

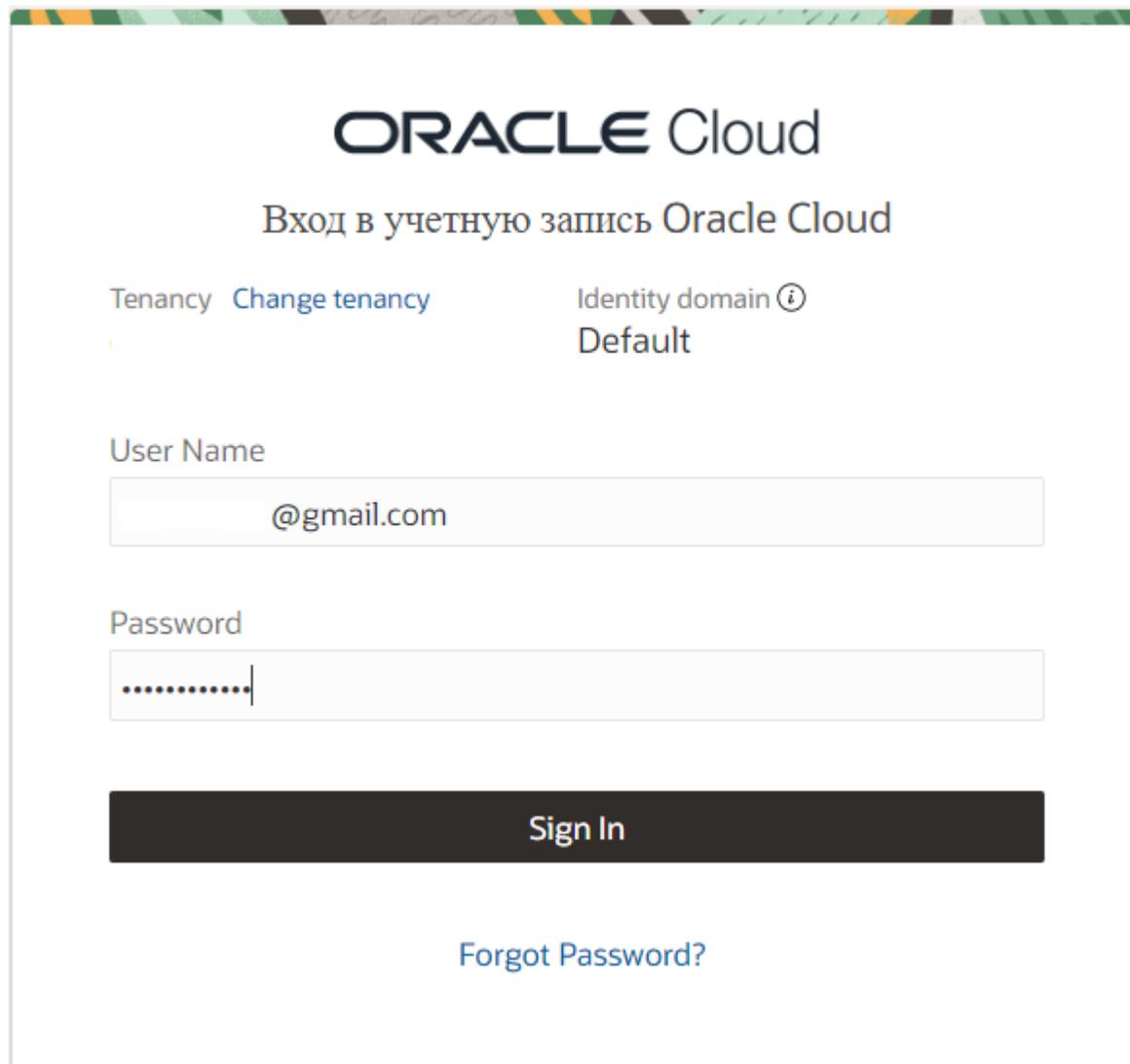
Настройка IPSec VPN туннеля между ZyWALL и Ubuntu на базе VPS сервера с маршрутизацией трафика через сервер

Содержание:

- [Создание и настройка VPS сервера](#)
- [Настройка IPSec VPN в Ubuntu](#)
- [Настройка IPSec VPN на ZyWALL](#)
- [Настройка маршрутизации](#)
- [Проверка работоспособности](#)

Создание и настройка VPS сервера

В качестве примера мы будем использовать бесплатный VPS сервер от Oracle (<https://www.oracle.com/cloud/free/>).



ORACLE Cloud

Вход в учетную запись Oracle Cloud

Tenancy [Change tenancy](#) Identity domain ⓘ
Default

User Name

@gmail.com

Password

.....|

Sign In

[Forgot Password?](#)

После регистрации и авторизации в Oracle Cloud необходимо создать виртуальную машину для установки Ubuntu.

Quickstarts

FEATURED

Predict the result of the next race

25-30 mins



APPLICATION DEVELOPMENT

Deploy a low-code app on Autonomous Database using APEX

3-5 mins

Always Free Eligible

APPLICATION DEVELOPMENT

Deploy a baseline landing zone

7-9 mins

COLLABORATION

Deploy self-hosted productivity platform Nextcloud

4-6 mins

Launch Resources

COMPUTE

Create a VM instance

2-6 mins

Always Free Eligible

AUTONOMOUS TRANSACTION PROCESSING

Create an ATP database

3-5 mins

Always Free Eligible

NETWORKING

Set up a network with a wizard

2-3 mins

RESOURCE MANAGER

Create a stack

2-6 mins

Always Free Eligible

Укажите любое имя и нажмите кнопку Edit в разделе Image and share для выбора образа в виртуальной машине.

Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

Create in compartment

Placement

[Edit](#)

Availability domain: AD-1

Capacity type: On-demand capacity

Fault domain: Let Oracle choose the best fault domain

Image and shape

[Edit](#)

Image: Oracle Linux 8

Image build: 2022.04.04-0

Shape: VM.Standard.E2.1.Micro Always Free-eligible

OCPU count: 1

Memory (GB): 1

Network bandwidth (Gbps): 0.48

Нажмите кнопку Change Image для смены образа.

Create compute instance

Fault domain: Let Oracle choose the best fault domain

Image and shape

[Collapse](#)

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image

 Oracle Linux 8 
Image build: 2022.04.04-0

[Change image](#)

Shape

 VM.Standard.E2.1.Micro Always Free-eligible
Virtual machine, 1 core OCPU, 1 GB memory, 0.48 Gbps network bandwidth

[Change shape](#)

Выберите образ Ubuntu (в качестве примера будет использоваться версия 20.04).

Browse all images

An image is a template of a virtual hard drive that determines the operating system and other software for an instance.

Image source

Platform images

Compartment

(root)

[Platform images](#) are pre-built operating systems for Oracle Cloud Infrastructure.

Image name	OS version	Image build
<input checked="" type="checkbox"/> Canonical Ubuntu <small>Always Free-eligible</small> 	20.04 	2022.03.02-0 
<input type="checkbox"/> CentOS <small>Always Free-eligible</small> 	8	2021.12.03-0
<input type="checkbox"/> Oracle Autonomous Linux <small>Always Free-eligible</small>	7.9	
<input type="checkbox"/> Oracle Linux <small>Always Free-eligible</small> 	8	2022.04.04-0

В разделе Networking создаём новые виртуальные сети в облаке или выбираем существующие, обязательно укажите Assign a public IPv4 address, чтобы сервер был доступен из интернета.

Create compute instance

Image: Canonical Ubuntu 20.04

Image build: 2022.03.02-0

Shape: VM.Standard.E2.1.Micro Always Free-eligible

OCPU count: 1

Memory (GB): 1

Network bandwidth (Gbps): 0.48

Networking [Collapse](#)

[Networking](#) is how your instance connects to the internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

Primary network

Select existing virtual cloud network Create new virtual cloud network Enter subnet OCID

Virtual cloud network in (root) [\(Change Compartment\)](#)

vcn-20 

Subnet

Select existing subnet Create new public subnet

Subnet in (root) [\(Change Compartment\)](#)

subnet-20 

Public IP address

Assign a public IPv4 address Do not assign a public IPv4 address

Затем необходимо сгенерировать SSH ключ для аутентификации на сервере, в качестве примера мы будем использовать утилиту PuTTYgen (она устанавливается вместе с SSH

клиентом Putty, который можно скачать на официальном сайте: <https://www.putty.org>).
Запустите её и нажмите кнопку Generate.

Create compute instance

The image shows the 'Add SSH keys' section of the AWS console. It includes options to generate a key pair, upload public key files, paste public keys, or use no SSH keys. Below these are instructions to download the private key and buttons for 'Save Private Key' and 'Save Public Key'. To the right, the PuTTY Key Generator utility is open, showing the 'Generate' button circled in red. The utility is configured to generate an RSA key with 2048 bits.

Водите мышкой по экрану, пока не будет создан ключ, который нужно копировать в буфер обмена (пока не закрываете утилиту PuTTYgen).

The image shows the PuTTY Key Generator utility with the 'Generate' button highlighted. The 'Key' section displays the generated public key, which is circled in red. The key is: ssh-rsa AAAAF... The 'Key fingerprint' is ssh-rsa 2048 SHA256... The 'Key comment' is rsa-key-20220419. The 'Parameters' section shows 'Type of key to generate' set to RSA and 'Number of bits in a generated key' set to 2048.

Выберите далее в настройках SSH - Paste public keys и вставьте ключ в строку ниже. Затем нажмите кнопку Create.

Create compute instance

Add SSH keys

Generate an [SSH key pair](#) to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

Generate a key pair for me Upload public key files (.pub) Paste public keys No SSH keys

SSH keys

ssh-rsa AA/

Example: ssh-rsa AAAAB3Nza...NWap6Prb ssh-key-2021-01-27 [See all supported key types](#)

Boot volume

A [boot volume](#) is a detachable device that contains the image used to boot the compute instance.

После создания виртуальной машины запустится процесс настройки, который займёт некоторое время.

