

Mikrotik събитие
за професионалисти ентусиасти
и всички, които имат желание да
се забавляват!

NetCamp 2020



WIREGUARD VPN B Mikrotik v7

Рожен 08.2020

Да се запознаем



инж. Георги Анастасов

*За мен! Сертифициран мрежов специалист и консултант за продукти на **Mikrotik**, с опит в проектиране и изграждане на малки и средни компютърни мрежи, сървъри и системи за архивиране.*

WEB: www.steadypc.com

E-mail: office@steadypc.com

GSM: +359 878806291



IPsec със сертификати.

Съдържание

01 **Wireguard** описание
Начин на работа. Автентикация, криптиране, портове, роуминг.

02 **Wireguard server**
Изисквания към ROS Генериране на ключове. Настройка.

03 **Wireguard клиент**
Настройка. Mikrotik client. Други клиенти



Wirguard

Описание. Начин на работа.
Автентикация, криптиране, портове,
роуминг.

01



Wireguard Описание

- ❑ [Curve25519](#) за key exchange
- ❑ [ChaCha20](#) за криптиране
- ❑ [Poly1305](#) за автентикация
- ❑ [SipHash](#) за hashtable keys
- ❑ [BLAKE2s](#) за hashing
- ❑ UDP-базиран.



Wireguard Описание Networks

1. Работи само с UDP.
2. Layer3 тунел.
3. IPv4, IPv6, V4-in-V6.
4. Топология.
 - Mesh, Point to point, Star - клиент/сървър.
5. Routing на клиентите.



Wireguard Описание Networks

MTU 1420

- 40 bytes for an IPv6 header without extension headers (20 bytes for IPv4 without options).
- 8 bytes for the UDP header.
- 32 bytes for the WireGuard message header: 4 bytes for the type and a reserved field, 4 bytes for the receiver index, 8 bytes for the message counter, and finally 16 bytes for the authentication tag.

<https://www.wireguard.com/papers/wireguard.pdf>

<https://lekensteyn.nl/files/pwu-wireguard-thesis-final.pdf>



Wireguard Описание Networks

```
C:\TEMP>mturoute 10.0.1.1
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
- ICMP payload of 1472 bytes is too big.
+ ICMP payload of 92 bytes succeeded.
+ ICMP payload of 782 bytes succeeded.
+ ICMP payload of 1127 bytes succeeded.
+ ICMP payload of 1299 bytes succeeded.
+ ICMP payload of 1385 bytes succeeded.
- ICMP payload of 1428 bytes is too big.
- ICMP payload of 1406 bytes is too big.
- ICMP payload of 1395 bytes is too big.
+ ICMP payload of 1390 bytes succeeded.
+ ICMP payload of 1392 bytes succeeded.
- ICMP payload of 1393 bytes is too big.
Path MTU: 1420 bytes.
```

```
C:\TEMP>
```



Wireguard server

Mikrotik Wirguard

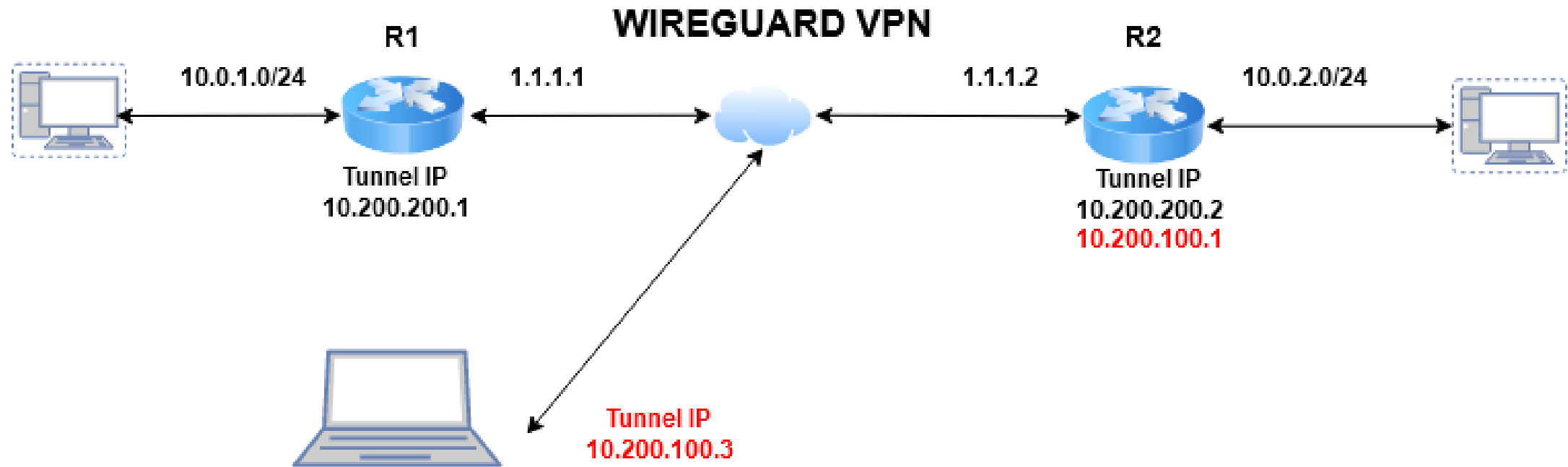
Изисквания към ROS. Генериране на ключове. Настройка.

