Лабораторная работа №8
«НАСТРОЙКА VPN-СОЕДИНЕНИЯ МЕЖДУ МСЭ PFSENSE (OPENVPN-PSK)»

Цель работы: развёртывание двух виртуальных защищённых сегментов сети, объединённых в VPN-сеть, при помощи технологии виртуализации (VirtualBox) и межсетевого экрана PfSense.

Задание:

1. Развернуть и запустить виртуальные машины с межсетевым экраном PfSense и операционной системой Ubuntu.
2. Осуществить настройку межсетевых экранов PfSense.
3. Проверить правильность прохождения сетевых пакетов через защищённое соединение.
4. Зафиксировать результаты настроек и проверок в отчёте.

Порядок выполнения:

1. Задать параметры виртуальной машины, предназначенной под установку межсетевого экрана PfSense.
2. Установить на подготовленную виртуальную машину межсетевой экран PfSense.
3. Через консоль на виртуальной машине определить IP адрес и параметры для получения доступа к web-интерфейсу межсетевого экрана PfSense, при необходимости изменить IP адрес доступа.
4. Запустить на виртуальной машине PC1 образ операционной системы Ubuntu.
5. Задать параметры виртуальной машины PC1 для получения доступа к виртуальному сегменту сети «vnet1».
6. Настроить начальные параметры межсетевого экрана PfSense, для управления использовать виртуальную машину PC1.
7. Настроить параметры VPN-соединения для межсетевого экрана PfSense.
8. Повторить аналогичные шаги 1-7 для виртуального сегмента «vnet2» (делает другая бригада).
9. Проверить прохождение сетевых пакетов через VPN-соединение.
10. В качестве отчёта по лабораторной работе привести содержимое конфигурационных файлов виртуальных машин (расширение *.vbox) и снимки экранов при настройке межсетевого экрана PfSense через web-интерфейс.

