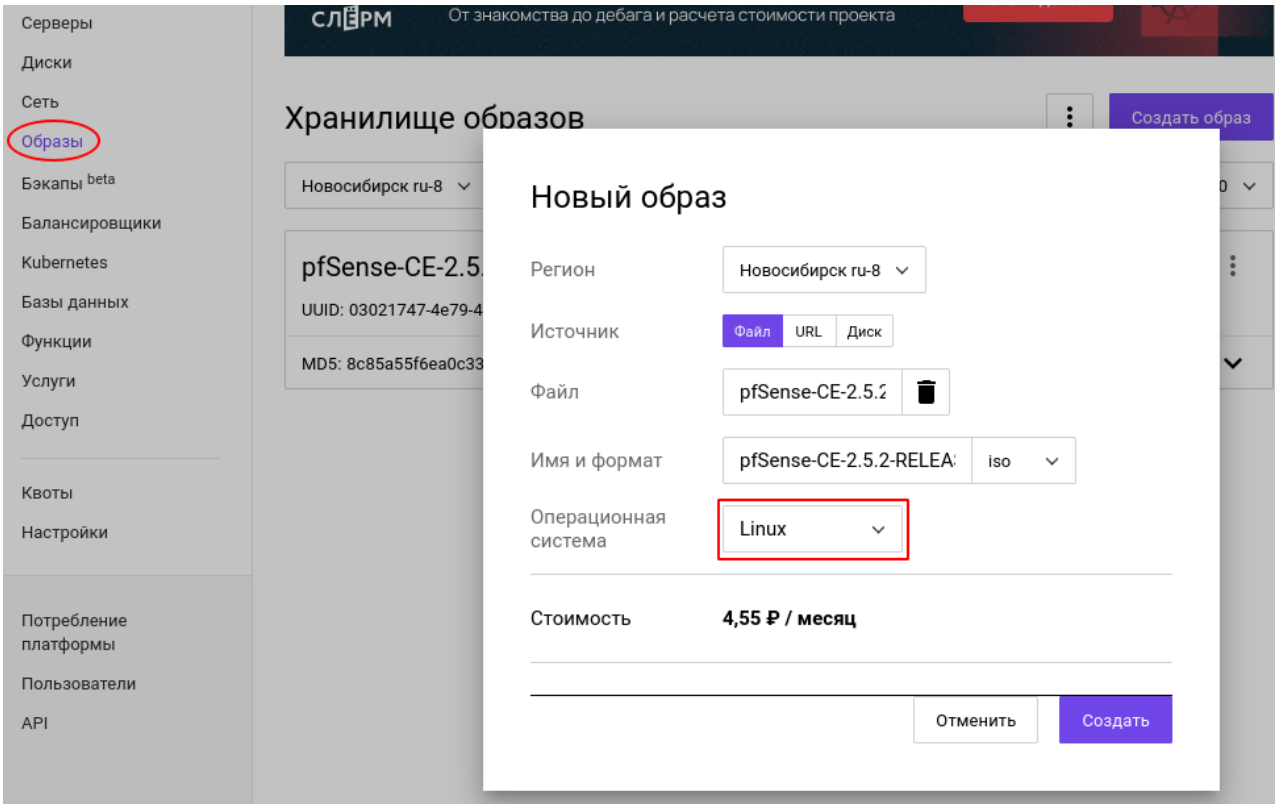


Выполняем проверку целостности загруженного архива и распаковываем его:

```
    $ 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
```

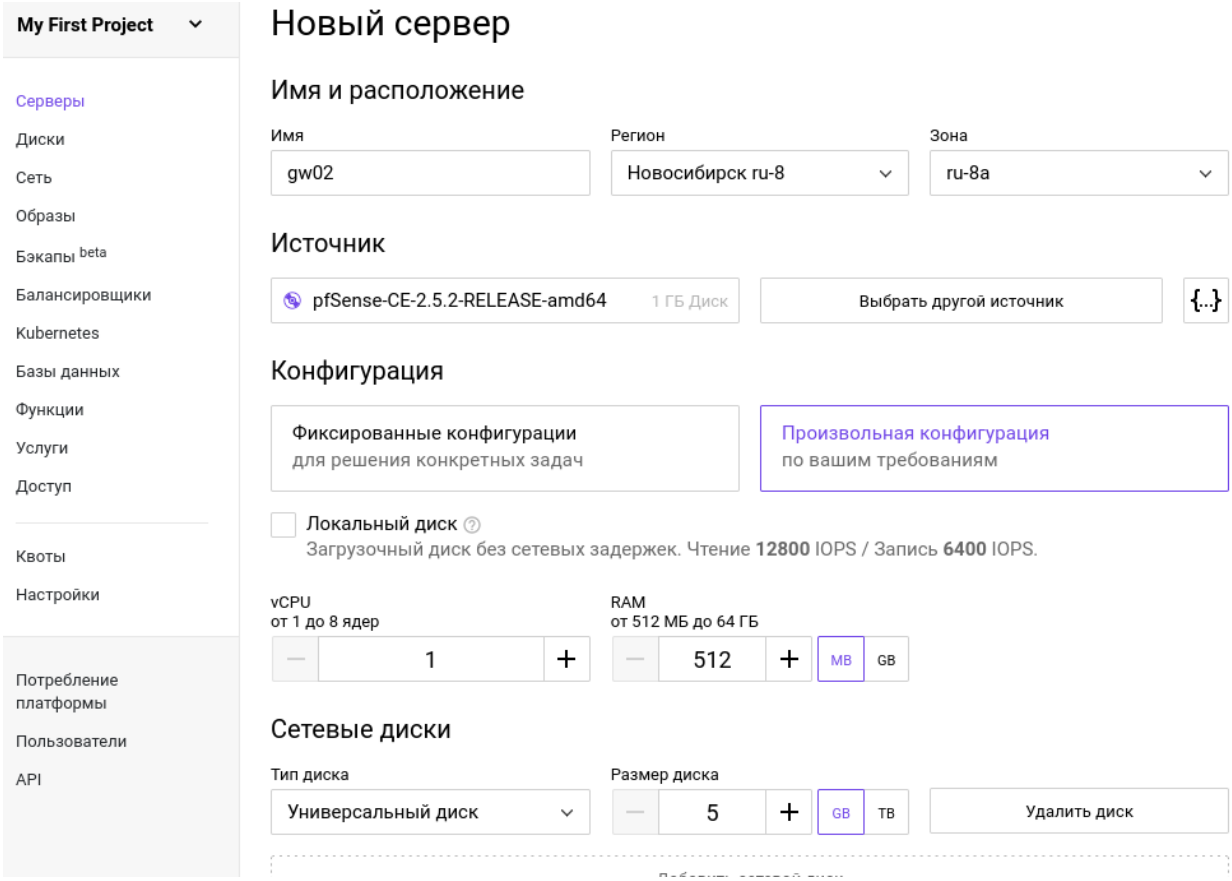
Значение контрольной суммы sha256 ***0266a16aa070cbea073fd4189a5a376d89c2d3e1dacc172c31f7e4e75b1db6bd*** *смотрим на странице загрузки. В примере указана для актуальной на момент написания версии 2.5.2.*

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

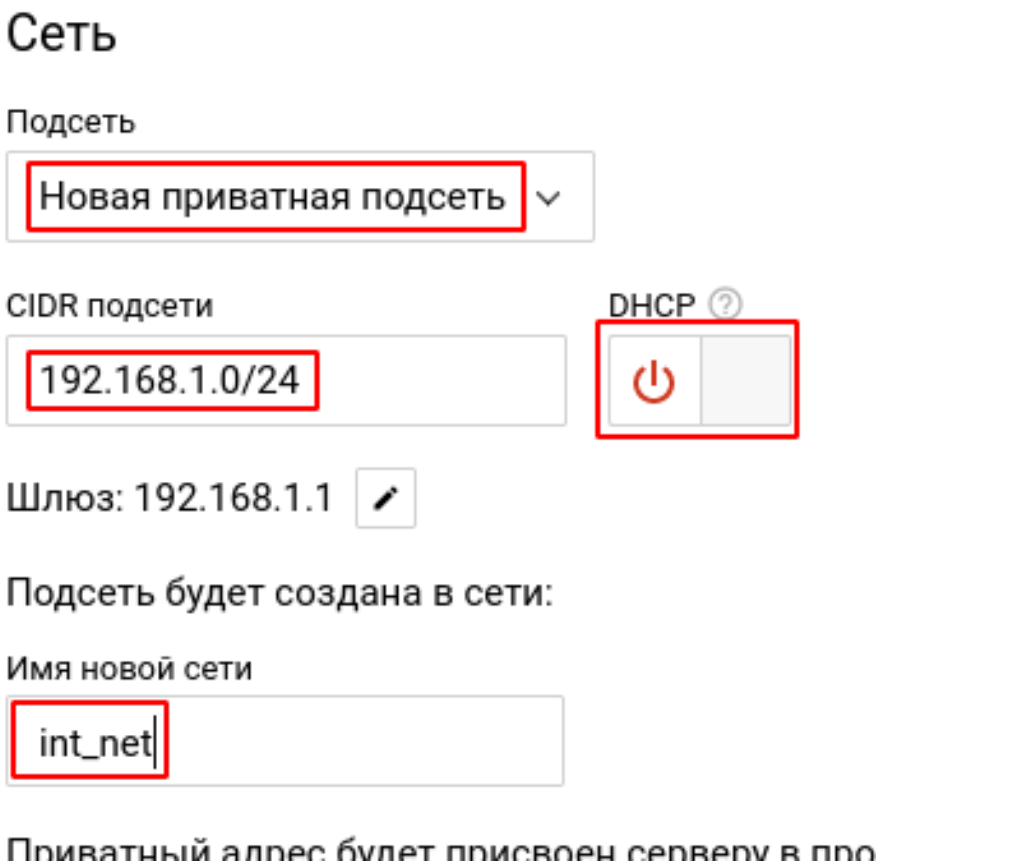


Установка и первоначальная настройка pfSense

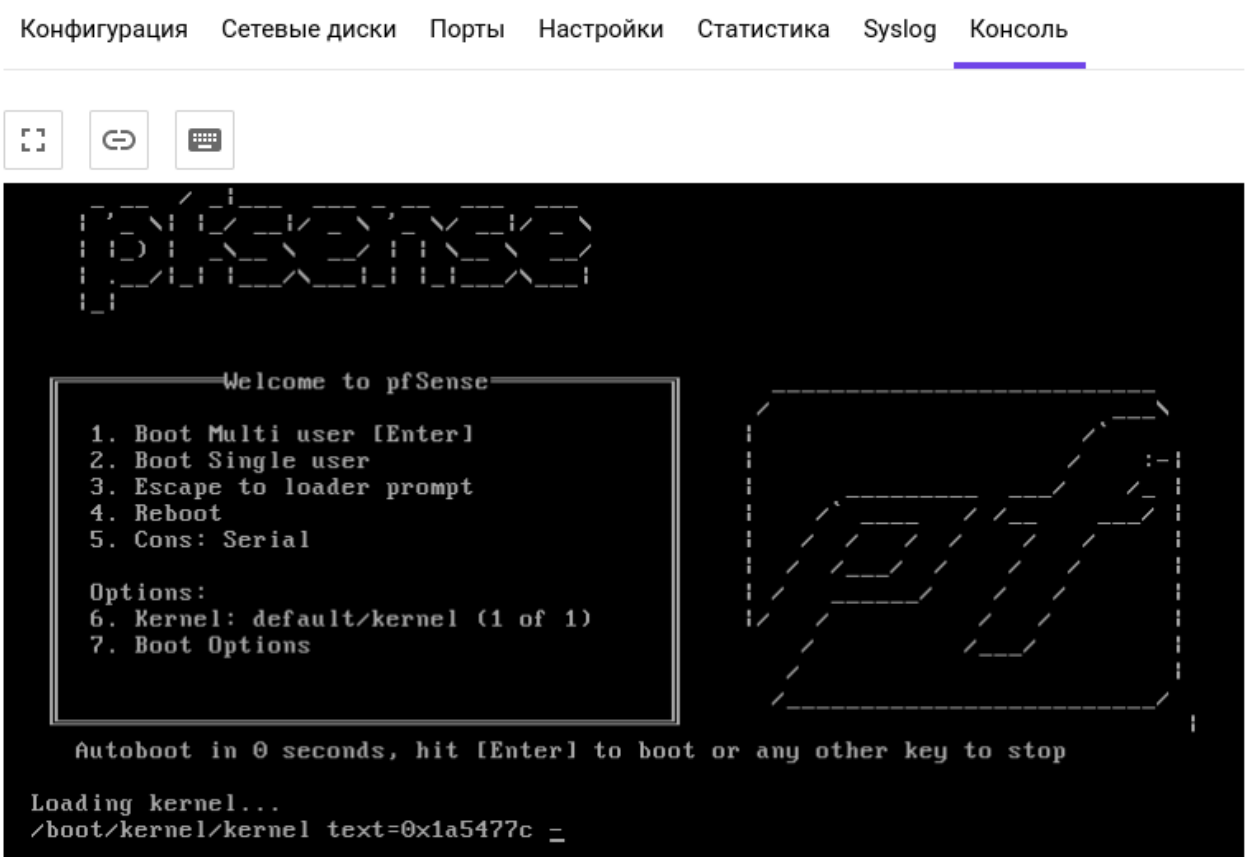
В разделе серверы «**Облачной платформы**» нажимаем кнопку «**Создать сервер**» вверху справа (или в центре, если это 1-й). Выбираем минимальную произвольную конфигурацию (1 vCPU/512 МиБ RAM/5 ГиБ Storage, 17,82 ₽/день по состоянию на август 2021) — в тестовых целях этого достаточно, для остальных случаев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



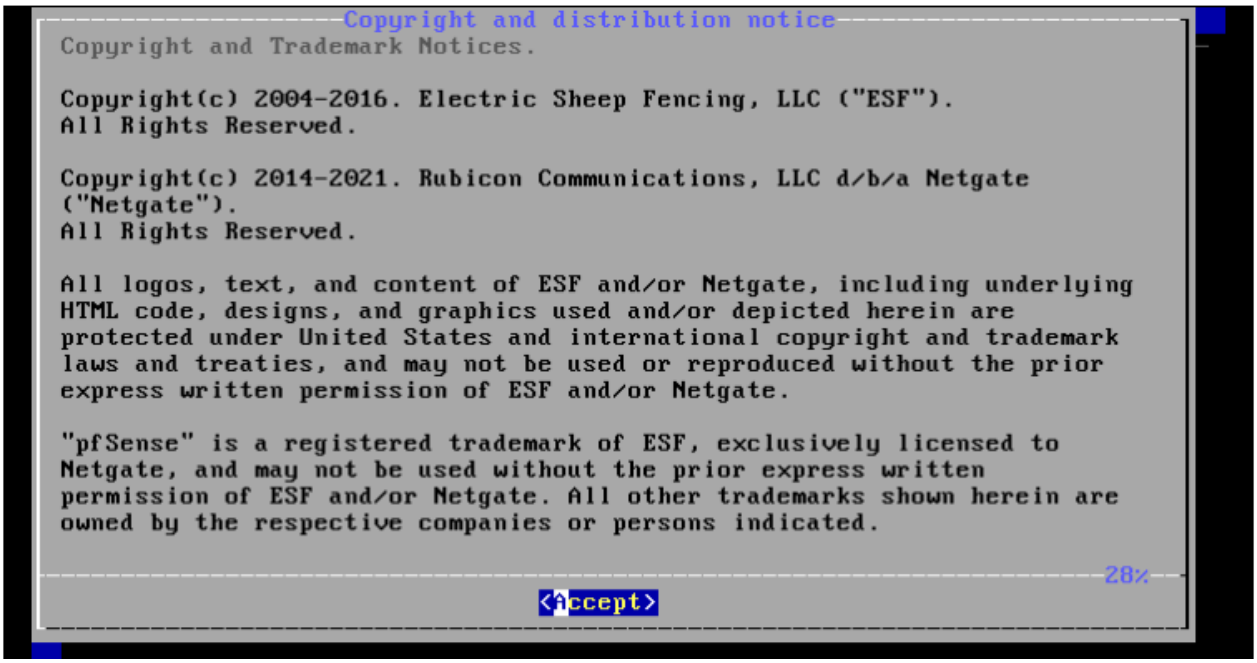
Сеть на данном этапе оставляем как «**Новая приватная сеть**» — она будет у нас внутренней, адрес 192.168.1.0/24. Присвоим имя i**nt_net**, DHCP — выключим. Настройка шлюза в данном случае ни на что не влияет, но убрать его невозможно.



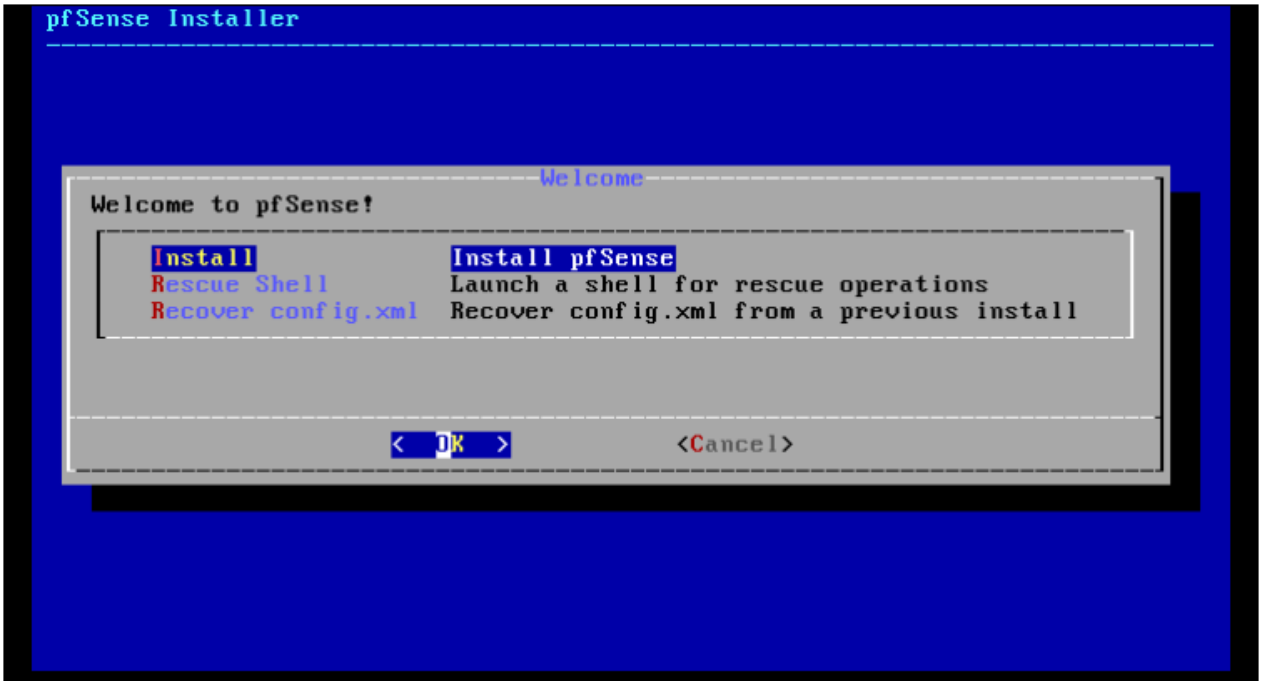
После указания необходимых параметров нажимаем кнопку «**Создать**». Сервер конфигурируется и будет доступен через 30 секунд. Если вы случайно закрыли вкладку, где создавалась машина — не проблема, теперь сервер доступен в глобальном разделе «**Серверы**». Для взаимодействия с консолью сервера мы переходим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



Читаем и соглашаемся с авторскими правами.