[Compute](#) » [Instances](#) » [Instance details](#) » Work requests



Server

Always Free

Start

Stop

Reboot

Edit

More Actions

Instance information

Shielded instance

Oracle Cloud Agent

Tags

General information

Availability domain: AD-1

Fault domain: FD-3

Region: eu-amsterdam-1

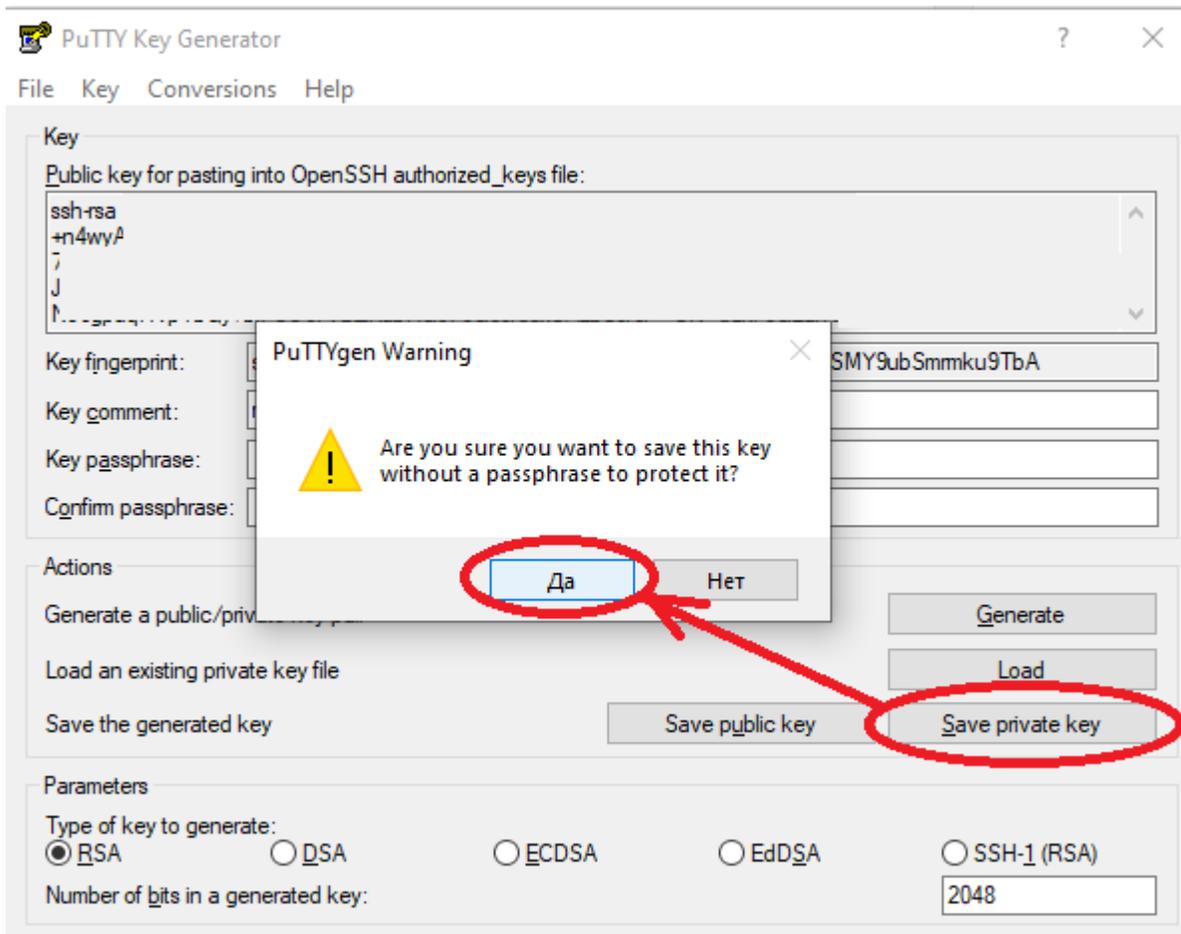
OCID: ...afs2rq [Show](#) [Copy](#)

Launched: Tue, Apr 19, 2022, 09:05:41 UTC

Compartment: (root)

Capacity type: On-demand

Тем временем в утилите PuTTYgen сохраняем закрытый ключ в надёжное место (без этого ключа вы больше никогда не сможете получить доступ к серверу). Путь к ключу также не должен содержать кириллицу.



В панели управления виртуальной машины ожидаем статуса RUNNING, затем открываем настройки виртуальной сети.



RUNNING

Server ██████████ Always Free

[Start](#) [Stop](#) [Reboot](#) [Edit](#) [More Actions](#) ▾

[Instance information](#) [Shielded instance](#) [Oracle Cloud Agent](#) [Tags](#)

General information

Availability domain: AD-1
Fault domain: FD-3
Region: eu-amsterdam-1
OCID: ...afs2rq [Show](#) [Copy](#)
Launched: Tue, Apr 19, 2022, 09:05:41 UTC
Compartment: ██████████ (root)
Capacity type: On-demand

Instance details

Virtual cloud network: [vcn-20](#) ██████████
Maintenance reboot: -
Image: [Canonical-Ubuntu-20.04-2022.03.02-0](#)

В разделе Resources нужно открыть Security Lists и выбрать Default Security List.



AVAILABLE

vcn-20

Move resource

Add Tags

Terminate

VCN Information

Tags

Compartment: (root)

Created: Fri, Apr 15, 2022, 08:34:17 UTC

IPv4 CIDR Block: 10.0.0.0/16

IPv6 Prefix: No Value

Resources

Subnets (1)

CIDR Blocks/Prefixes (1)

Route Tables (1)

Internet Gateways (1)

Dynamic Routing Gateways
Attachments (0)

Network Security Groups (0)

Security Lists (1)

Security Lists in (root) Compartment

Create Security List

Name

State

[Default Security List for vcn-20](#)

● Available



Затем в разделе Ingress Rules добавляем разрешающее правило для UDP портов 500/4500, которые используются при построении IPSec VPN туннеля. В качестве источника указаны все адреса (0.0.0.0/0), но вы можете указать только адрес шлюза.

Networking » Virtual Cloud Networks » vcn-20* » Security List Details

Default Security List

Instance traffic is controlled by the default security list.

SL

AVAILABLE

Resources

Ingress Rules (5)

Egress Rules (1)

Add Ingress Rules

Ingress Rule 1

Allows UDP traffic 500,4500

Stateless ⓘ

Source Type: CIDR

Source CIDR: 0.0.0.0/0

IP Protocol: UDP

Source Port Range: All

Destination Port Range: 500,4500

Description: VPN

[+ Another Ingress Rule](#)

[Add Ingress Rules](#) [Cancel](#)

После добавления правила вы увидите соответствующие разрешения для UDP портов.

Ingress Rules

[Add Ingress Rules](#) [Edit](#) [Remove](#)

<input type="checkbox"/>	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	
<input type="checkbox"/>	No	0.0.0.0/0	UDP	All	500		UDP traffic for ports: 500	VPN
<input type="checkbox"/>	No	0.0.0.0/0	UDP	All	4500		UDP traffic for ports: 4500	VPN

Возвращаемся к панели управления виртуальной машиной, копируем публичный IP-адрес и вставляем его в SSH клиенте Putty.