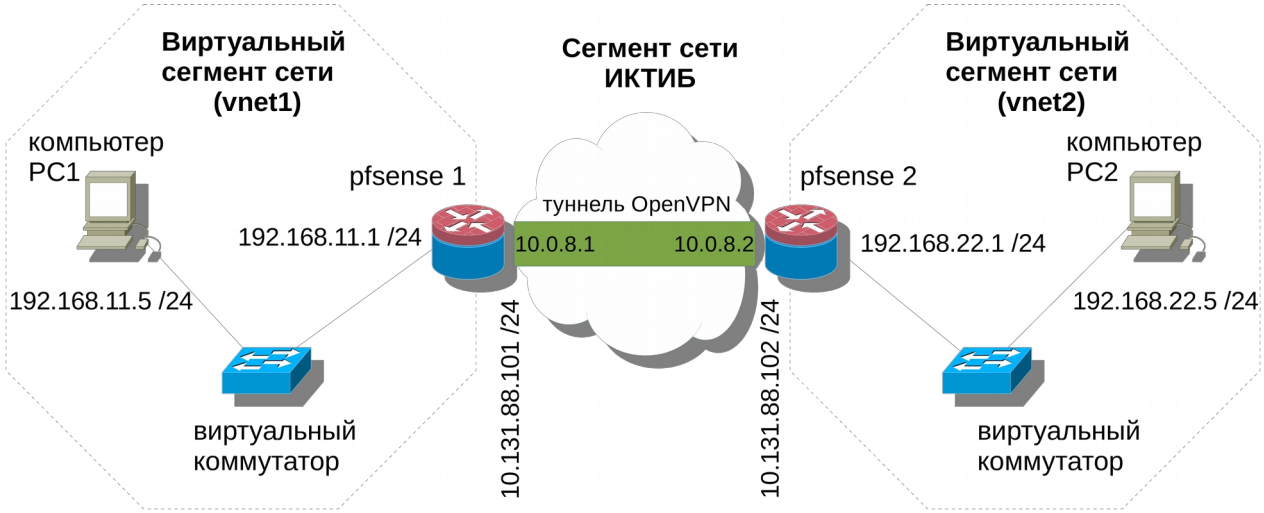
Таблица 1 – Варианты заданий

№ бригады	1	2	3	4	5
Имя межсетевого экрана	pf1	pf2	pf3	pf4	pf5
Имя виртуального сегмента сети	vnet1	vnet2	vnet3	vnet4	vnet5
IP-адрес внешнего интерфейса	10.131.88.101 /24	10.131.88.102 /24	10.131.88.103 /24	10.131.88.104 /24	10.131.88.105 /24
IP-адрес внутреннего интерфейса	192.168.11.1 /24	192.168.22.1 /24	192.168.33.1 /24	192.168.44.1 /24	192.168.55.1 /24
Шлюз для внешнего интерфейса	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24
IP-адрес PC1	192.168.11.5 /24	192.168.22.5 /24	192.168.33.5 /24	192.168.44.5 /24	192.168.55.5 /24

Таблица 1 – Варианты заданий (продолжение)

№ бригады	6	7	8	9	10
Имя межсетевого экрана	pf6	pf7	pf8	pf9	pf10
Имя виртуального сегмента сети	vnet6	vnet7	vnet8	vnet9	vnet101
IP-адрес внешнего интерфейса	10.131.88.106 /24	10.131.88.107 /24	10.131.88.108 /24	10.131.88.109 /24	10.131.88.110 /24
IP-адрес внутреннего интерфейса	192.168.66.1 /24	192.168.77.1 /24	192.168.88.1 /24	192.168.99.1 /24	192.168.101.1 /24
Шлюз для внешнего интерфейса	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24	10.131.88.1/24
IP-адрес PC1	192.168.66.5 /24	192.168.77.5 /24	192.168.88.5 /24	192.168.99.5 /24	192.168.101.5 /24

Пример топологии сети:



Пример выполнения

Необходимое программное обеспечение:
1. Установленная программа виртуализации VirtualBox.
2. ISO-образ межсетевого экрана PfSense.
3. Файлы виртуальной машины «ubuntu_min» для виртуализации компьютеров PC1 и PC2.

1. Развёртывание виртуального сегмента vnet1.

Запускаем программу VirtualBox.

Создаём новую виртуальную машину для межсетевого экрана PfSense:

Создать → Имя «pfsense_1», тип ОС «BSD», версия ОС «FreeBSD».

Объём памяти: 512 МБ

Не подключать виртуальный жёсткий диск.

Подтвердить создание виртуальной машины.

Производим настройку виртуальной машины «pfsense_1»

Во вкладке «Система»:

Отключаем все носители, кроме CD/DVD.

Включаем I/O APIC.

Включаем все возможности по аппаратной виртуализации.

Во вкладке «Носители»:

Указываем для CD/DVD ISO-образ межсетевого экрана PfSense.

Во вкладке «Сеть»:

Включаем «Адаптер 1»:

Указываем тип подключения «Сетевой мост», имя интерфейса «eth1» (тот, который подключен к внешней сети. Просмотр интерфейсов можно осуществить через консольную команду ifconfig.)

Данный интерфейс будем использовать как внешний интерфейс межсетевого экрана PfSense.

Включаем «Адаптер 2»:

Указываем тип подключения «Внутренняя сеть», имя «vnet1», кабель подключен.

Запускаем виртуальную машину «pfsense_1» и выбираем режим загрузки «Boot Multi User».

После успешной загрузки в консоли будет выведена оболочка управления.

```
Starting CRON... done.
Nov  2 22:52:29 php-fpm[331]: /rc.start_packages: Restarting/Starting all packag
es.
pfSense (cdrom) 2.2.4-RELEASE amd64 Sat Jul 25 19:57:37 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-cdrom (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.113/24
 LAN (lan)       -> em1        ->
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

99) Install pfSense to a hard drive, etc.

Enter an option:
```