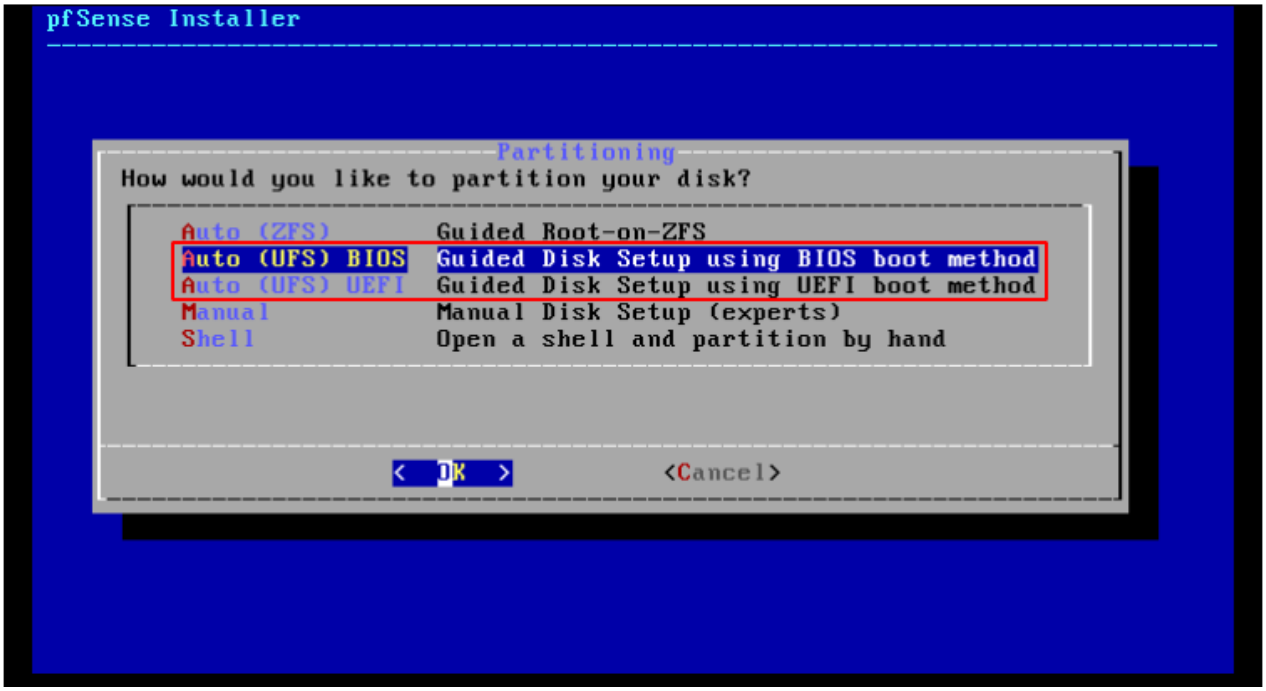


Выбор режима установки. На этом же этапе работы установщика можно задействовать и встроенный режим восстановления.

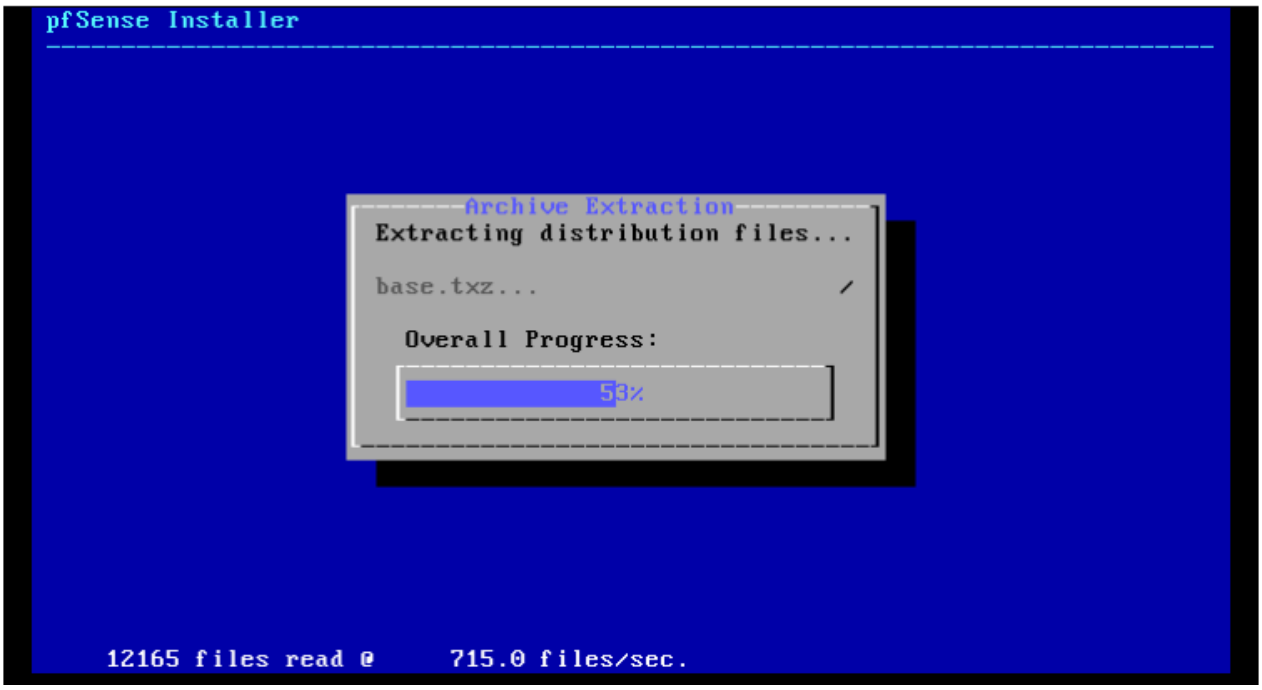


Консоль системы не будет видна рядовым пользователям, нет смысла менять локализацию — оставляем по умолчанию.

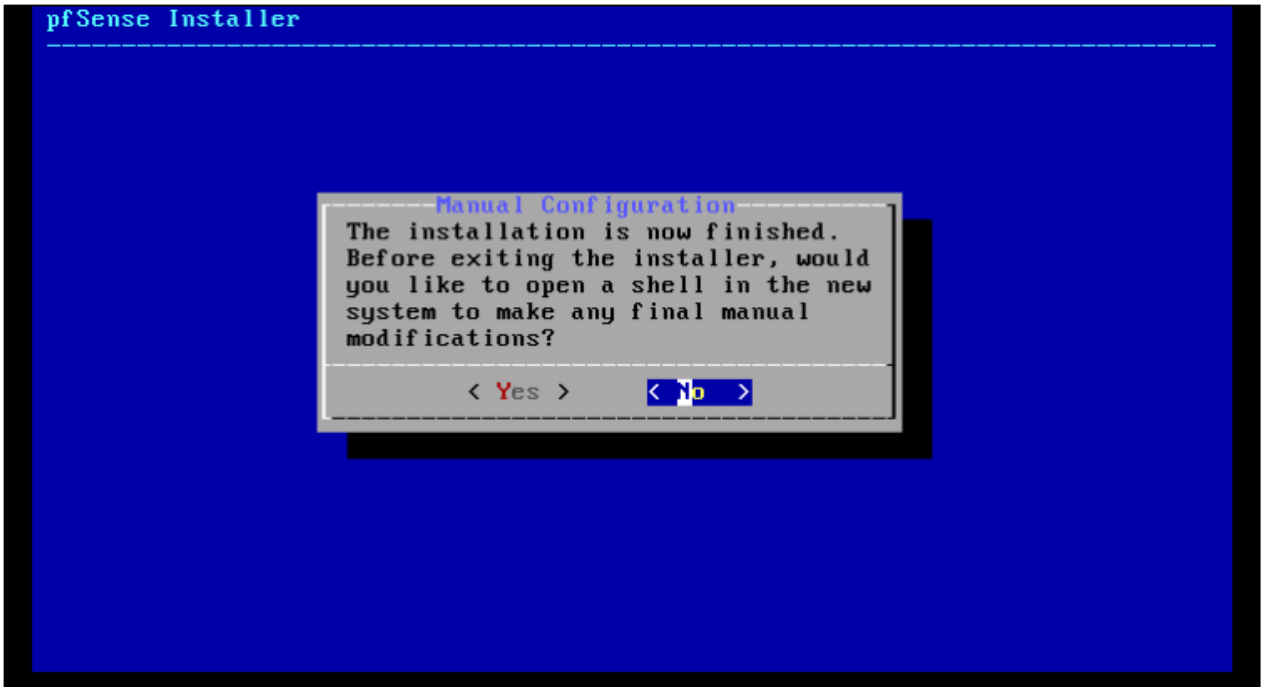
В зависимости от аппаратной архитектуры выбираем метод загрузки и разметки накопителя, для ВМ — BIOS.



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
```

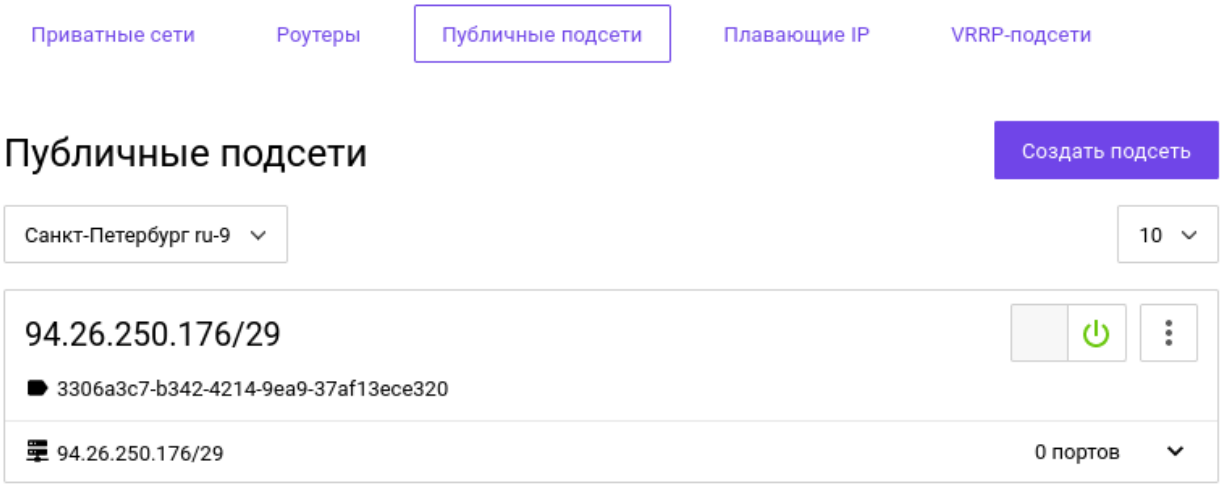
В реальной жизни при установке на своем сервере этот этап не потребуется.

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).

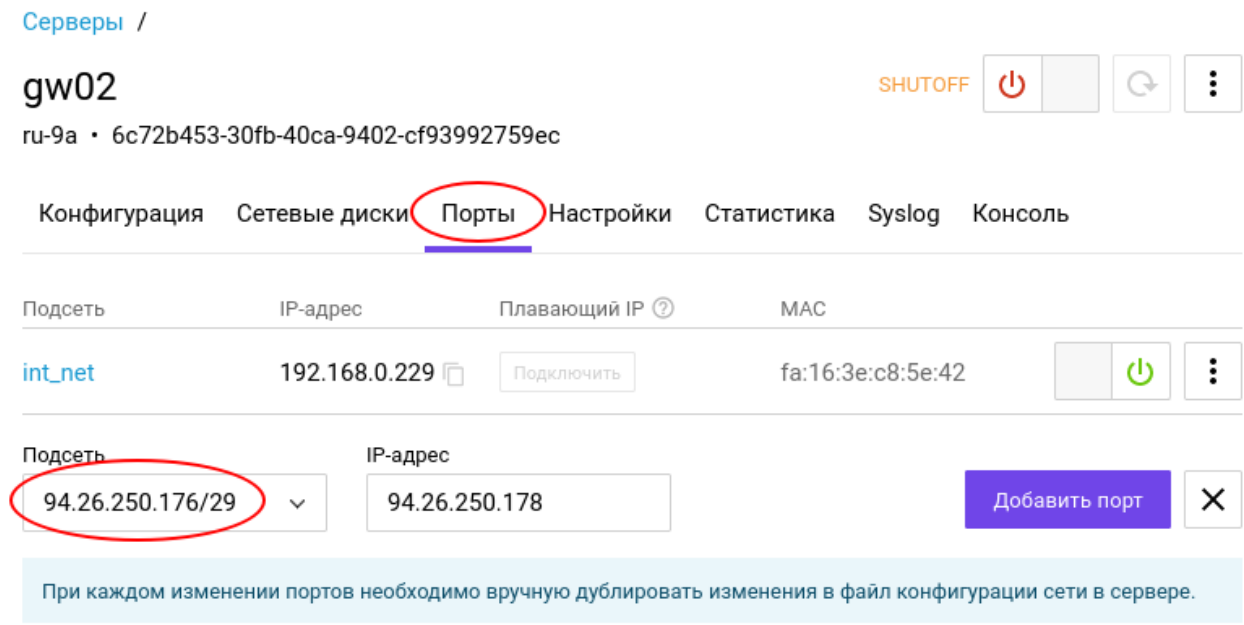
Переходим в глобальную панель «**Сеть**»->«**Публичные подсети**» и нажимаем «**Создать подсеть**».

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



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**».



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
  VT-x: PAT,HLT,MTF,PAUSE,EPT,UG,VPID,VID,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]?
```

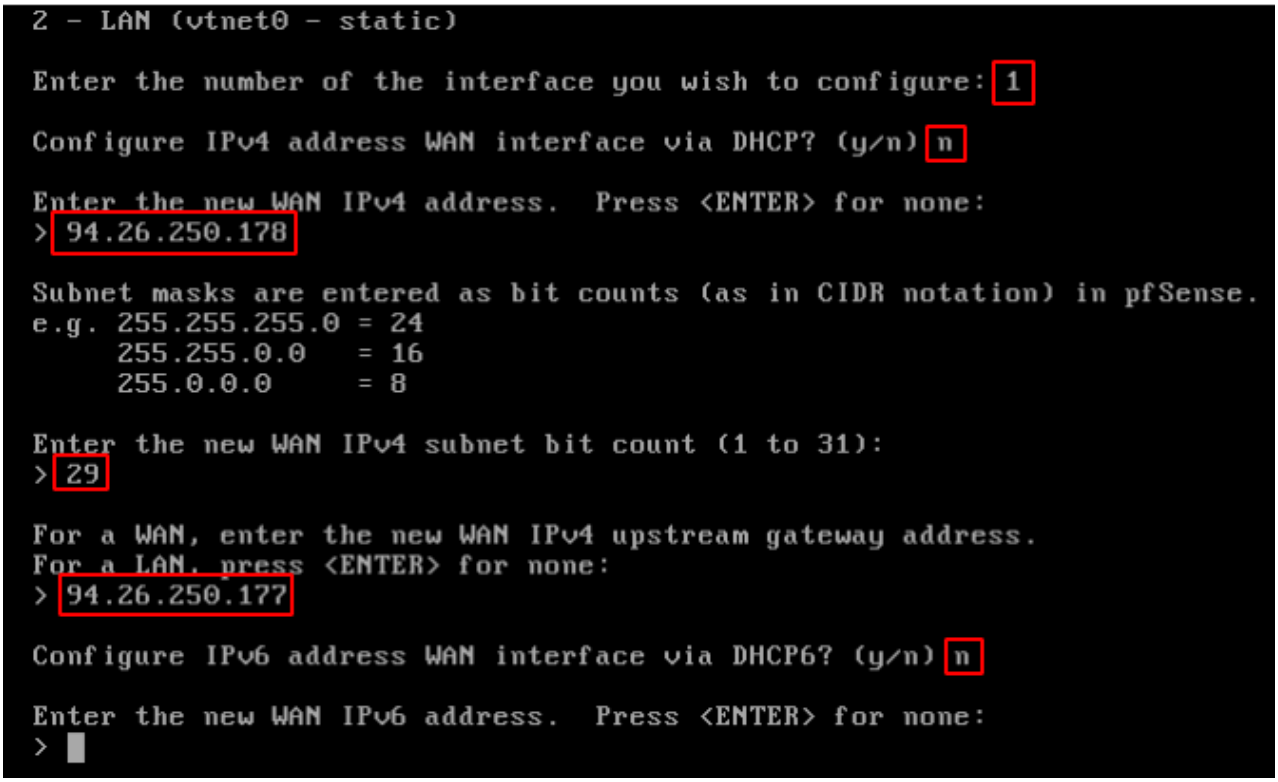
Для применения настроек и продолжения установки нажимаем клавишу **y**.

```
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).

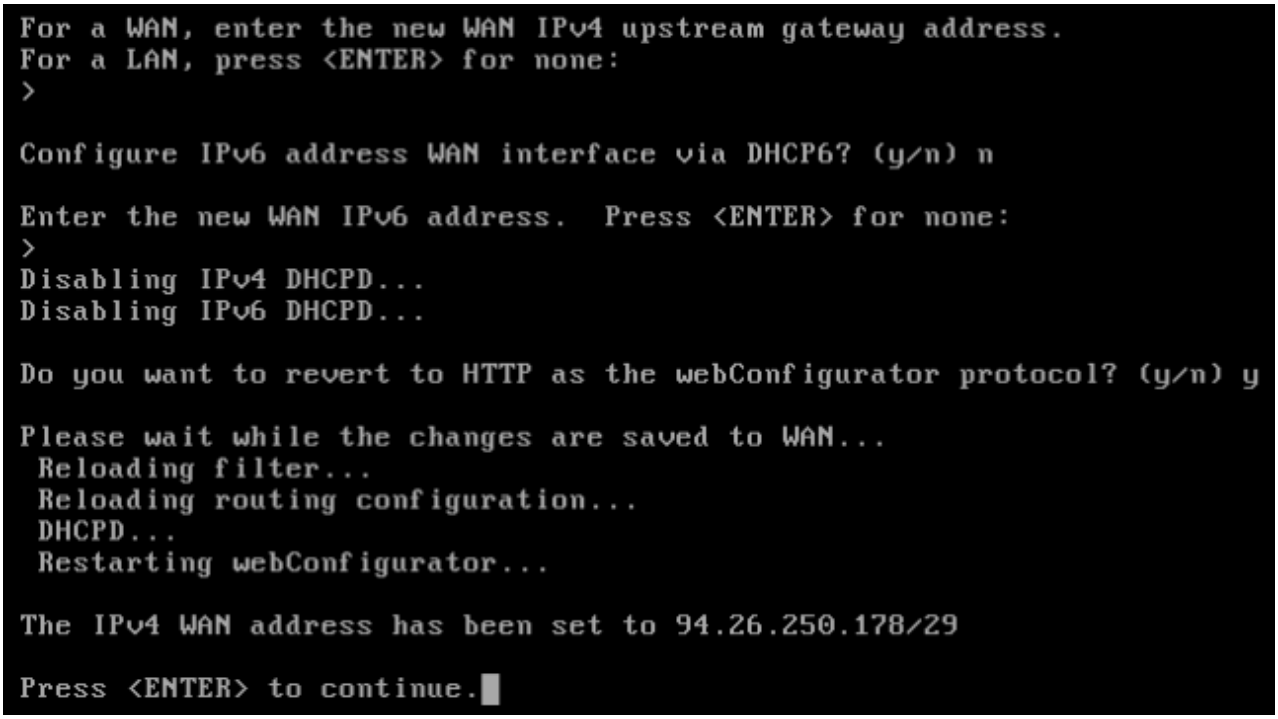
```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 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.**

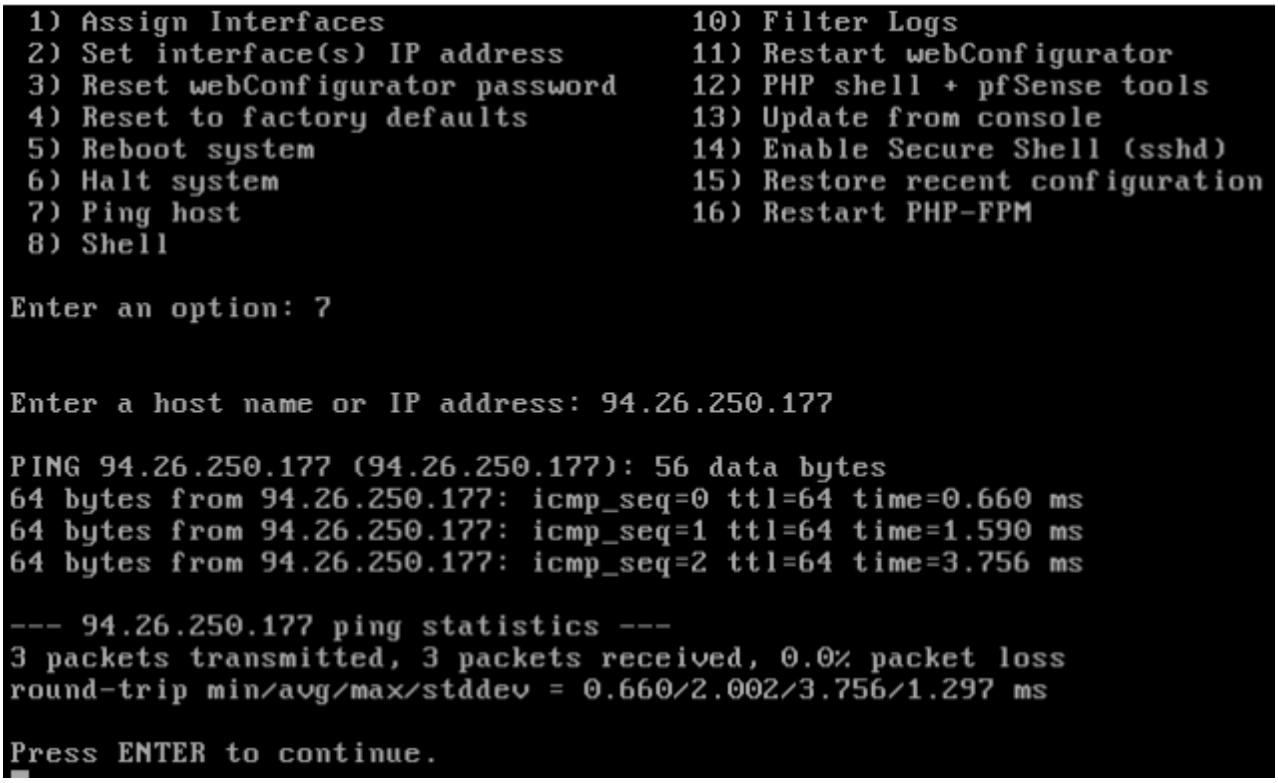


Следом система предложит изменить настройки IPv6. В нашем сценарии это не требуется, настройки не меняем.