Server

Always Free

Start Stop Reboot Edit More Actions

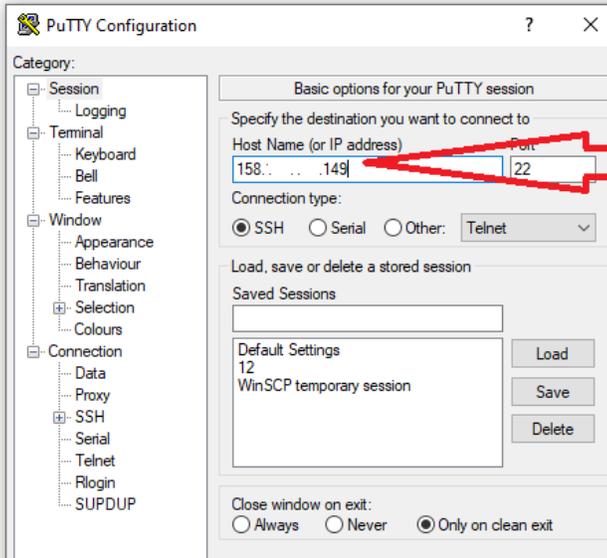
Instance information Shielded instance Oracle Cloud Agent Tags

General information

Availability domain: AD-1
Fault domain: FD-3
Region: eu-amsterdam-1
OCID: ...afs2rq Show Copy
Launched: Tue, Apr 19, 2022, 09:05:41 UTC
Compartment: (root)
Capacity type: On-demand

Instance details

Virtual cloud network: [vcn-20](#)
Maintenance reboot: -
Image: [Canonical-Ubuntu-20.04-2022.03.02-0](#)



Instance access

You [connect to a running Linux instance](#) using a key pair that was used to create the instance

Public IP address [158.149.149.149](#) Copy

Username: ubuntu

Primary VNIC

Private IP address: 10.0.0.118

Network security groups: None [Edit](#)

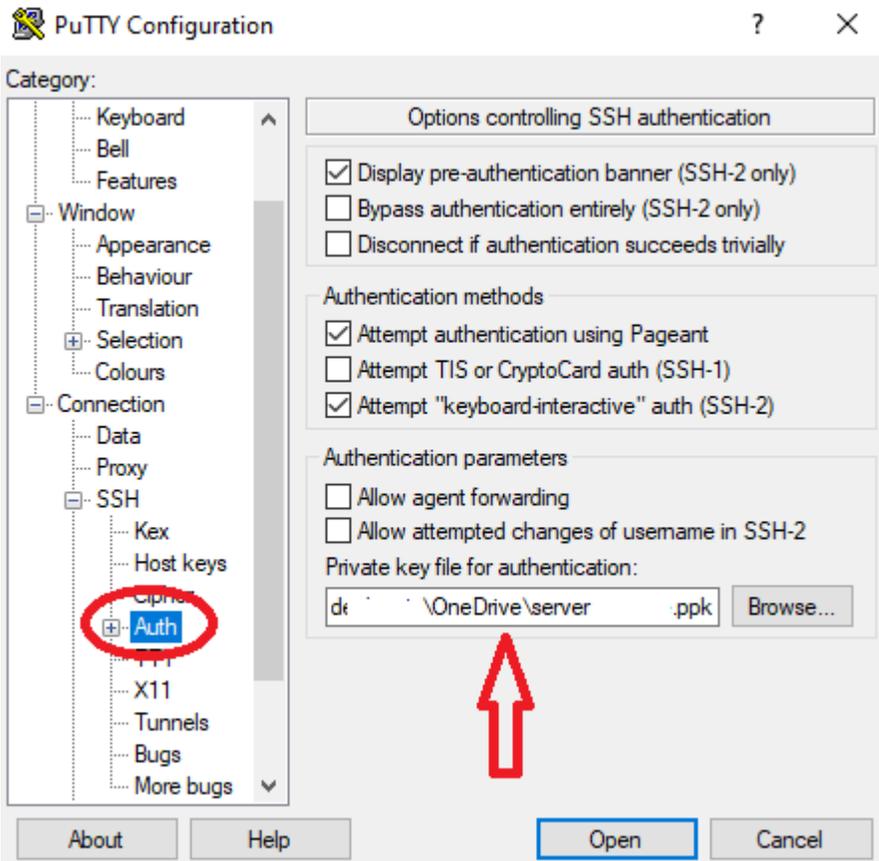
Subnet: [subnet-20](#)

