Домашнее задание к занятию 23

*ДЗ на тему «**Настройка безопасных VPN-соединений»:***

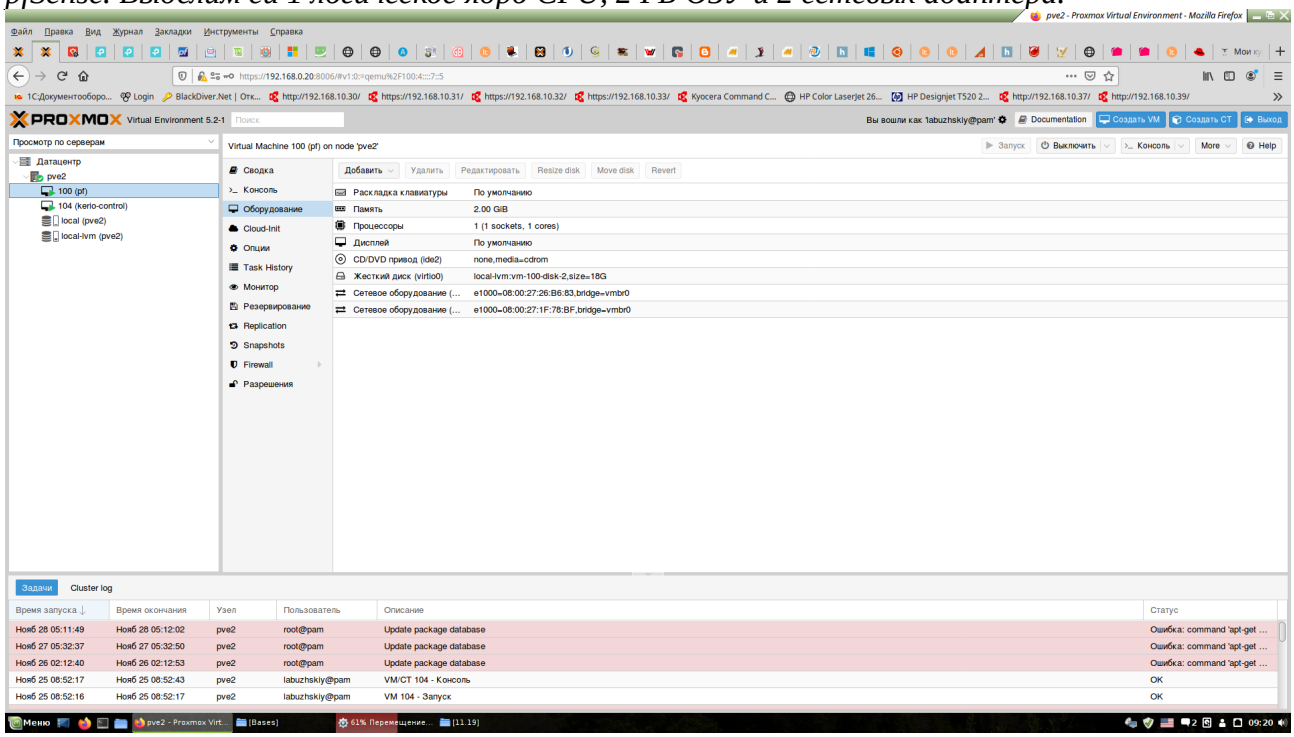
создать несколько VPN-соединений к другим компьютерам на базе Linux, находящихся в другом сегменте сети Интернет, настроить криптографические протоколы защищенного обмена

Цели занятия

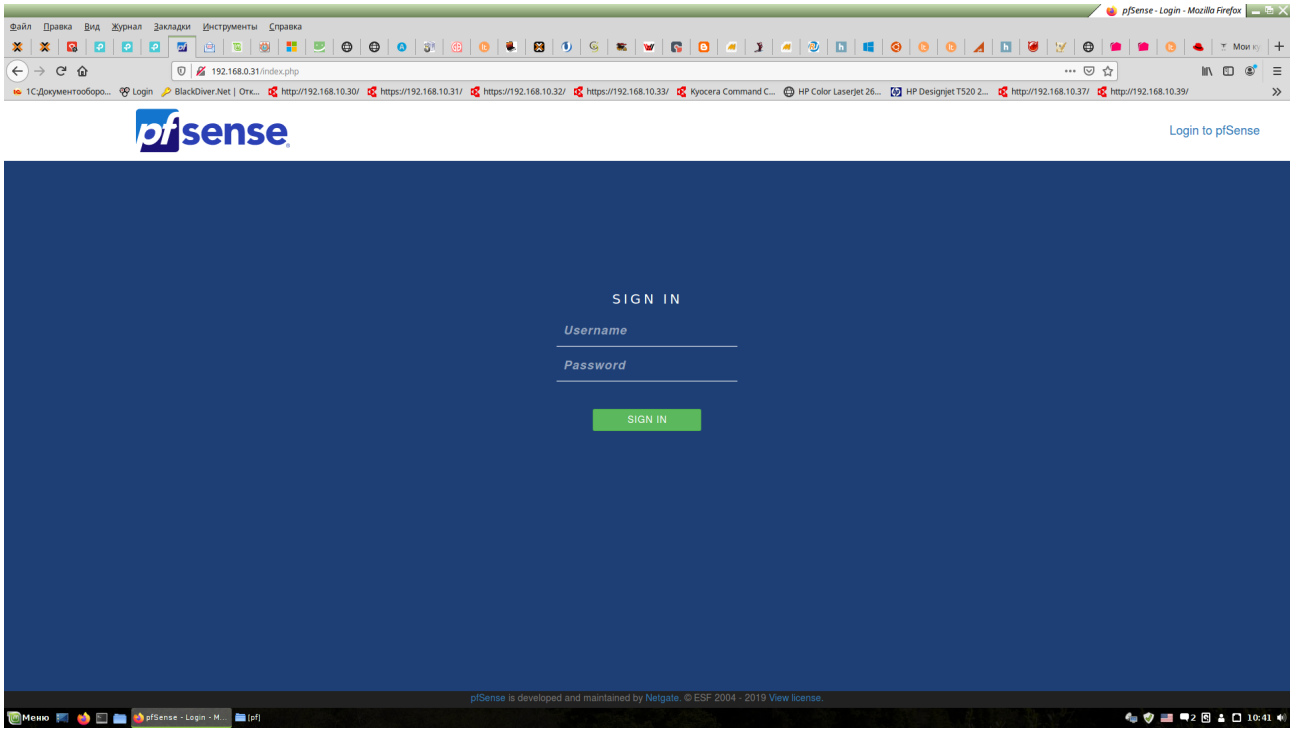
научиться практическим аспектам управления защищенными соединениями (SSH, VPN, VLAN, DMZ-сегментация)

*На мой взгляд, реализация выполнения данного домашнего задания выглядела бы интереснее на базе ОС **pfSense;** разворачивать тестовый стенд предлагаю **в ProxMoxVE.***

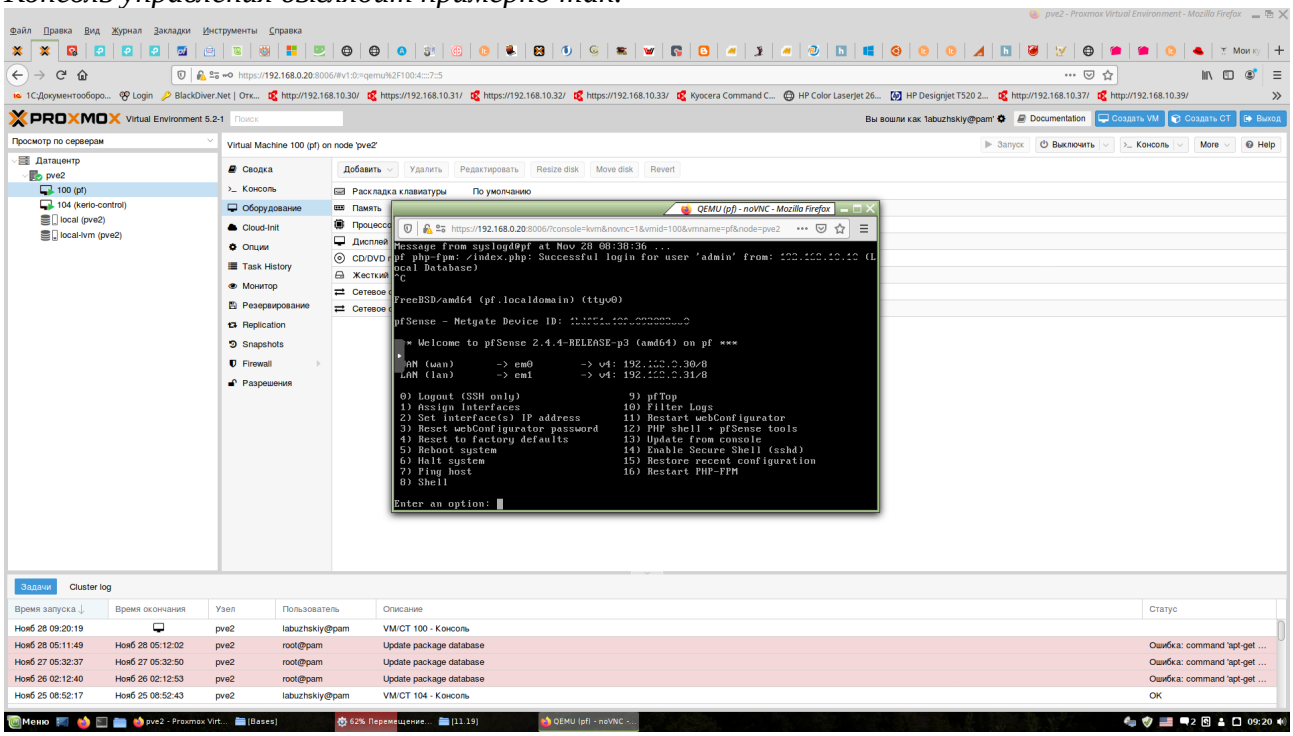
1. Подготовительный этап: создание шаблона VM, в котором произведём развёртывание pfSense. Выделим ей 1 логическое ядро CPU, 2 ГБ ОЗУ и 2 сетевых адаптера.



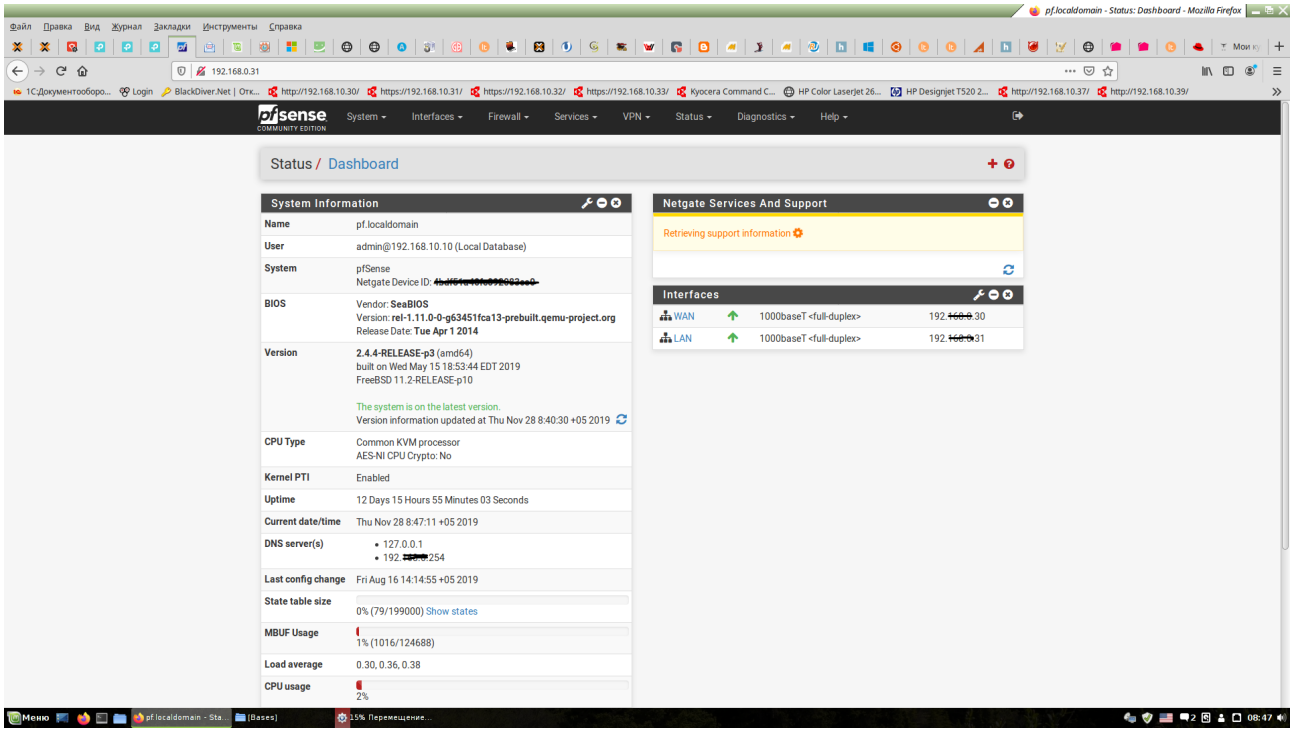
После установки, его можно настраивать в веб-браузере, он имеет приветливый дружественный интерфейс:

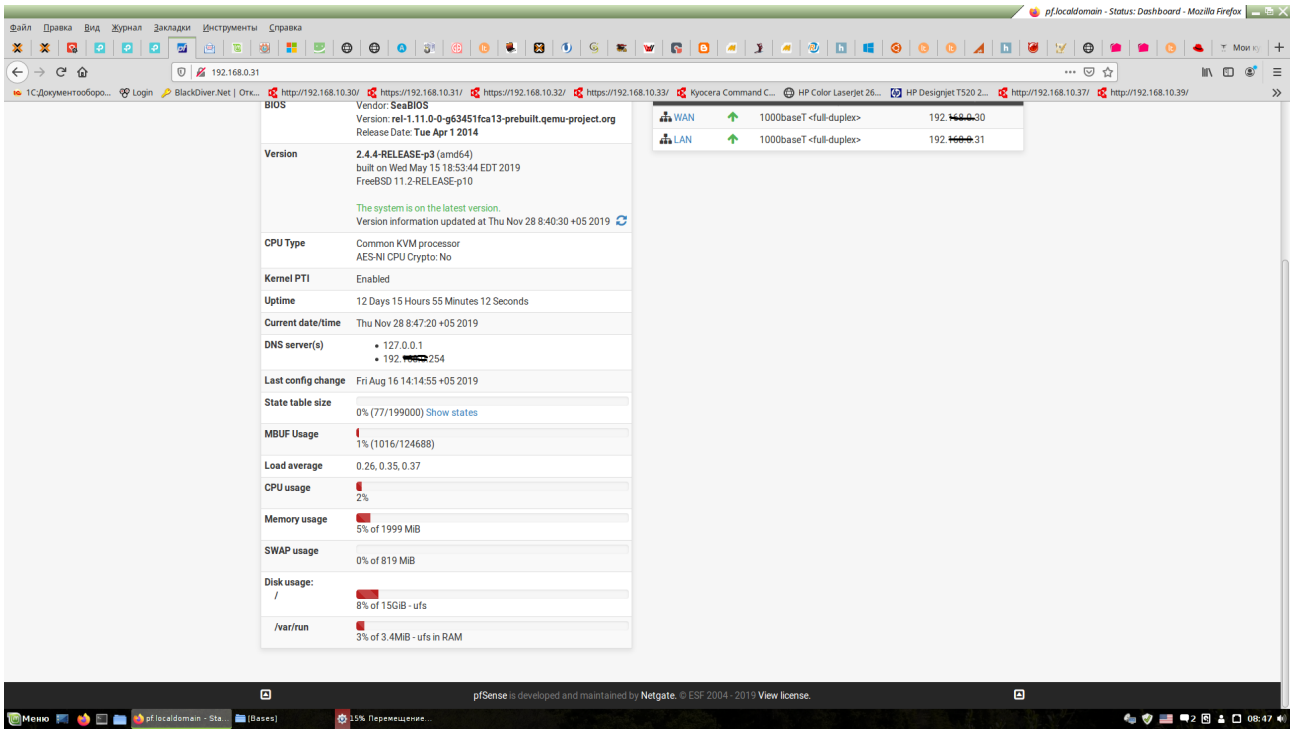


Консоль управления выглядит примерно так:



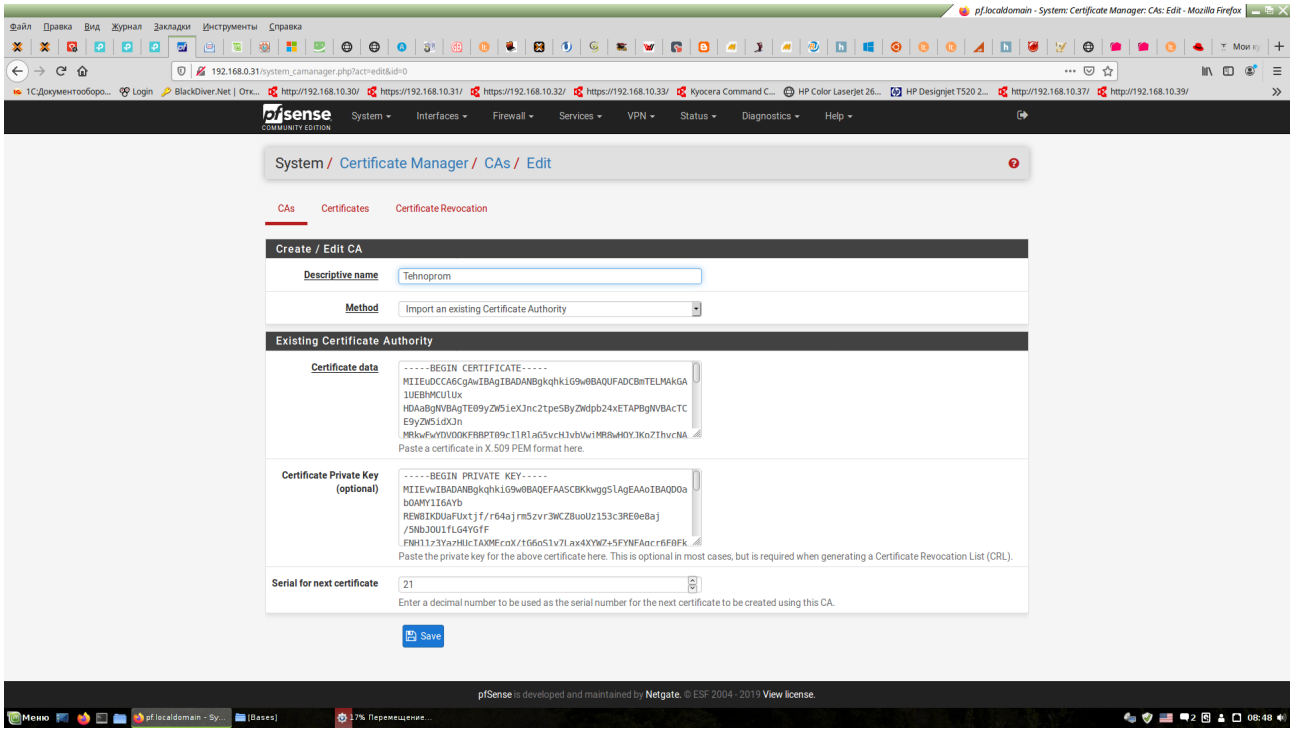
После процедуры аутентификации, попадаем на её главную страницу, которая выглядит так:

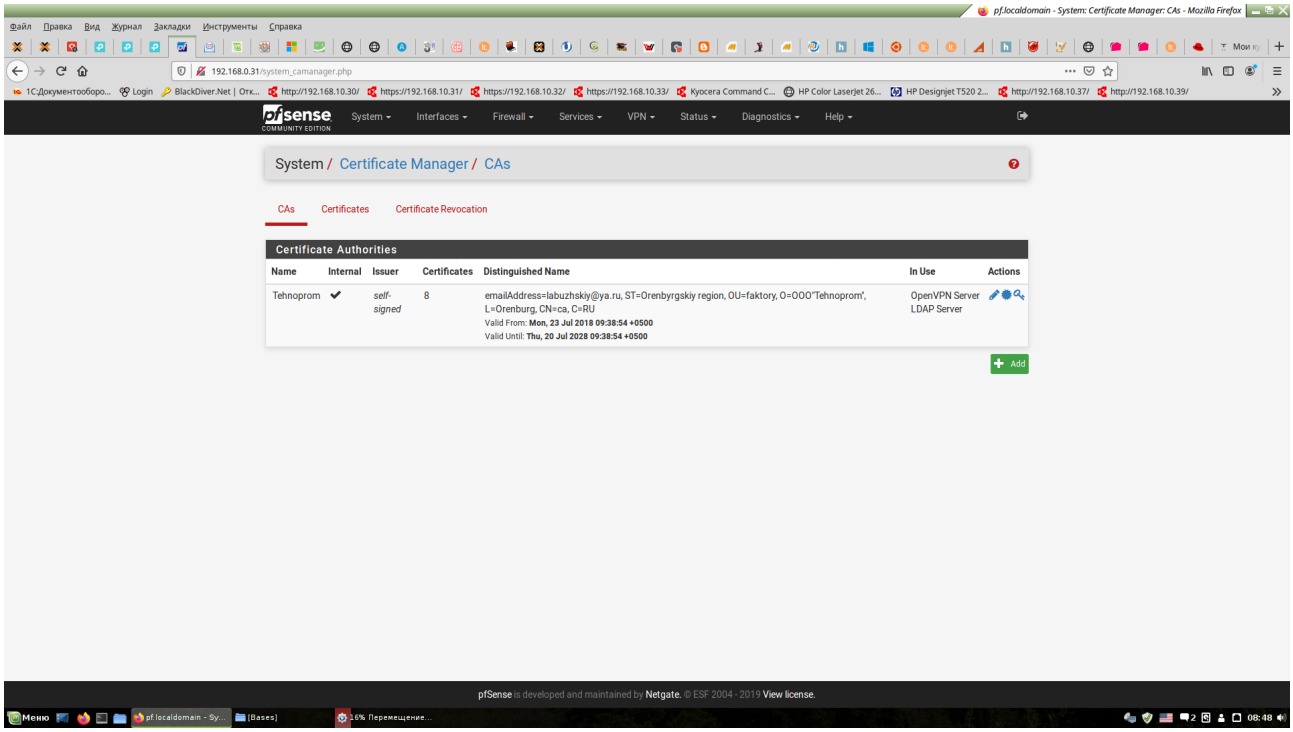




Пробежимся по настройкам нашего сервера:

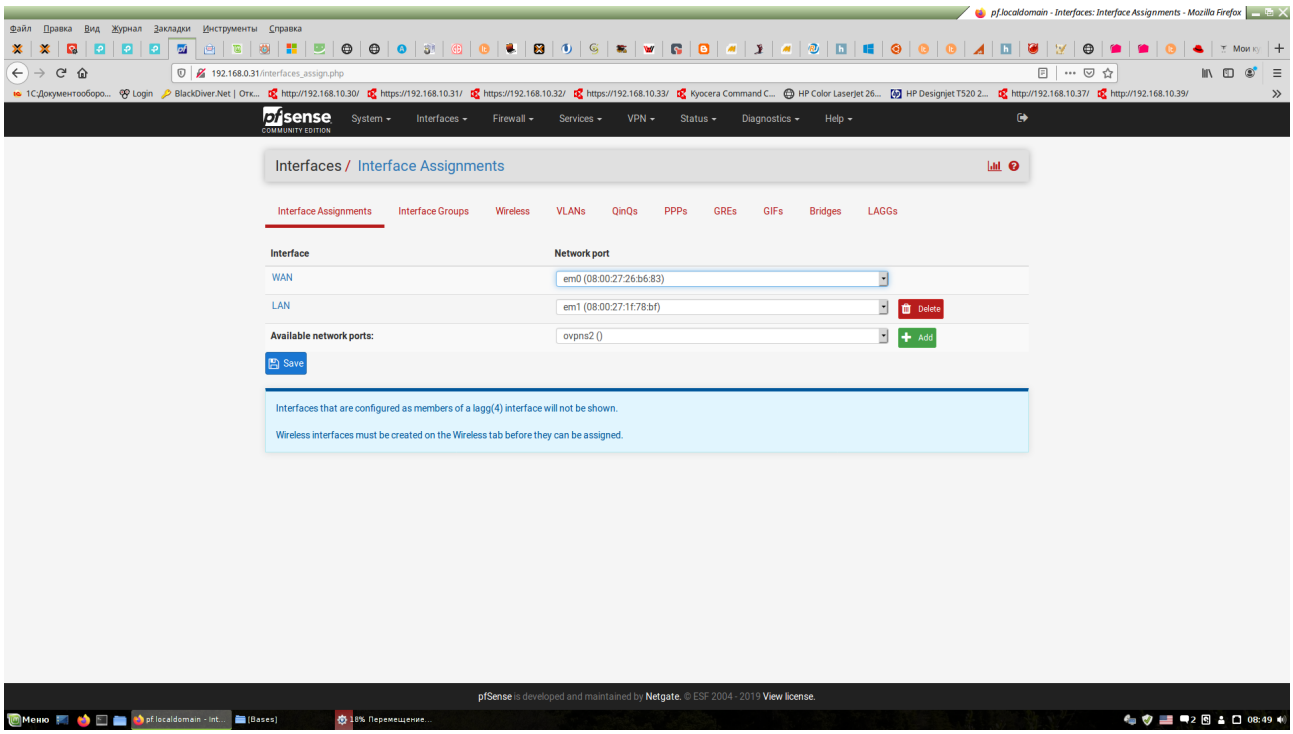
В менеджере сертификатов выполним генерацию нового сертификата сервера

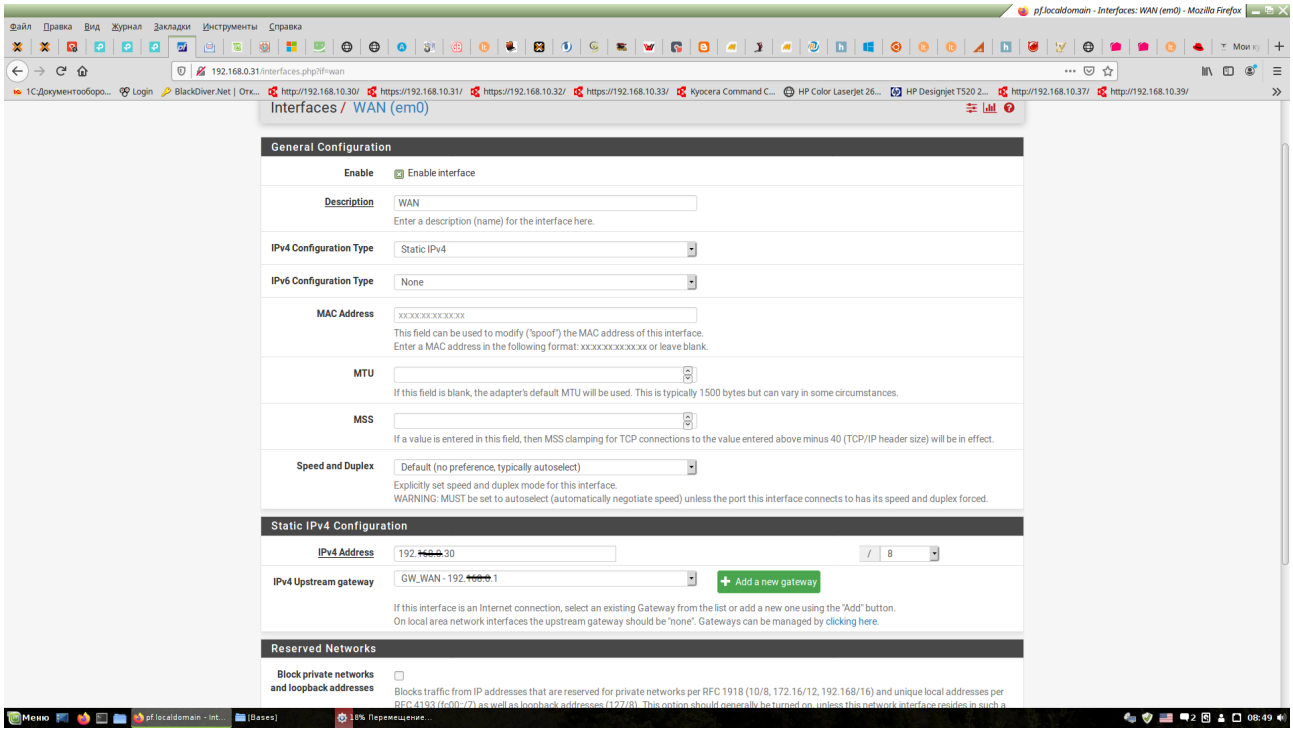


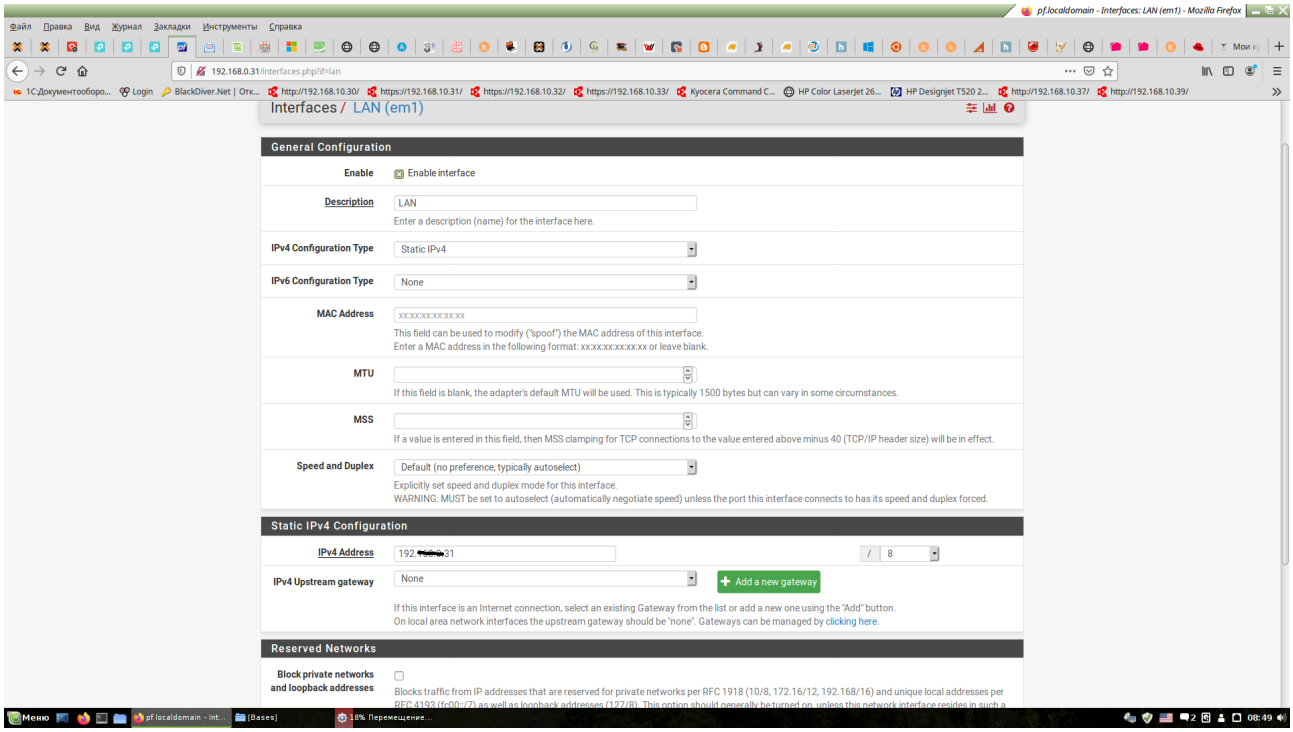


В параметрах сетевых интерфейсов зададим настройки сетевым адаптерам по WAN и LAN

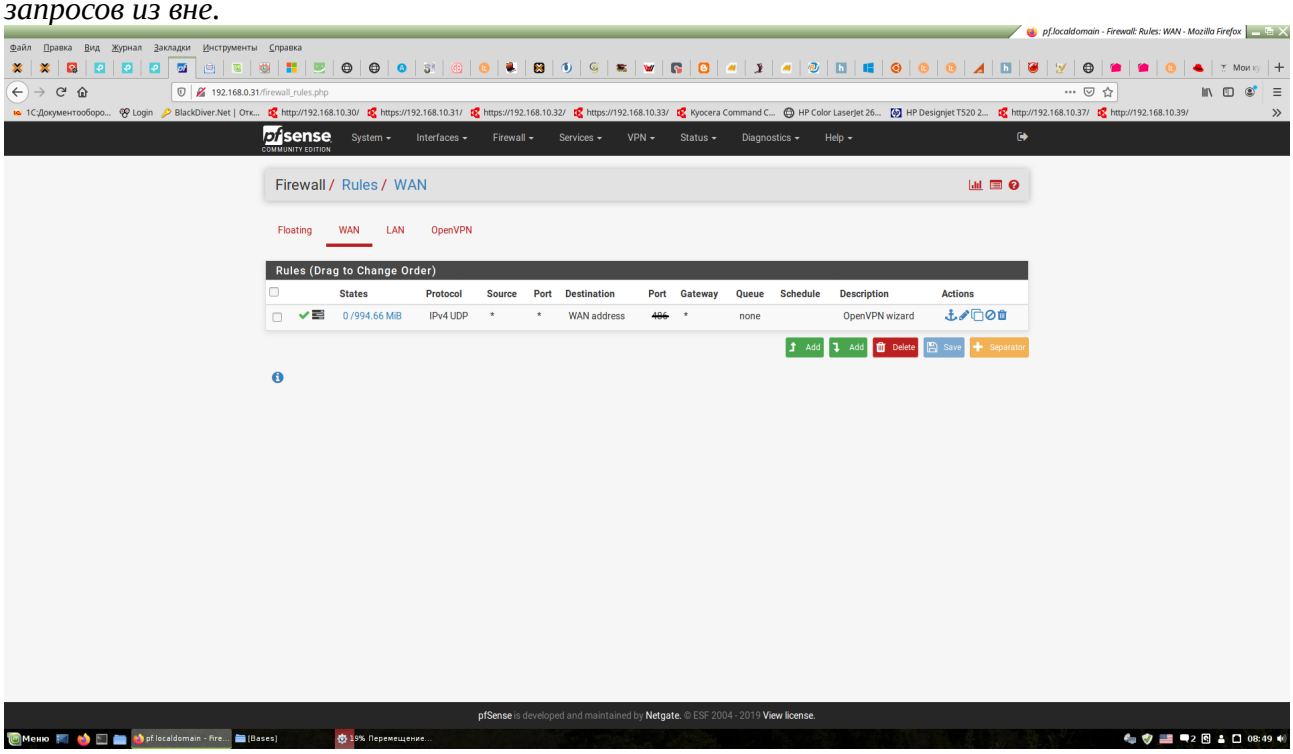
При этом в настройках интерфейса WAN зададим использование шлюза, для доступа в сеть интернет, а в настройках LAN нет. (LAN будем в дальнейшем использовать исключительно для настройки сервера, для доступа в веб-интерфейс через ЛВС, а WAN для взаимодействия с удалёнными клиентами приёма и передачи трафика офтоп рабочих станций). При настройке WAN и LAN выделим из диапазона 2 рядом стоящих ip-адреса.

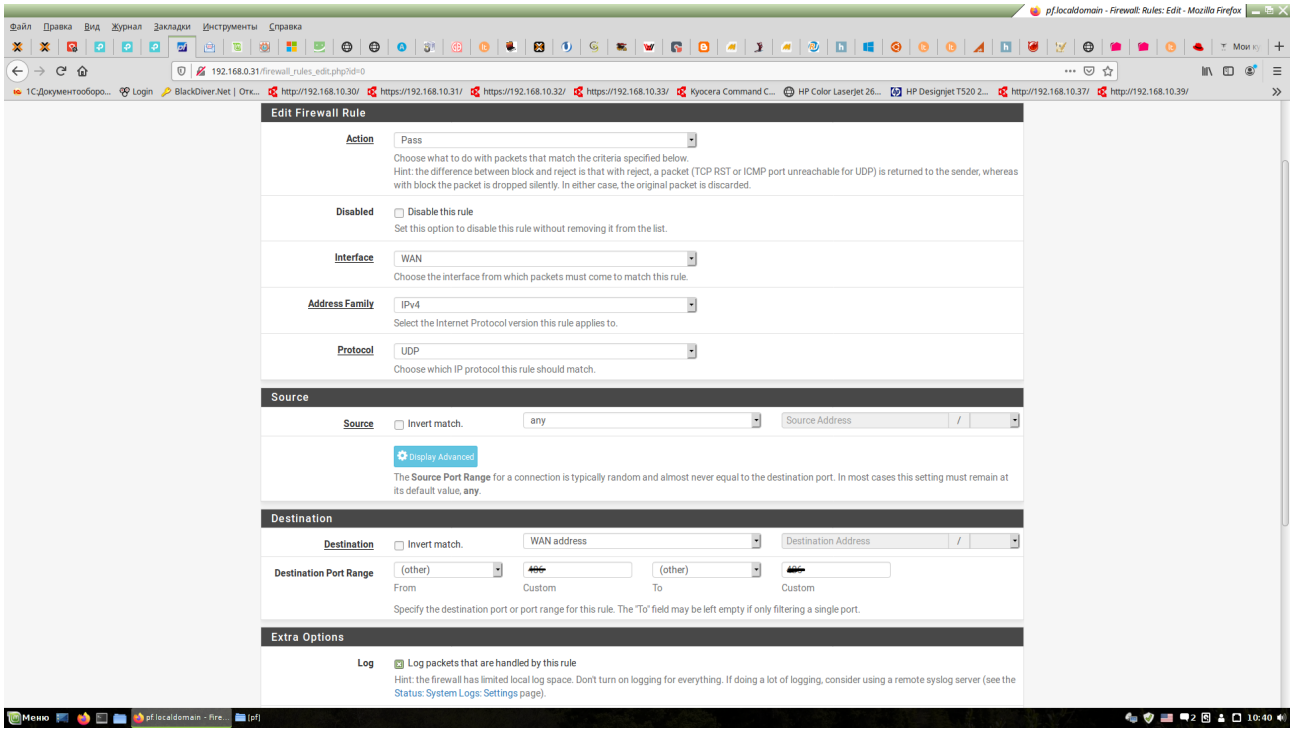

pf.localdomain - Interfaces: Interface Assignments - Mozilla Firefox
192.168.0.31/interfaces_assign.php
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / Interface Assignments
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (08:00:27:26:b6:83)
LAN
em1 (08:00:27:1f:78:bf)
Delete
Available network ports:
ovpns2 ()
Add
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.
pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.


pf.localdomain - Interfaces: WAN (em0) - Mozilla Firefox
192.168.0.31/interfaces.php?if=wan
Interfaces / WAN (em0)
General Configuration
Enable
Enable interface
Description
WAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.0.30
/ 8
IPv4 Upstream gateway
GW_WAN - 192.168.0.1
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a

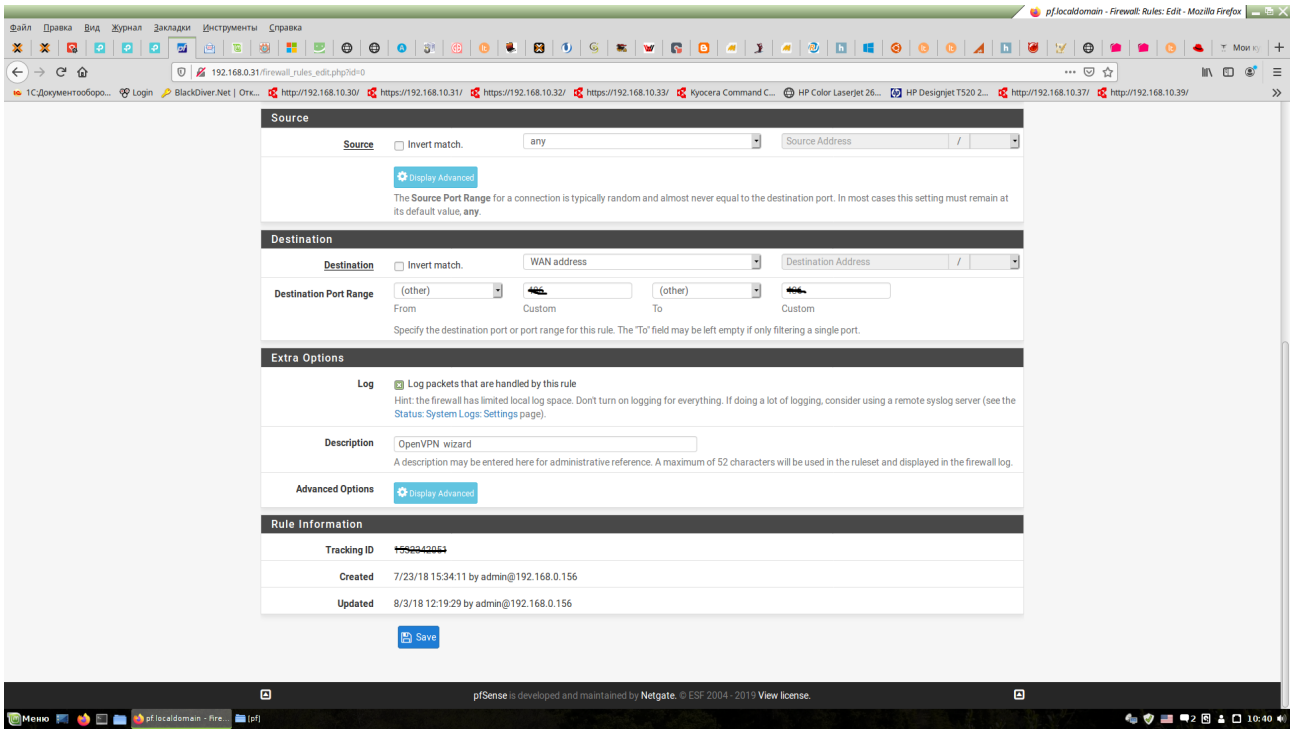


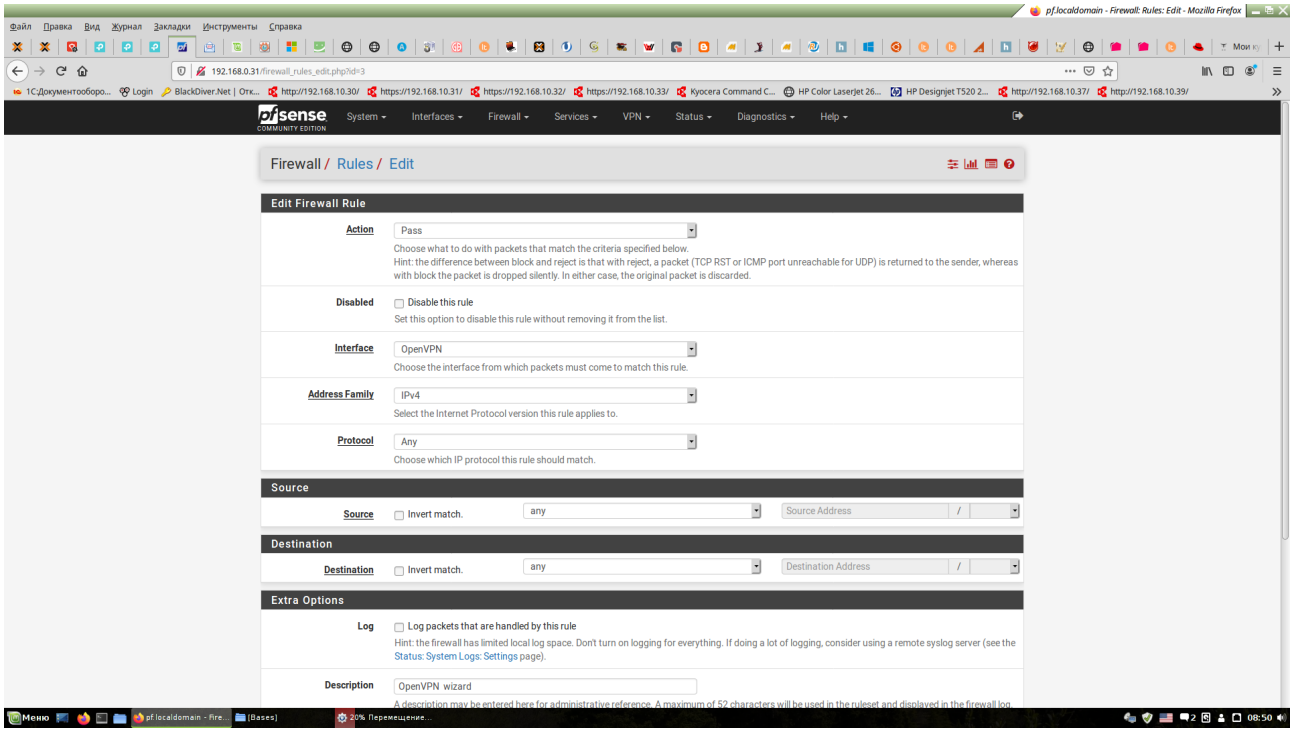
Далее выполним настройку файервола для внешнего порта, который назначим на приём запросов из вне.