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



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

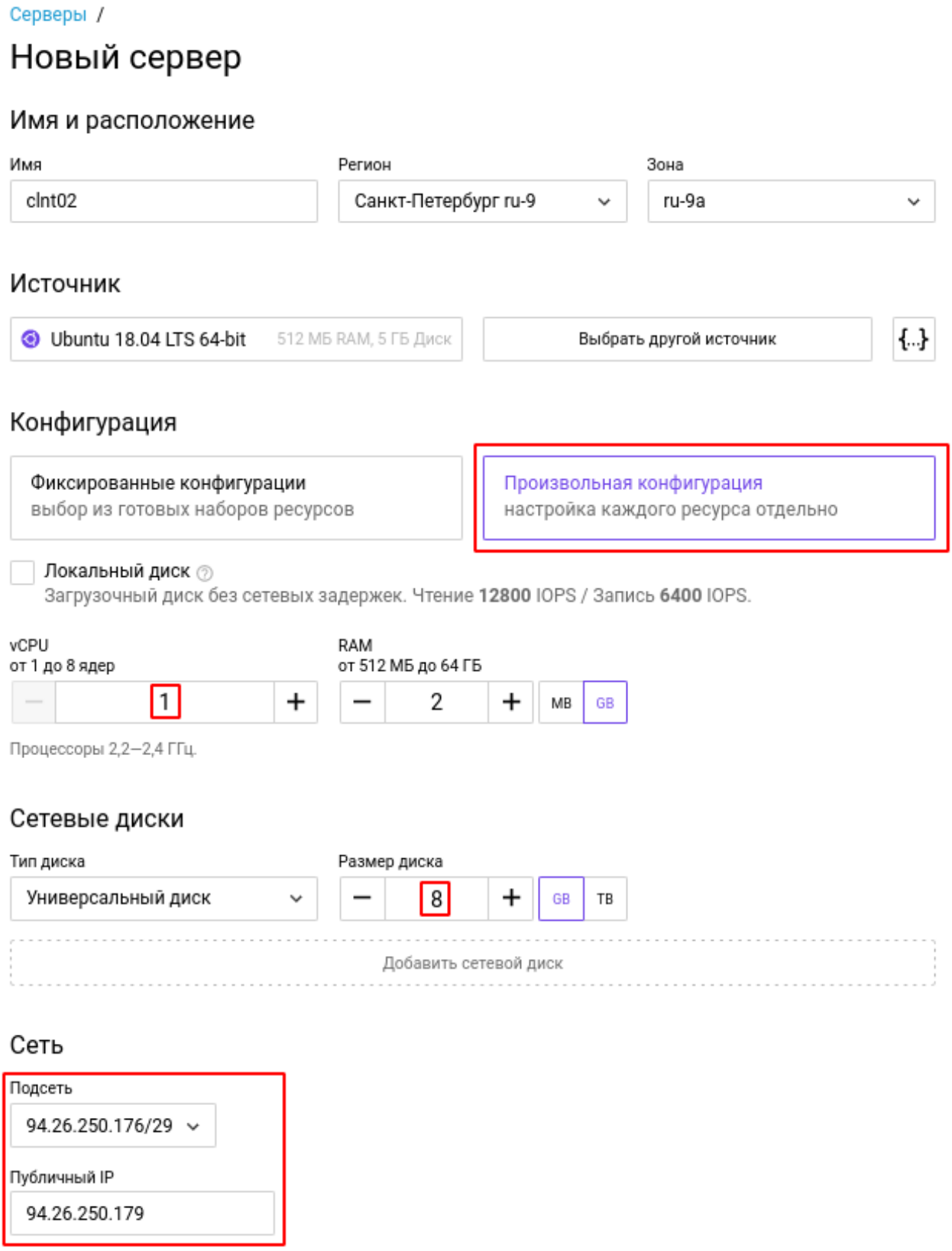


После выбора пункта **Ping host** указываем адрес шлюза провайдера или, в нашей лаборатории, платформы.

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.



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.