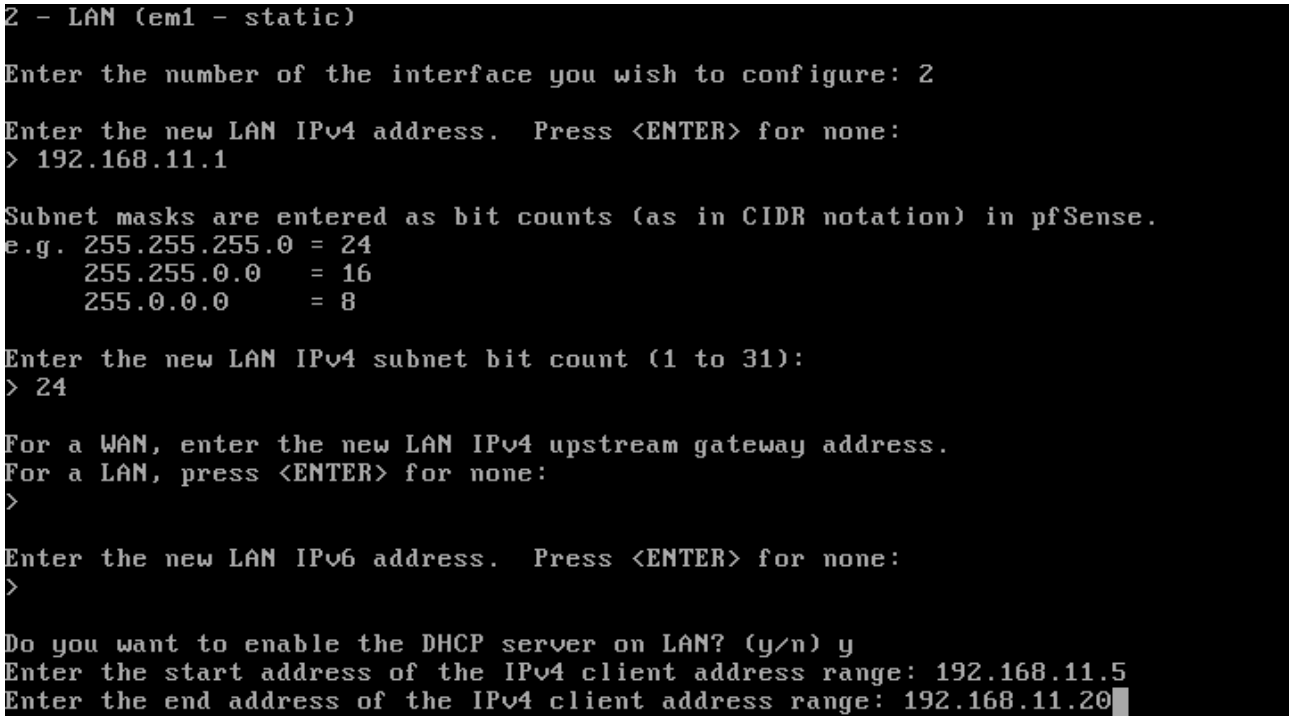
При необходимости следует настроить IP адреса для внешнего (em0) и внутреннего интерфейсов (em1).

Настройка IP адреса для внутреннего интерфейса:

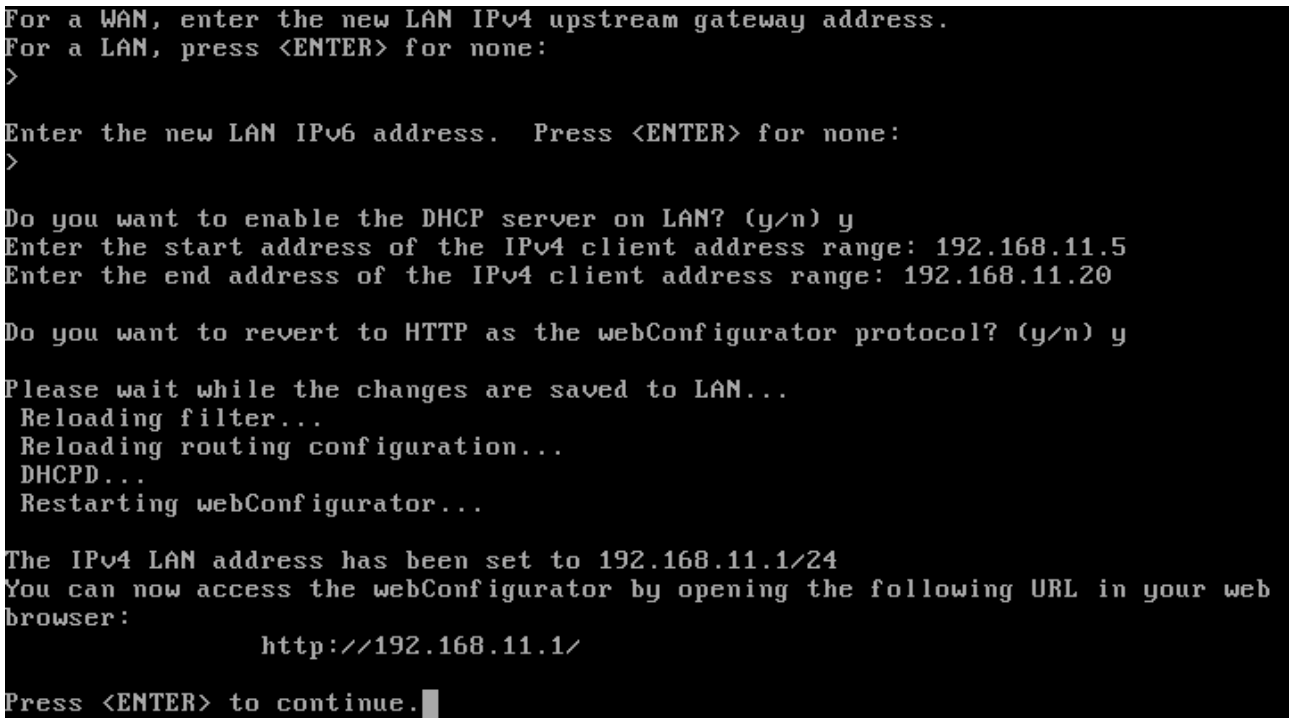
Нажать кнопку «2» для активизации настройки IP-адреса, выбрать интерфейс LAN, задать новый IP-адрес и указать для него маску подсети.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.11.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

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

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

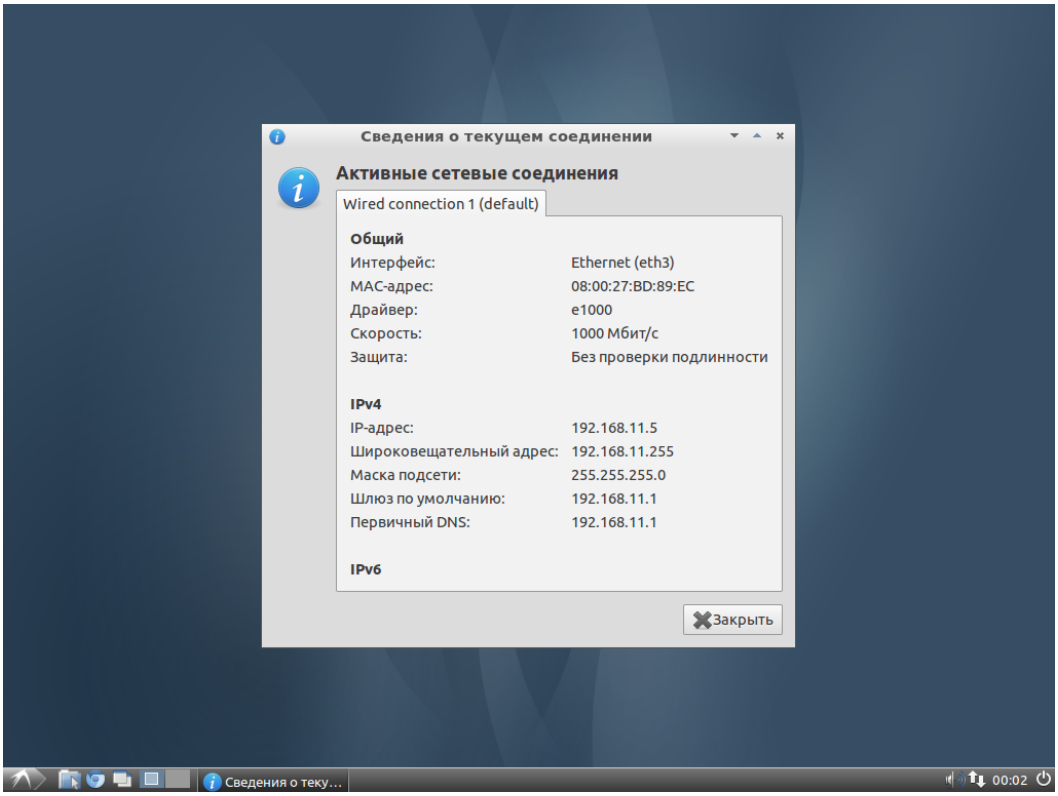
Активировать DHCP сервер на интерфейсе LAN и указать начальный и конечный IP-адреса для автоматического назначения узлам внутренней сети.