02



Wireguard

Mikrotik server



Wireguard

Mikrotik server

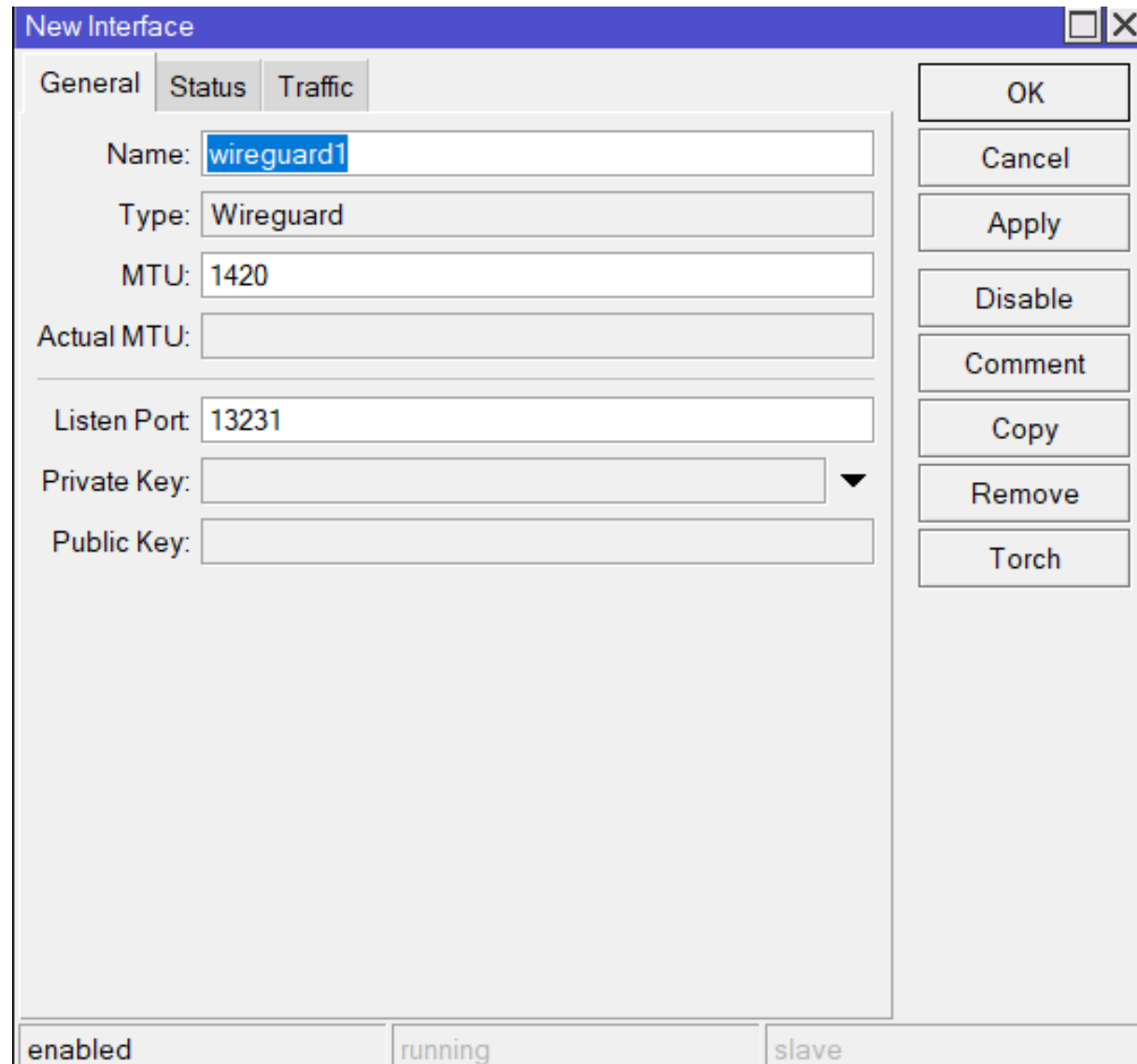
1. Добавяне на интерфейс.
2. Добавяне на IP адрес на интерфейса.
3. Добавяне на Peer.
3. Проверка и добавяне на порт.
5. Добавяне на Routes.