Private DNS record: Enable

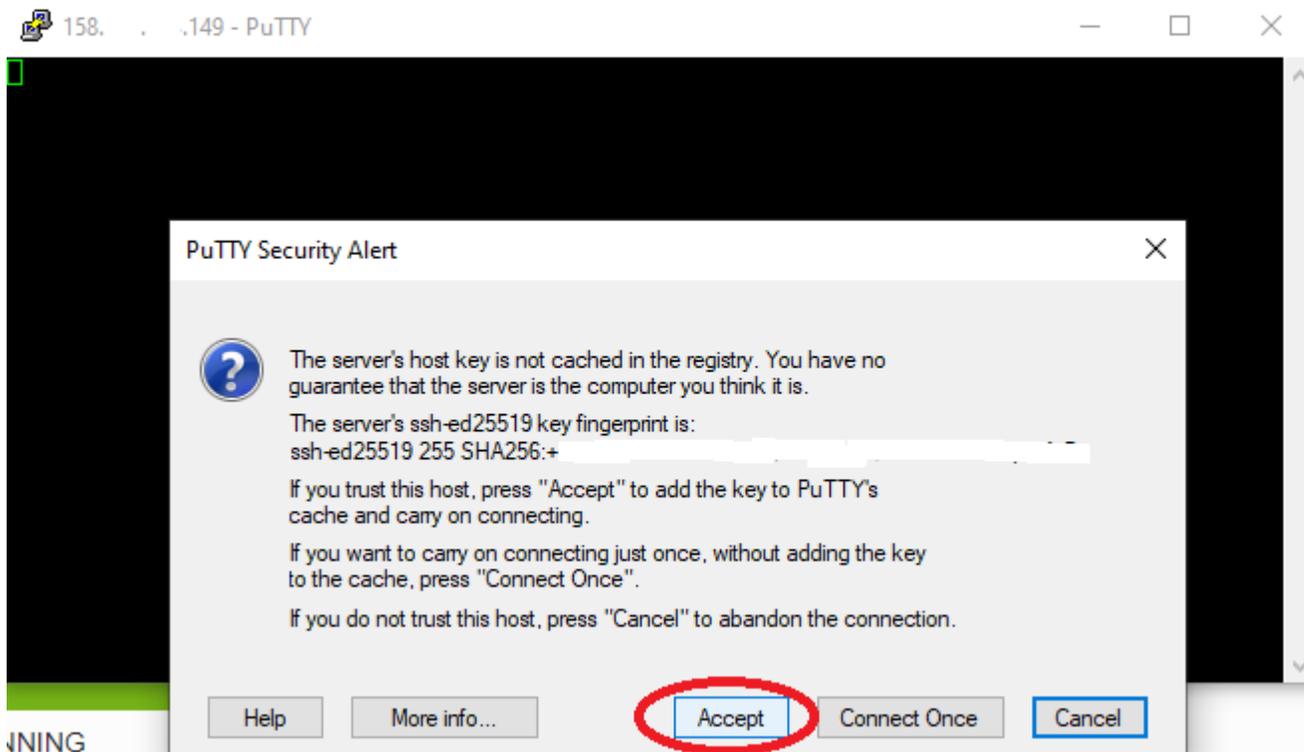
Hostname: server

Internal FQDN: server [Show](#)

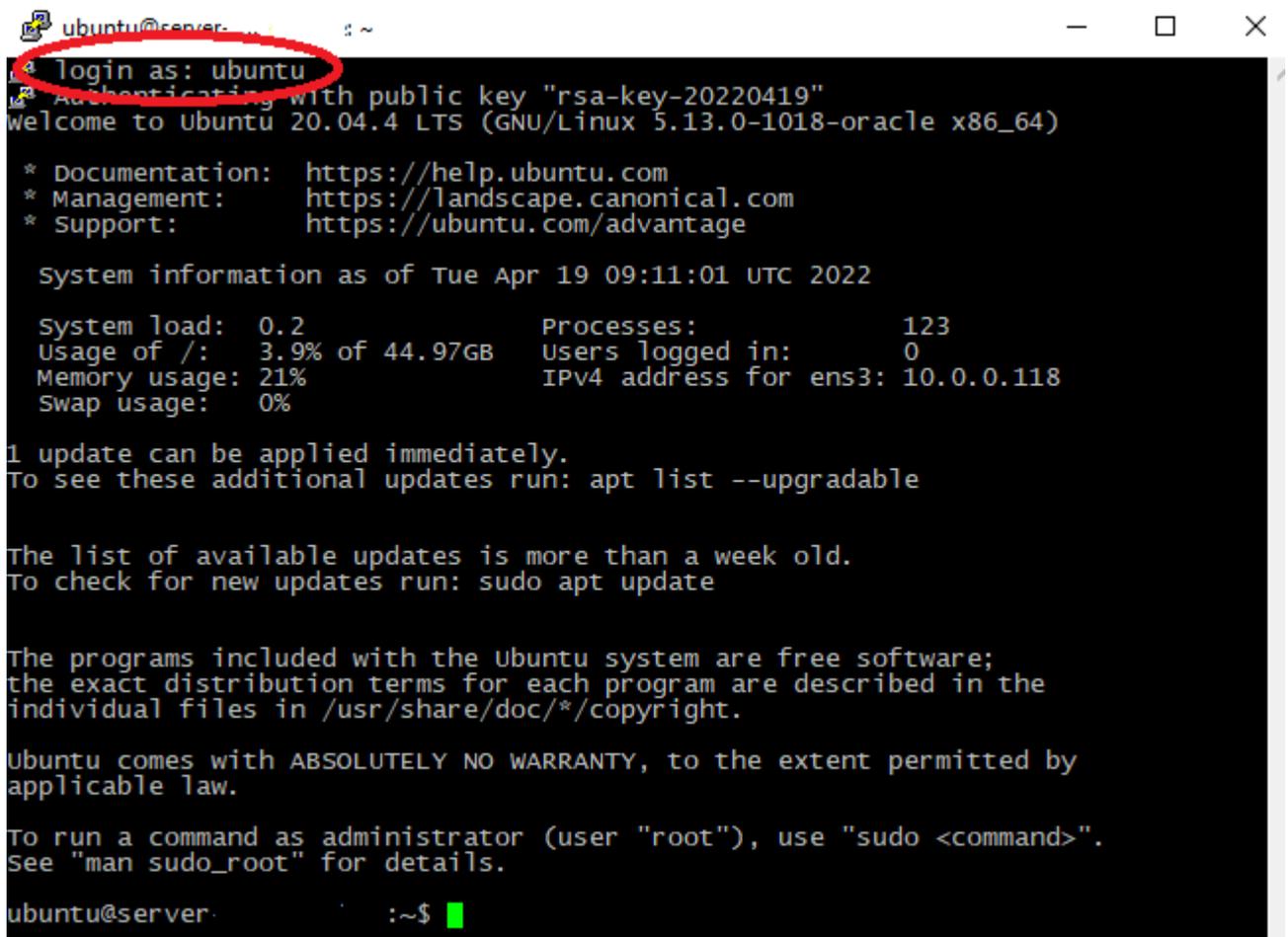
В настройках Putty открываем раздел Connection – SSH – Auth и в строке Private key указываем путь к ранее сохраненному закрытому ключу. Затем запускаем соединение, нажав кнопку Open.