Активировать перенастройку webConfigurator под новые параметры интерфейса.



Запускаем виртуальную машину «ubuntu_min», осуществляем вход в ОС используя login: student и passw: studentstudent проверяем сетевые настройки.



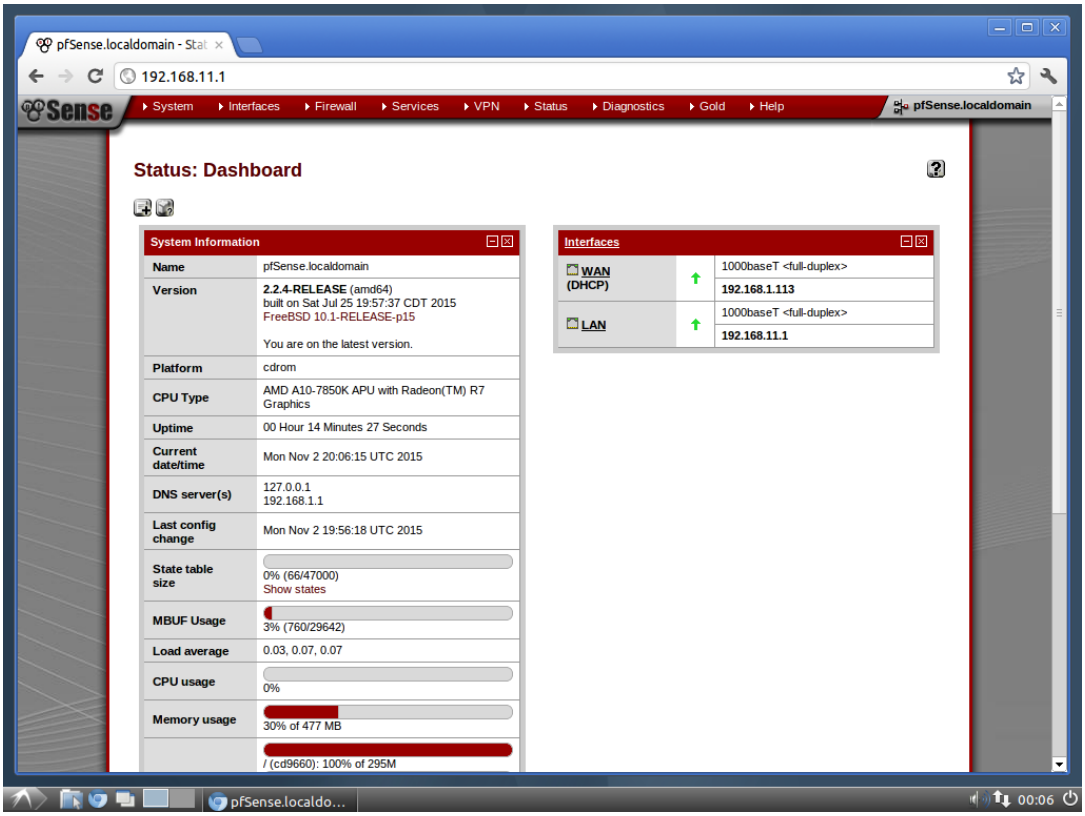
Проверяем связь с внутренним интерфейсом виртуальной машины «pfsense_1»:

ping 192.168.11.1

Запускаем на «ubuntu_min» веб-браузер (chromium) и пытаемся получить доступ к web-интерфейсу управления «pfsense_1». Для этого в строке адреса вводим IP-адрес внутреннего интерфейса «pfsense_1» (192.168.11.1).

После успешного подключения к web-интерфейсу управления «pfsense_1» указываем в качестве username: admin и Password: pfsense.