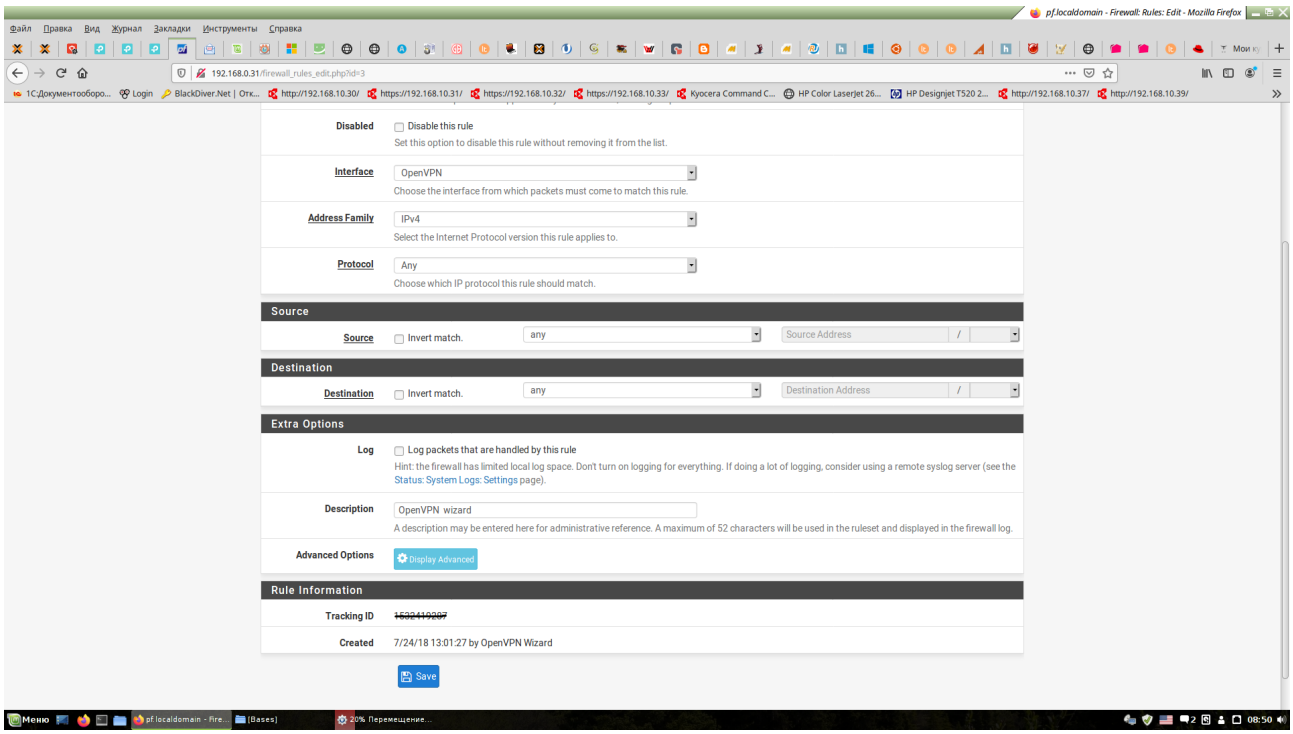


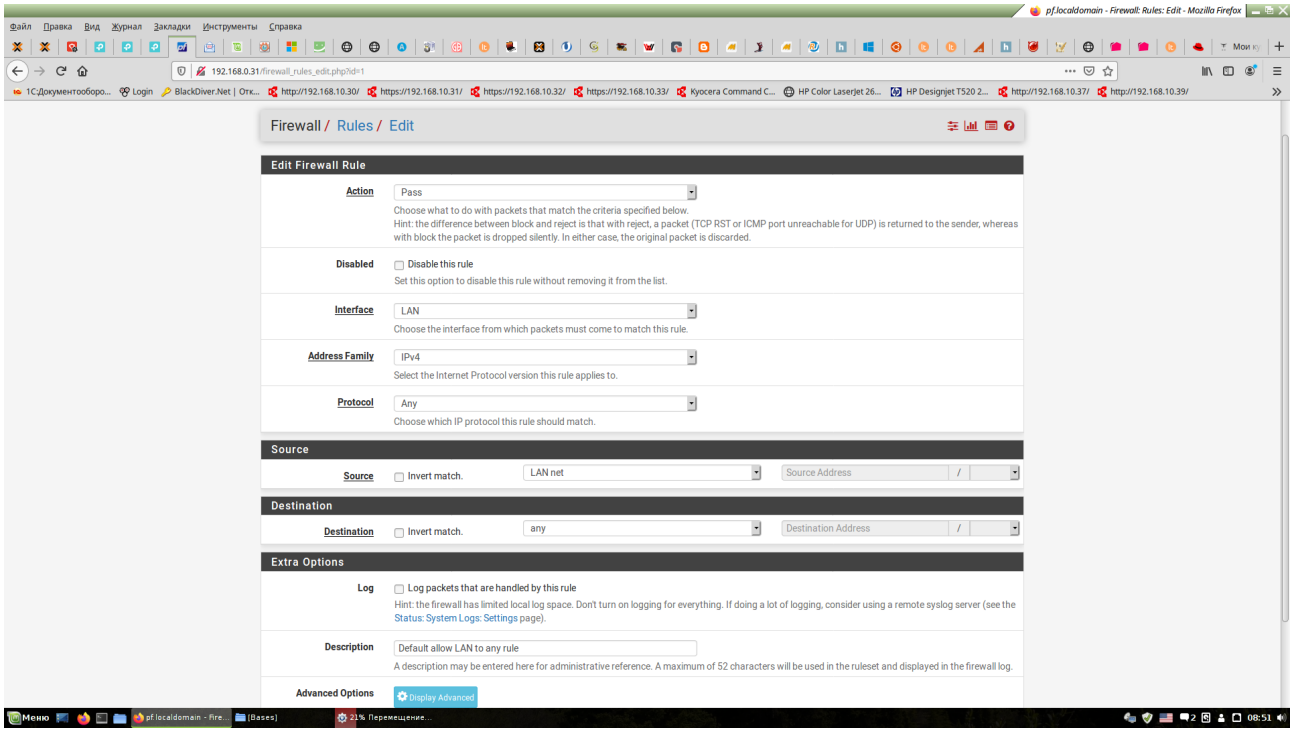


Не забываем сохраняться, внизу присутствует синяя кнопка «Save»

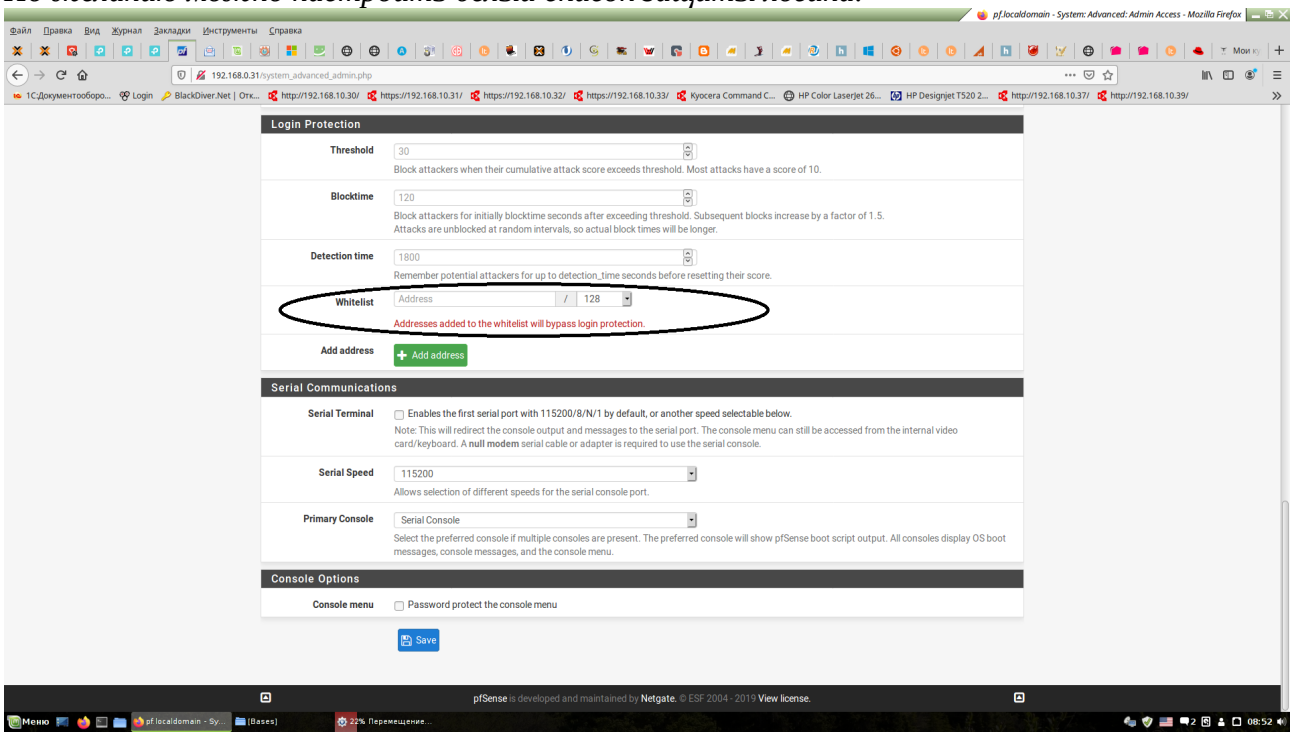



pf.localdomain - Firewall: Rules: Edit - Mozilla Firefox
192.168.0.31/firewall_rules_edit.php?id=3
pfSense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified 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
OpenVPN
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
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match.
any
Source Address
Destination
Destination
Invert match.
any
Destination Address
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
OpenVPN wizard
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.

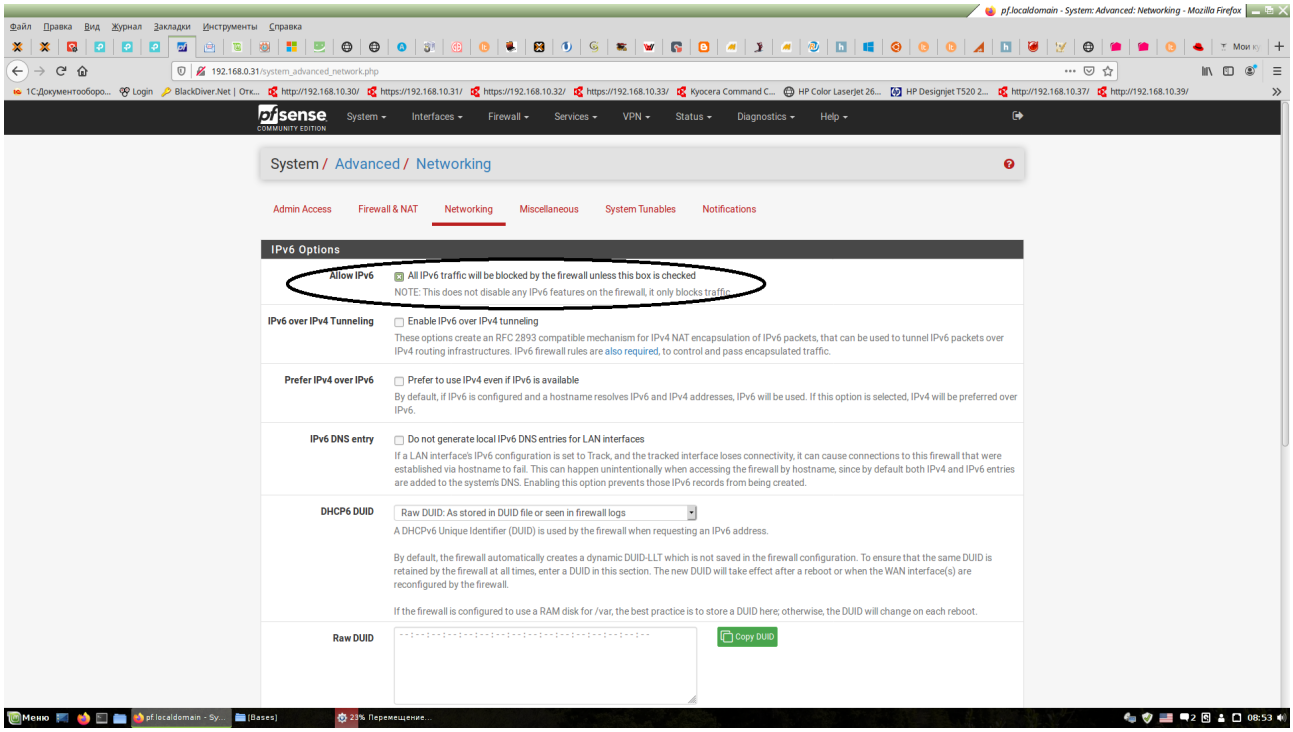

pf.localdomain - Firewall: Rules: Edit - Mozilla Firefox
192.168.0.31/firewall_rules_edit.php?id=3
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
OpenVPN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match.
any
Source Address
Destination
Destination
Invert match.
any
Destination Address
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
OpenVPN wizard
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
Rule Information
Tracking ID
1532419287
Created
7/24/18 13:01:27 by OpenVPN Wizard
Save



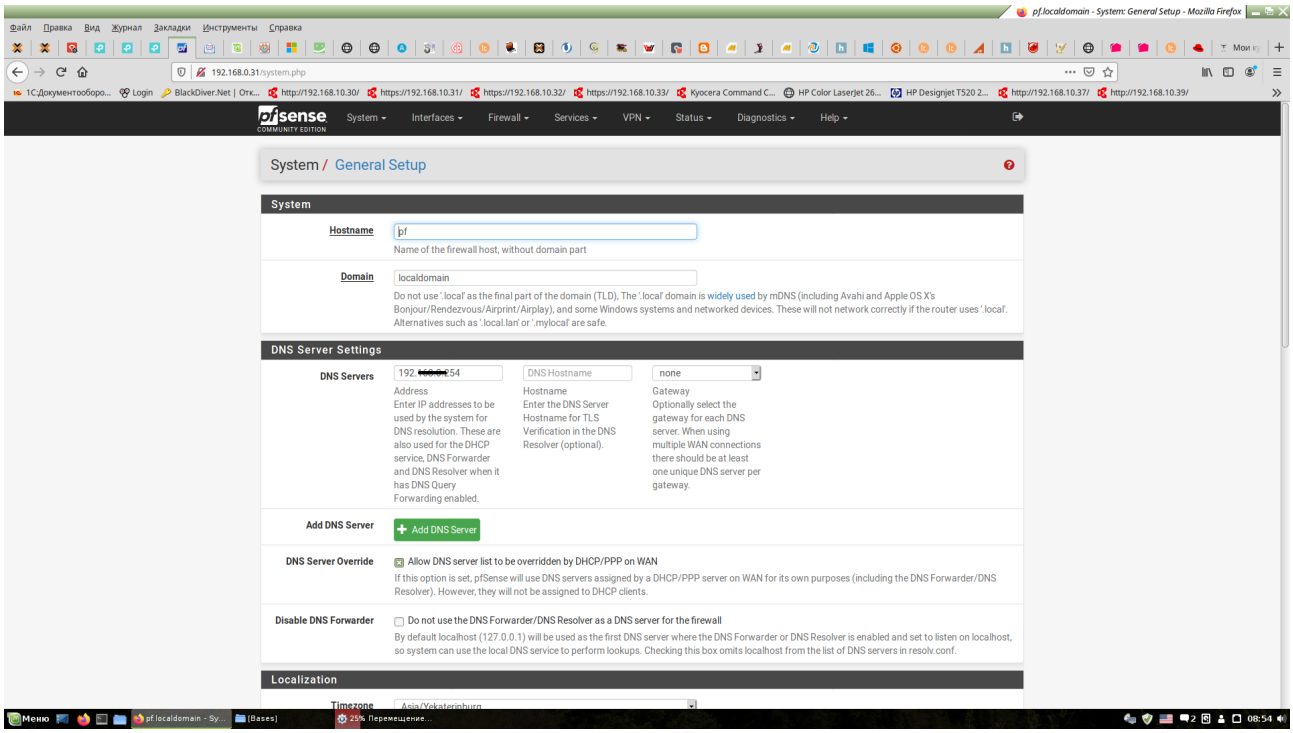
По желанию можно настроить белый список защиты логина.



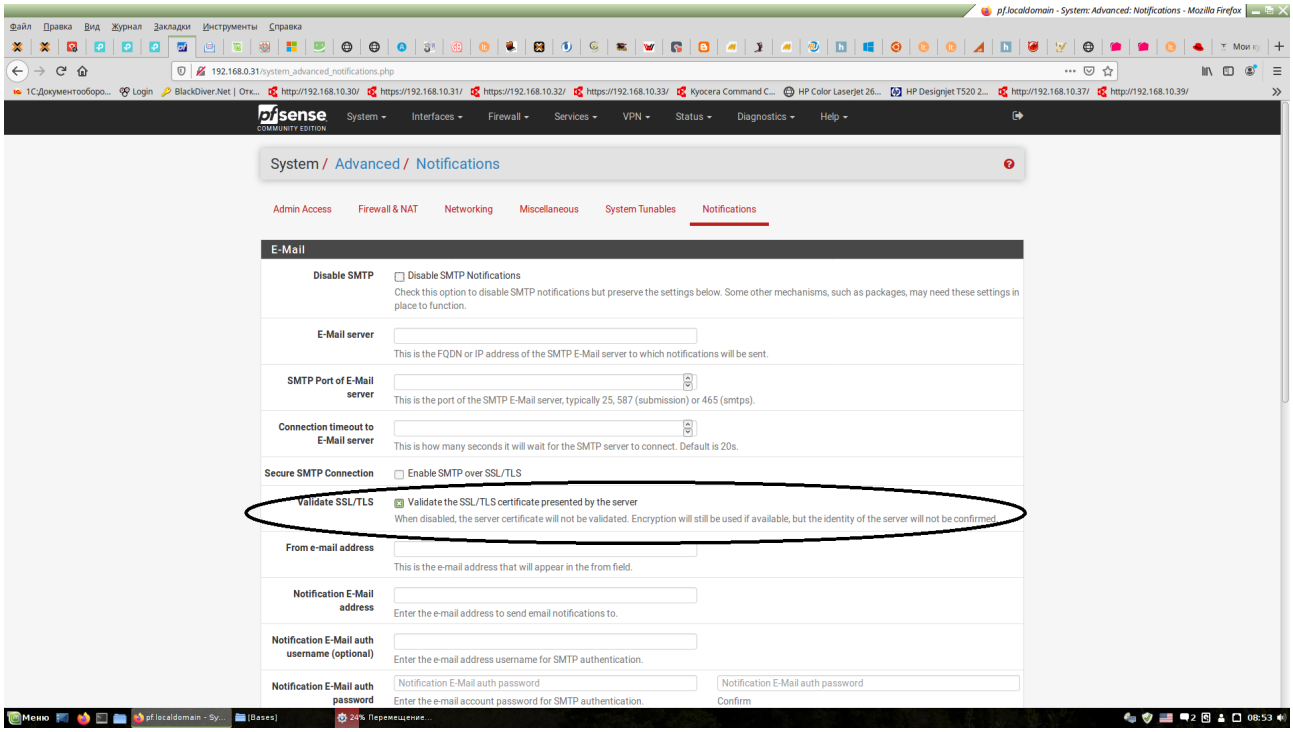
Так же по желанию можно выполнять блокировку трафика по протоколу ipv6, при этом, блокируя трафик по протоколу, сам протокол по прежнему остаётся включенным.



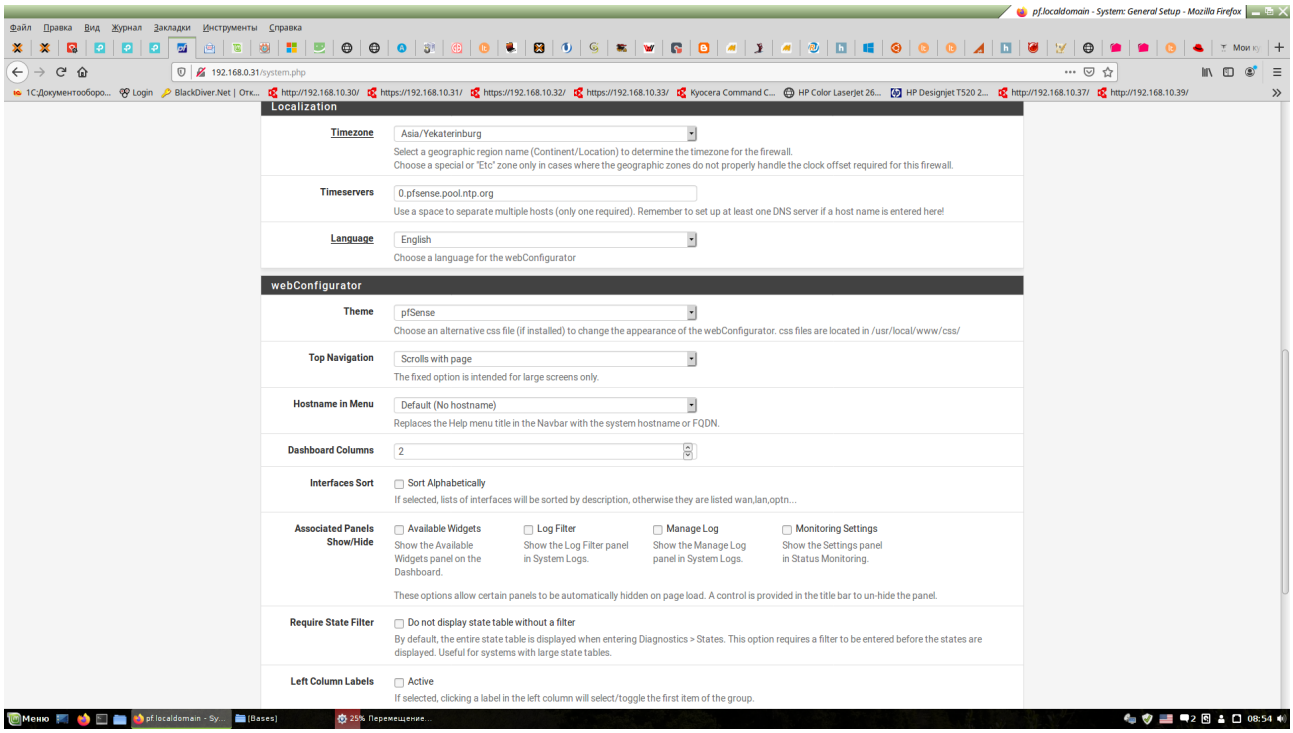
Далее настраиваем имя хоста, его домен и DNS:



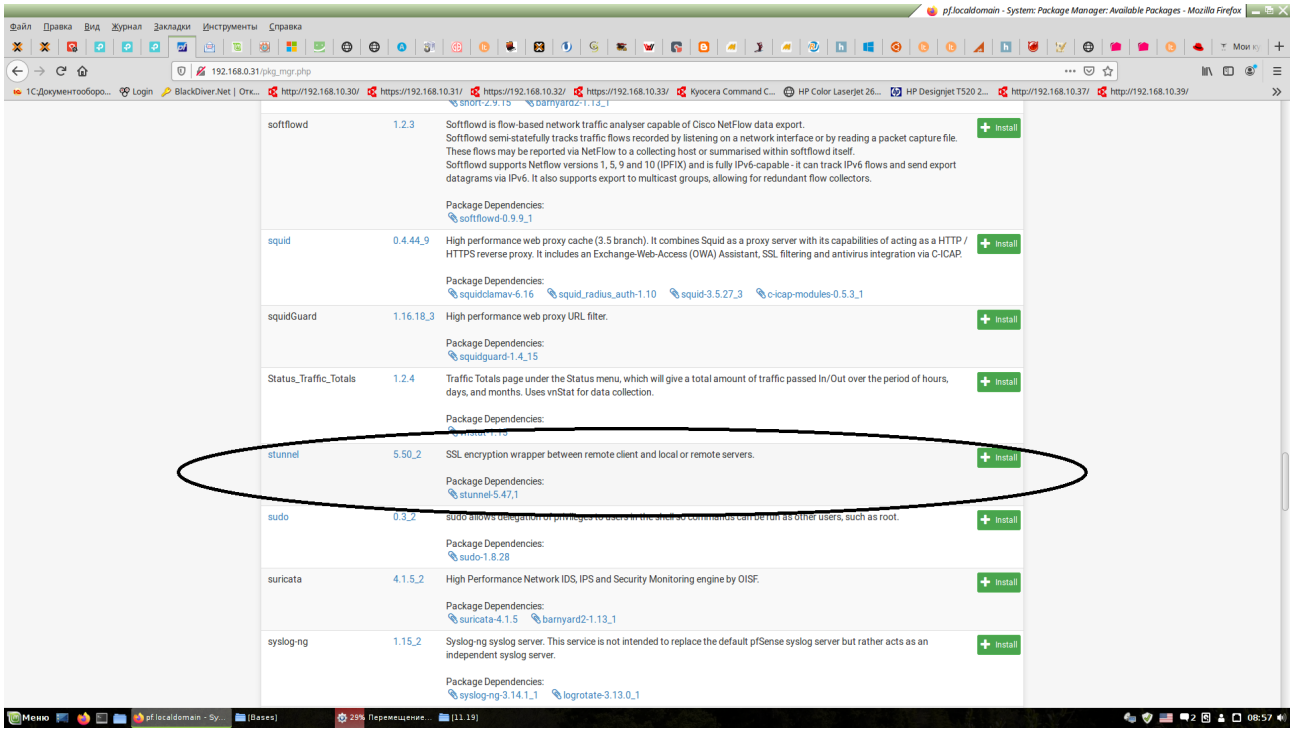
Разрешаем проверку валидности сертификата:

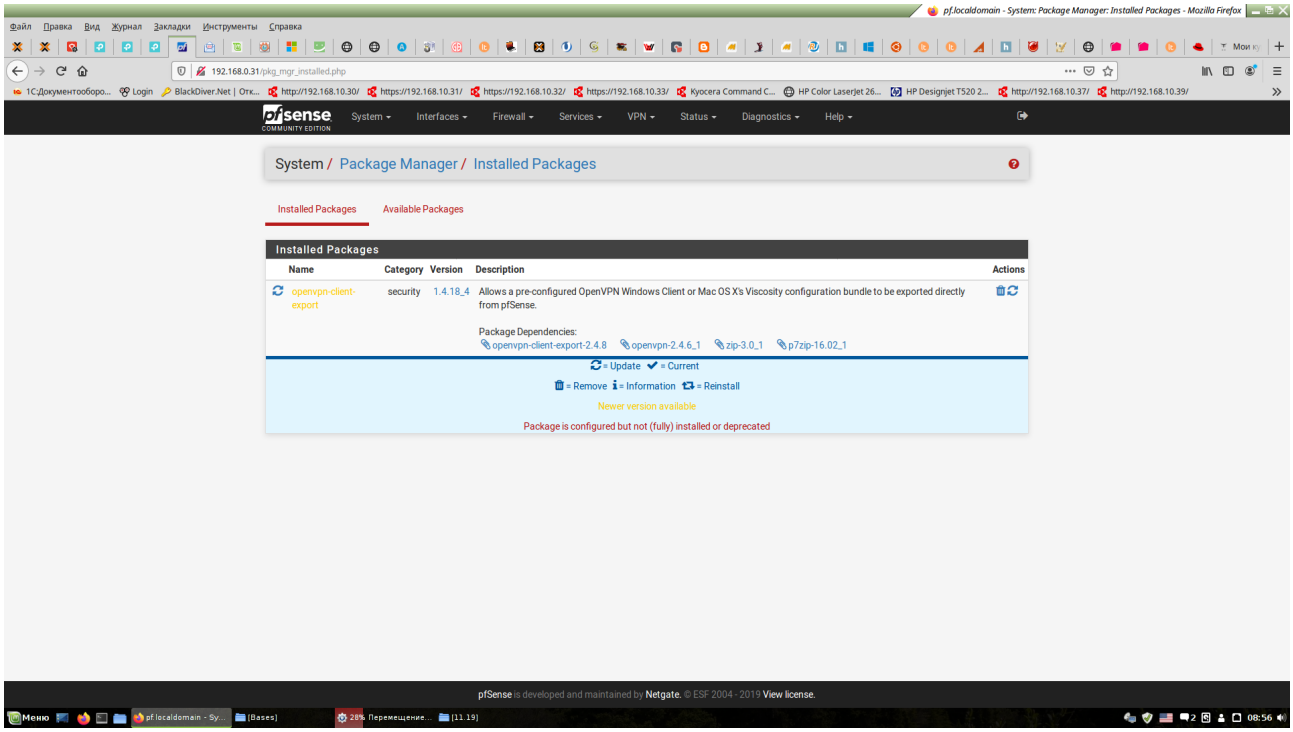


Проверяем настройки системы:

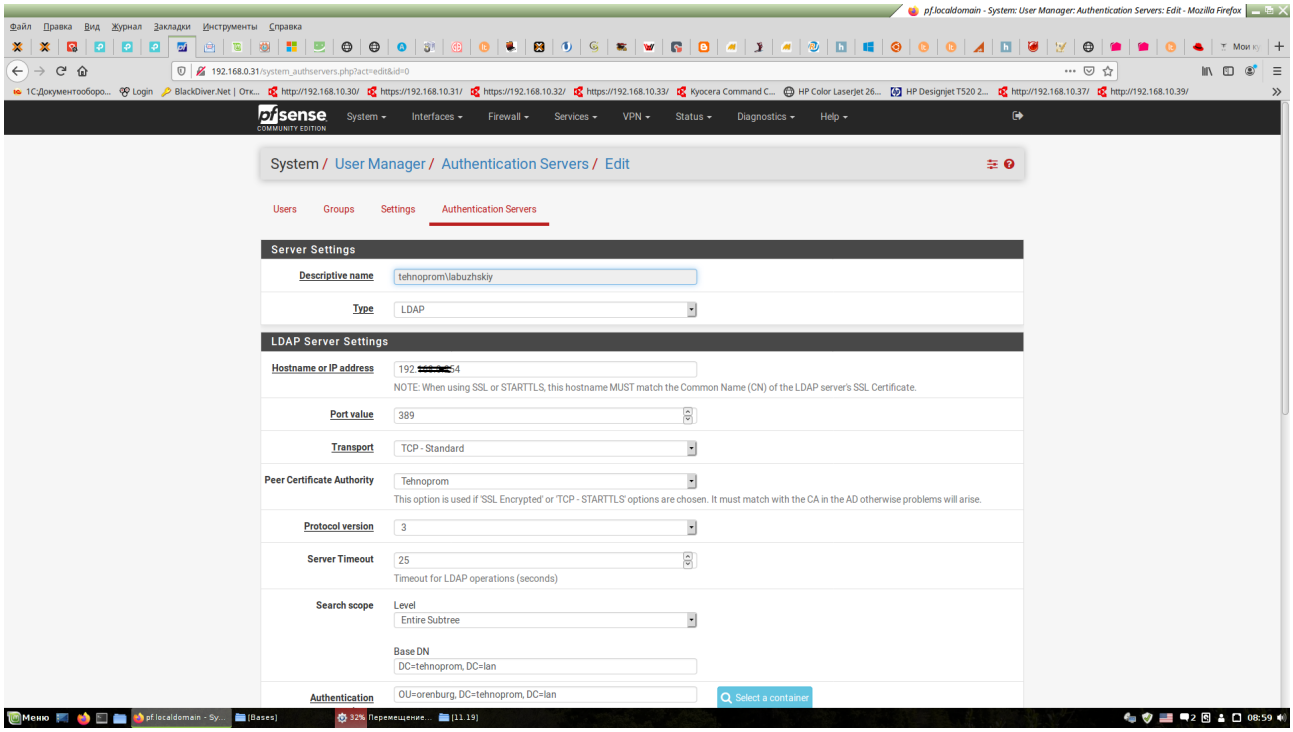


В менеджере пакетов можно рассмотреть перечень доступных (среди них, кстати, присутствует stunnel, способный маскировать и шифровать OpenVPN под https). Устанавлвается банальным нажатием кнопки Install, но в текущиу момент это не сама суть вопроса, поскольку нам потребуется другой пакет для экспорта настроек клиентов: нам нужен OpenVPN-client-export.

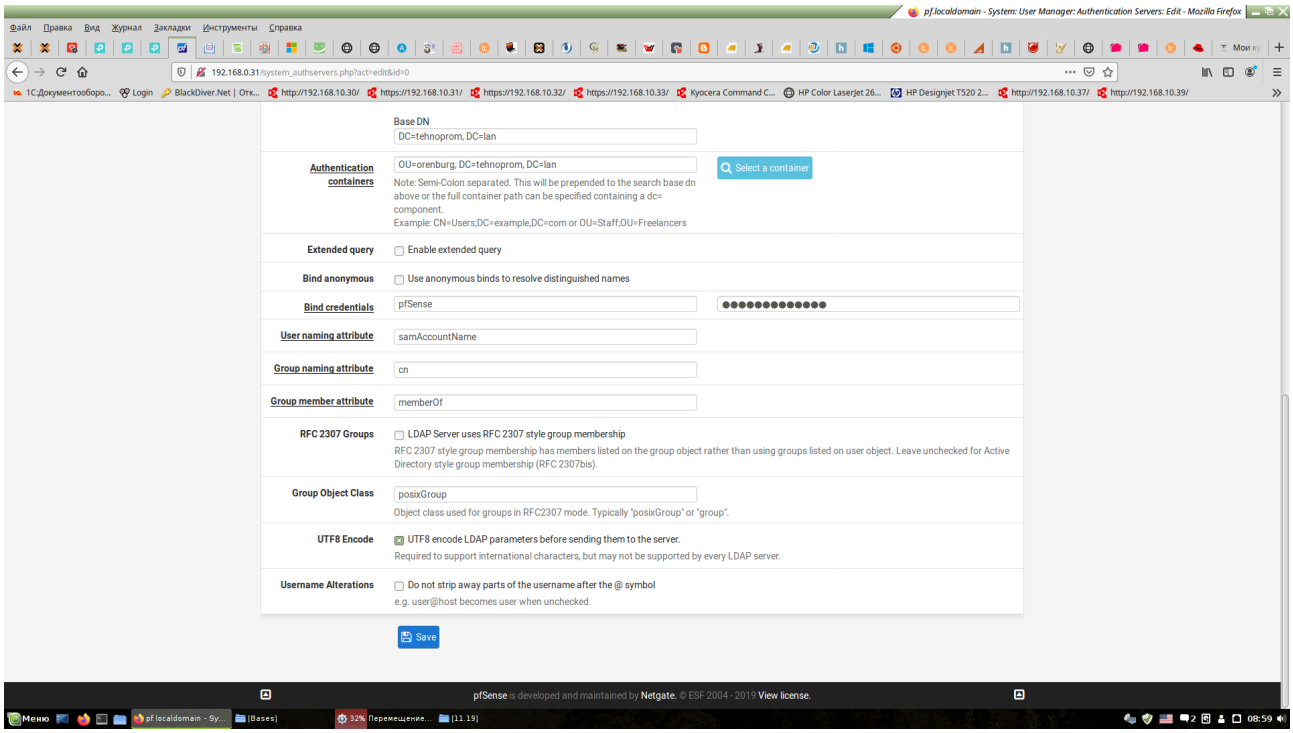




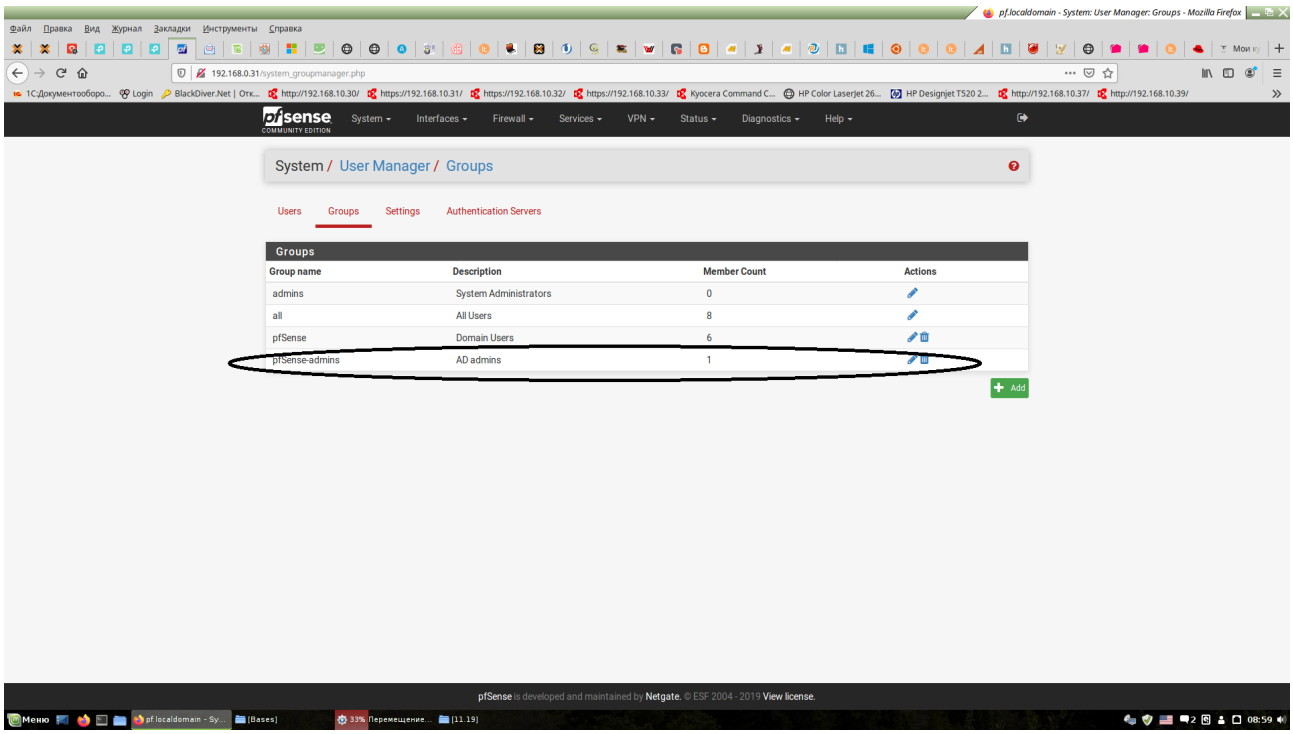
Далее выставляем параметры AD, тип аутентификации LDAP, открываем на контролере домена tcp-порт 389, если закрыт, создаём группу пользователей pfSense, на которую деллигируем полномочия администратора, нажимает на кнопку Select a container, и вабираем наши DC и OU.



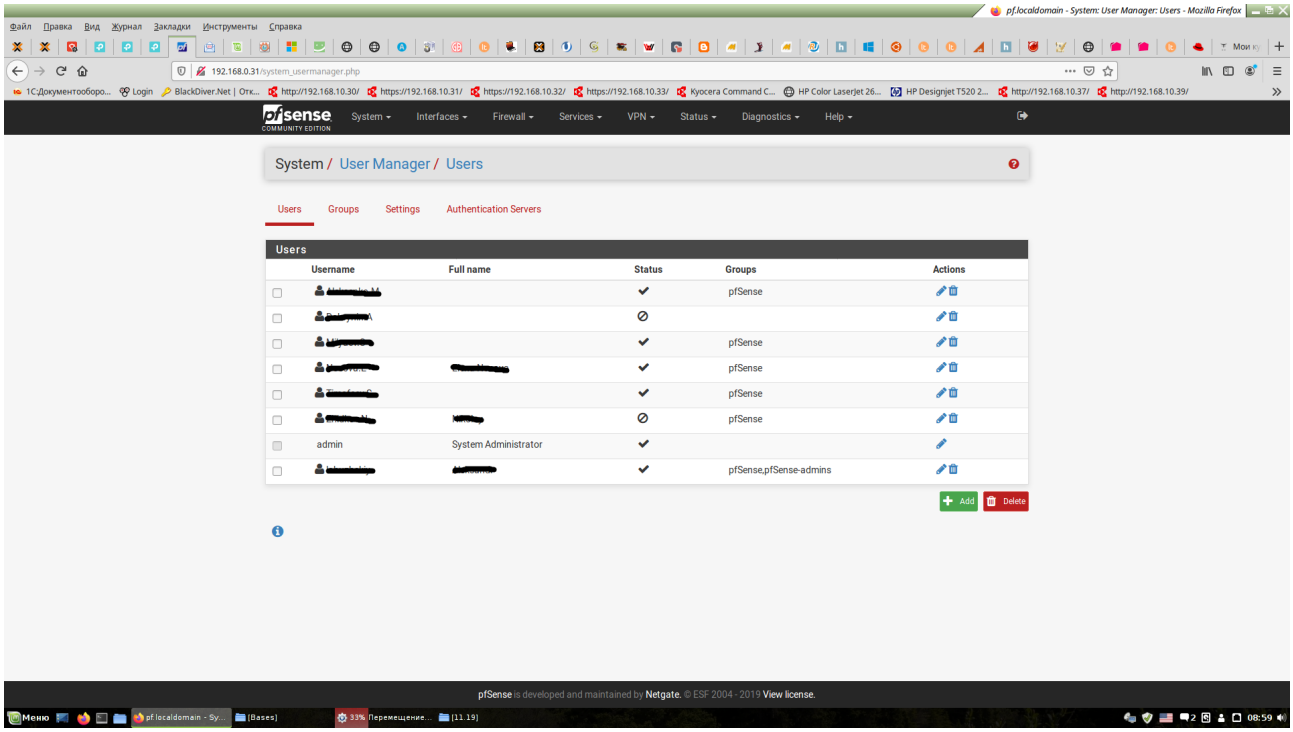
Не забываем внизу нажимать на кнопку «Save»



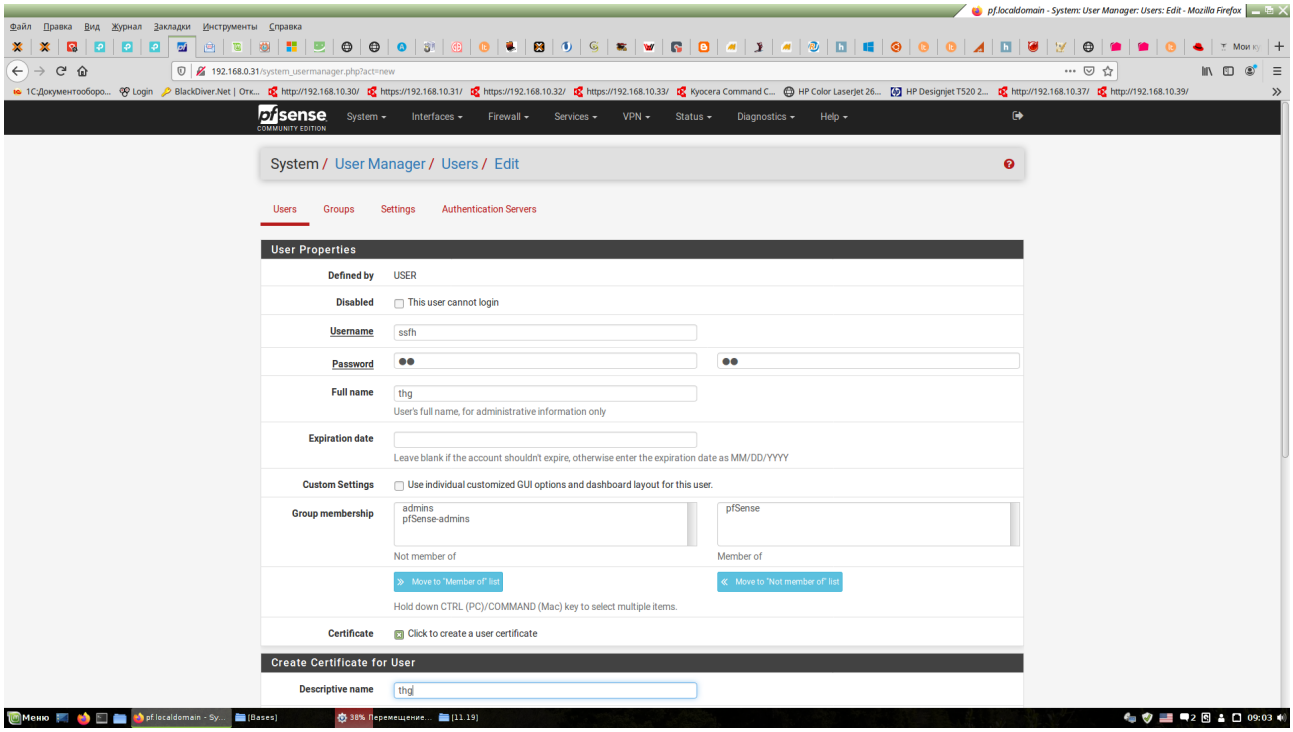
Создаём «сквозную» группу пользователей, с повышенными привилегиями, аналогичную той, на которую деллигированы полномочия в AD.