В открывшемся окне необходимо нажать кнопку Accept.



Далее вводим имя пользователя "ubuntu" (у него пока нет пароля) и подключаемся к нашему серверу.



Обязательно нужно установить пароль при помощи команды `sudo passwd ubuntu`.

```
ubuntu@server-1... :~$ sudo passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
ubuntu@server-1... :~$
```

Теперь можно переходить к следующему шагу.

Настройка IPsec VPN в Ubuntu

Вводим поочерёдно следующие команды для установки пакета `libreswan`, который отвечает за работу IPsec, и пакета `net-tools` для использования сетевых утилит:

```
sudo apt-get update
```

```
sudo apt-get upgrade (здесь нужно будет нажать Y для согласия)
```

```
sudo apt-get install libreswan (Y)
```

```
sudo apt install net-tools
```

Дожидаемся установки пакетов и определяем локальный адрес сервера при помощи команды `ifconfig`.

`ens3: inet 10.0.0.118` – это локальный адрес сервера (он может быть другим)

Открываем настройки ядра при помощи команды `sudo nano /etc/sysctl.conf` и вставляем следующие строки для форвардинга пакетов и отключения ICMP редиректов:

```
net.ipv4.ip_forward = 1
```

```
net.ipv4.conf.all.accept_redirects = 0
```

```
net.ipv4.conf.all.send_redirects = 0
```

```
net.ipv4.conf.default.accept_redirects = 0
```

```
net.ipv4.conf.default.send_redirects = 0
```

Так это будет выглядеть в командной строке:

```
ubuntu@server- ~
GNU nano 4.8 /etc/sysctl.conf Modified
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPV6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Затем нажимаем Ctrl+X для выхода, Y для сохранения и Enter для продолжения.

Вводим команду `sudo sysctl -p` для сохранения настроек.

Чтобы создать конфигурацию IPsec VPN, используйте команду `sudo nano /etc/ipsec.d/route-based-ipsec-vpn.conf` и вставьте следующие строки:

`config setup`

`protostack=netkey`

`conn vpn`

`authby=secret`

`pfs=no`

`rekey=yes`

`keyingtries=3`

`type=tunnel`

auto=start

ike=aes256-sha1;modp1536 - алгоритмы шифрования 1 фазы

phase2alg=aes256-sha1;modp1536 - алгоритмы шифрования 2 фазы

left=10.0.0.118 - локальный адрес сервера

leftid=158.xxx.xxx.149 - публичный адрес сервера

right=109.xxx.xxx.6 - адрес шлюза

leftsubnet=1.1.1.1/32 - локальная политика (local policy)

rightsubnet=192.168.11.1/32 - удаленная политика (remote policy)

mark=5/0xffffffff

vti-interface=vti01

vti-routing=no

Локальная политика – это адрес (подсеть), к которому нужен доступ со стороны ZyWALL через туннель с сервером.

Удаленная политика – это адрес (подсеть) на стороне ZyWALL, который должен иметь доступ к адресу в локальной политике через туннель с сервером.

В данном примере мы будем использовать LAN IP адрес ZyWALL, т.е. сам шлюз будет обращаться к адресу 1.1.1.1 через туннель с сервером, а не через WAN-интерфейс. Вы можете указать в локальной политике, например, весь диапазон адресов, а в удаленной – всю локальную подсеть ZyWALL – в таком случае весь трафик будет идти через туннель.

Затем нажимаем Ctrl+X для выхода, Y для сохранения и Enter для продолжения.

С помощью команды *sudo nano /etc/ipsec.d/route-based-ipsec-vpn.secrets* добавляем строку с pre-shared key:

158.xxx.xxx.149 109.xxx.xxx.6: PSK "12345678"

где 158.xxx.xxx.149 – это публичный адрес сервера, 109.xxx.xxx.6 – адрес шлюза, 12345678 – pre-shared key (без кавычек)

Нажимаем Ctrl+X для выхода, Y для сохранения и Enter для продолжения.

После этого проверяем конфигурацию при помощи команд:

sudo ipsec restart

sudo ipsec verify

```
ubuntu@server:~$ sudo ipsec verify
verifying installed system and configuration files