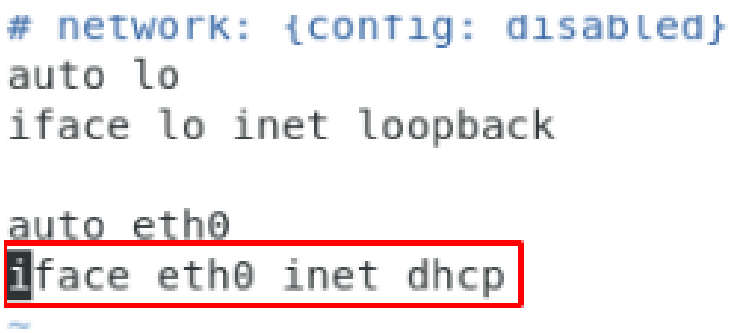
В нашей лаборатории это не нужно, наш DHCP работает на pfSense и именно он должен задавать сетевые параметры клиента. Поведение гостевой машины меняется командой.

```
    $ 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:



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:

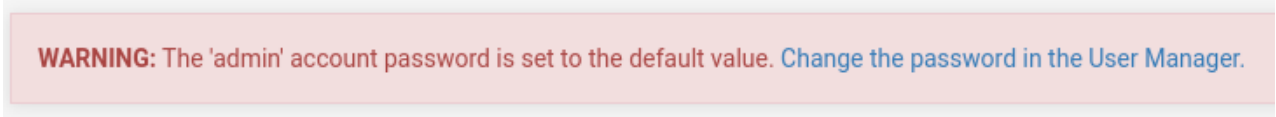
```
myuser@clnt02:~$ grep ident /var/lib/dhcp/dhclient.eth0.leases |tail -n 1
  option dhcp-server-identifier 192.168.1.1;
```

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.

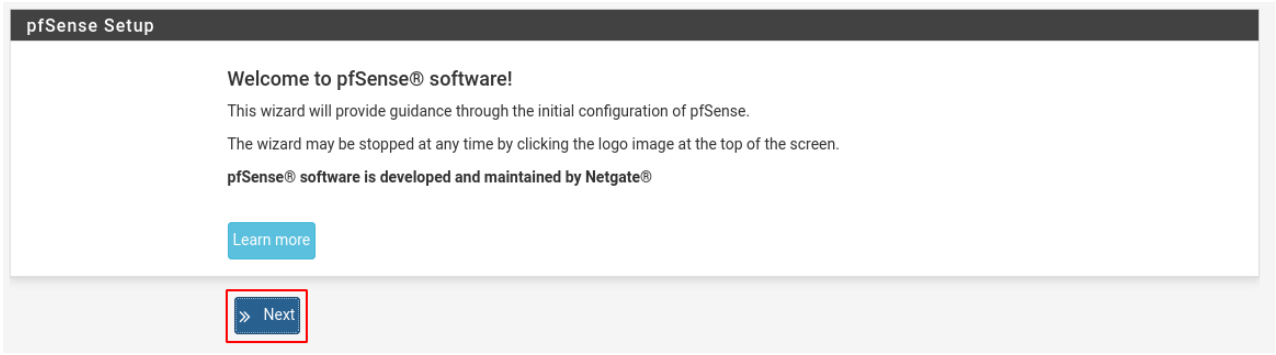
9 шагов мастера настройки pfSense

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.

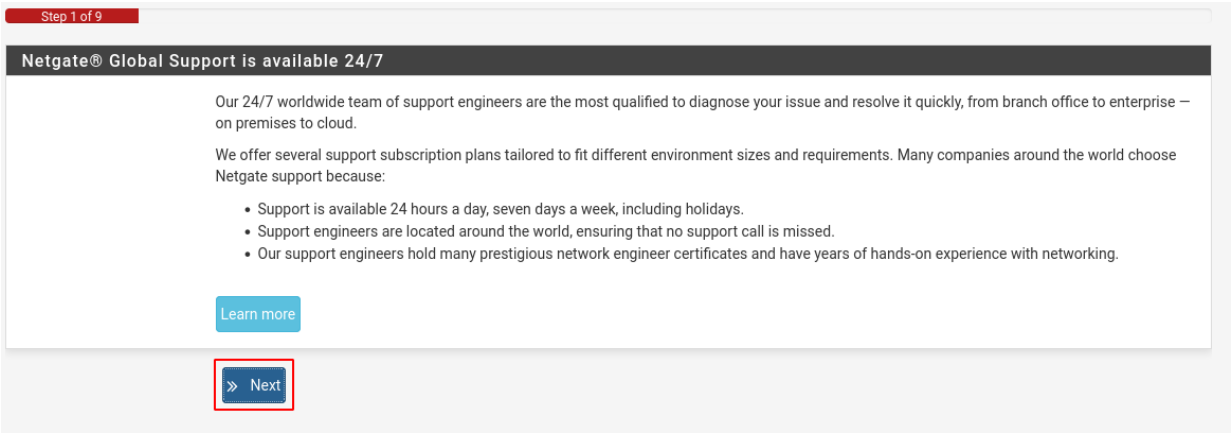
Баннер вверху напоминает о необходимости изменить пароль по умолчанию на свой. На 6-м шаге мастер настройки предложит поменять пароль, поэтому сейчас можно баннер проигнорировать.



Видим приветствие мастера настройки.



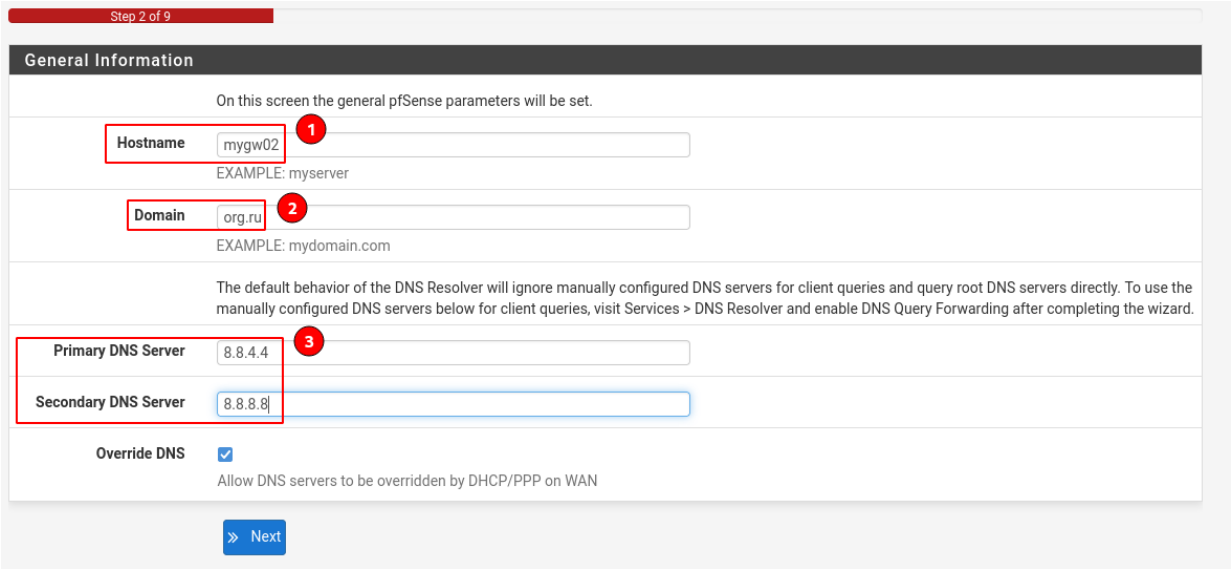
Шаг 1. Начало настройки



Шаг 2. Указание имени и домена шлюза

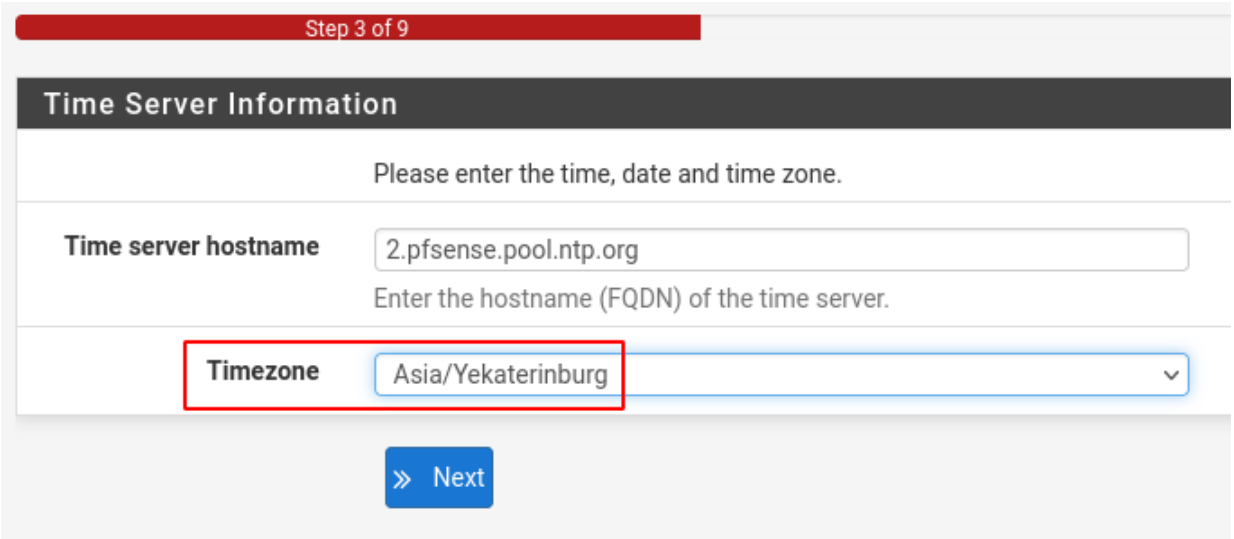
В мастере указываем имя и домен нашего шлюза (шаг 2, например, mygw02 & myorg.ru), DNS-серверы (напр., dns.google — 8.8.4.4 & 8.8.8.8).

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



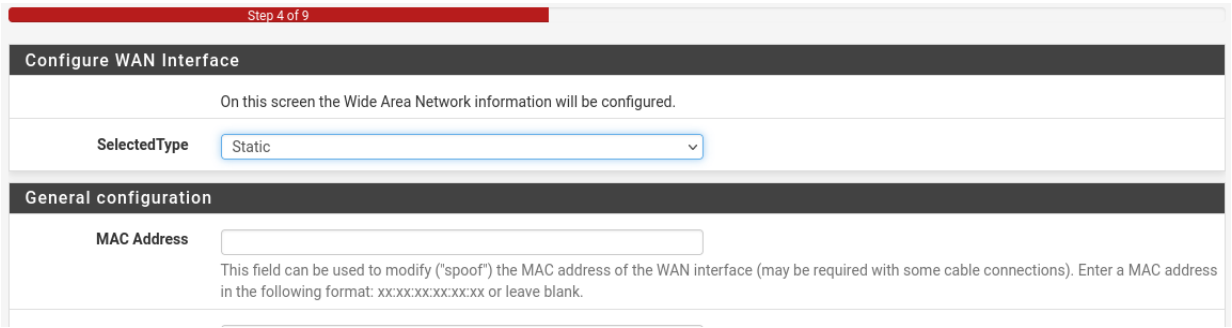
Шаг 3. Настройка синхронизации времени

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).



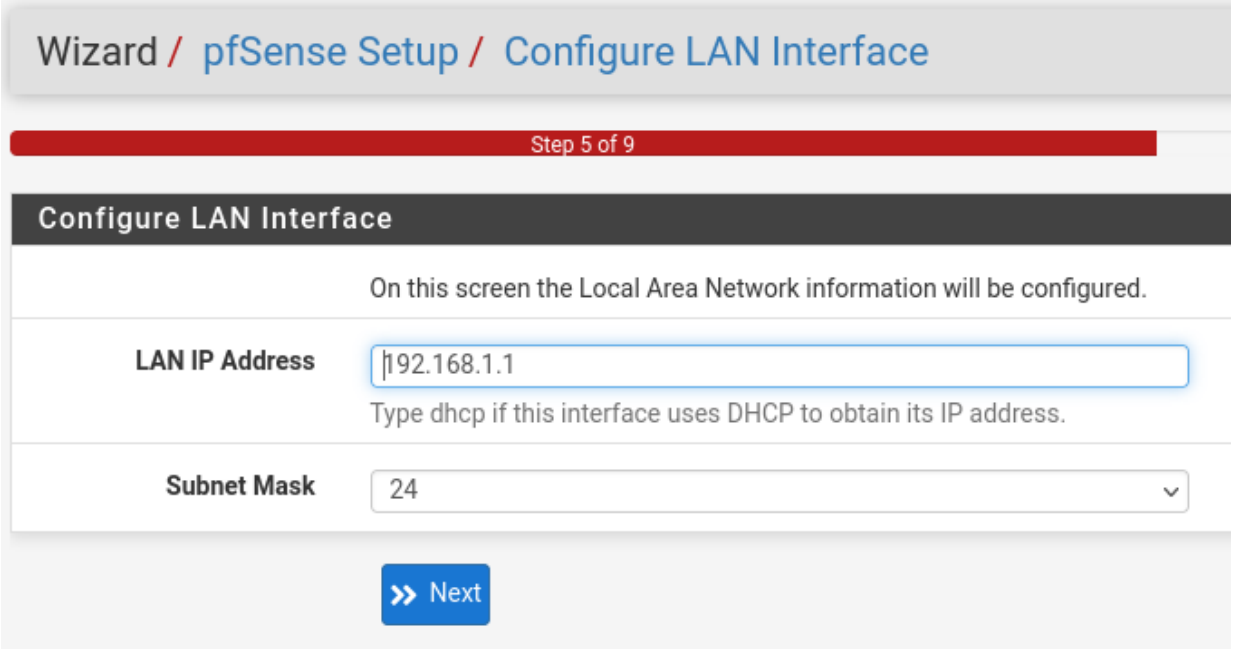
Шаг 4. Настройка PPPoE

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.



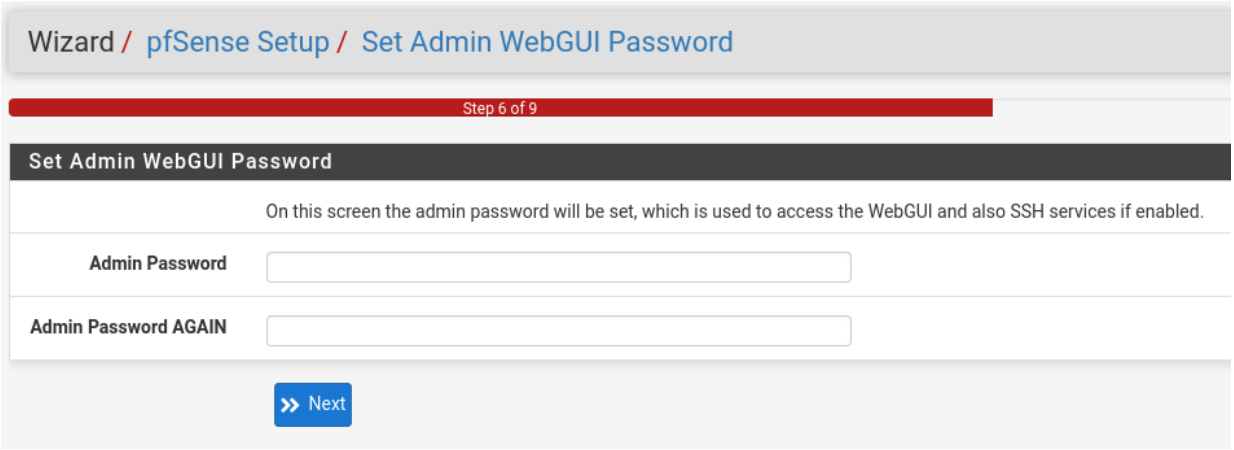
Шаг 5. Настройка внутреннего интерфейса

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



Шаг 6. Пароль администратора

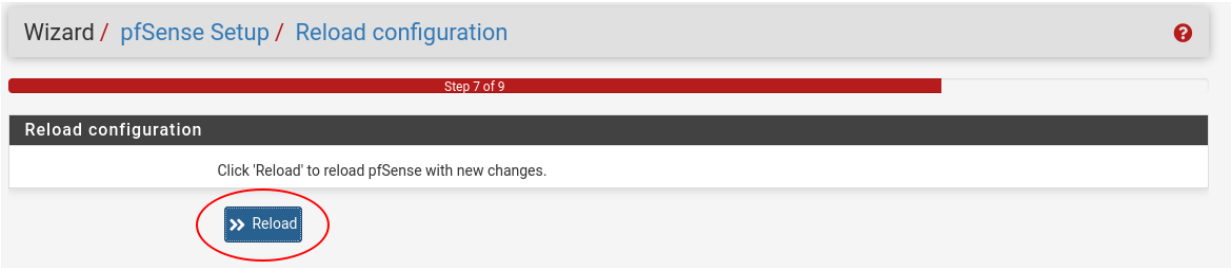
На этом шаге система потребует изменить пароль администратора:



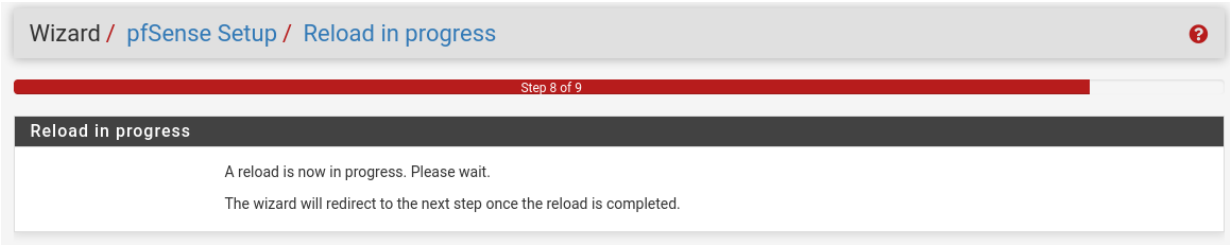
Проверка соответствия предыдущему (в том числе установленному по умолчанию) паролю не производится. Технически можно повторить, но из соображений безопасности следует установить стойкий пароль.