Wireguard

Mikrotik server R1

1. Добавяне на интерфейс.



The screenshot shows the 'New Interface' dialog box in Mikrotik WinBox. The 'General' tab is selected. The interface name is 'wireguard1', the type is 'Wireguard', and the MTU is '1420'. The 'Listen Port' is set to '13231'. The 'Private Key' and 'Public Key' fields are empty. The 'Actual MTU' field is also empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch'. At the bottom, there are three status indicators: 'enabled', 'running', and 'slave'.

Field	Value
Name	wireguard1
Type	Wireguard
MTU	1420
Actual MTU	
Listen Port	13231
Private Key	
Public Key	

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

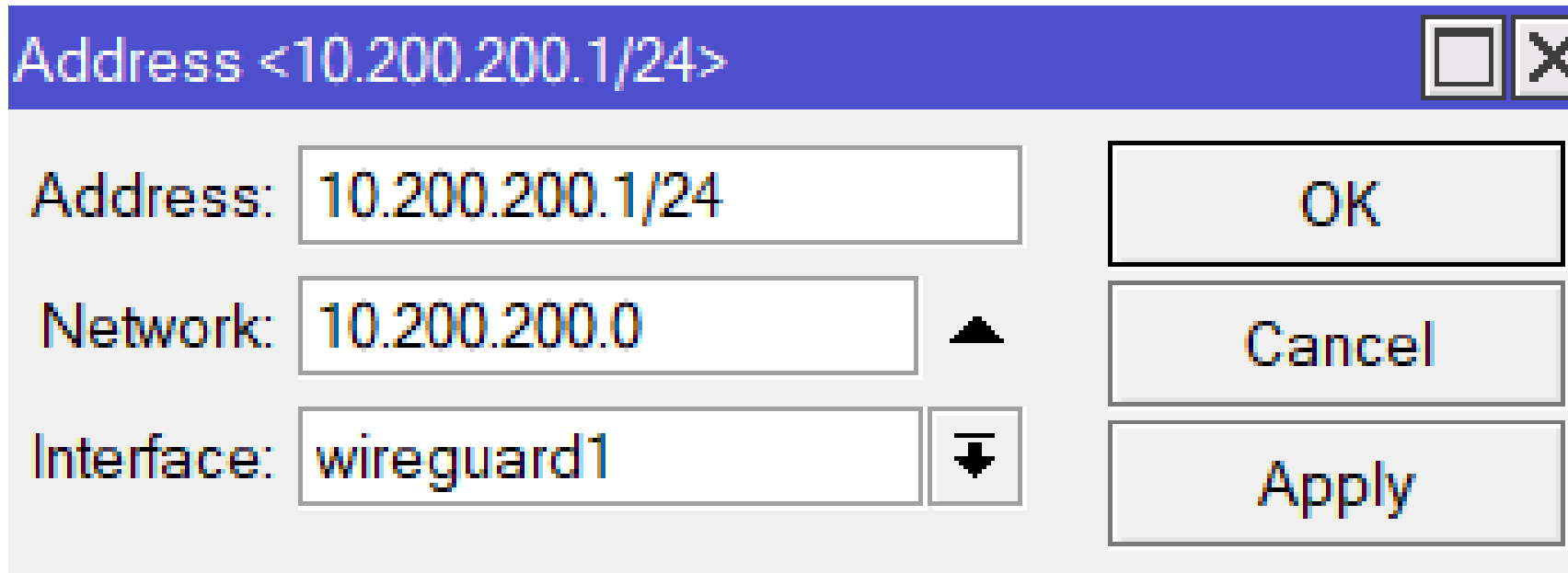
Status: enabled, running, slave



Wireguard

Mikrotik server R1

2. Добавяне на адрес на тунела.