version check and ipsec on-path [OK]
Libreswan 3.29 (netkey) on 5.13.0-1018-oracle
Checking for IPsec support in kernel [OK]
NETKEY: Testing XFRM related proc values
  ICMP default/send_redirects [OK]
  ICMP default/accept_redirects [OK]
  XFRM larval drop [OK]
Pluto ipsec.conf syntax [OK]
Checking rp_filter [OK]
Checking that pluto is running [OK]
Pluto listening for IKE on udp 500 [OK]
Pluto listening for IKE/NAT-T on udp 4500 [OK]
Pluto ipsec.secret syntax [OK]
checking 'ip' command [OK]
checking 'iptables' command [OK]
checking 'prelink' command does not interfere with FIPS [OK]
checking for obsolete ipsec.conf options [OK]
ubuntu@server:~$
```

Если ошибок нет, то можно перейти к настройке IPsec на ZyWALL.

[Настройка IPsec VPN на ZyWALL](#)

Для настройки 1 фазы IPsec VPN откройте раздел Configuration – VPN – IPsec VPN – VPN Gateway и внесите следующие настройки (обязательно укажите версию IKEv2):

Edit VPN Gateway Ubuntu [?] [X]

Hide Advanced Settings Create New Object ▼

Enable

VPN Gateway Name:

IKE Version

IKEv1

IKEv2

Gateway Settings

My Address

Interface **IP-адрес шлюза** DHCP client -- 109. . . /255.255.255.0

Domain Name / IPv4

Peer Gateway Address **Публичный IP-адрес сервера**

Static Address ⓘ

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

Dynamic Address ⓘ

Authentication

Pre-Shared Key

unmasked

Certificate (See [My Certificates](#))

Advance

Local ID Type:

Content:

Peer ID Type:

Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Advance

Proposal

#	Encryption	Authentication
1	AES256	SHA1

Key Group:

OK Cancel

Затем откройте меню Configuration – VPN – IPsec VPN – VPN Connection и добавьте 2 фазу IPsec VPN:

Edit VPN Connection Ubuntu

Hide Advanced Settings Create New Object

General Settings

Enable

Connection Name:

Advance

- Nailed-Up
- Enable Replay Detection
- Enable NetBIOS broadcast over IPSec

MSS Adjustment

Custom Size (200 - 1460 Bytes)

Auto

Narrowed

VPN Gateway

Application Scenario

- Site-to-site**
- Site-to-site with Dynamic Peer
- Remote Access (Server Role)
- Remote Access (Client Role)
- VPN Tunnel Interface **1 фаза IPSec**

VPN Gateway: wan1 158. . .149,0.0.0

Policy

Локальная политика (в данном случае LAN IP шлюза)

Local Policy: INTERFACE IP, 192.168.11.1

Remote Policy: HOST, **1.1.1.1**

Advance **Удаленная политика**

- Enable GRE over IPSec
- Policy Enforcement

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

Advance

Active Protocol:

Encapsulation:

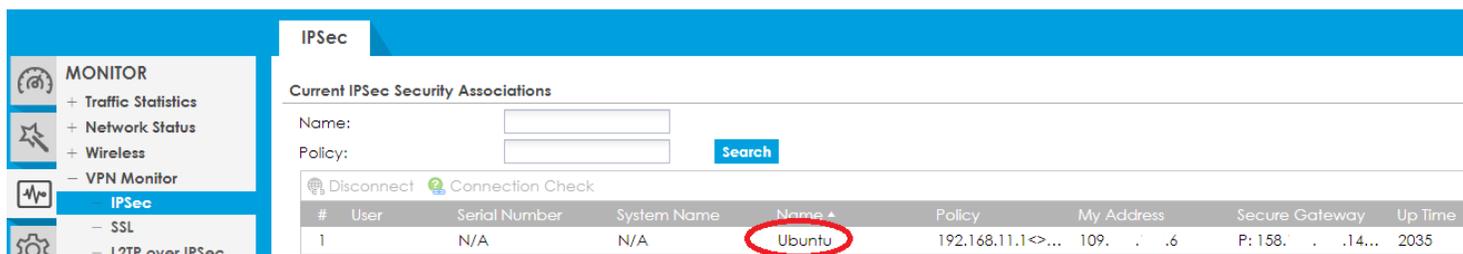
Proposal

+ Add Edit Remove		
#	Encryption	Authentication
1	AES256	SHA1

Perfect Forward Secrecy (PFS):

Если всё настроено верно, то в течение минуты туннель поднимется и можно перейти к дальнейшей настройке.

Проверить установку туннеля можно в разделе Monitor – VPN Monitor – IPsec:



The screenshot shows the IPsec configuration interface. On the left is a sidebar with a 'MONITOR' section containing 'Traffic Statistics', 'Network Status', 'Wireless', 'VPN Monitor', 'IPSec', 'SSL', and 'L2TP over IPsec'. The main area is titled 'IPSec' and 'Current IPsec Security Associations'. It has search fields for 'Name' and 'Policy' with a 'Search' button. Below are 'Disconnect' and 'Connection Check' buttons. A table lists security associations:

#	User	Serial Number	System Name	Name *	Policy	My Address	Secure Gateway	Up Time
1		N/A	N/A	Ubuntu	192.168.11.1<>...	109. . . .6	P: 158. . . .14...	2035

Или при помощи команды `sudo systemctl status ipsec` в Ubuntu.

Настройка маршрутизации

Теперь нужно добавить правила маршрутизации и фаервола на Ubuntu (мы не будем подробно рассматривать их настройку, укажем только минимально необходимые правила для образа Ubuntu в VPS от Oracle).

Маршрут в локальную сеть ZyWALL:

```
sudo ip route add 192.168.11.1/32 dev vti01
```

Маскарадинг для трафика:

```
sudo iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE
```

Удаление дефолтного запрещающего правила в цепочке FORWARD:

```
sudo iptables -D FORWARD 1
```

Список всех правил фаервола можно посмотреть командой:

```
sudo iptables -L
```

Для проверки прохождения трафика можно запустить захват пакетов на туннельном интерфейсе:

```
sudo tcpdump -i vti01 -n
```

На стороне ZyWALL также необходимо добавить правила маршрутизации (политики безопасности мы менять не будем, так как по умолчанию трафик для IPsec VPN разрешен в обе стороны).

Для нашего случая, чтобы **сам шлюз** отправлял трафик к адресу 1.1.1.1 в туннель, нужно добавить статический маршрут в меню Configuration – Network – Routing – Static Route:

IPv4 Static Route Setting

Destination IP: 1.1.1.1

Subnet Mask: 255.255.255.255

Gateway IP

Interface: lan1

Metric: 0

Интерфейс с адресом 192.168.11.1

OK Cancel

Для локальных хостов требуется создавать политику маршрутизации в разделе Configuration – Network – Routing – Policy Route:

Add Policy Route

Show Advanced Settings Create New Object

Configuration

Enable

Description: (Optional)

Criteria

User: any

Incoming: any (Excluding ZyV

Source Address: LAN1_SUBNET **Подсеть с локальными хостами**

Destination Address: IP_1_1_1_1 **1.1.1.1**

DSCP Code: any

Schedule: none

Service: any

Next-Hop

Type: VPN Tunnel

VPN Tunnel: Ubuntu **IPSec VPN туннель**

DSCP Marking

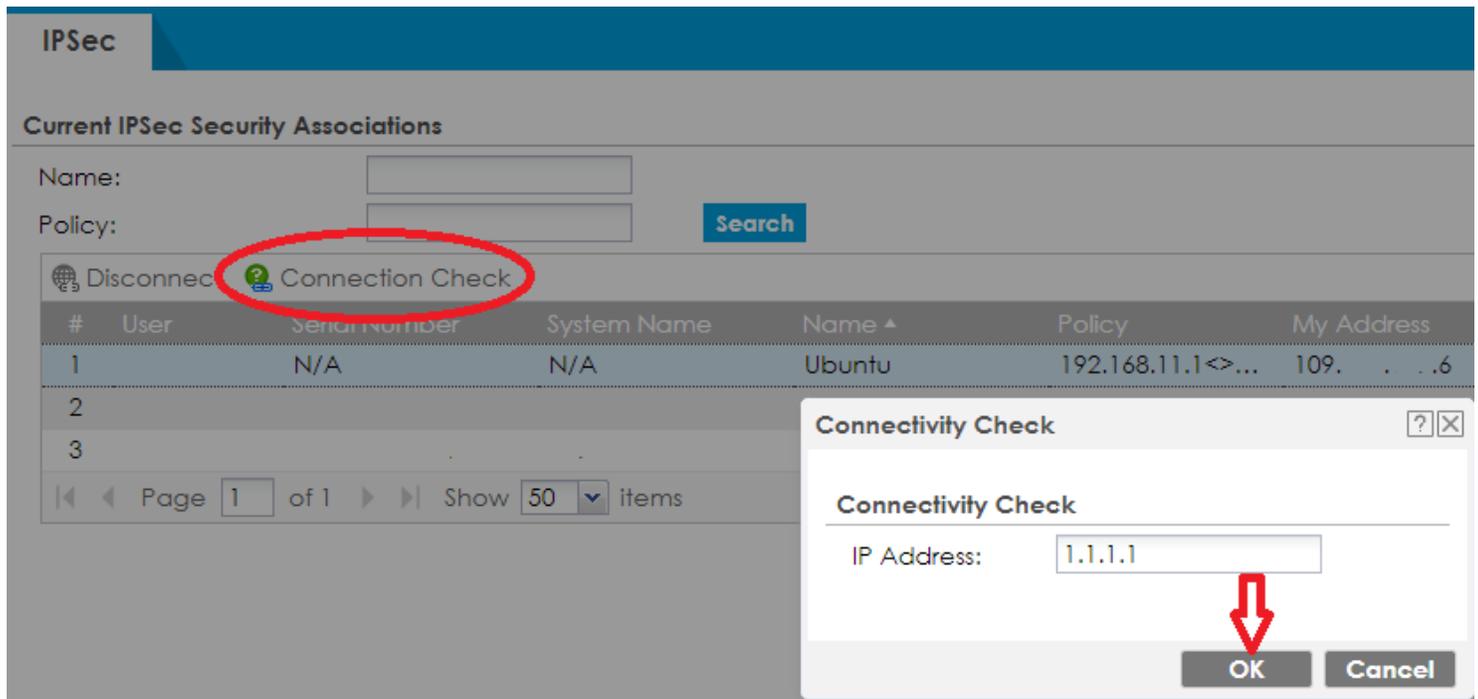
DSCP Marking: preserve

Advance

OK Cancel

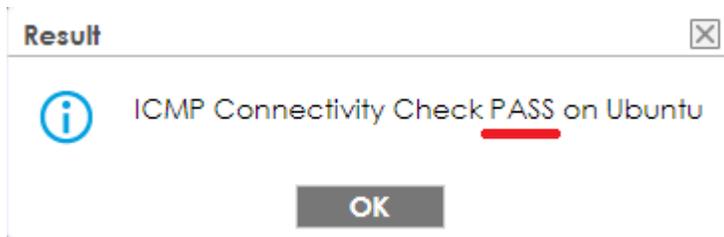
Проверка работоспособности

Проверить прохождение трафика через туннель можно в меню Monitor – VPN Monitor – IPSec:



The screenshot shows the 'IPSec' configuration window. Under 'Current IPSec Security Associations', there is a table with columns: #, User, Serial Number, System Name, Name, Policy, and My Address. The first row shows a connection to 'Ubuntu' with serial number 'N/A'. A 'Connection Check' button is circled in red. A dialog box titled 'Connectivity Check' is open, with 'IP Address: 1.1.1.1' and 'OK'/'Cancel' buttons. A red arrow points to the 'OK' button.

Если всё настроено корректно, то будет положительный результат:



The screenshot shows a 'Result' dialog box with an information icon and the text 'ICMP Connectivity Check PASS on Ubuntu'. An 'OK' button is at the bottom.

При этом на стороне Ubuntu, если включить захват трафика, будут видны ICMP пакеты:

```
ubuntu@server:~$ sudo tcpdump -i vti01 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vti01, link-type RAW (Raw IP), capture size 262144 bytes
15:08:30.215322 IP 192.168.11.1 > 1.1.1.1: ICMP echo request, id 17770, seq 20668, length 40
15:08:30.223856 IP 1.1.1.1 > 192.168.11.1: ICMP echo reply, id 17770, seq 20668, length 40
```