Шаг 7. Применение настроек

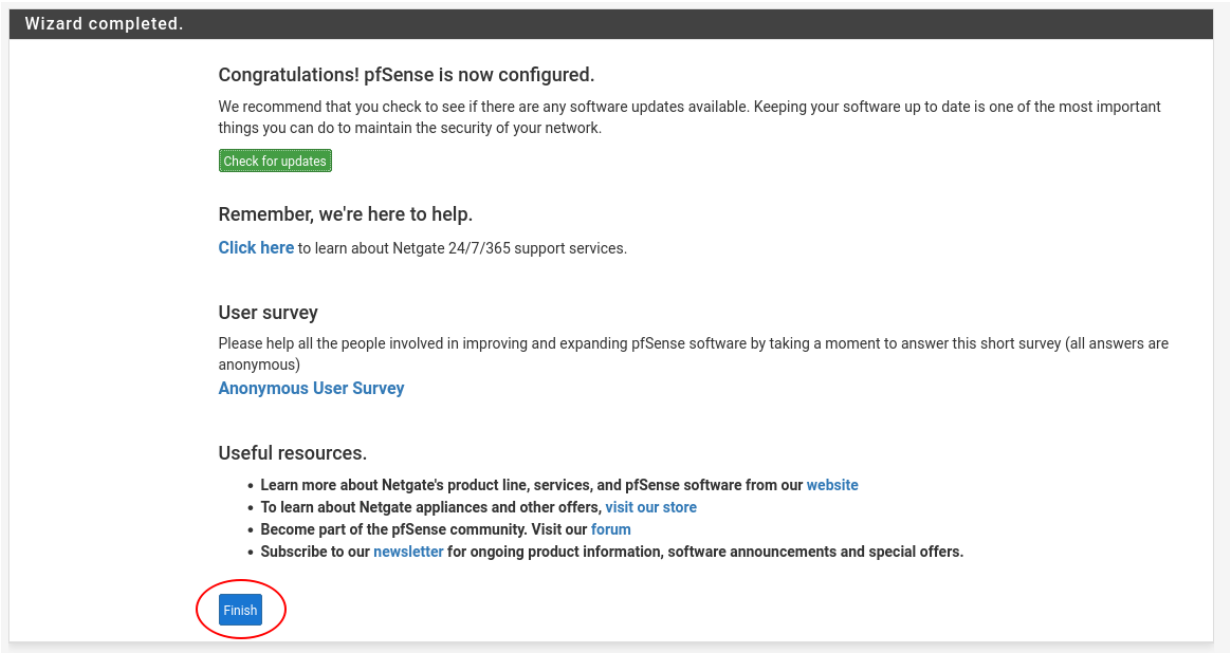
И затем предложит применить настройки.



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.

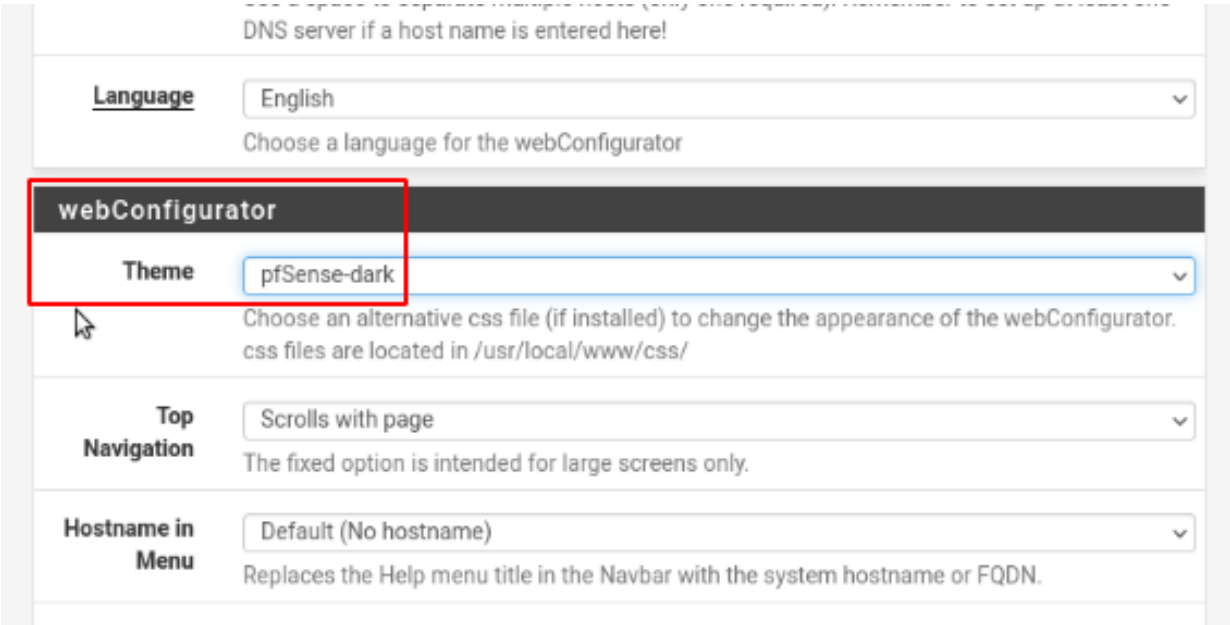
Структура меню

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**:

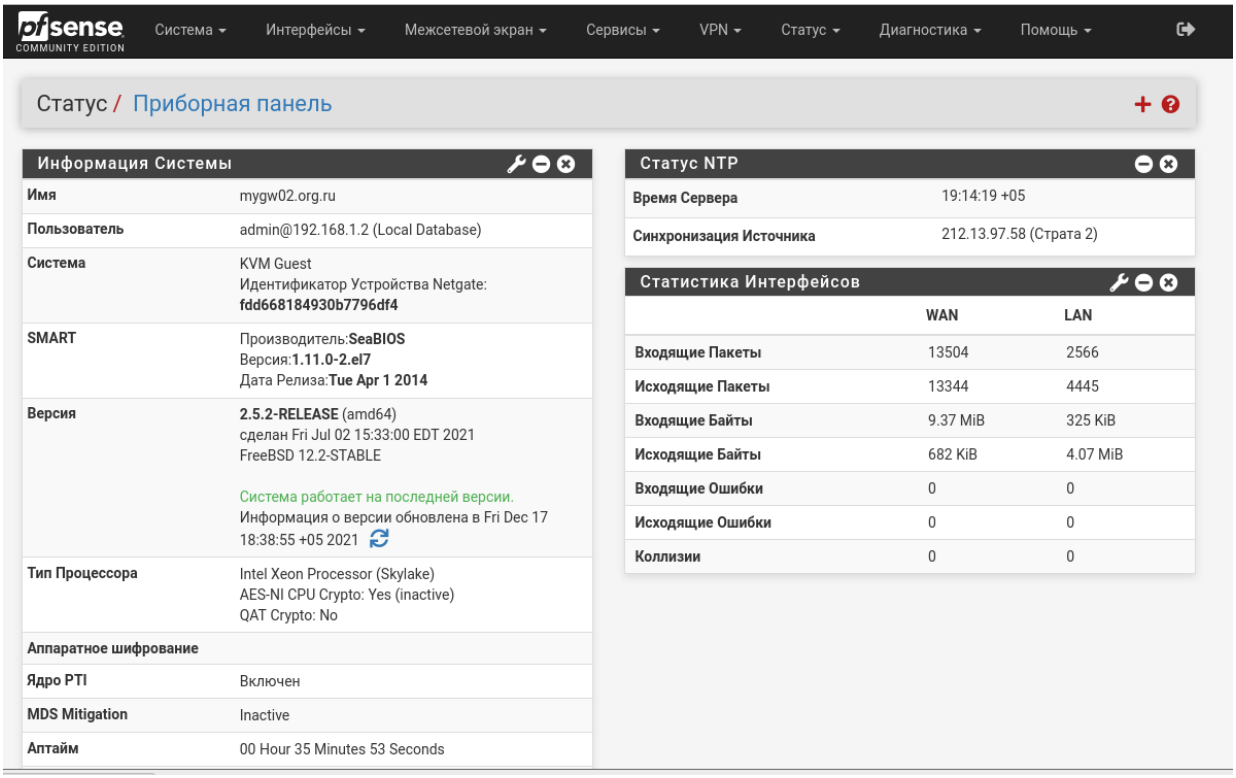


В статье будет чередоваться темная и светлая тема, используемая по умолчанию.

Локализация

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

Пример интерфейса на русском языке:



Диагностика

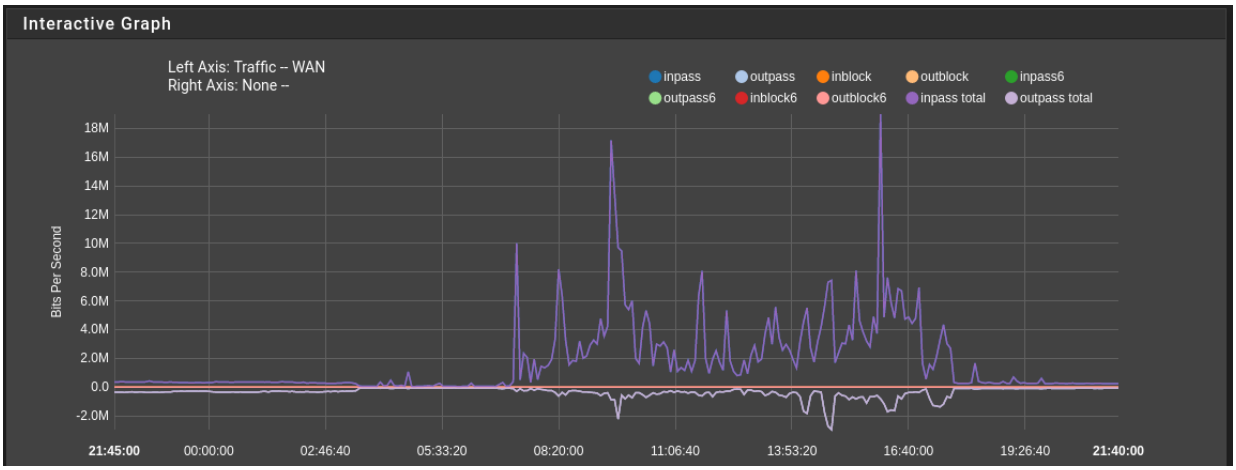
Первичная диагностика обычно начинается с анализа журналов работы системы и компонентов, после чего полезно проанализировать историческую загрузку системы на определенном интервале, например, в течение последних суток или часа.

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

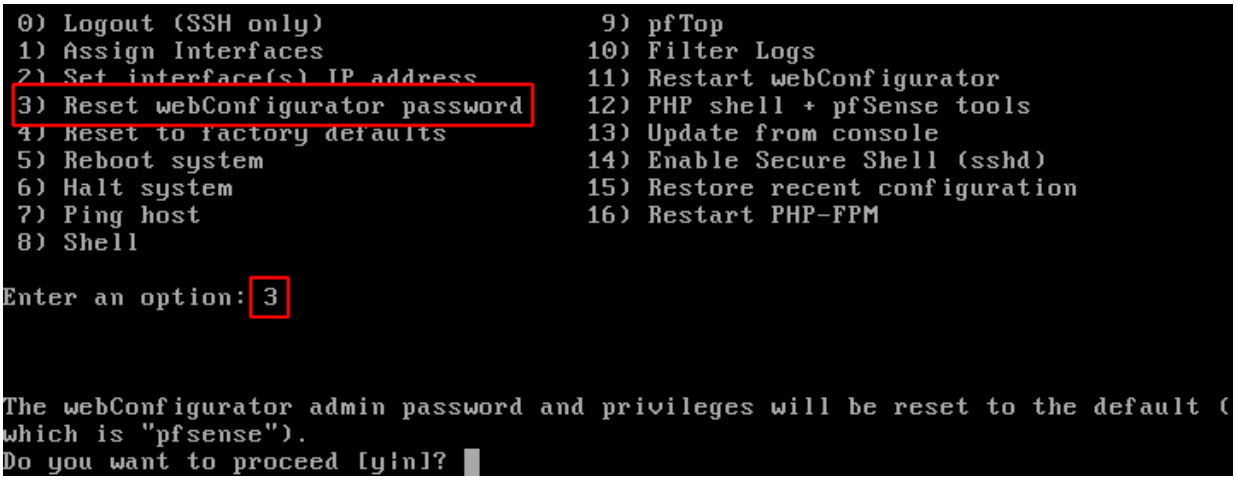
Оценить нагрузку на систему удобно в графическом виде в разделе **Status/Monitoring**.



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):



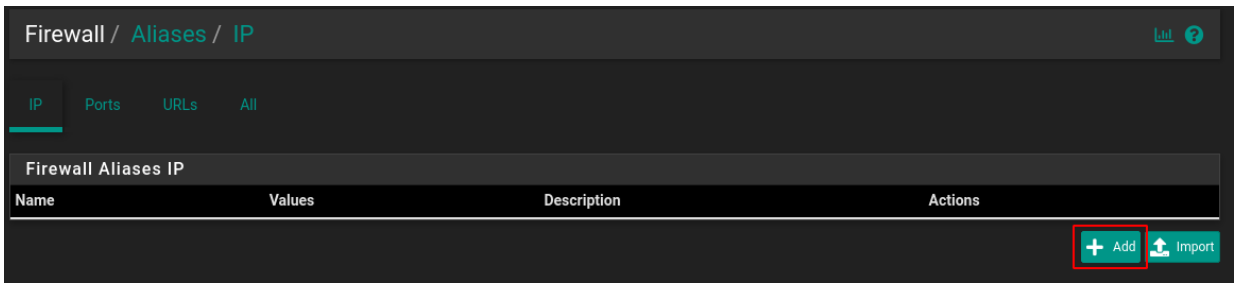
Расширенные настройки

Правила брандмауэра

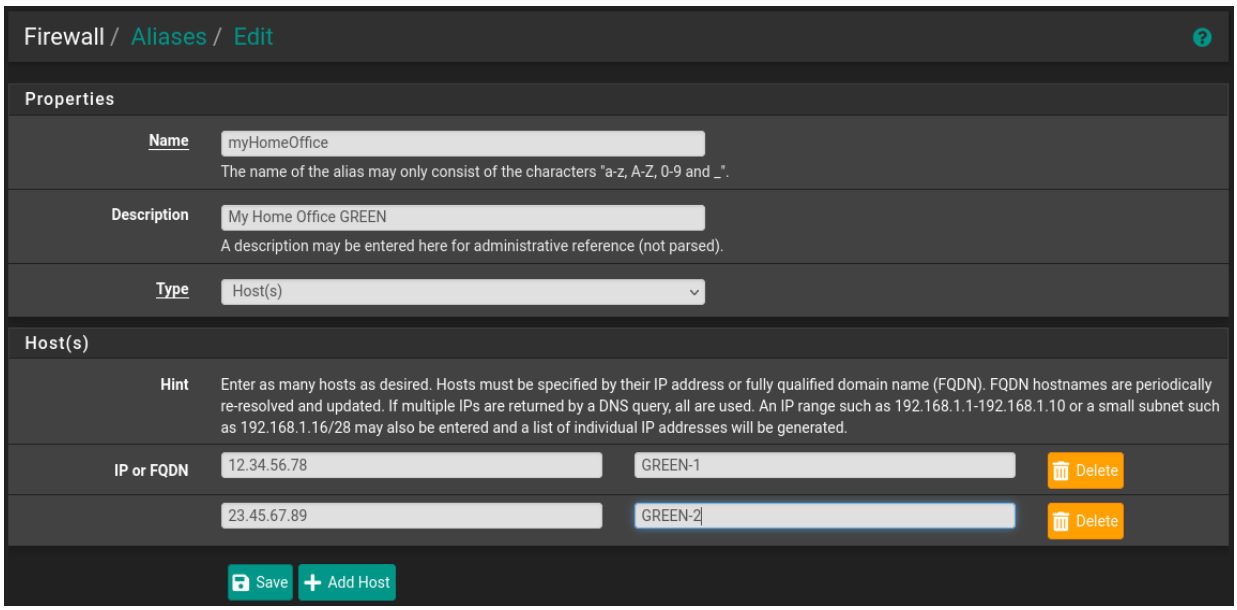
Настройки по умолчанию запрещают подключение к pfSense из глобальной сети и разрешают доступ клиентов наружу с использованием трансляции адресов NAT (точнее, наиболее частый вариант динамической NAT — NAPT по RFC 2663, она же NAT overload, маскарадинг или PAT — здесь и далее будем говорить только об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

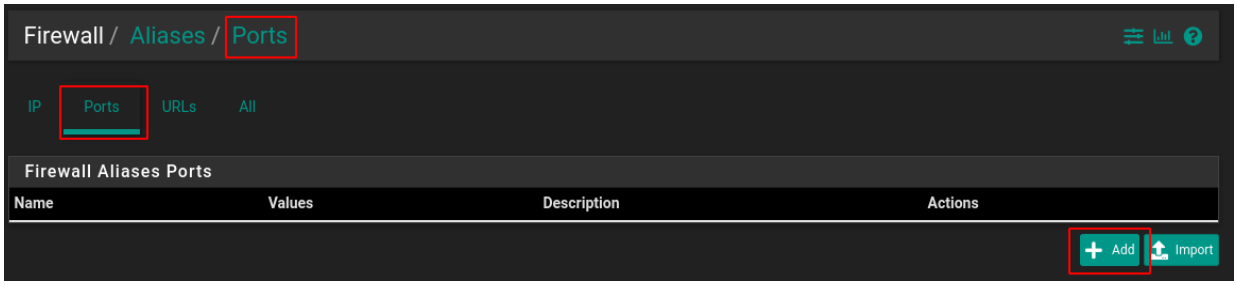


Откроется редактор псевдонимов для IP-адресов:

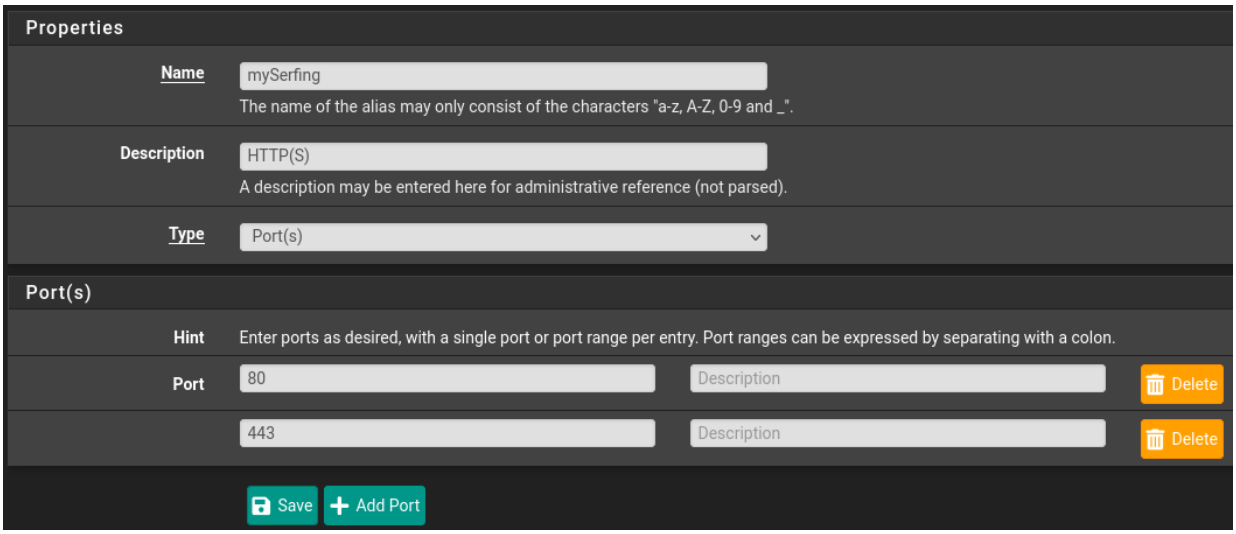


В редакторе присвоим имя псевдониму, укажем тип (Host(s)) и добавим IP-адреса.

На вкладке Ports аналогичным образом создаем правило для служб:



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

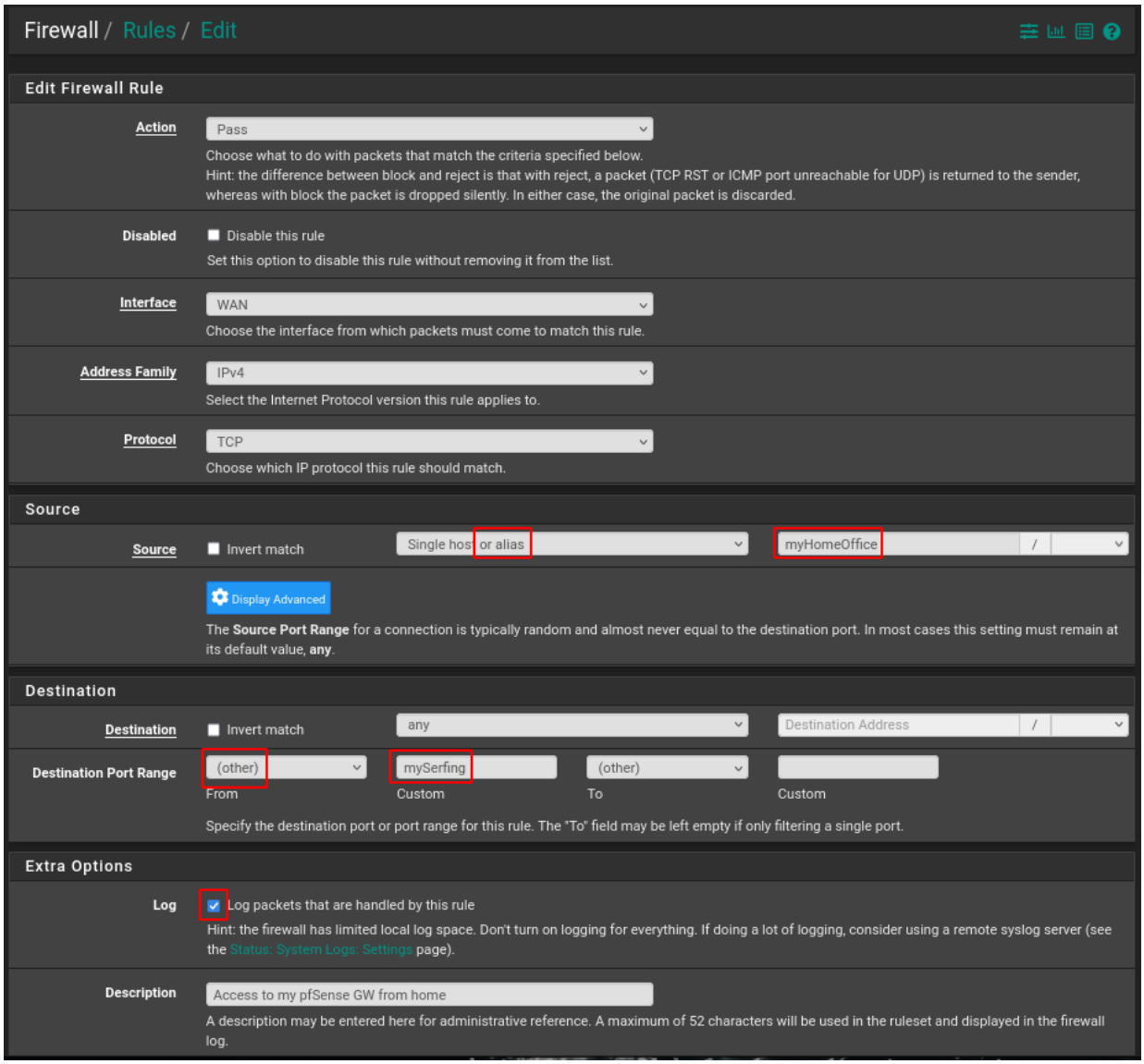


В подсказке указан удобный способ создания псевдонима для диапазона портов.