The image shows a dialog box titled "Address <10.200.200.1/24>". It contains three input fields: "Address" with the value "10.200.200.1/24", "Network" with the value "10.200.200.0", and "Interface" with the value "wireguard1". To the right of the "Network" and "Interface" fields are small icons: an upward-pointing triangle and a downward-pointing triangle, respectively. On the right side of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".



Wireguard

Mikrotik server R1

3. Добавяне на реер.

Wireguard Peer <xSrUE4DpUQvQJtJB4TVQosNO1MzIFoY+s/5SqqswBwU=>

Interface:	wireguard1	▼	OK
Public Key:	xSrUE4DpUQvQJtJB4TVQosNO1MzIFoY		Cancel
Endpoint:	1.1.1.2	▲	Apply
Allowed Address:	10.200.200.2/32	◄	Comment
	10.0.2.0/24	◄	
Preshared Key:		▼	Copy
Persistent Keepalive:	00:00:30	▲	Remove



Wireguard

Mikrotik server R1

4.1. Добавяне порт на на peer в cli.

```
/command          Use command at the base level
[admin@R1 Elsinor] > interface/wireguard/peer print
0 interface=wireguard1 public-key="xSrUE4DpUQvQJtJB4TVQosNO1MzlFoY+s/5SqqswBwU="
  endpoint=1.1.1.2:0 allowed-address=10.200.200.2/32,10.0.2.0/24
  persistent-keepalive=30 rx=0 tx=54.6KiB
[admin@R1 Elsinor] > █
```

interface/wireguard/peer print



Wireguard

Mikrotik server R1

4.2. Добавяне порт на на peer в cli.

```
[admin@R1 Elsinor] >  
[admin@R1 Elsinor] > interface/wireguard/peer set endpoint=1.1.1.2:13231  
numbers: 0  
[admin@R1 Elsinor] > █
```

interface/wireguard/peer set endpoint=1.1.1.2:13231



Wireguard

Mikrotik server R1

5. Добавяна route за мрежата на R2.