Результат успешного входа в web-интерфейс управления «pfsense_1»:



2. Настройка «pfsense_1» через web-интерфейс управления.

Создаём OpenVPN сервер:

VPN → OpenVPN → Add Server

Задаём параметры OpenVPN сервера:

Server Mode → to Peer to Peer (Shared Key) (PSK)

Shared Key → set box for automatically generation

Tunnel settings:

IPv4 Tunnel : 10.0.8.0/24 – сеть для виртуального соединения между OpenVPN

IPv4 Remote Network : 192.168.22.0/24

Настраиваем правила фильтрации межсетевого экрана:

Firewall → Rules

на вкладке WAN добавляем новое правило для входящих пакетов:

add rule

protocol → set UDP

Destination → set WAN address

Destination Port → set OpenVPN (1194)

На вкладке OpenVPN добавляем новое правило для входящих пакетов:

add rule

protocol → set any

Переходим назад в VPN->OpenVPN

нажимаем «e» для редактирования OpenVPN сервера и копируем общий ключ (Shared Key) в буфер обмена:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
```

6824dbad7bffe2563aa5ea2ba02b9fd2
82e53f384925d5bd3d0d8da53b339211
42611b47cd010d9b034af0b33128b593
5c03ab9b9116fcd223c99149db8adfe8
27d8a4a32e21608d47ca897785532f84
d62cec087e87bfd0be748add2c2e918e
9146fdab8f836039c3a253650b45cad1
cf8bcc2f31c00f4d6981c951443a3860
30a4c43a9b9916f73dbe658c2d4d7d37
c8415742b73dc716ffa5d908ef838d76
9093c31455eef85862a541bf2c583c7f
178d391551501b189d46f0e44f34a4eb
197ad863863b66dcaac42545063df653
aba1027a8225c330cd21352766221b35
49bad0bc7cfad90327d505c4d7ed8836
33a89fc0d3e90caadf69f3f777a92ae8
-----END OpenVPN Static key V1-----

Преходим к настройке клиента.

3. Развёртывание виртуального сегмента vnet2.

Аналогично развёртыванию виртуального сегмента vnet1, только необходимо указать соответствующие IP-адреса интерфейсов.

4. Настройка «pfsense_2» через web-интерфейс управления.

Настраиваем правила фильтрации межсетевого экрана аналогично «pfsense_1».

После этого, в меню VPN – OpenVPN «pfsense_2» переходим на вкладку Client и нажимаем кнопку “+” для создания клиента:

Server Mode → to Peer to Peer (Shared Key) (PSK)
Server host or address → 10.131.88.105 (адрес внешнего интерфейса pfsense с OpenVPN сервером)

Снять опцию «automatically generate a shared key» и вставить общий ключ, скопированный ранее с OpenVPN сервера.

Указать сеть для туннеля и удалённую сеть:

IPv4 Tunnel Network → 10.0.8.0/24
IPv4 Remote Network/s → 192.168.11.0/24

Проверить соединение с OpenVPN сервером, для этого смотрим информацию во вкладке «Status – OpenVPN». Если соединение не устанавливается, то переходим на сервере (pfsense_1) во вкладку

Status → System Logs → Firewall

видим, что от 10.131.88.106:44545 блокируются входящие соединения.

Нажимаем на красный крест в событии для просмотра дополнительной информации и получаем информацию вида

The rule that triggered this action is:

@62(1000001584) block drop in log quick on em0 inet from 192.168.0.0/16 to any label "Block private networks from WAN block 192.168/16"

Где поясняется, что блокировка идёт правилом «Block private networks».

Переходим в меню «Firewall: Rules» и видим, что удалить правило «Block private networks» не можем, но после нажатия «edit rules», переходим на вкладку, где его можно отключить.

Аналогично удаляем блокирующее правило на клиенте.

5. Проверка VPN-соединения.

Из виртуальной сети «vnet_1» проверяем прохождение пакетов в сеть «vnet_2». Для этого на виртуальной машине «ubuntu_min» сети «vnet_1» запускаем команду:

```
ping 192.168.22.5
```

для проверки связи с «ubuntu_min» сети «vnet_2».