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.

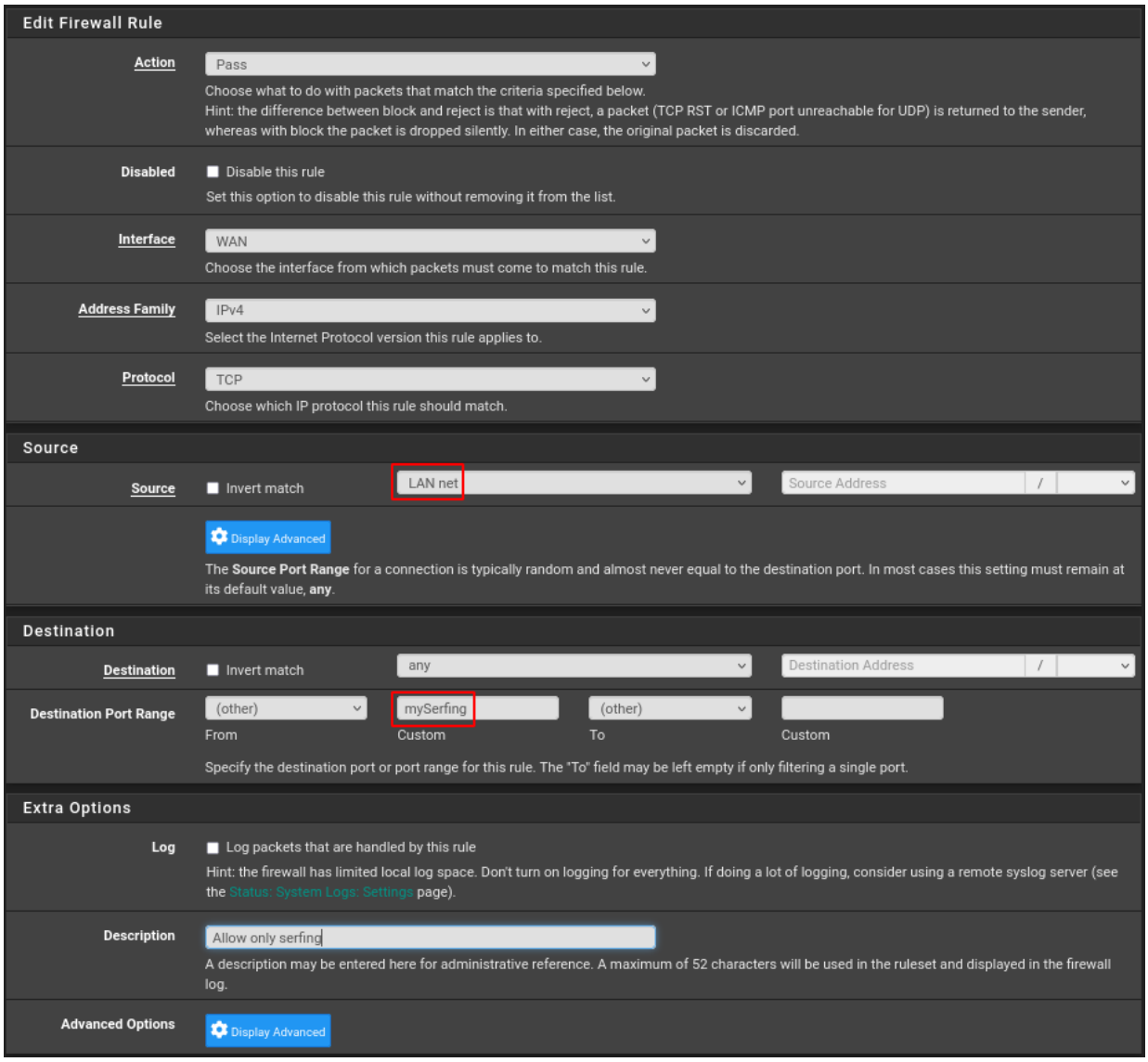
В этом случае достаточно скорректировать только один псевдоним.



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

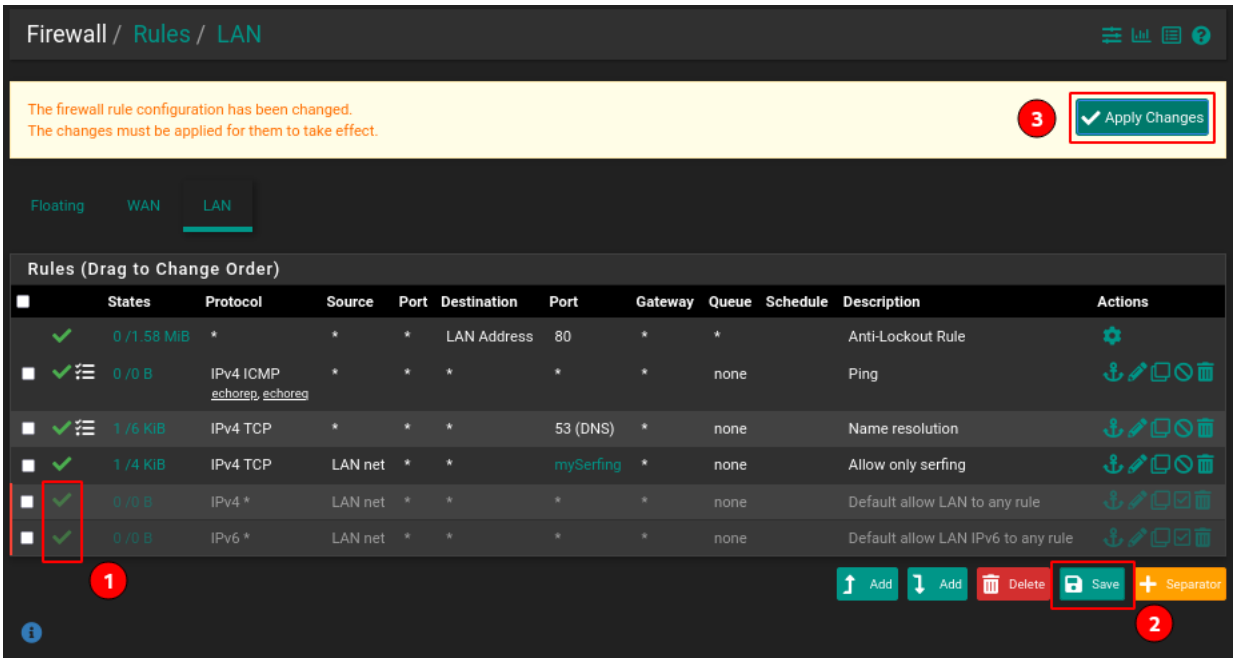
После настройки не забываем нажимать **Apply Changes**. Теперь можно проверять подключение.

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



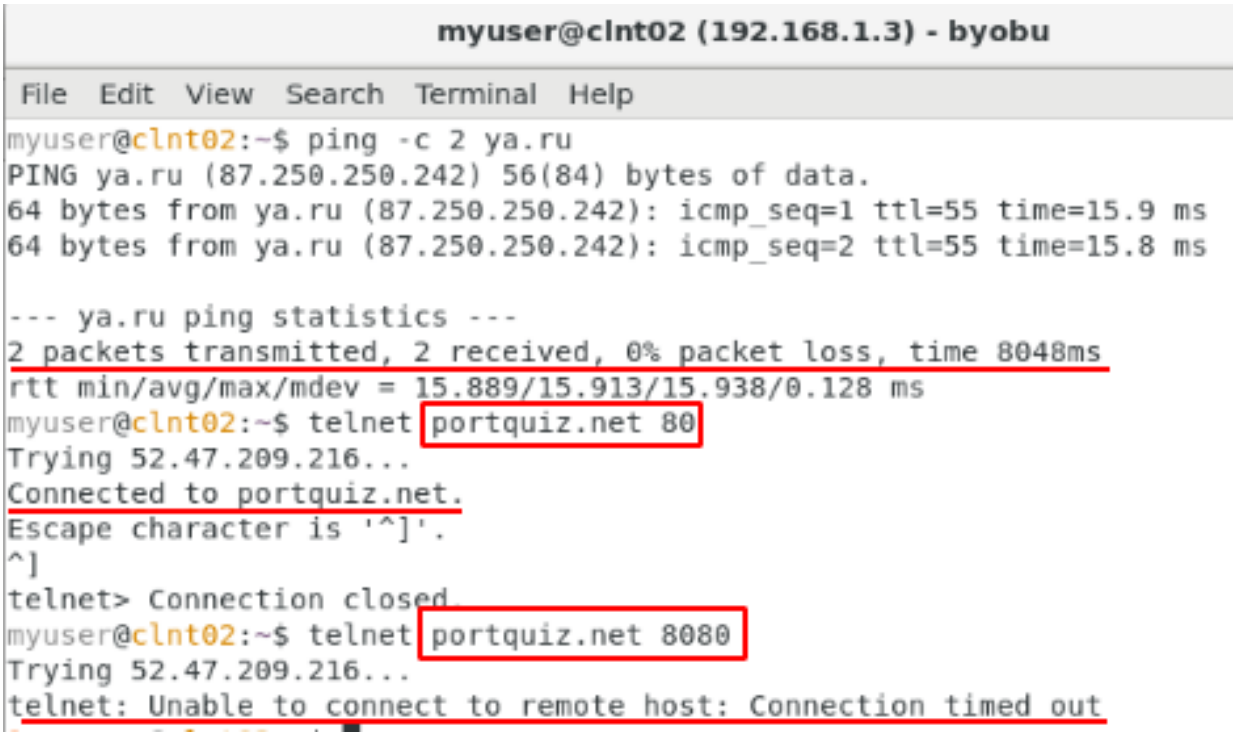
Далее на этом же интерфейсе создаем правила для DNS (udp:53) и (необязательно, облегчает диагностику) ICMP (достаточно echo request, echo reply).

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

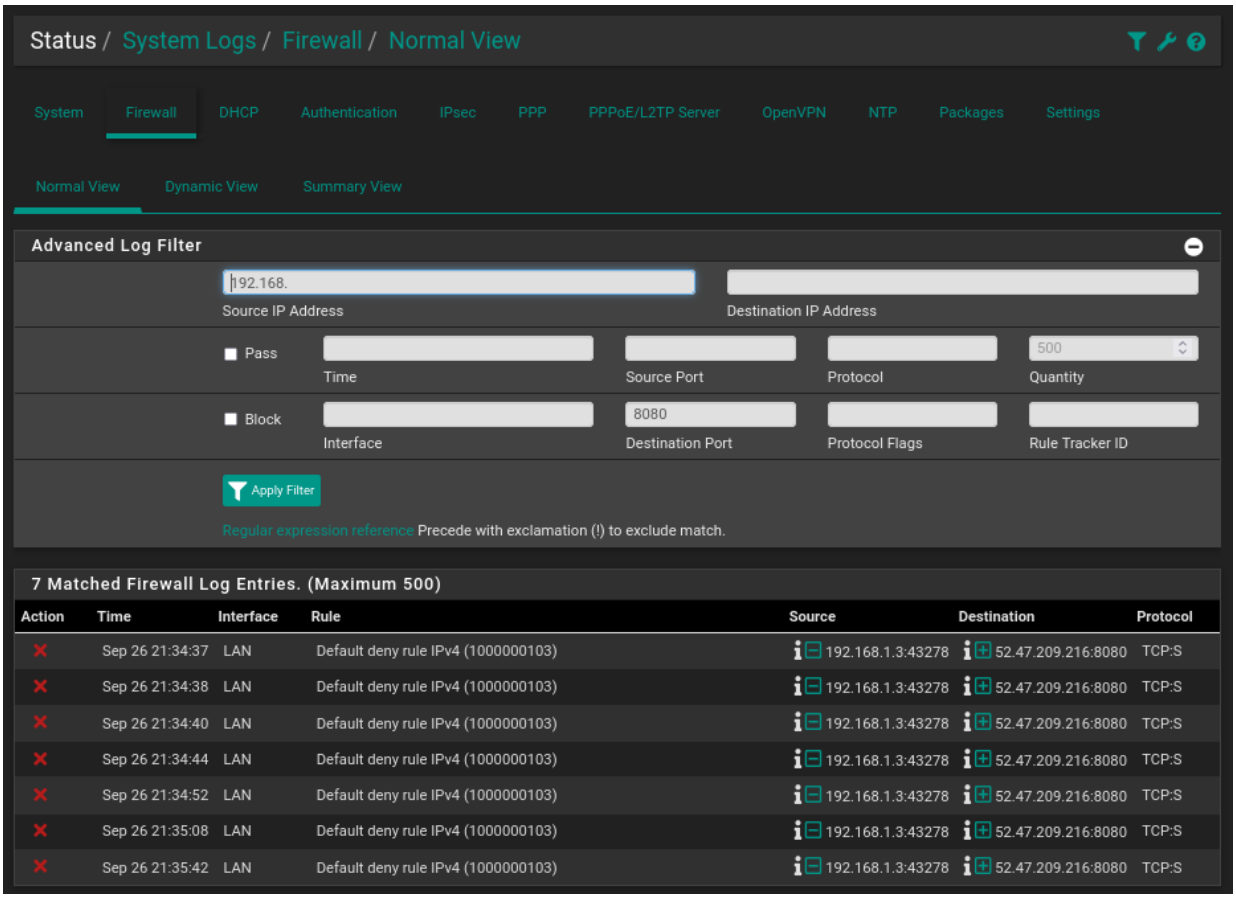


Проверяем доступ к web-сайтам, затем к нестандартным портам, используя ресурс portquiz.net:

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



О чем также видим записи в журнале:



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();

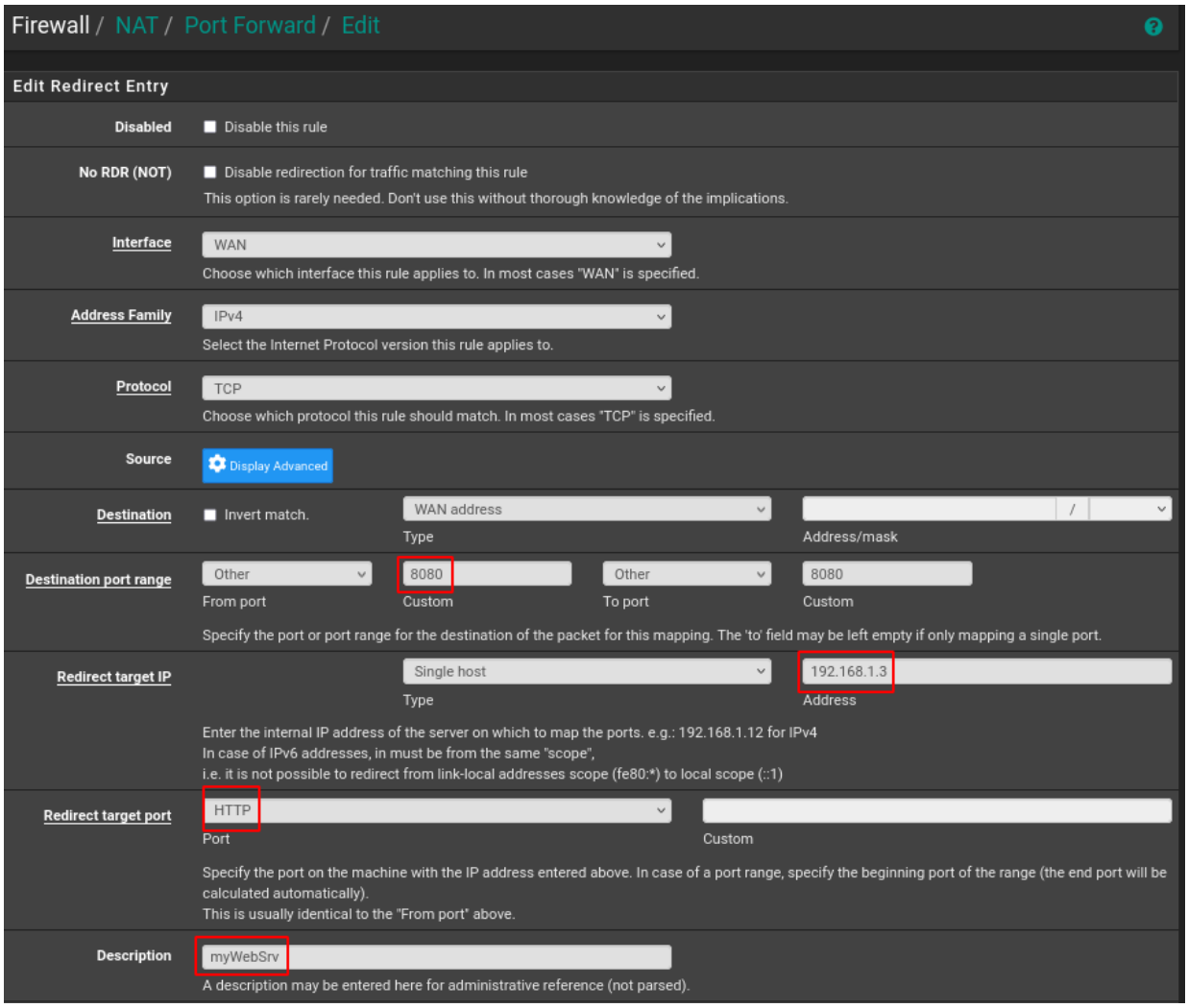
?>

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.

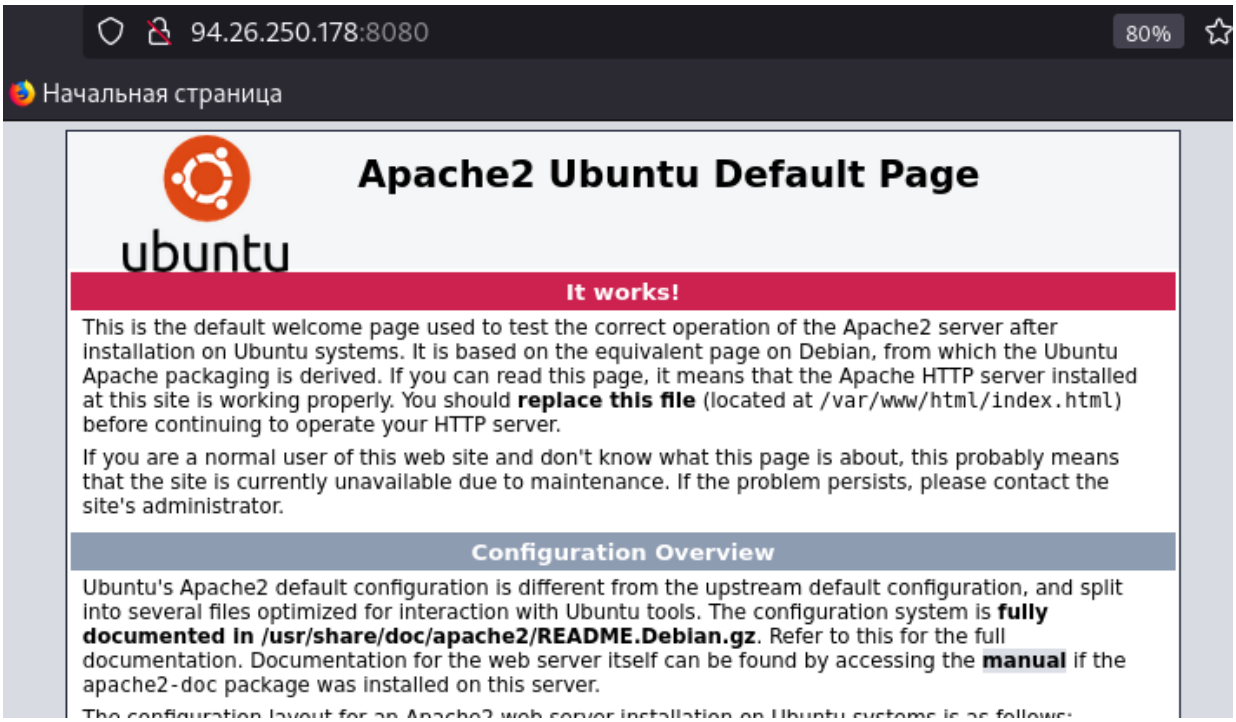


Как видим, все настраивается очень просто. pfSense слушает TCP порт 8080 и транслирует его в tcp:80 тестового хоста 192.168.1.3, на котором мы в предыдущем шаге настроили веб-сервер.

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

Проверка

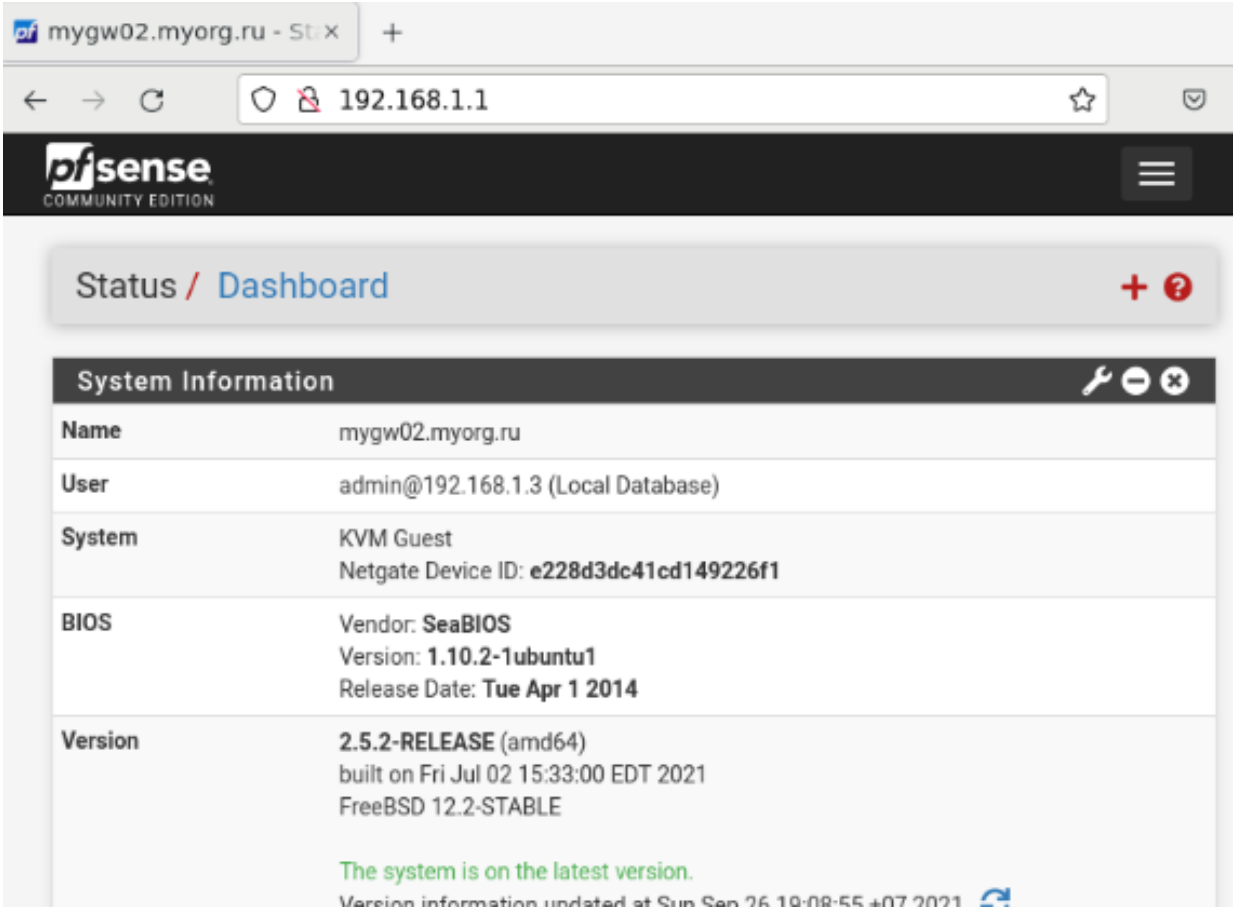
Проверяем наши настройки, зайдя на WAN-адрес pfSense с указанием порта 8080.

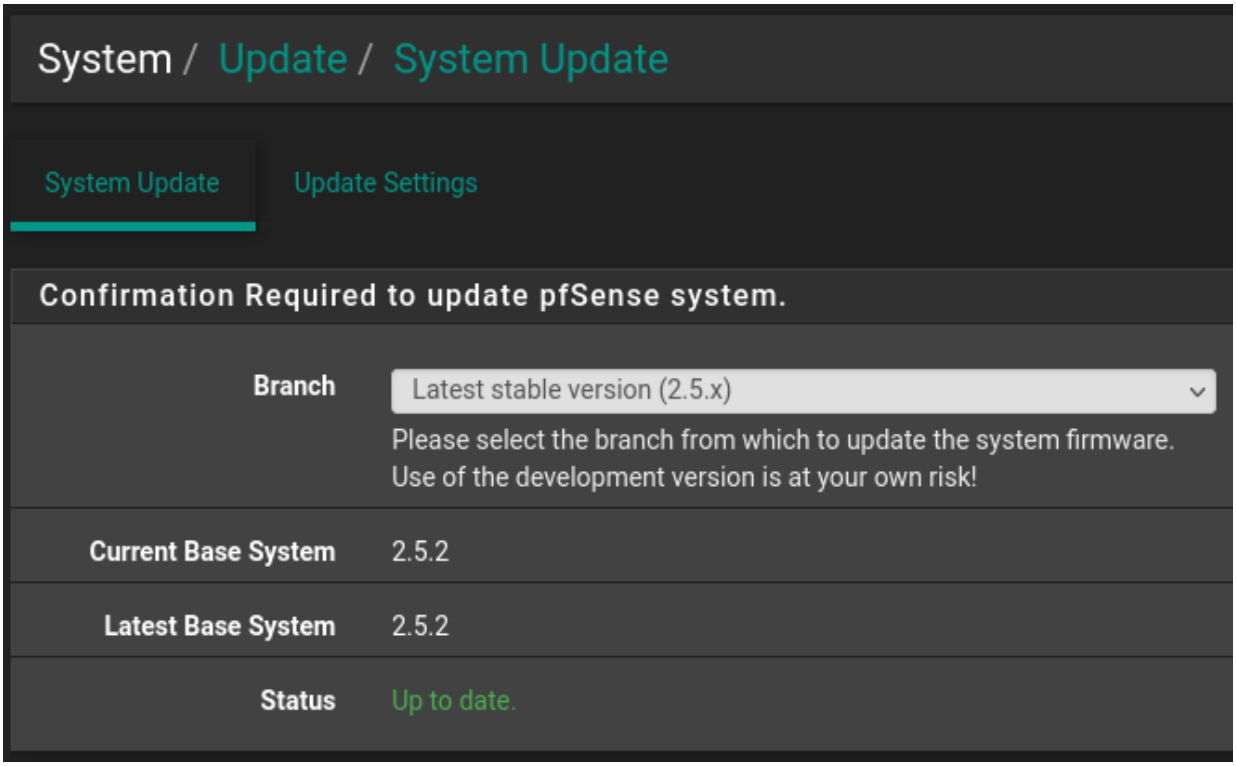


Внутренний веб-сервер ответил на публичном адресе. Добавляем название демо-странички и видим, что она также успешно опубликована.

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**.

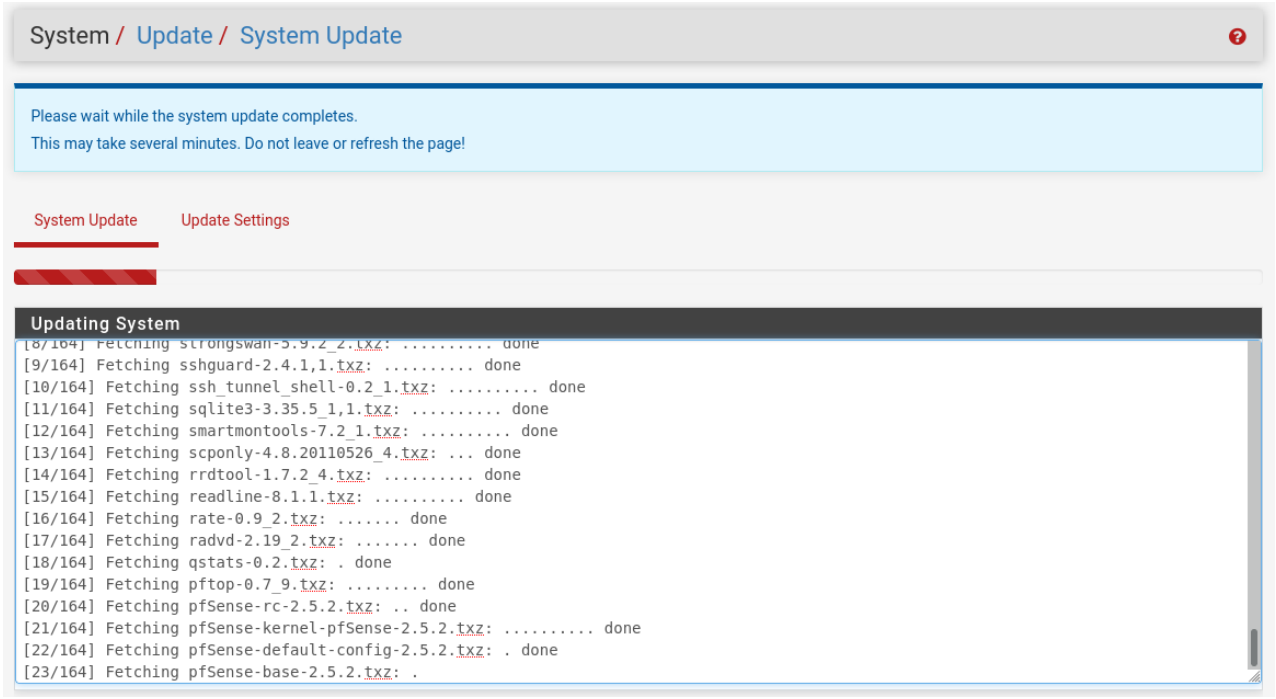




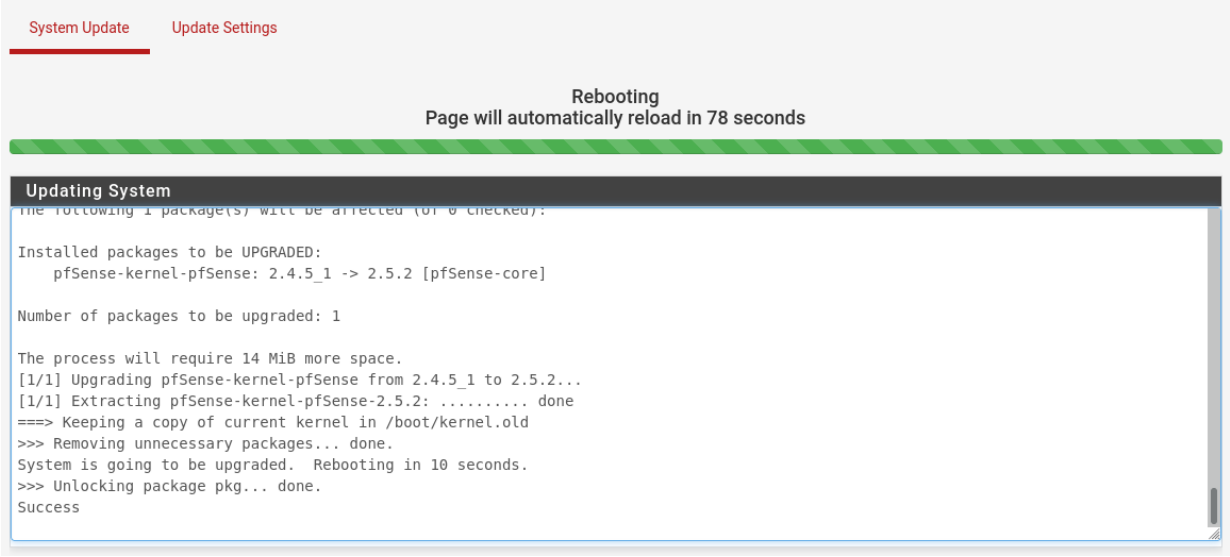
Наша система установлена из свежего дистрибутива, а значит уже актуальна, обновление не требуется. Обновления выходят примерно раз в полгода.

Если готовы к экспериментам, можно обновиться до экспериментальной ветки.

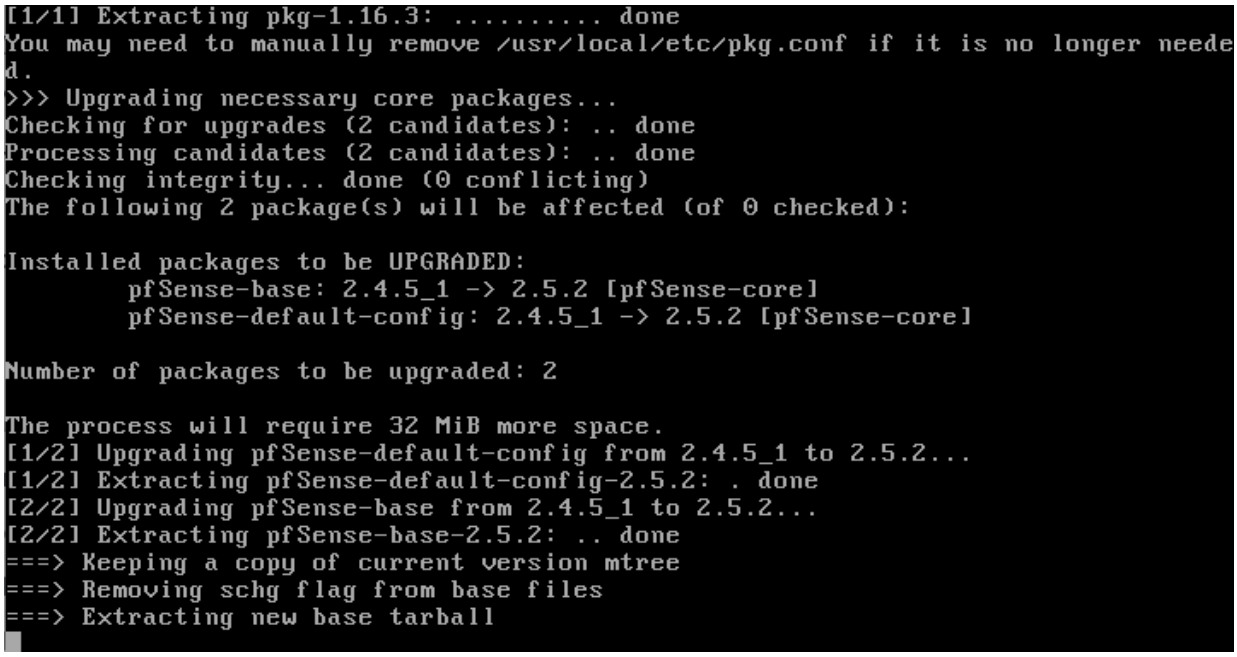