Route <10.0.2.0/24->10.200.200.2>

General	BGP	RIP	OSPF	MPLS
---------	-----	-----	------	------

Dst. Address: 10.0.2.0/24

Gateway: 10.200.200.2



03

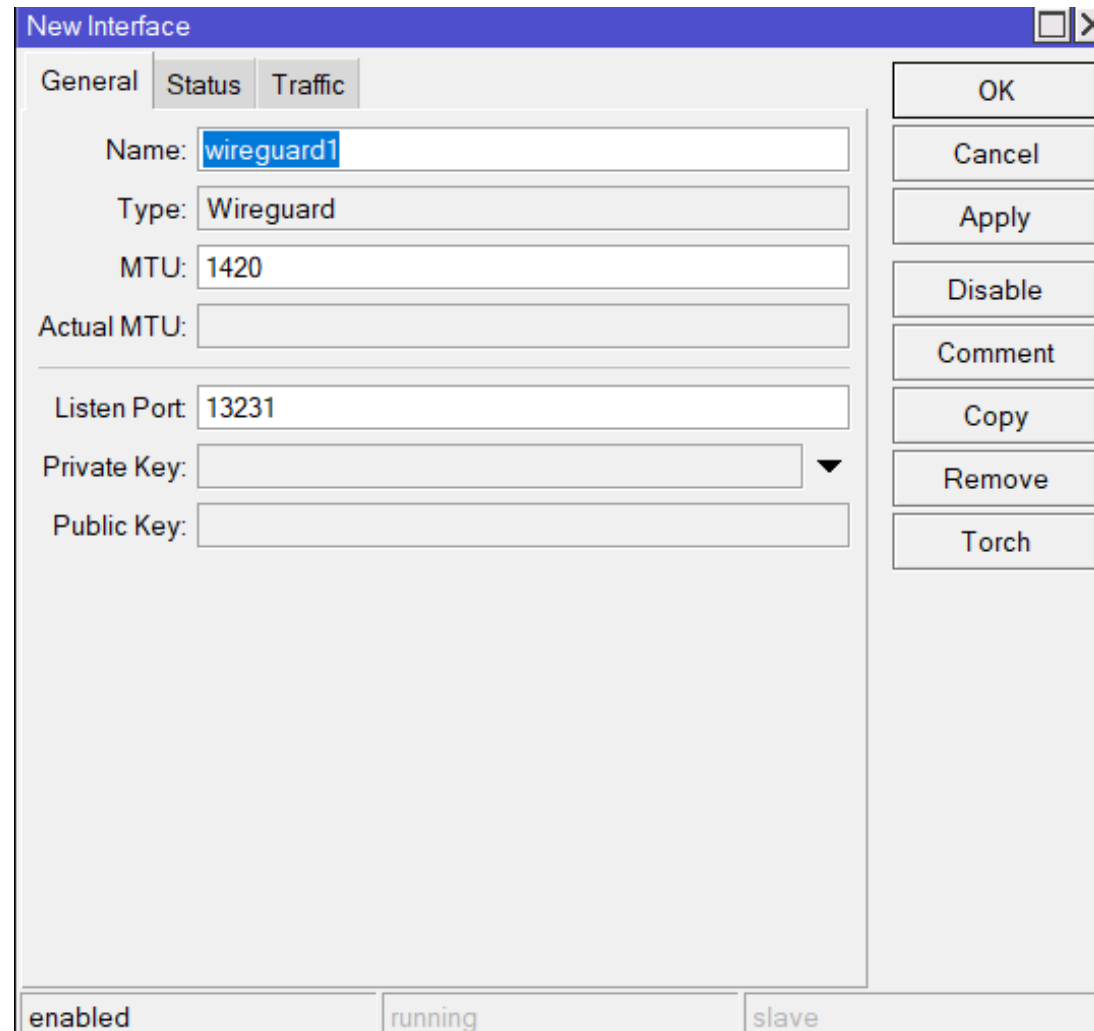
Mikrotik client Настройка. Други клиенты.

Wireguard клиент

Wireguard

Mikrotik client R2 (site-to-site VPN)

1. Добавяна на интерфейс.



The screenshot shows the 'New Interface' dialog box in Mikrotik WinBox. The 'General' tab is selected. The interface name is 'wireguard1', the type is 'Wireguard', and the MTU is '1420'. The 'Listen Port' is set to '13231'. The 'Private Key' and 'Public Key' fields are empty. The 'Status' tab shows 'enabled', 'running', and 'slave'. The 'Traffic' tab is also visible. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch'.

Field	Value
Name	wireguard1
Type	Wireguard
MTU	1420
Actual MTU	
Listen Port	13231
Private Key	
Public Key	

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

Status: enabled, running, slave



Wireguard

Mikrotik client R2

2. Добавяне на реер.