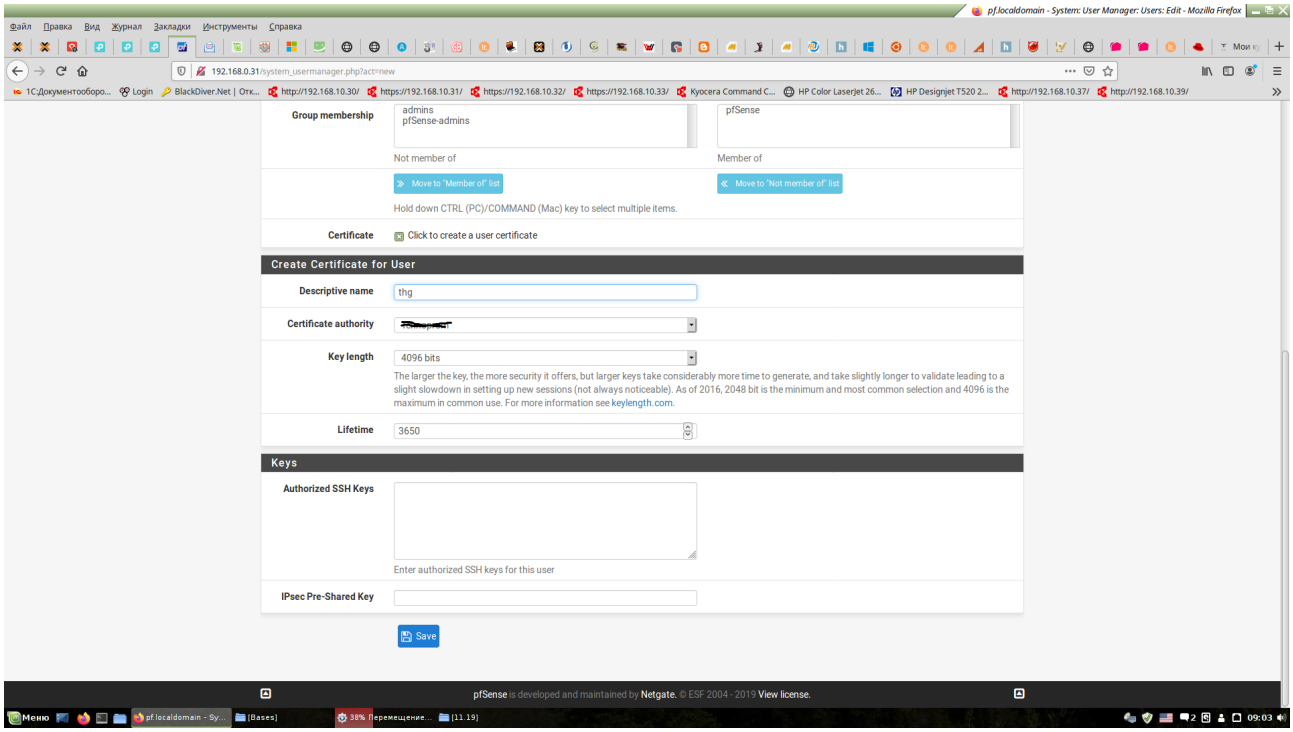


И так мы добрались до управления пользователями. На сервере psSense это выглядит таким образом:

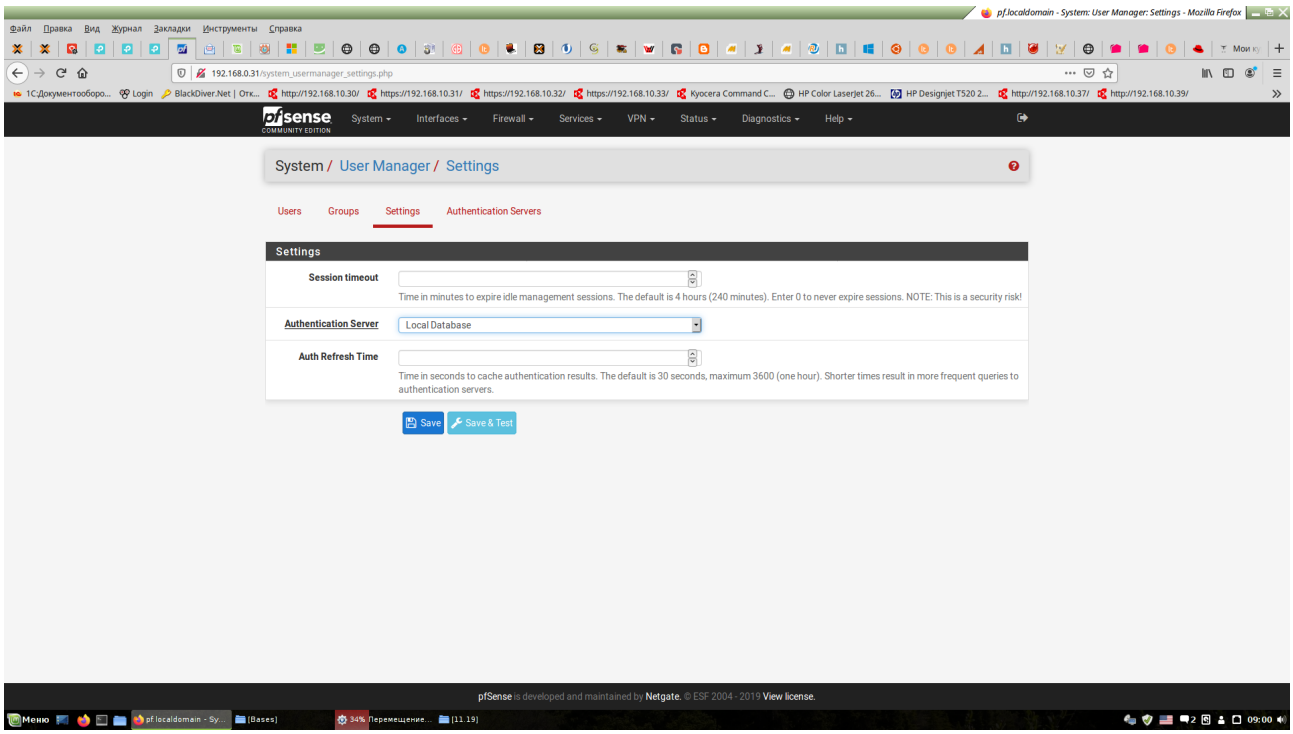


Добавление новых пользователей pfSense выглядит примерно так:

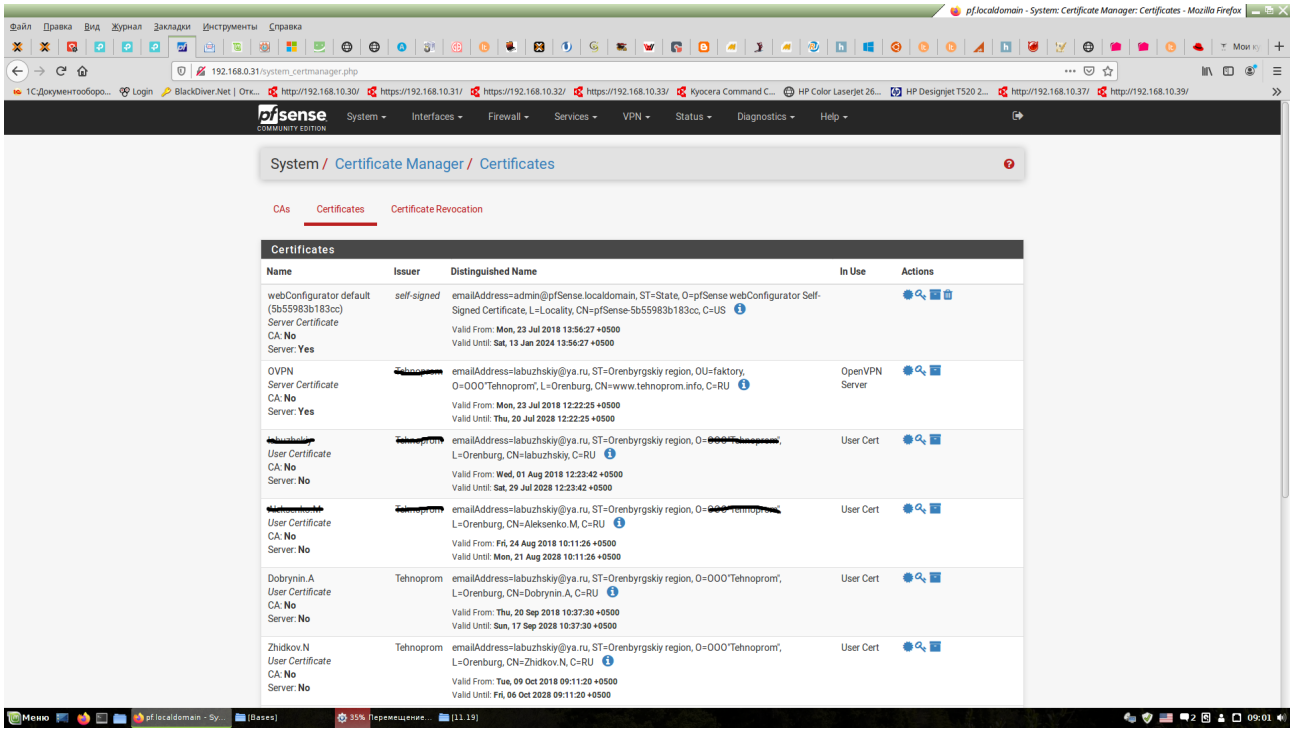




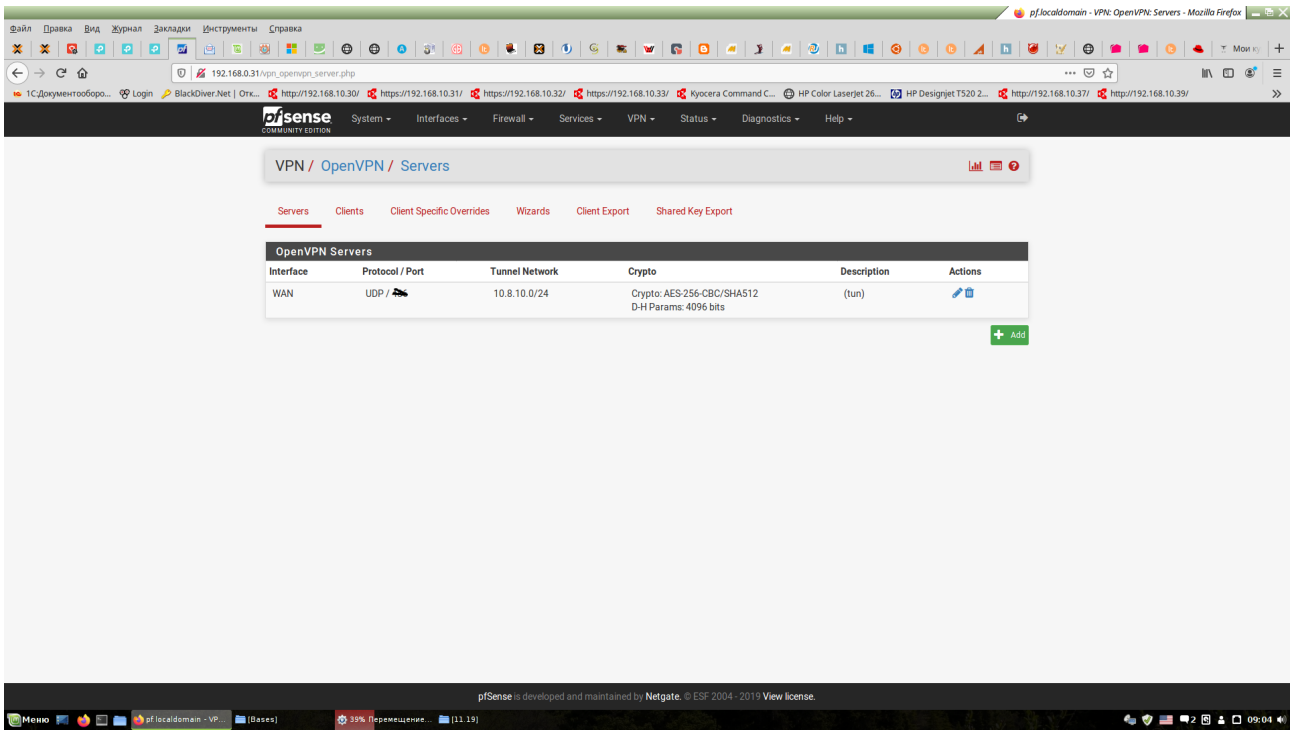
При этом создание и хранение может вестись как в Локальной БД, так и в БД, из AD.
На изобажении ниже в развёртывающемся списке выбрана локальная БД пользователей.

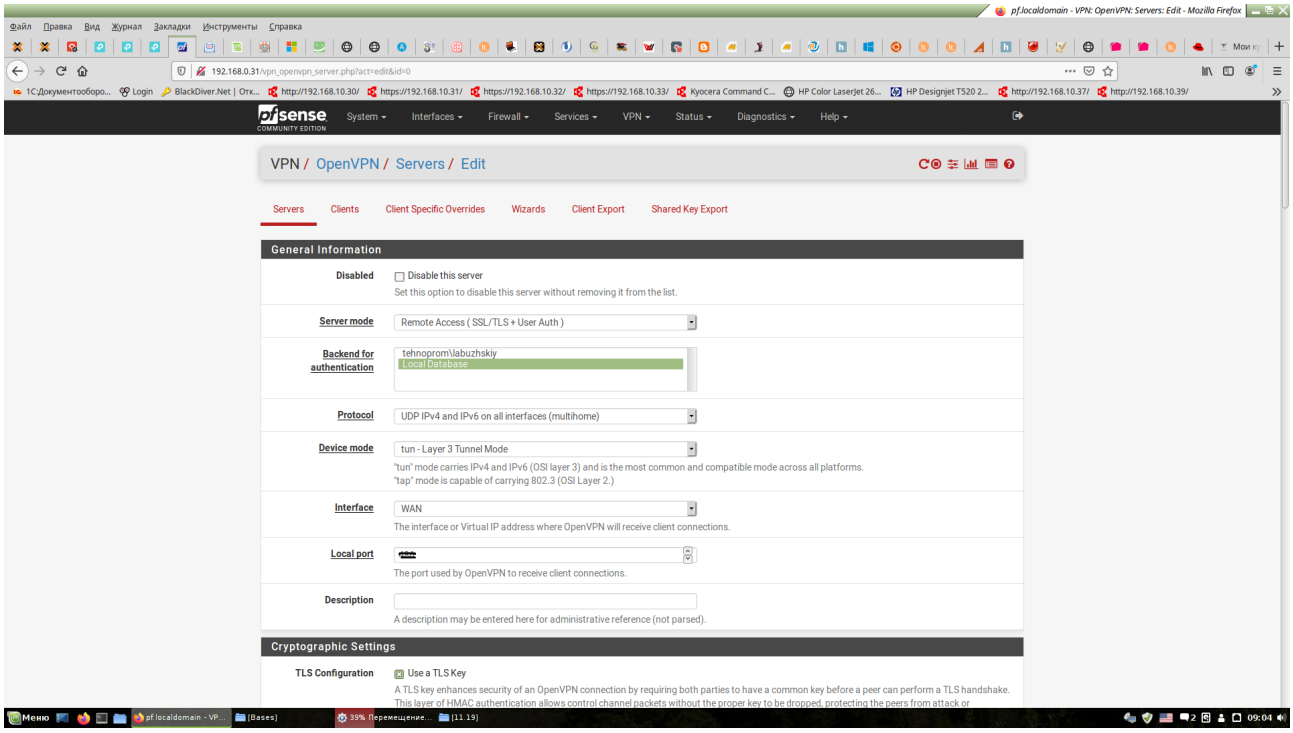


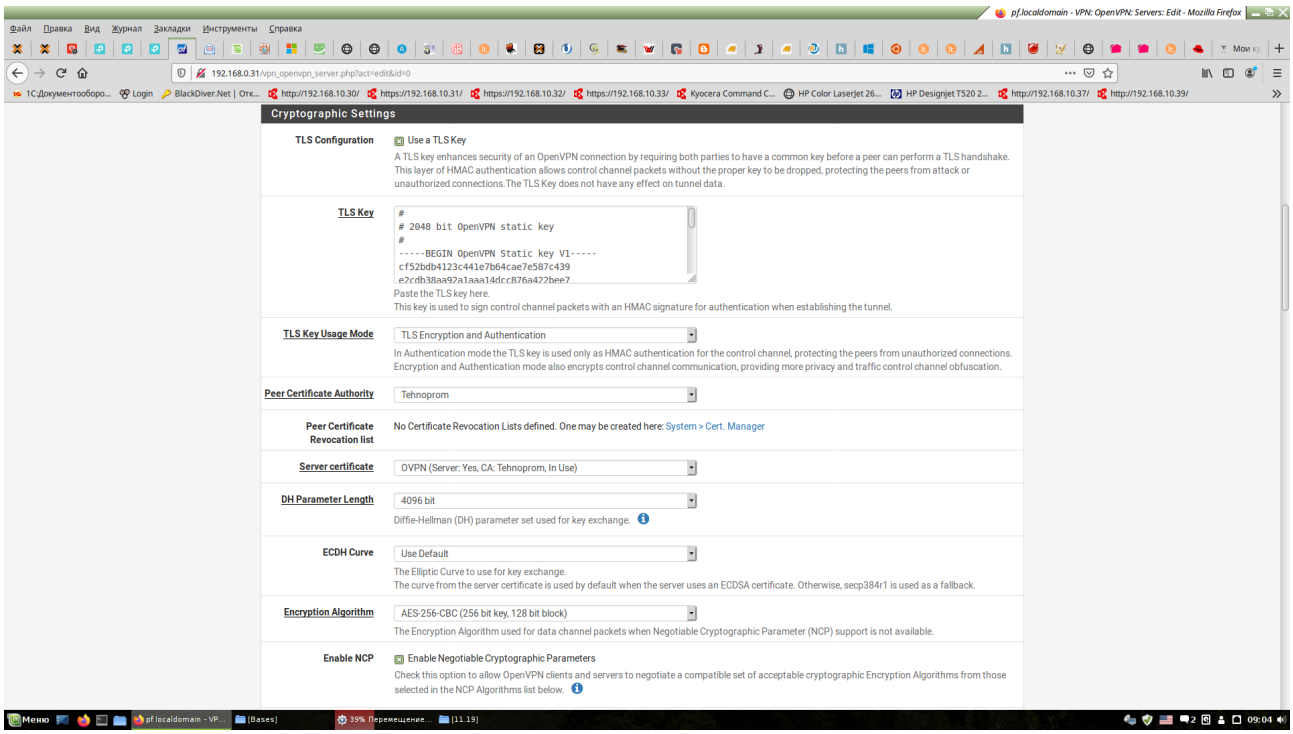
По завершении создания нового пользователя в списке доступных сертификатов генерируется назначенный ему сертификат.
Примечание: после удаления пользователя не забывать вычищать из списка лишние сертификаты (они не всегда вычещаются в автоматическом режиме).

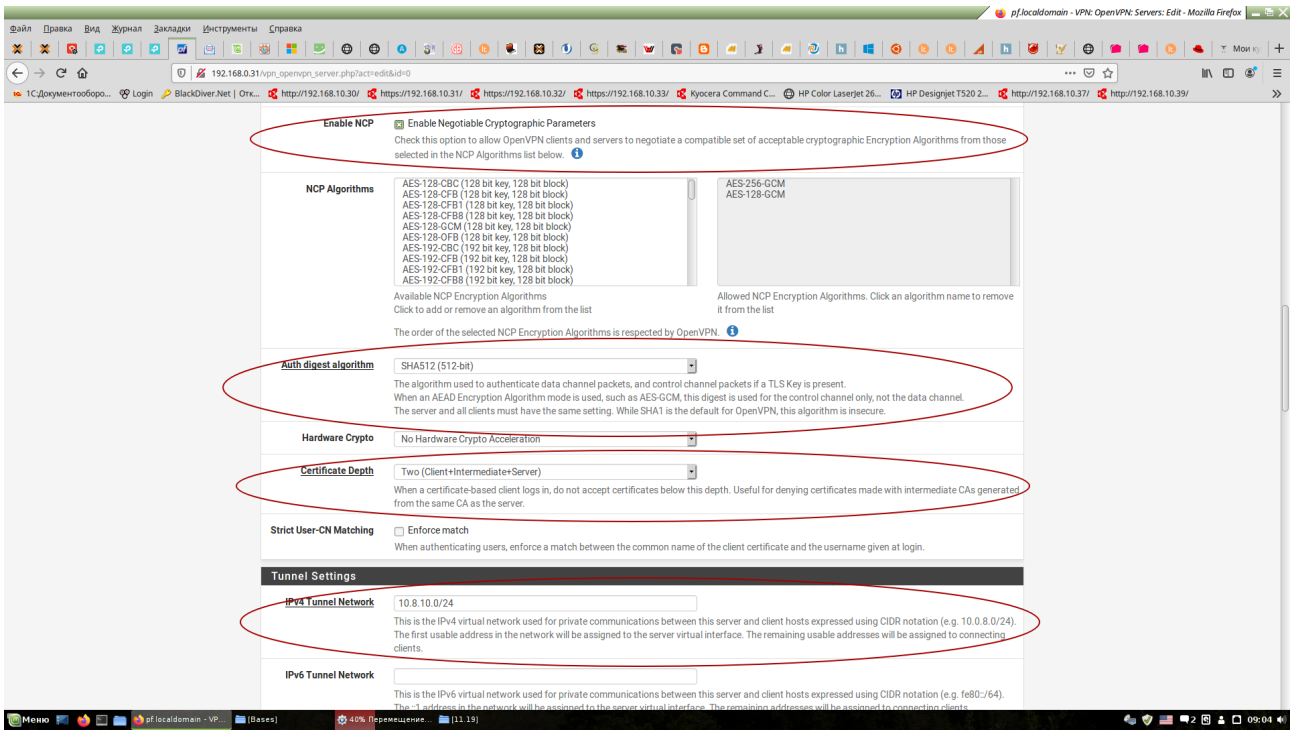


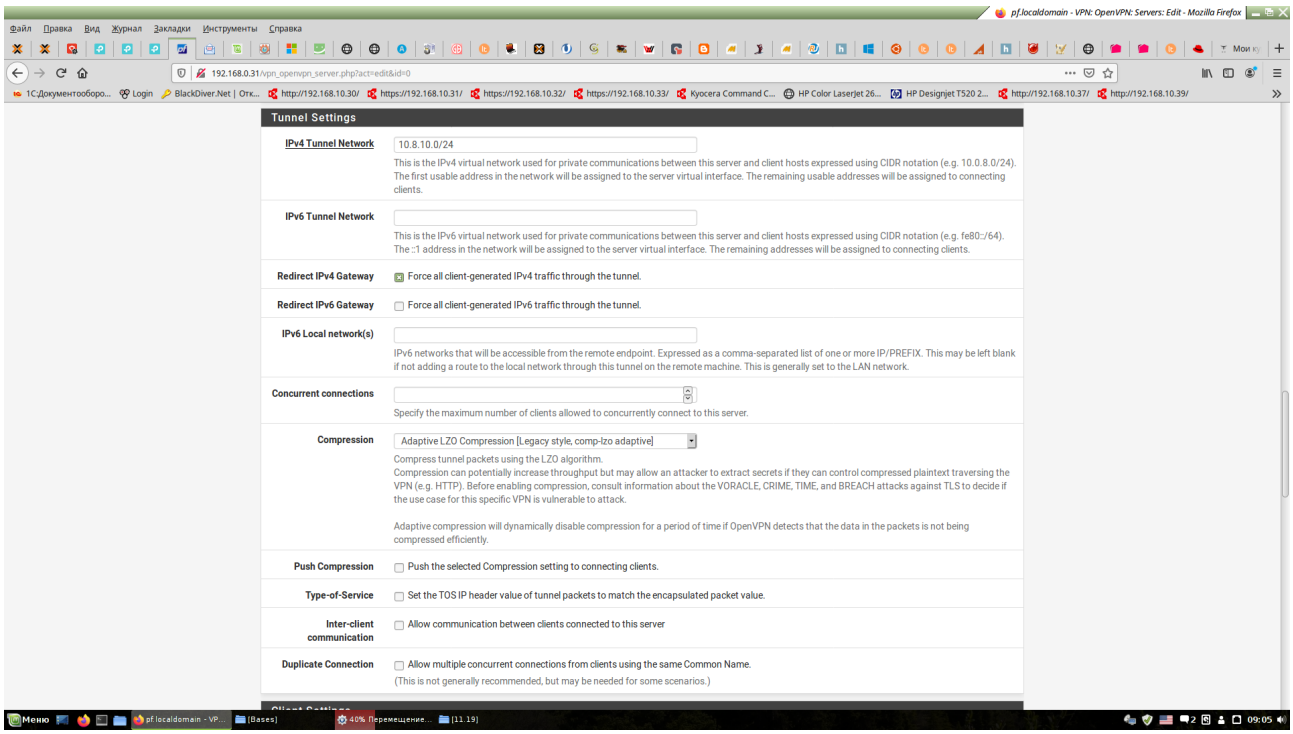
Внесём изменения в настройки сервера:


pf.localdomain - VPN: OpenVPN: Servers - Mozilla Firefox
192.168.0.31/vpn_openvpn_server.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
VPN / OpenVPN / Servers
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export
OpenVPN Servers
Interface Protocol / Port Tunnel Network Crypto Description Actions
WAN UDP / [redacted] 10.8.10.0/24 Crypto: AES-256-CBC/SHA512
D-H Params: 4096 bits (tun)
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