Так выглядит процедура обновления с предыдущей версии (2.4.5):



По окончании процесса система автоматически перезагрузится:



После перезагрузки в консоли наблюдаем распаковку и установку обновленных пакетов:



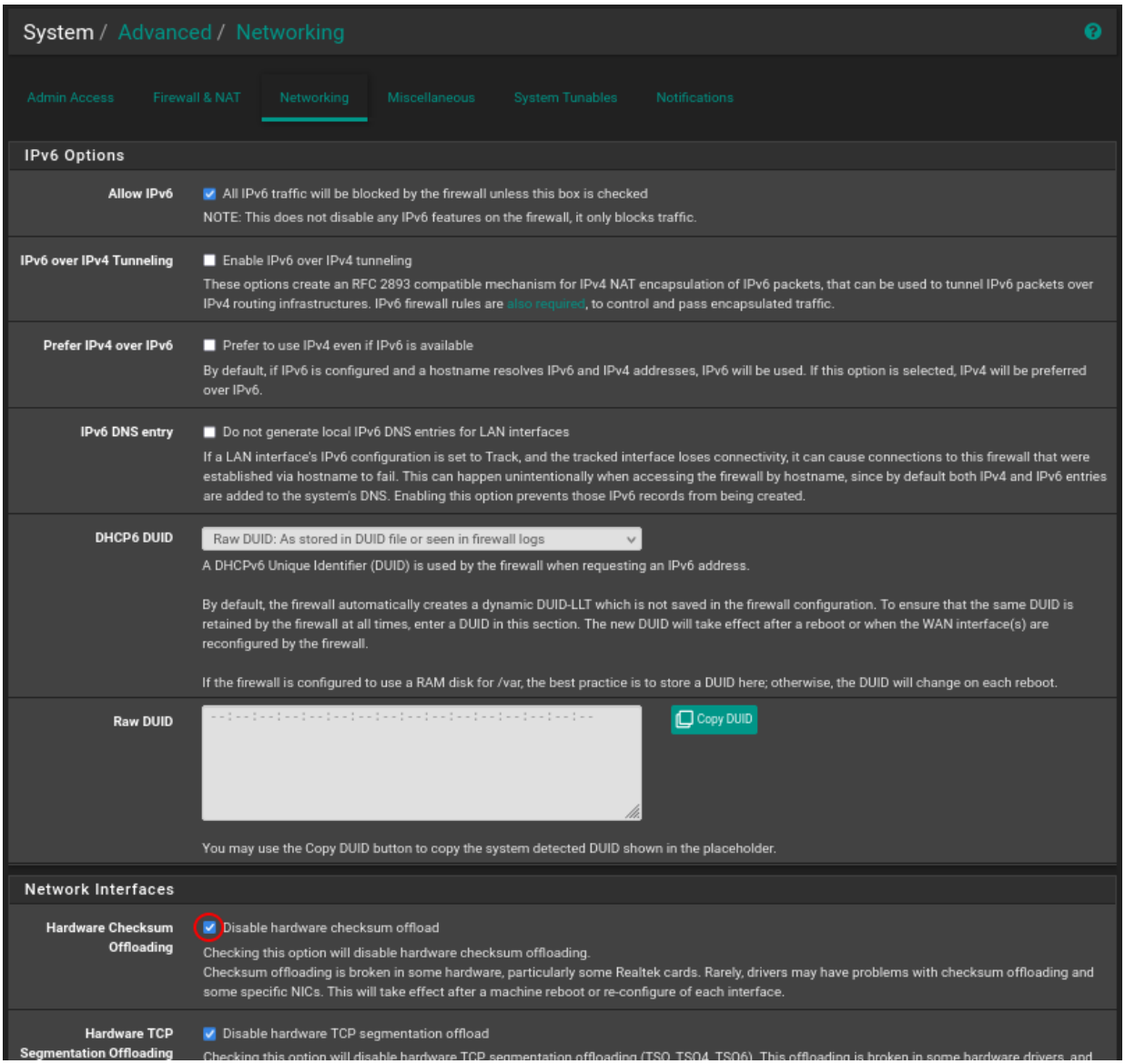
Виртуализация

pfSense отлично работает в виртуальной среде. Надо понимать, что возможно несущественное 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.

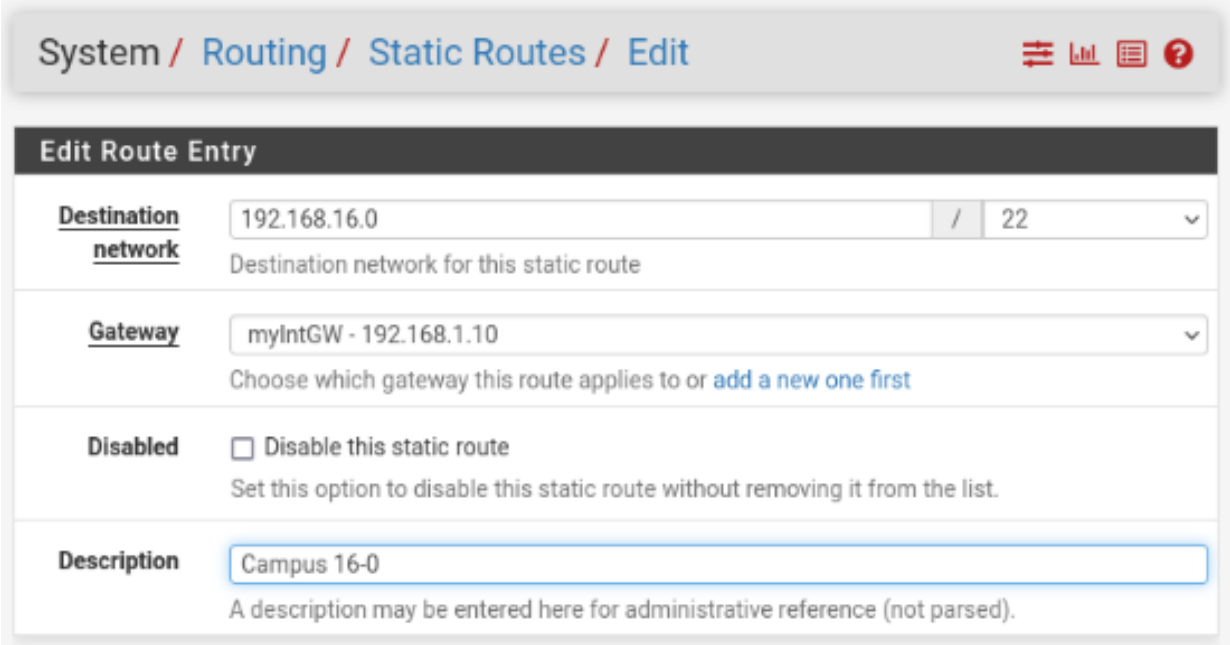


Hardware Checksum Offloading также рекомендовано отключать для адаптеров Realtek.

Внутренняя маршрутизация

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

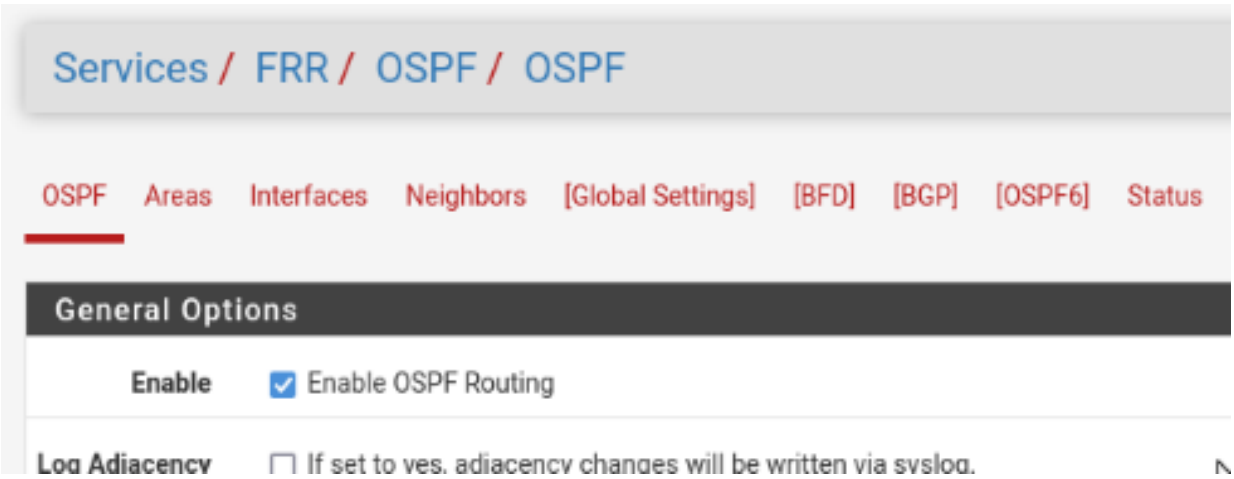
Сперва на вкладке **System -> Routing -> Gateways** создается внутренний шлюз(ы), например, myIntGW, затем маршрут добавляется на вкладке **System -> Routing -> Static Routes**:



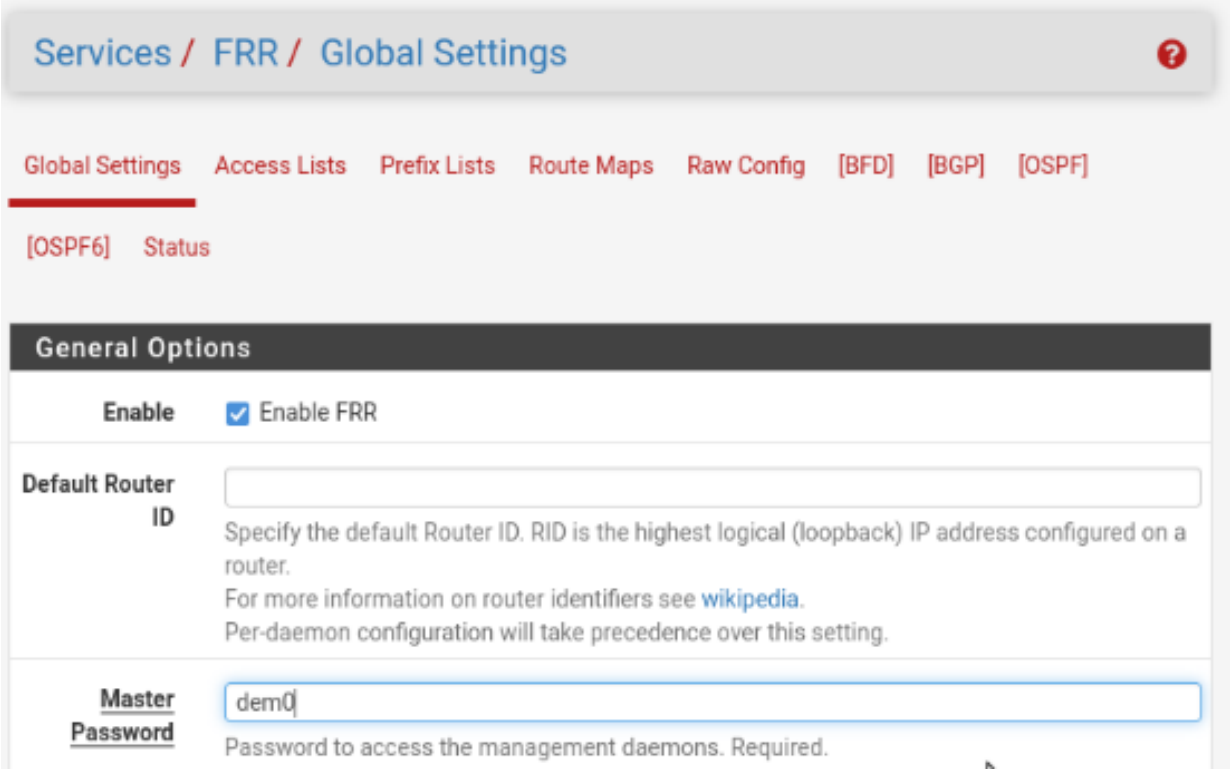
После внесения настроек не забываем нажимать кнопку **Apply changes**.

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:

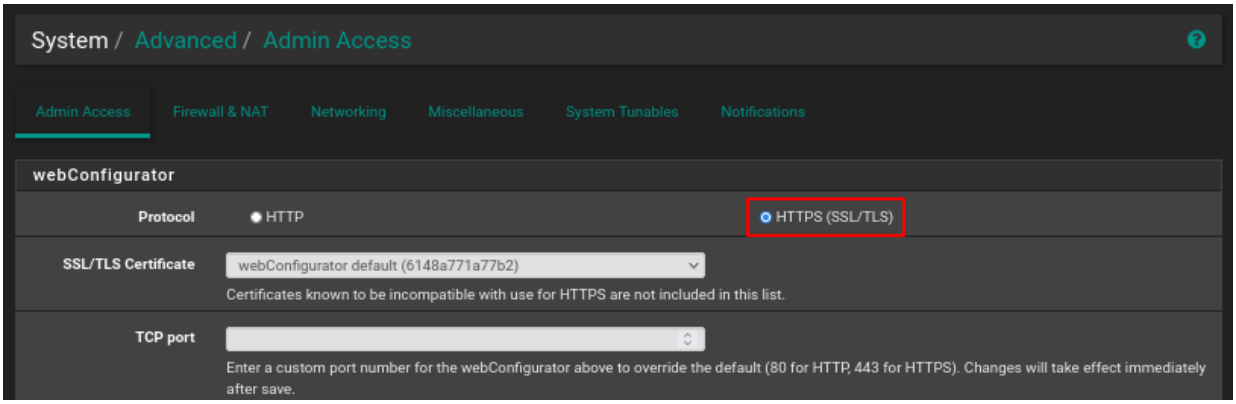


Перед настройкой динамической маршрутизации в Global Settings нужно включить FRR и задать обязательный мастер-пароль:

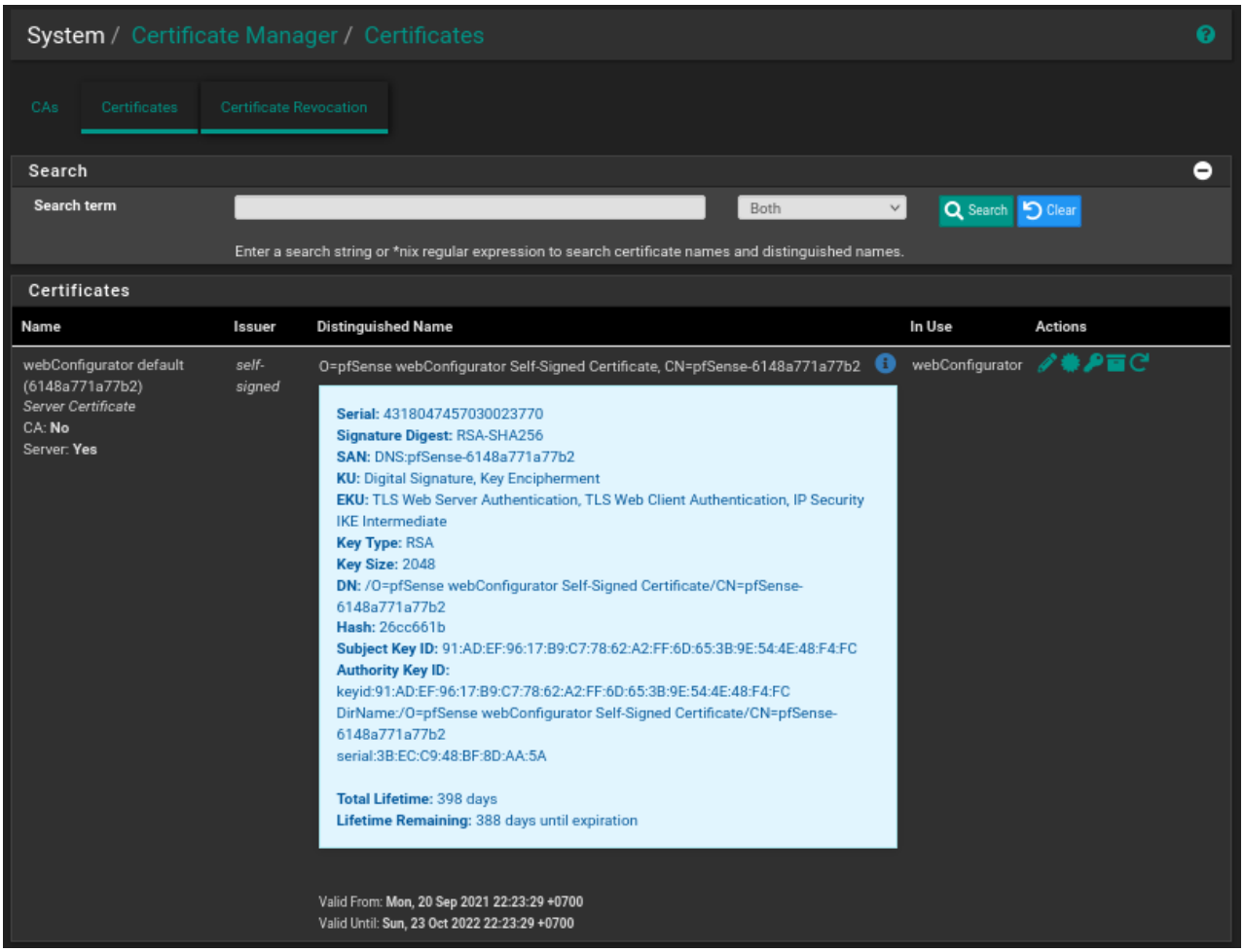


SSL

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



При установке генерируется самоподписанный сертификат на 13 месяцев.

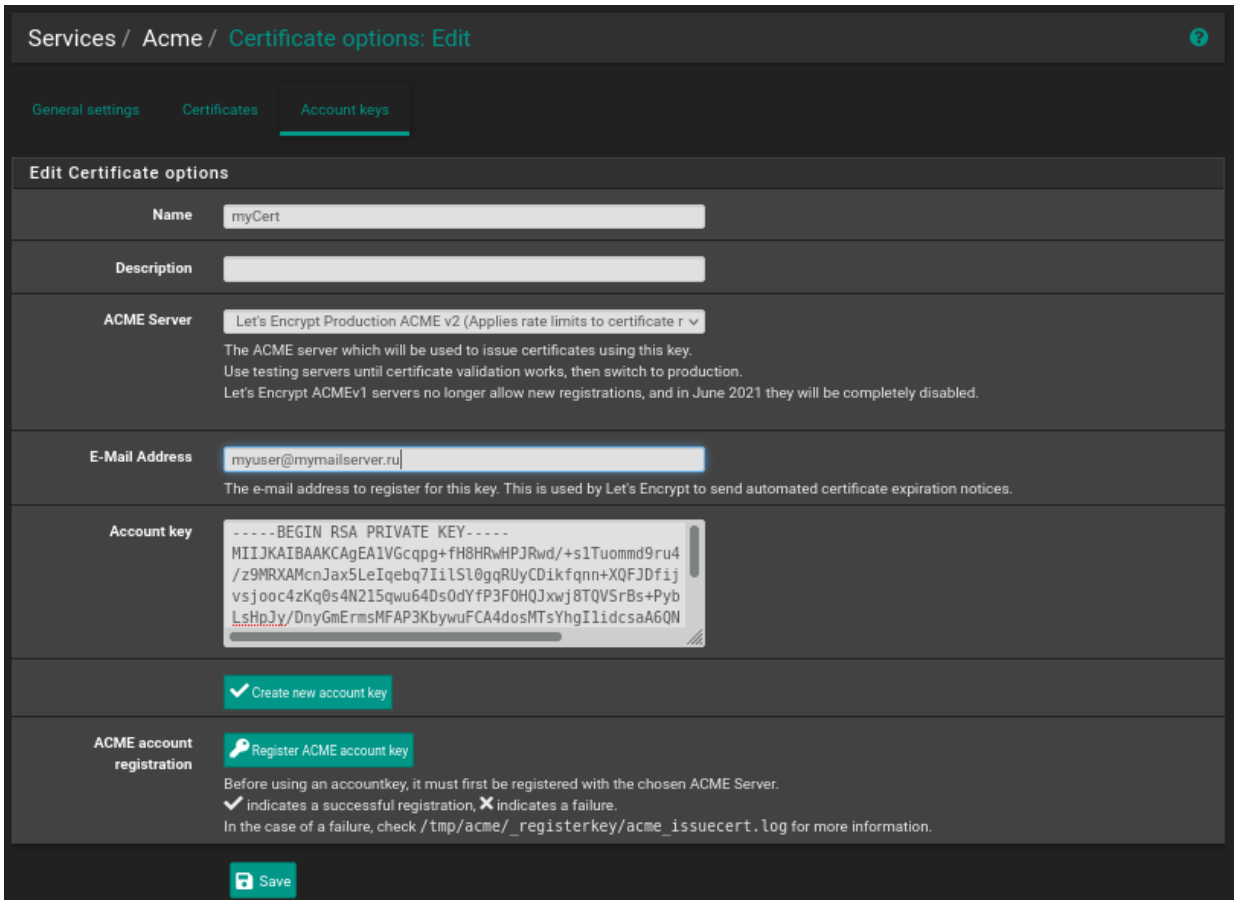


В этом же меню кнопка **Add/Sign** позволяет сформировать запрос к корпоративному центру сертификации и затем установить полученный сертификат, либо перевыпустить самоподписанный сертификат на другой срок.

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 acme:

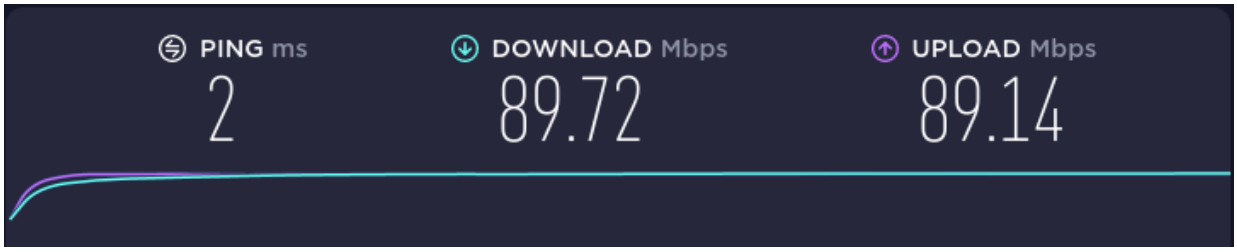


Ограничение полосы

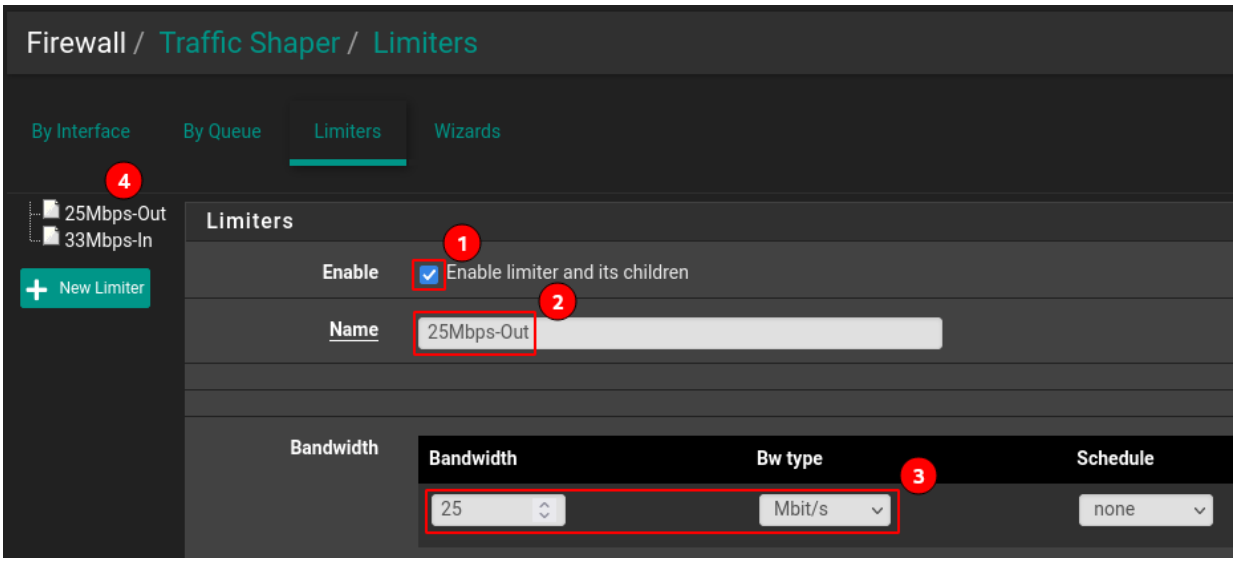
Часто в организации бывают пользователи, которым приходится разрешать неограниченные подключения к интернет-ресурсам. Это чревато забиванием всего канала и затруднением в работе остальных пользователей и сервисов. На помощь придет ограничение ширины канала. Шейпер имеет множество настроек, рассмотрим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

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

Измерим текущую скорость.



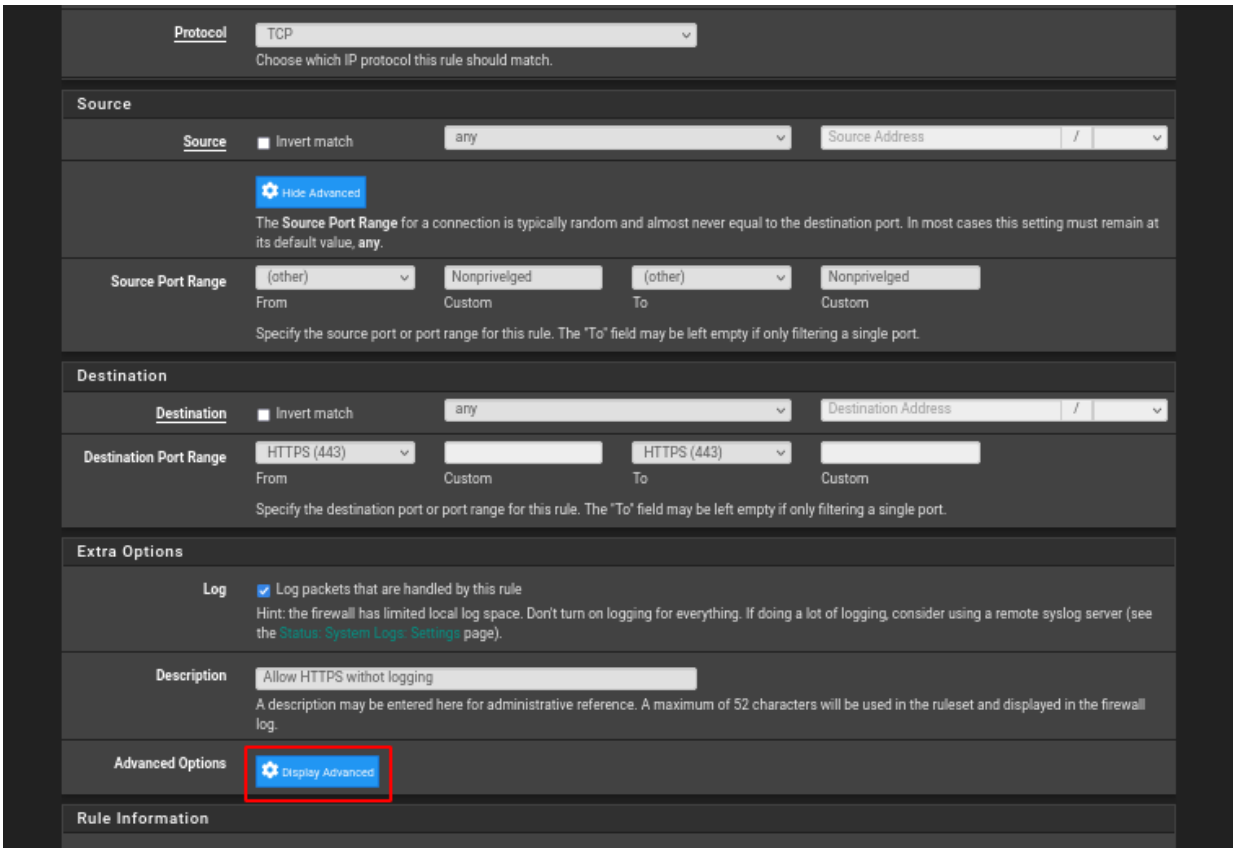
Как указано выше, заходим в пункт Traffic Shapers меню Firewall, переходим на вкладку Limiters и создаем 2 ограничителя.



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

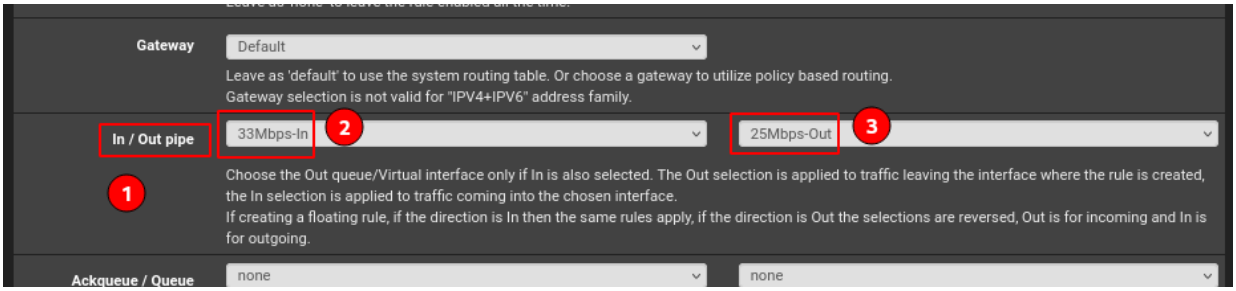
Непосредственное включение шейпера выполняется в правилах брандмауэра (**Firewall →Rules**). Так как нас интересует ограничение со стороны наших внутренних клиентов, правила необходимо модифицировать/добавлять для интерфейса LAN. При этом лимиты рассматриваются со стороны интерфейса: **In** — входящий, **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):



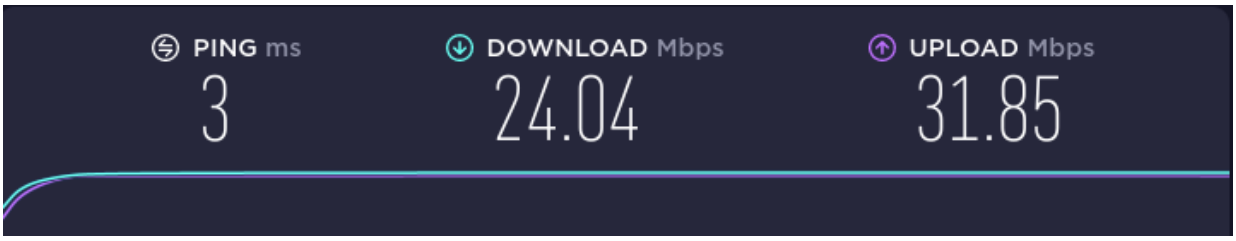
Примечание: в примере на картинке выше использовано существующее правило, разрешающее внутренним клиентам использовать подключение по https.

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.



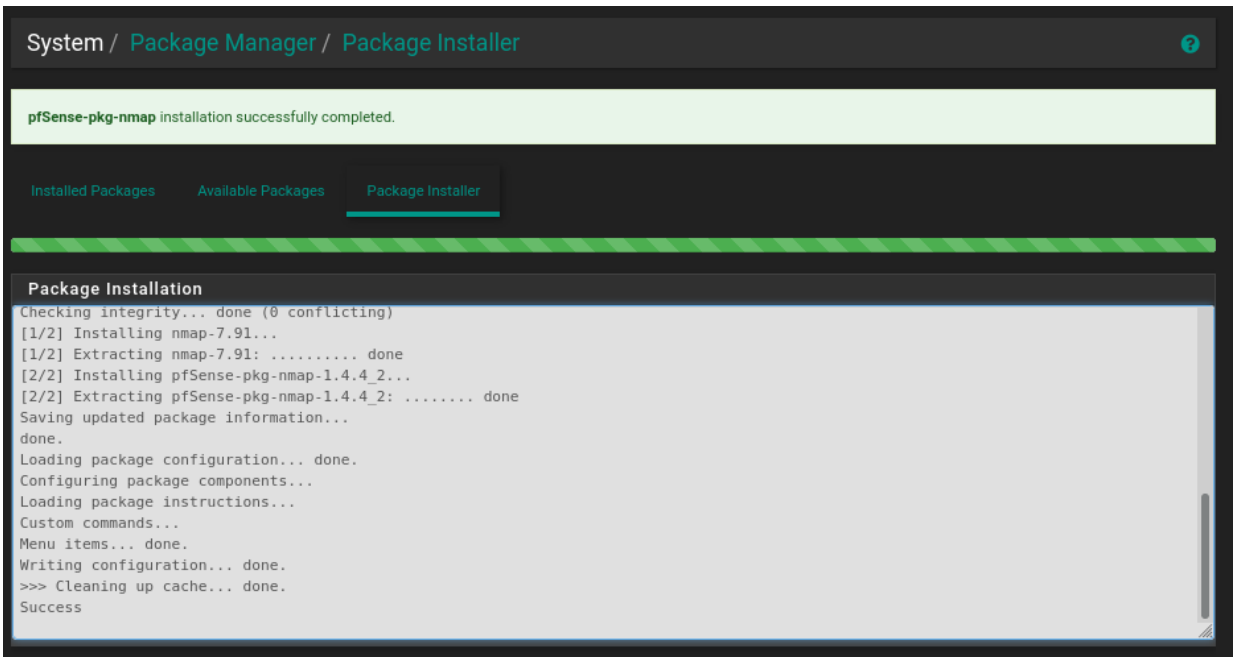
Дополнительные функции

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

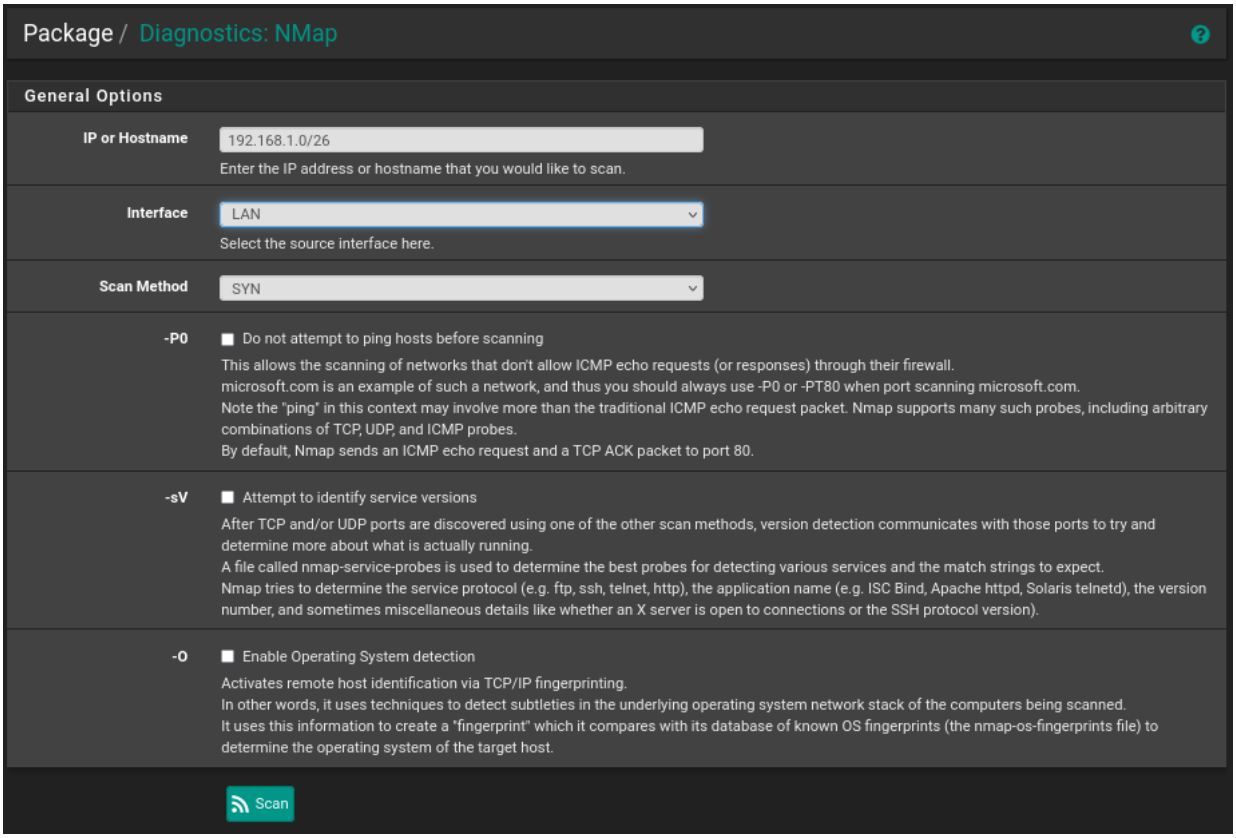
- apcupsd — демон для связи с ИБП APC (ныне Schneider);
- arpwatch — мониторинг активности MAC/IP-адресов;
- cron — планировщик;
- filer — файловый менеджер;
- squid/lightsquid/squidGuard — прокси, генератор отчетов и фильтр;
- lldpd — предоставляет поддержку обнаружения по Link Layer Discovery Protocol, 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.

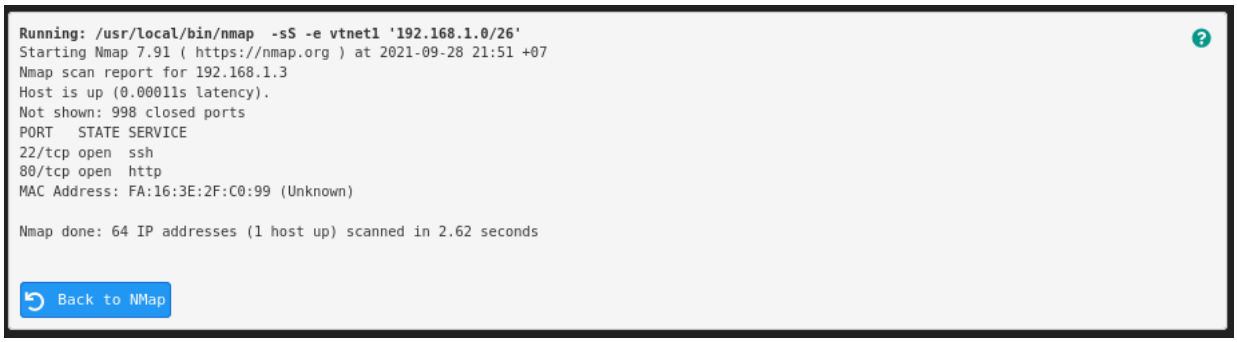
Проведем демонстрацию расширения функциональности на популярном сканере nmap. В меню **System** заходим в пункт **Package Manager**, вкладка **Available Packages**, рядом с пакетом NMap нажимаем на кнопку **Install**, ждем и получаем встроенный сканер:



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



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



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 серверыСетевые технологии