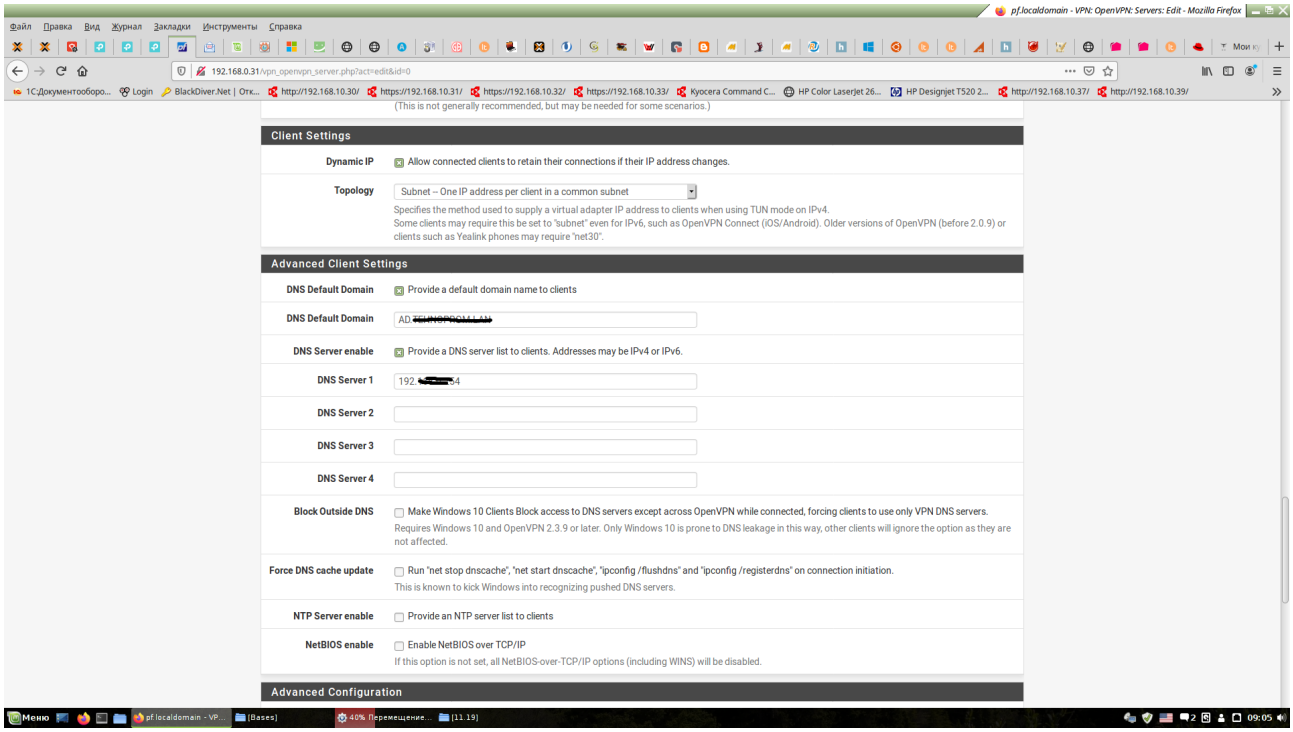

pf.localdomain - VPN: OpenVPN: Servers: Edit - Mozilla Firefox
192.168.0.31/vpn_openvpn_server.php?act=edit&id=0
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
VPN / OpenVPN / Servers / Edit
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export
General Information
Disabled Disable this server
Set this option to disable this server without removing it from the list.
Server mode Remote Access (SSL/TLS + User Auth)
Backend for authentication tehnoprom\labuzhskiy
Local Database
Protocol UDP IPv4 and IPv6 on all interfaces (multihome)
Device mode tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Interface WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port [redacted]
The port used by OpenVPN to receive client connections.
Description
A description may be entered here for administrative reference (not parsed).
Cryptographic Settings
TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake.
This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or

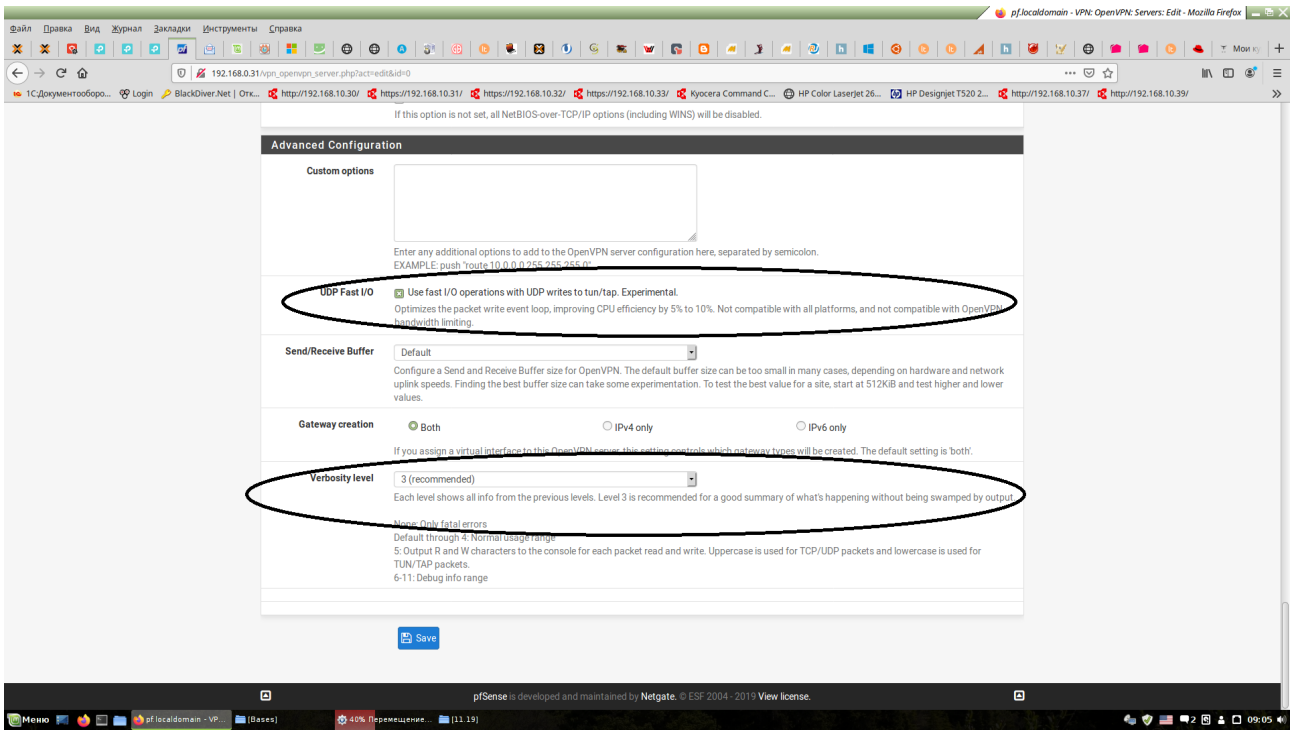

pf.localdomain - VPN: OpenVPN: Servers: Edit - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
192.168.0.31/vpn_openvpn_server.php?act=edit&id=0
Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
TLS Key
#
2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
cf52bdb4123c441e7b64cae7e587c439
e2cdb38aa92a1aaa1ddcc876a422bee7
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode
TLS Encryption and Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
Peer Certificate Authority
Tehnoprom
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
Server certificate
OVPN (Server: Yes, CA: Tehnoprom, In Use)
DH Parameter Length
4096 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.
Enable NCP
Enable Negotiable Cryptographic Parameters
Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

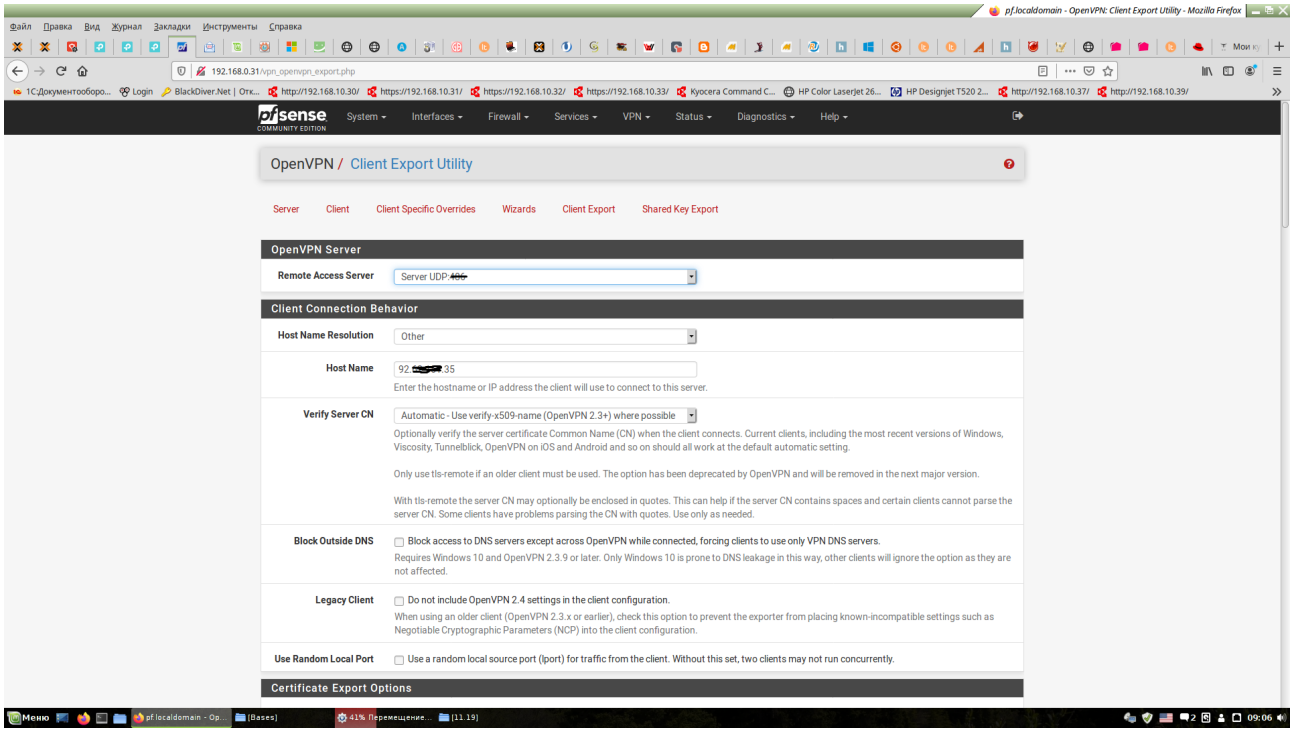

pf.localdomain - VPN: OpenVPN: Servers: Edit - Mozilla Firefox
Enable NCP
Enable Negotiable Cryptographic Parameters
Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.
NCP Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
Available NCP Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected NCP Encryption Algorithms is respected by OpenVPN.
Auth digest algorithm
SHA512 (512-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto
No Hardware Crypto Acceleration
Certificate Depth
Two (Client+Intermediate+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Strict User-CN Matching
Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
Tunnel Settings
IPv4 Tunnel Network
10.8.10.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64).



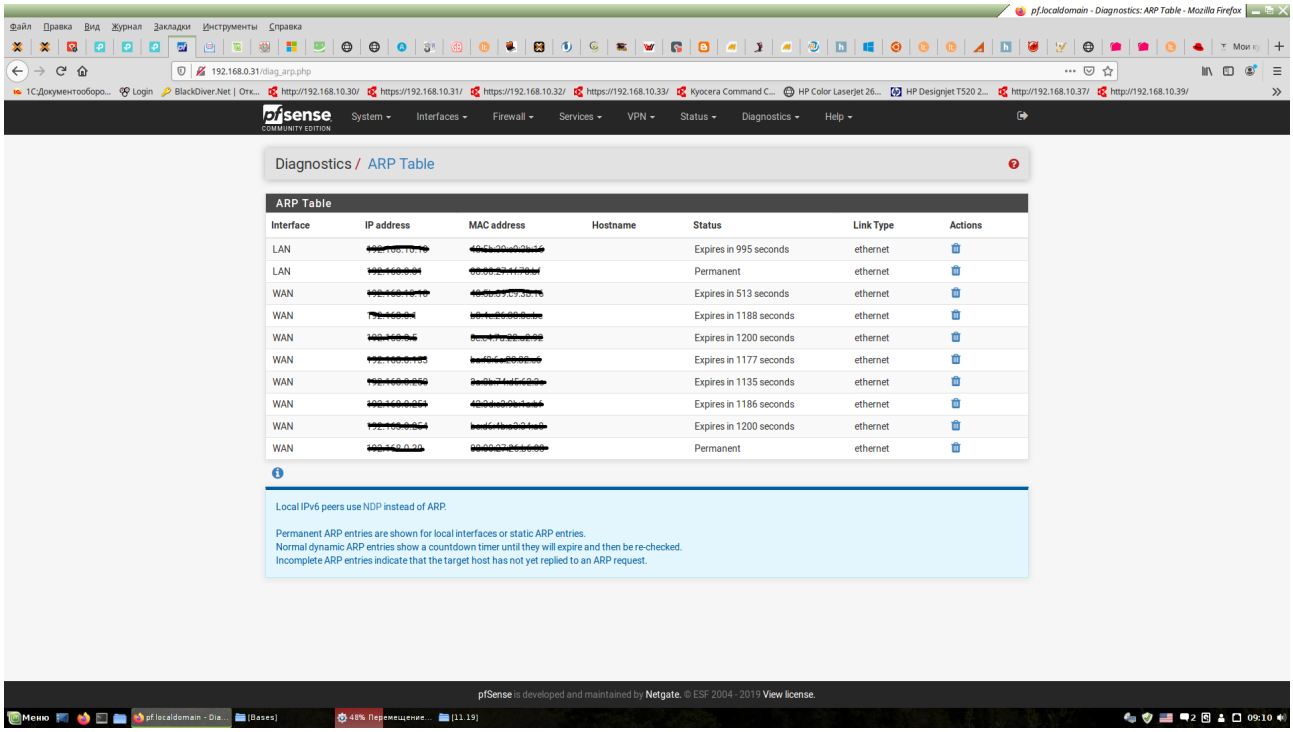
Теперь внесём изменения в настройки клиентов, оптимизации CPU, и параметры ip-адреса, для внешних клиентских подключений.



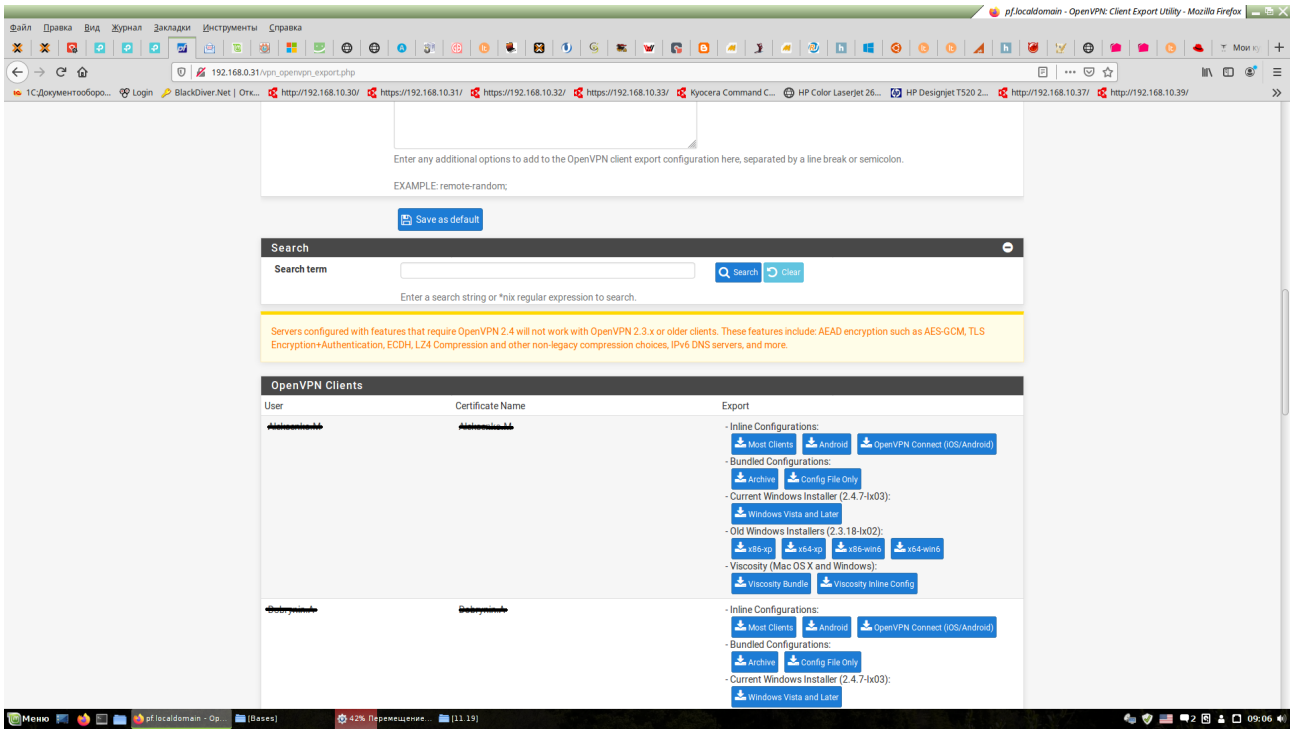




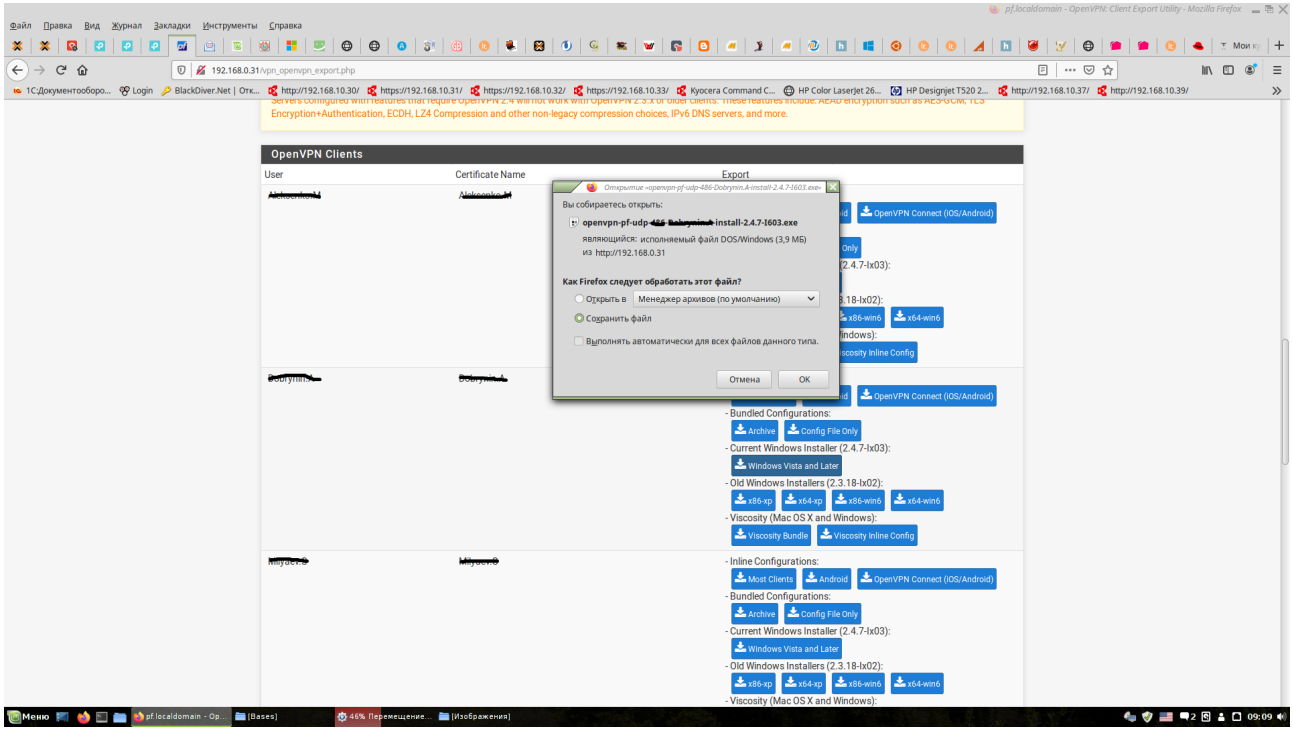
ARP-таблица по клиентам:



Так будет выглядеть экспорт клиентов через установленный нами ранее пакет:

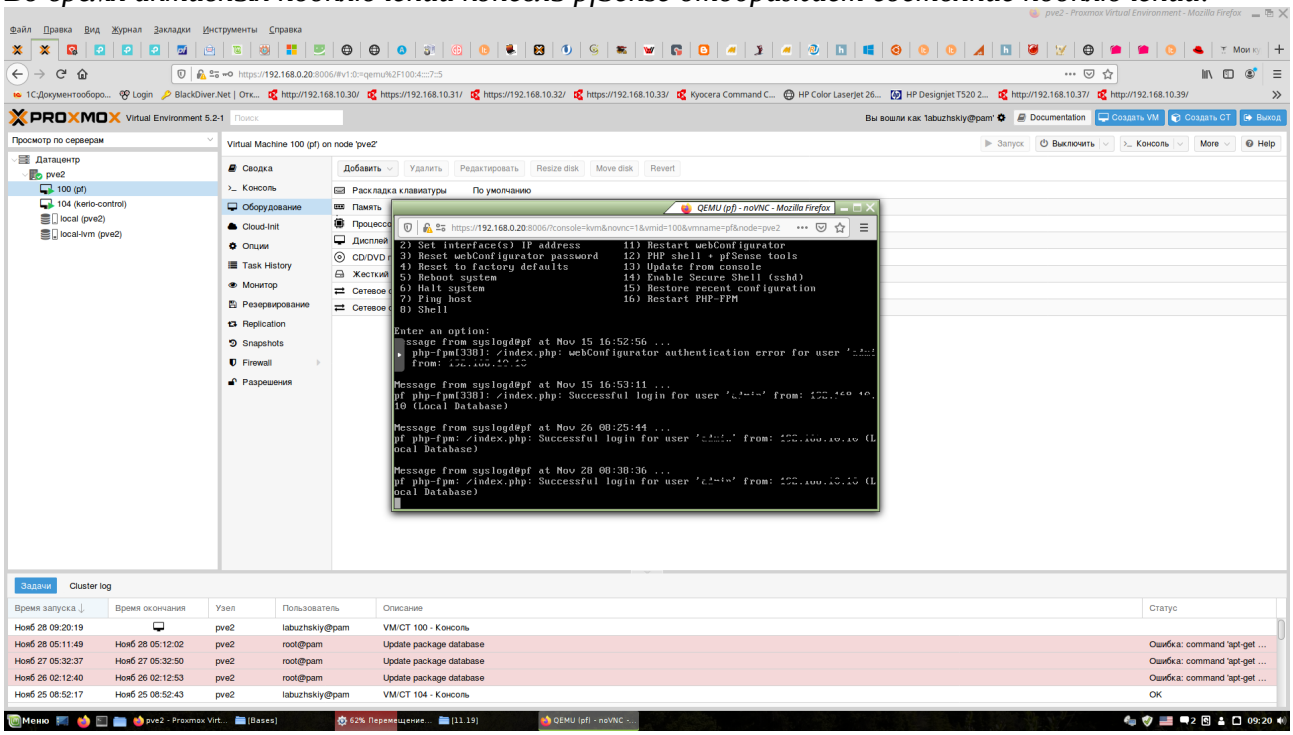


Для Microsoft Windows скачивается готовый инсталляционный SFX-архив, включающий в себя все необходимые настройки.



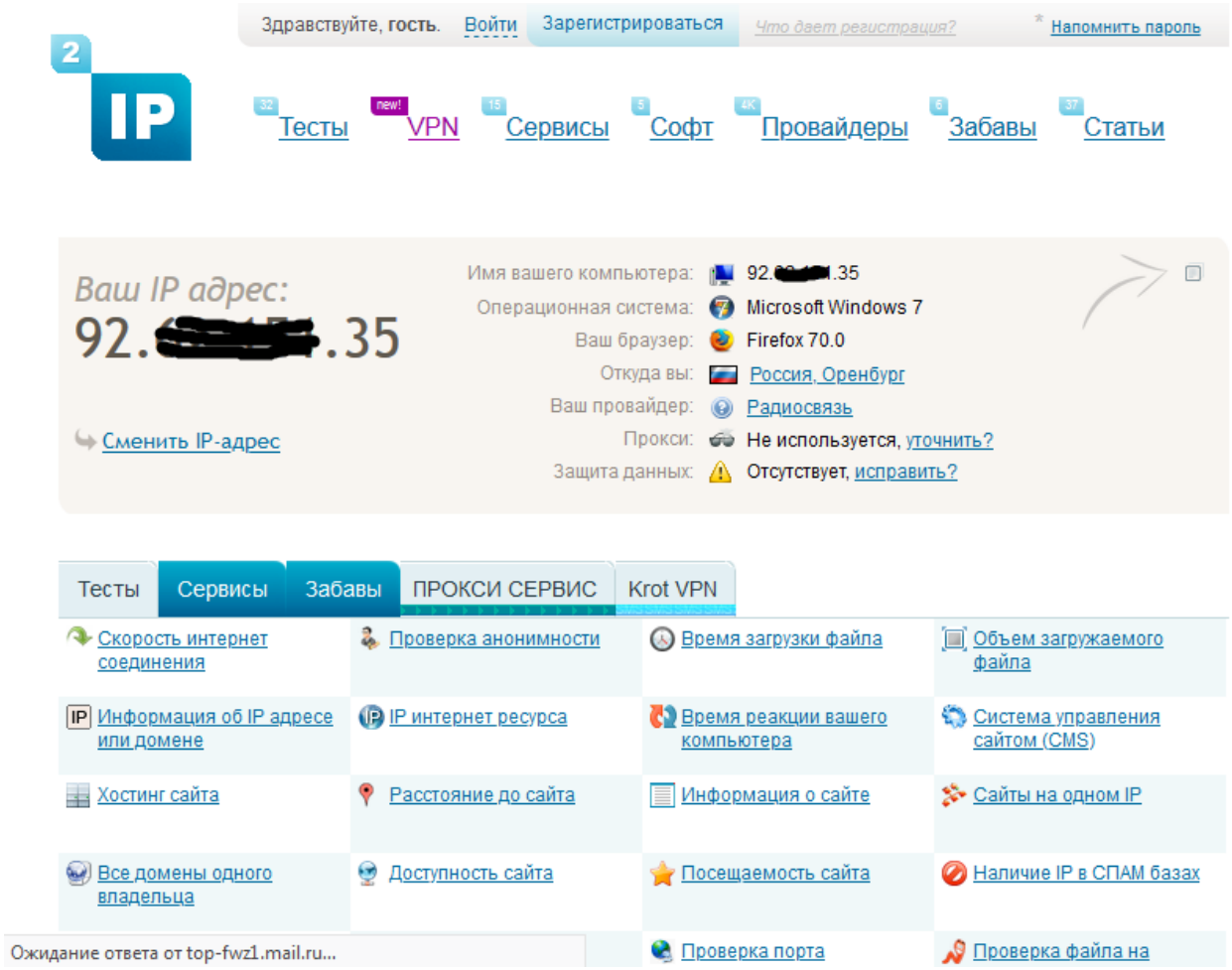
*Для Linux платформы скачивается архив в *.zip формате, содержащий все необходимые для настройки файлы.*

Во время активных подключений консоль pfSense отображает состояние подключений:

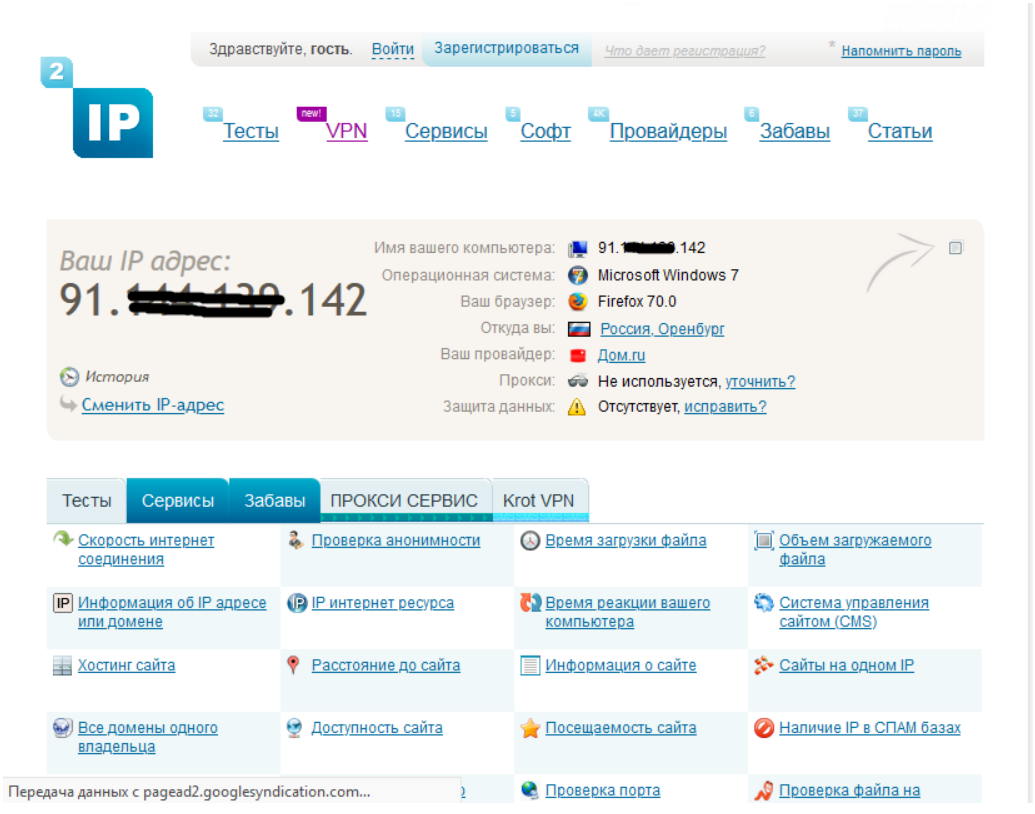


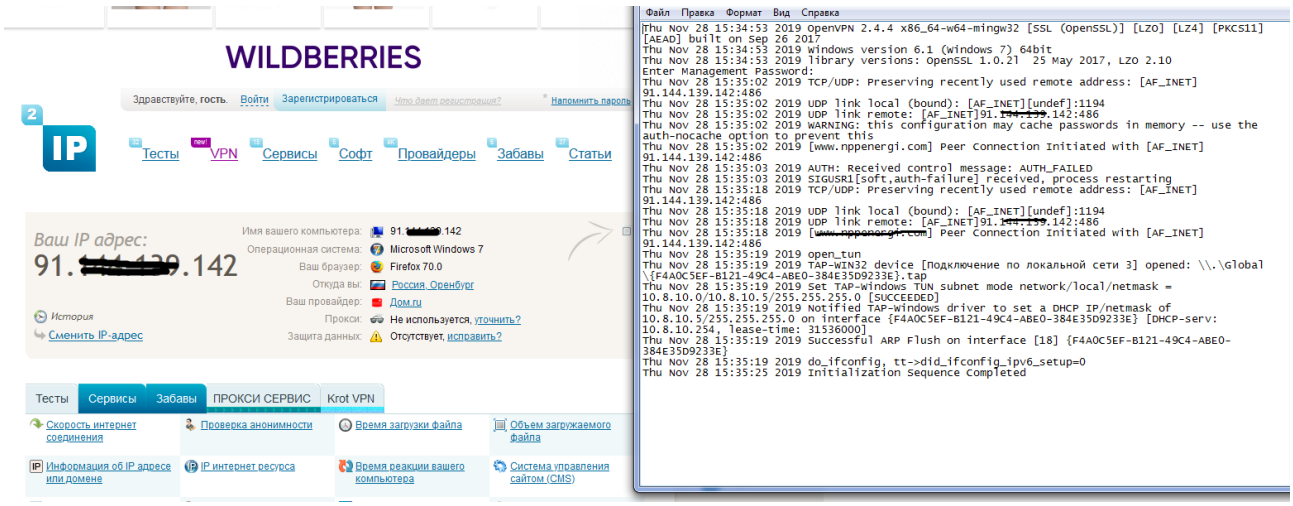
На этом наш подготовительных этап завершён, переходим к выполнению поставленой задачи.

1-й сегмент сети:
Картина до подключения:



картина после подключения:

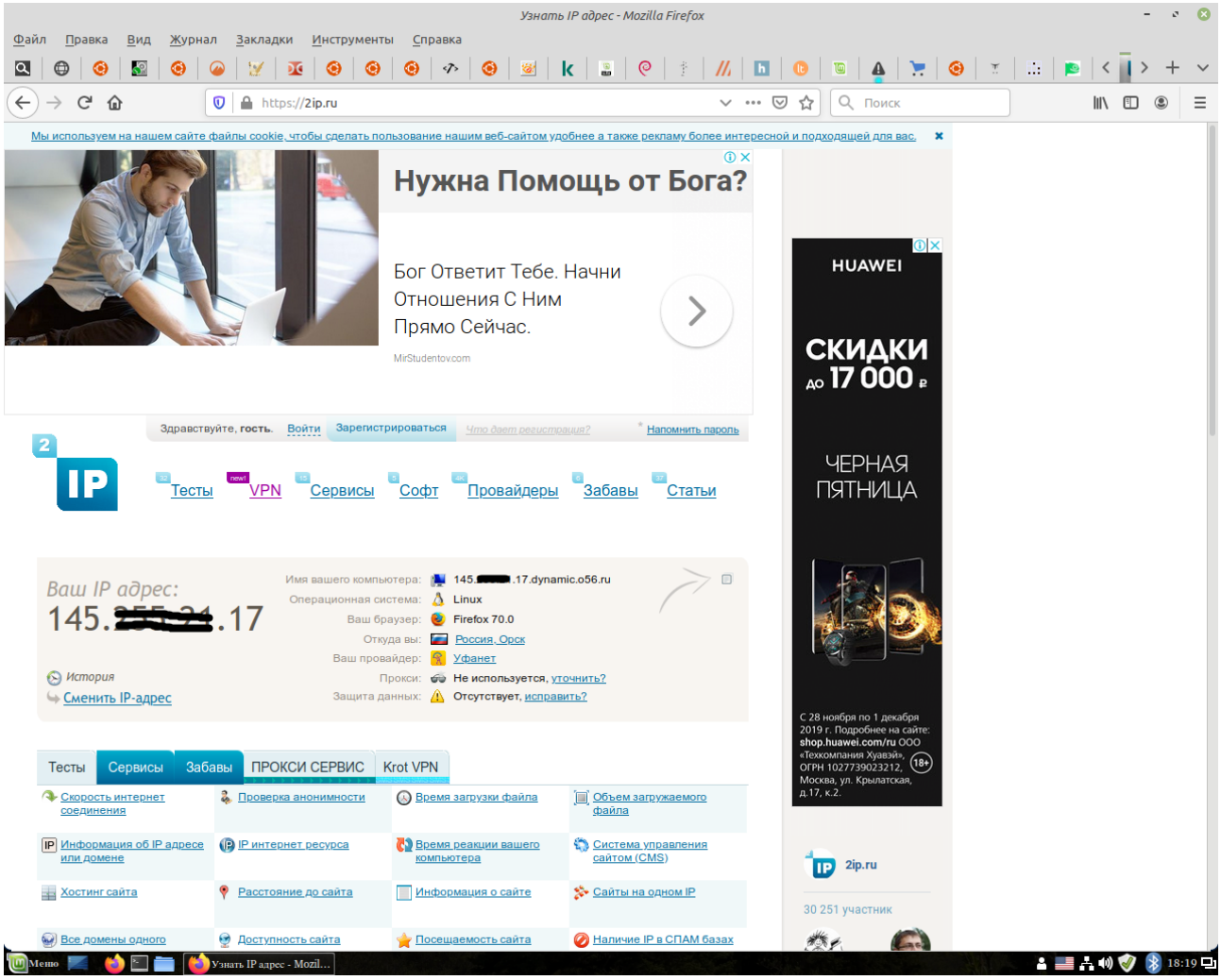




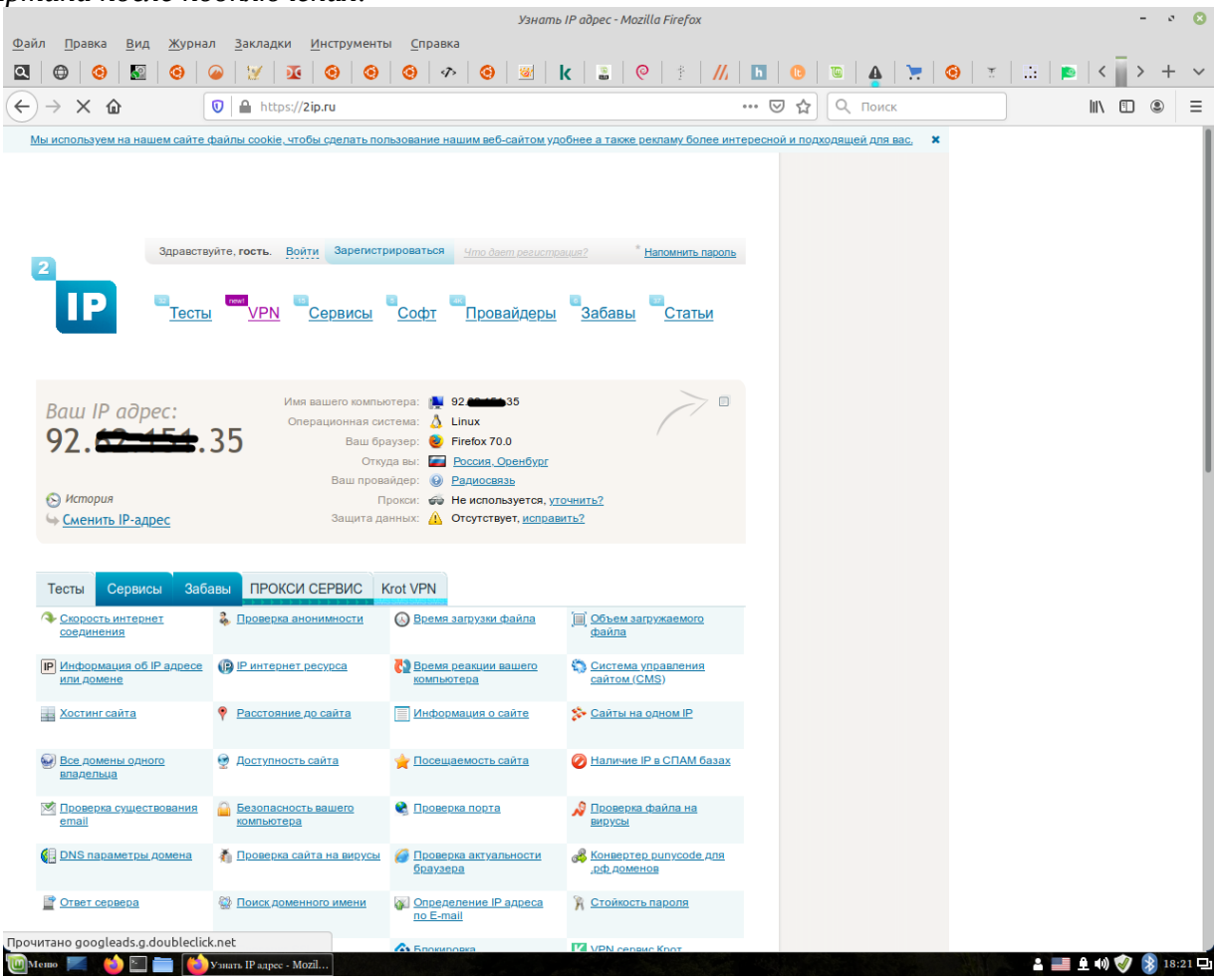
Как видно из скриншотов выше была выполнена подмена ip-адреса, находясь в другом сегменте сети Internet, на интерфейс tun0 в момент подключения был назначен новый ip-адрес.

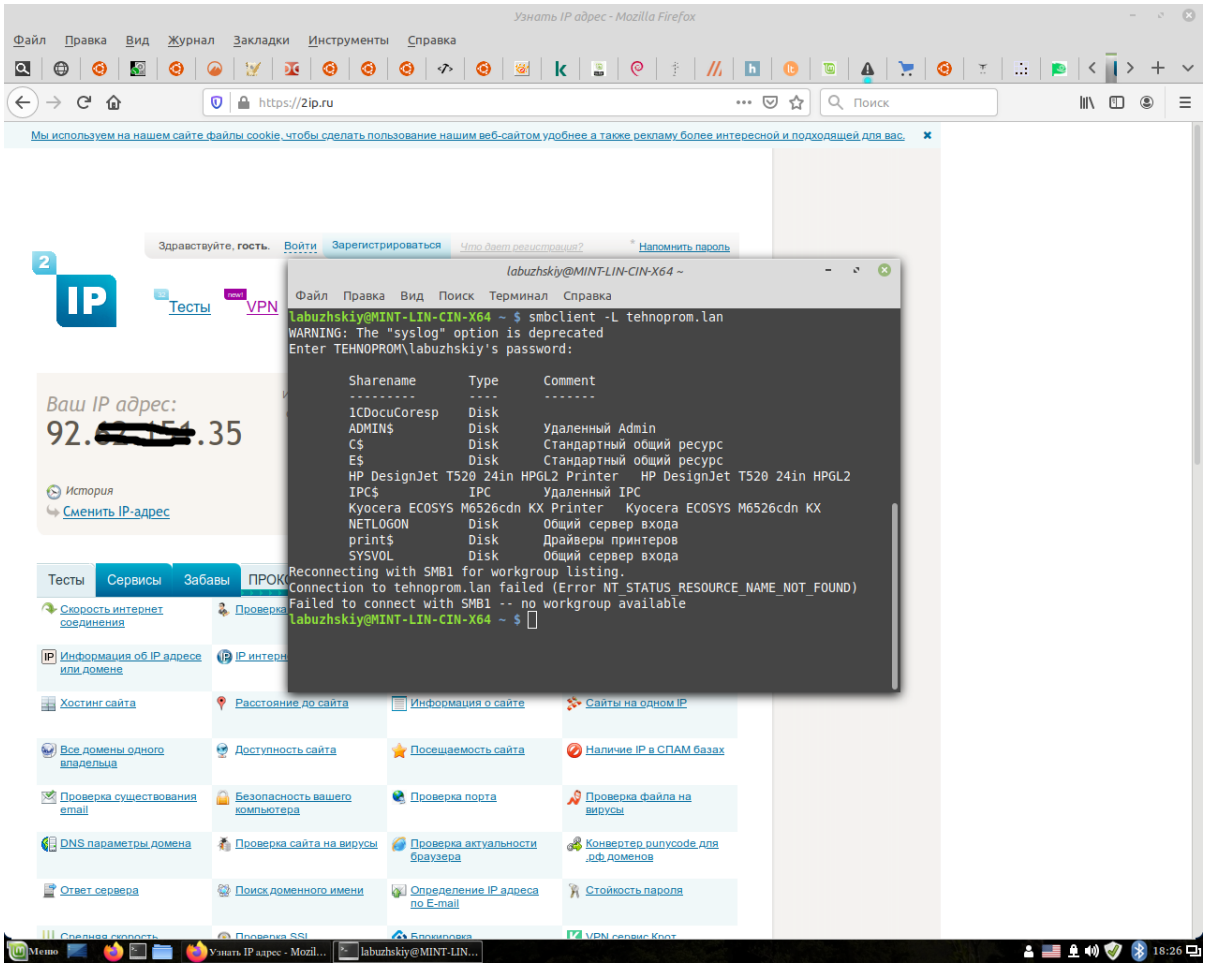
Пример 2:

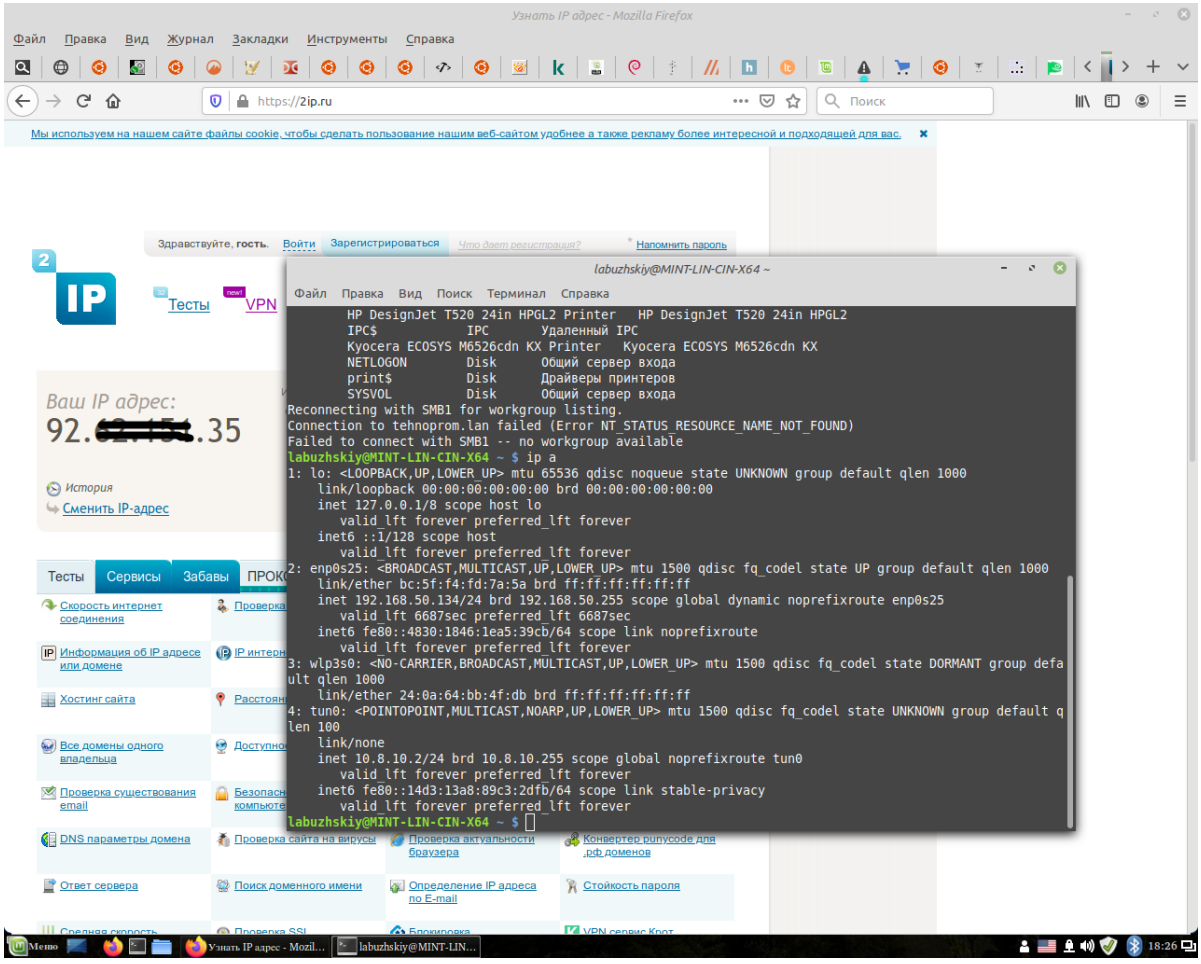
Картинка перед подключением:



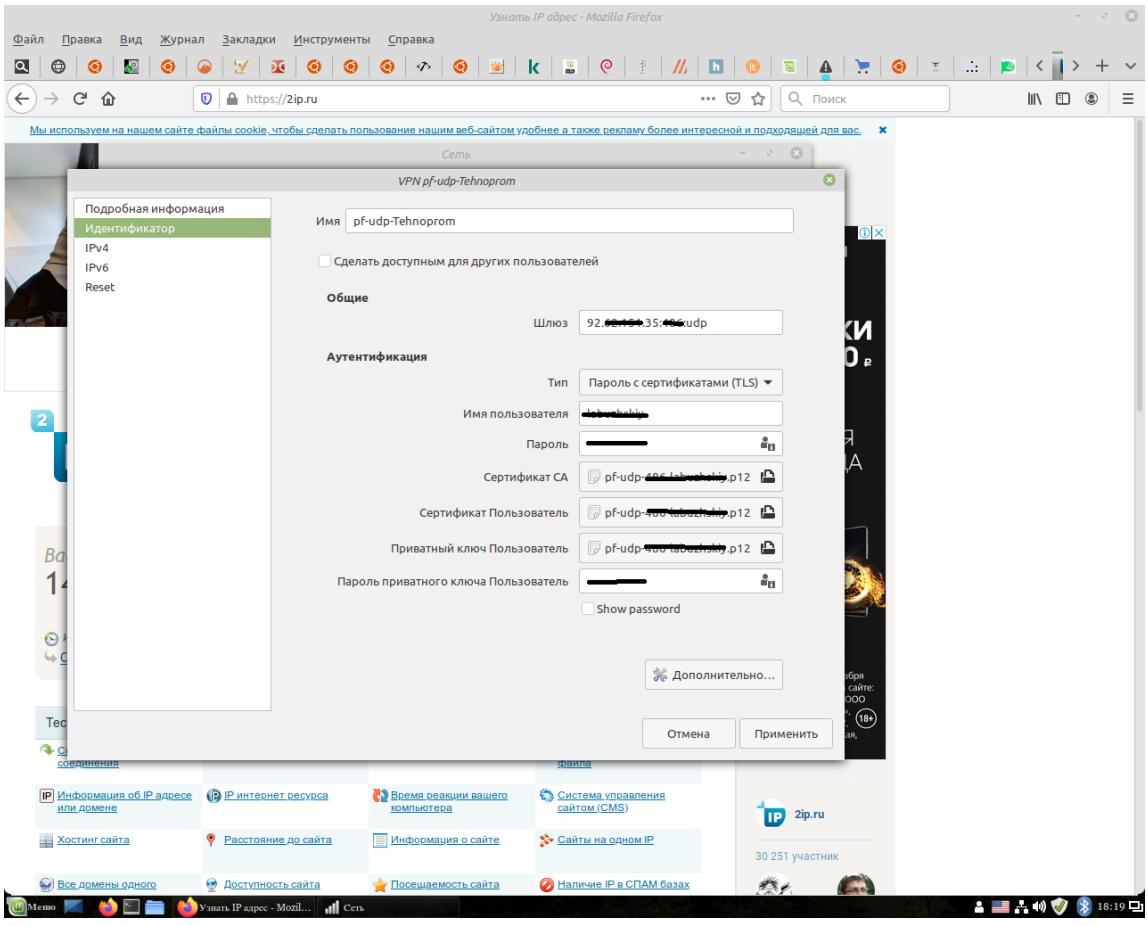
Картина после подключения:

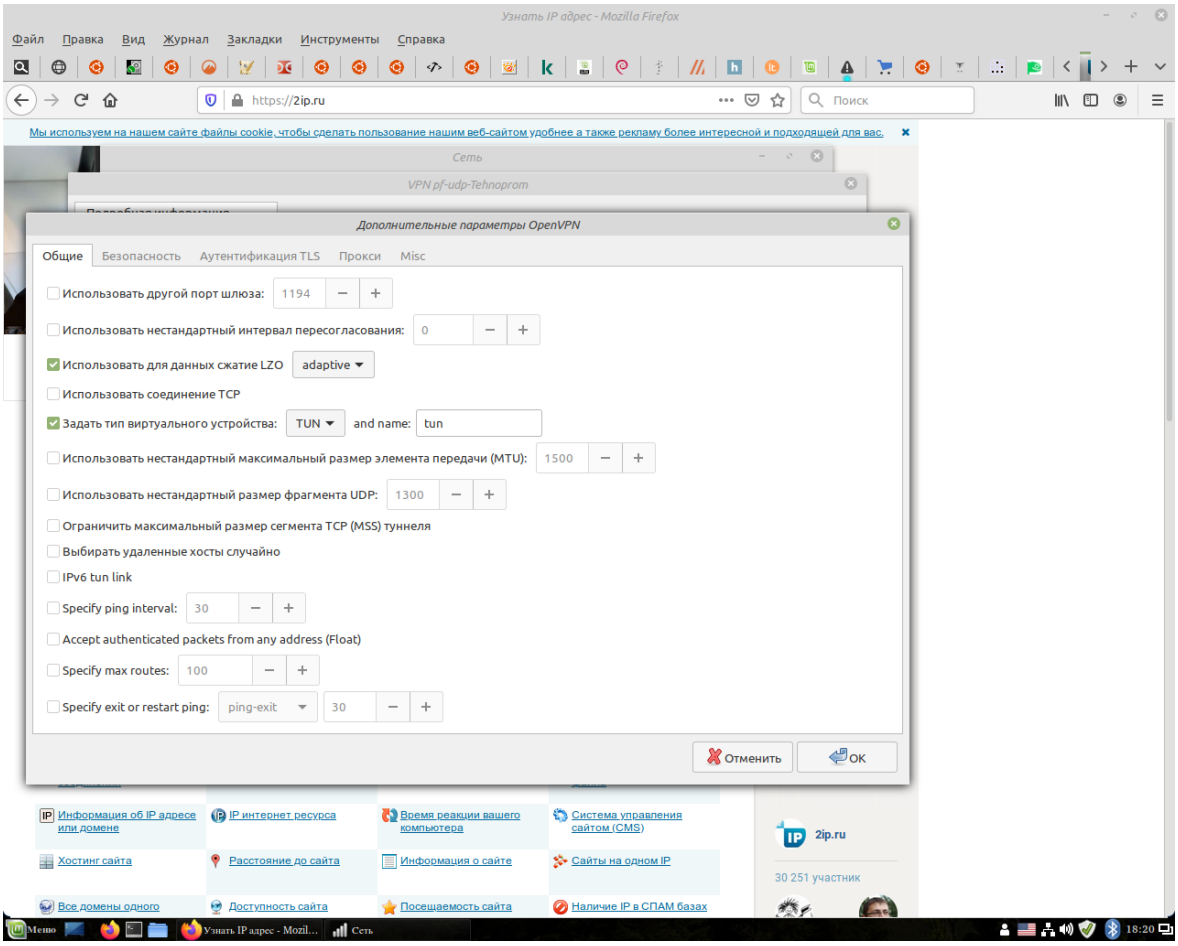


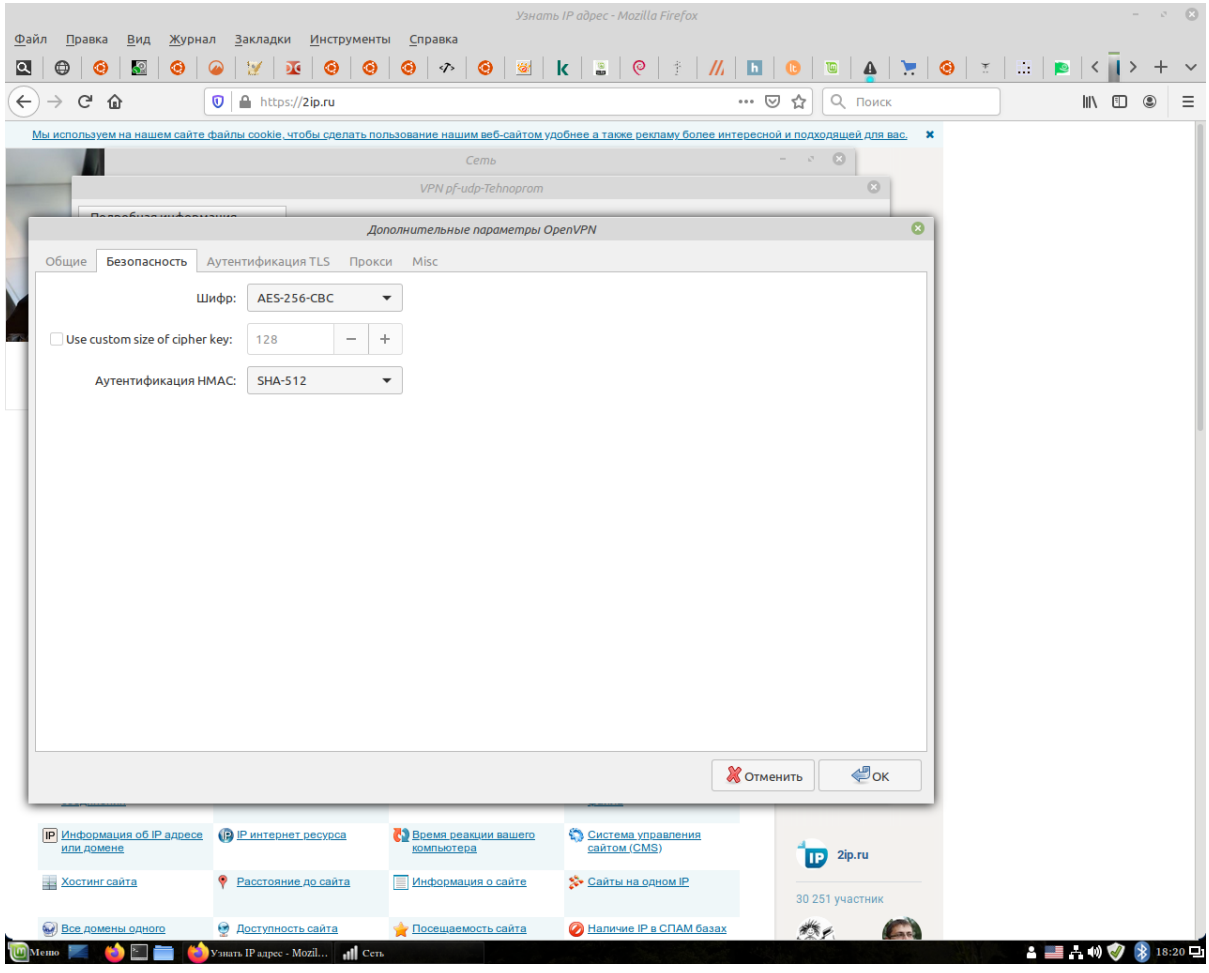


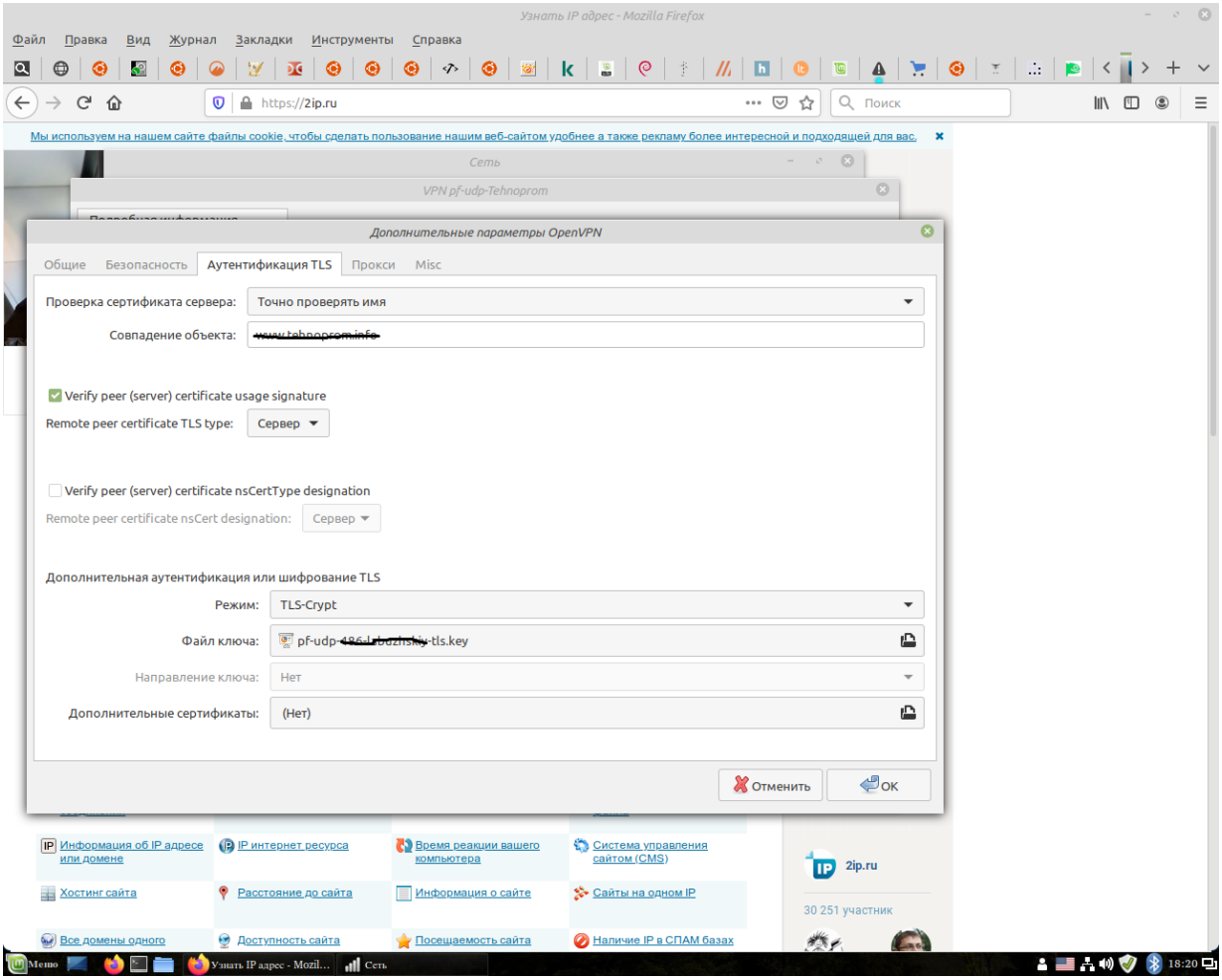


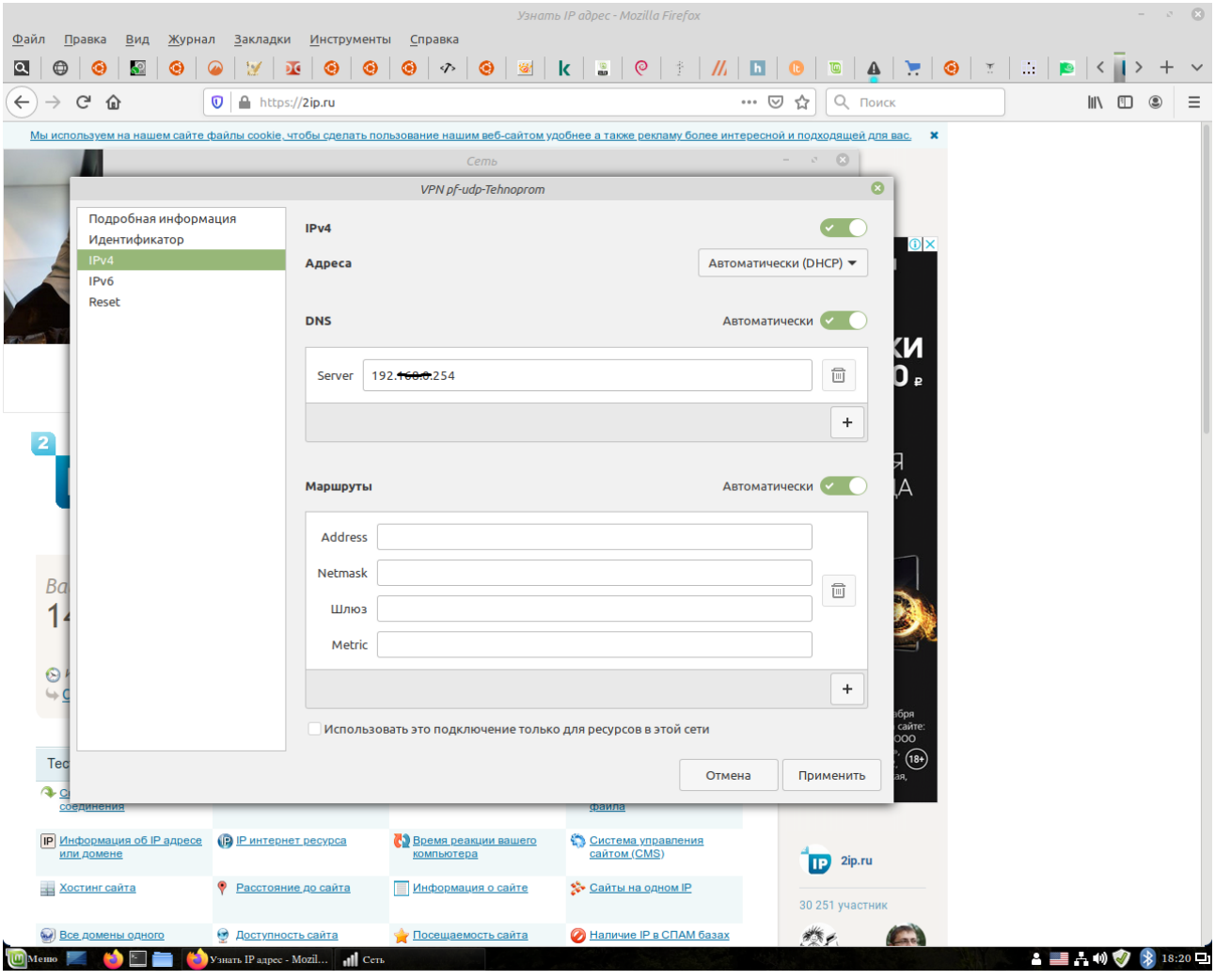
Настройки подключения:




Узнать IP адрес - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru
Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Сеть
VPN pf-udp-Tehnoprom
Дополнительные параметры OpenVPN
Общие Безопасность Аутентификация TLS Прокси Misc
Использовать другой порт шлюза: 1194
Использовать нестандартный интервал пересогласования: 0
Использовать для данных сжатие LZO adaptive
Использовать соединение TCP
Задать тип виртуального устройства: TUN and name: tun
Использовать нестандартный максимальный размер элемента передачи (MTU): 1500
Использовать нестандартный размер фрагмента UDP: 1300
Ограничить максимальный размер сегмента TCP (MSS) туннеля
Выбирать удаленные хосты случайно
IPv6 tun link
Specify ping interval: 30
Accept authenticated packets from any address (Float)
Specify max routes: 100
Specify exit or restart ping: ping-exit 30
Отменить
OK
Информация об IP адресе или домене
IP интернет ресурса
Время реакции вашего компьютера
Система управления сайтом (CMS)
Хостинг сайта
Расстояние до сайта
Информация о сайте
Сайты на одном IP
Все домены одного
Доступность сайта
Посещаемость сайта
Наличие IP в СПАМ базах
2ip.ru
30 251 участник
Меню
Узнать IP адрес - Mozil...
Сеть
18:20


Узнать IP адрес - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru
Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Сеть
VPN pf-udp-Tehnoprom
Дополнительные параметры OpenVPN
Общие Безопасность Аутентификация TLS Прокси Misc
Шифр: AES-256-CBC
Use custom size of cipher key: 128
Аутентификация HMAC: SHA-512
Отменить
OK
Информация об IP адресе или домене
IP интернет ресурса
Время реакции вашего компьютера
Система управления сайтом (CMS)
Хостинг сайта
Расстояние до сайта
Информация о сайте
Сайты на одном IP
Все домены одного
Доступность сайта
Посещаемость сайта
Наличие IP в СПАМ базах
2ip.ru
30 251 участник
Меню
Узнать IP адрес - Mozil...
Сеть
18:20


Узнать IP адрес - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru
Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Сеть
VPN pf-udp-Tehnoprom
Дополнительные параметры OpenVPN
Общие
Безопасность
Аутентификация TLS
Прокси
Misc
Проверка сертификата сервера:
Точно проверять имя
Совпадение объекта:
Verify peer (server) certificate usage signature
Remote peer certificate TLS type:
Сервер
Verify peer (server) certificate nsCertType designation
Remote peer certificate nsCert designation:
Сервер
Дополнительная аутентификация или шифрование TLS
Режим:
TLS-Crypt
Файл ключа:
pf-udp-tls.key
Направление ключа:
Нет
Дополнительные сертификаты:
(Нет)
Отменить
OK
Информация об IP адресе или домене
IP интернет ресурса
Время реакции вашего компьютера
Система управления сайтом (CMS)
Хостинг сайта
Расстояние до сайта
Информация о сайте
Сайты на одном IP
Все домены одного
Доступность сайта
Посещаемость сайта
Наличие IP в СПАМ базах
2ip.ru
30 251 участник
Меню
Узнать IP адрес - Mozil...
Сеть
18:20


Узнать IP адрес - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru
Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Сеть
VPN pf-udp-Tehnoprom
Подробная информация
Идентификатор
IPv4
IPv6
Reset
IPv4
Адреса
Автоматически (DHCP)
DNS
Автоматически
Server
192.168.0.254
Маршруты
Автоматически
Address
Netmask
Шлюз
Metric
Использовать это подключение только для ресурсов в этой сети
Отмена
Применить
Информация об IP адресе или домене
IP интернет ресурса
Время реакции вашего компьютера
Система управления сайтом (CMS)
Хостинг сайта
Расстояние до сайта
Информация о сайте
Сайты на одном IP
Все домены одного
Доступность сайта
Посещаемость сайта
Наличие IP в СПАМ базах
2ip.ru
30 251 участник
Меню
Узнать IP адрес - Mozil...
Сеть
18:20