Wireguard Peer <NVfis+JyU6JX69bYNzoo1EpFg8G8gOvdWi/CC997qGU=>

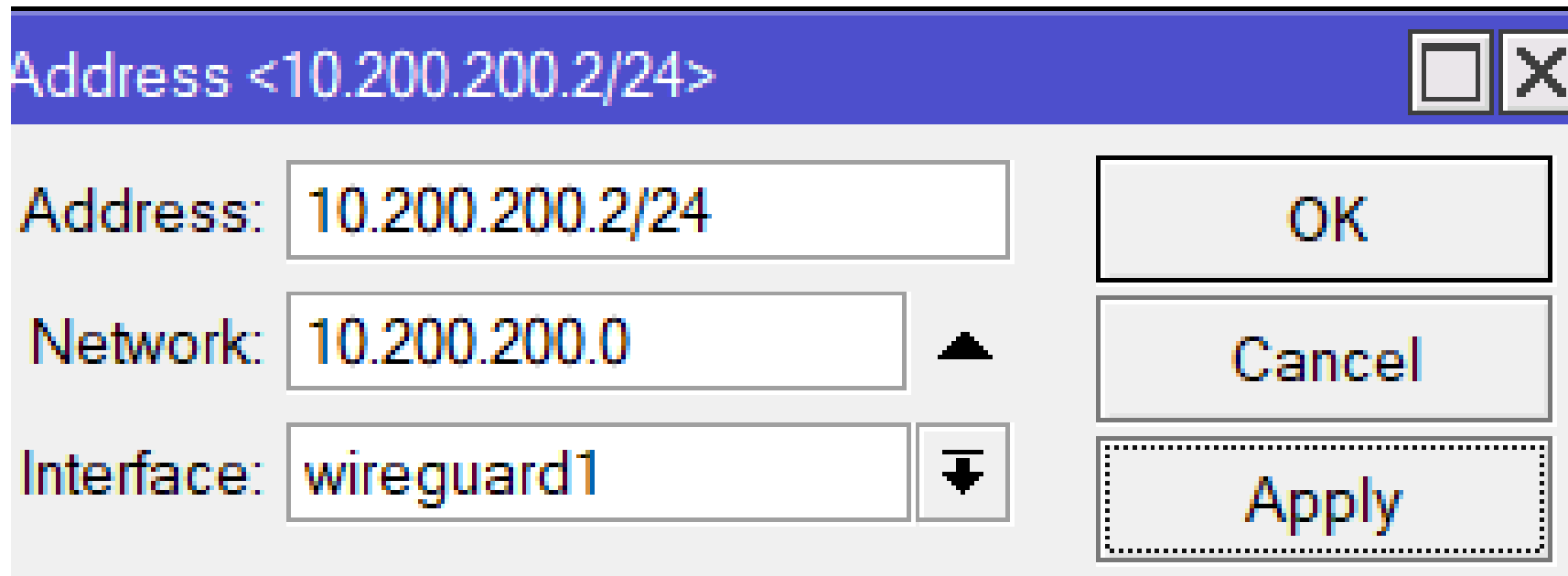
Interface:	wireguard1	▼	OK
Public Key:	6JX69bYNzoo1EpFg8G8gOvdWi/CC997qGU		Cancel
Endpoint:	1.1.1.1	▲	Apply
Allowed Address:	10.0.1.0/24	◆	Comment
Preshared Key:		▼	Copy
Persistent Keepalive:	00:00:30	▲	Remove



Wireguard

Mikrotik client R2

3. Добавяне на адрес на тунела.



A screenshot of a Mikrotik WinBox dialog box titled "Address <10.200.200.2/24>". The dialog has a blue header bar with the title and window control buttons (minimize, maximize, close). The main area contains three input fields: "Address:" with the value "10.200.200.2/24", "Network:" with the value "10.200.200.0" and an upward-pointing arrow button, and "Interface:" with the value "wireguard1" and a downward-pointing arrow button. On the right side, there are three buttons: "OK", "Cancel", and "Apply" (which has a dotted border).



Wireguard

Mikrotik client R2

4. Добавяне на route за мрежата на R2.

Route <10.0.1.0/24->10.200.200.1>

General	BGP	RIP	OSPF	MPLS
---------	-----	-----	------	------

Dst. Address:

Gateway:

5. Добавяна порт на на peer в cli.



Wireguard

Mikrotik Тест скорост на трансфер

Скорости на трансфер:

MAP2nD

CPU Intensive: 100%

Tx:5.6Mbps

The screenshot shows the MikroTik Bandwidth Test v0.1 application window. The interface is divided into a configuration area and a results area. The configuration area includes fields for Address (10.0.1.1), Protocol (udp), Local Tx Size (1420), Remote Tx Size (1420), Direction (send), Local Tx Speed (0 bps), Remote Tx Speed (0 bps), Connection Count (1), User (admin), and Password. There are also buttons for Start, Stop, Save..., and Load..., and a checkbox for Random Data. The results area shows a grid with a red bar indicating a transmission speed of 5.6 Mbps. The status bar at the bottom shows 'UDP admin@10.0.1.1 Tx(1)' and 'disconnected'.

MikroTik Bandwidth Test v0.1

MikroTik.com

Client Server

Address: 10.0.1.1

Protocol: udp

Local Tx Size: 1420

Remote Tx Size: 1420

Direction: send

Local Tx Speed: 0 bps

Remote Tx Speed: 0 bps

Connection Count: 1

User: admin

Password:

Random Data

Start

Stop

Save...

Load...

Tx: 5.6 Mbps

UDP admin@10.0.1.1 Tx(1) disconnected



Wireguard

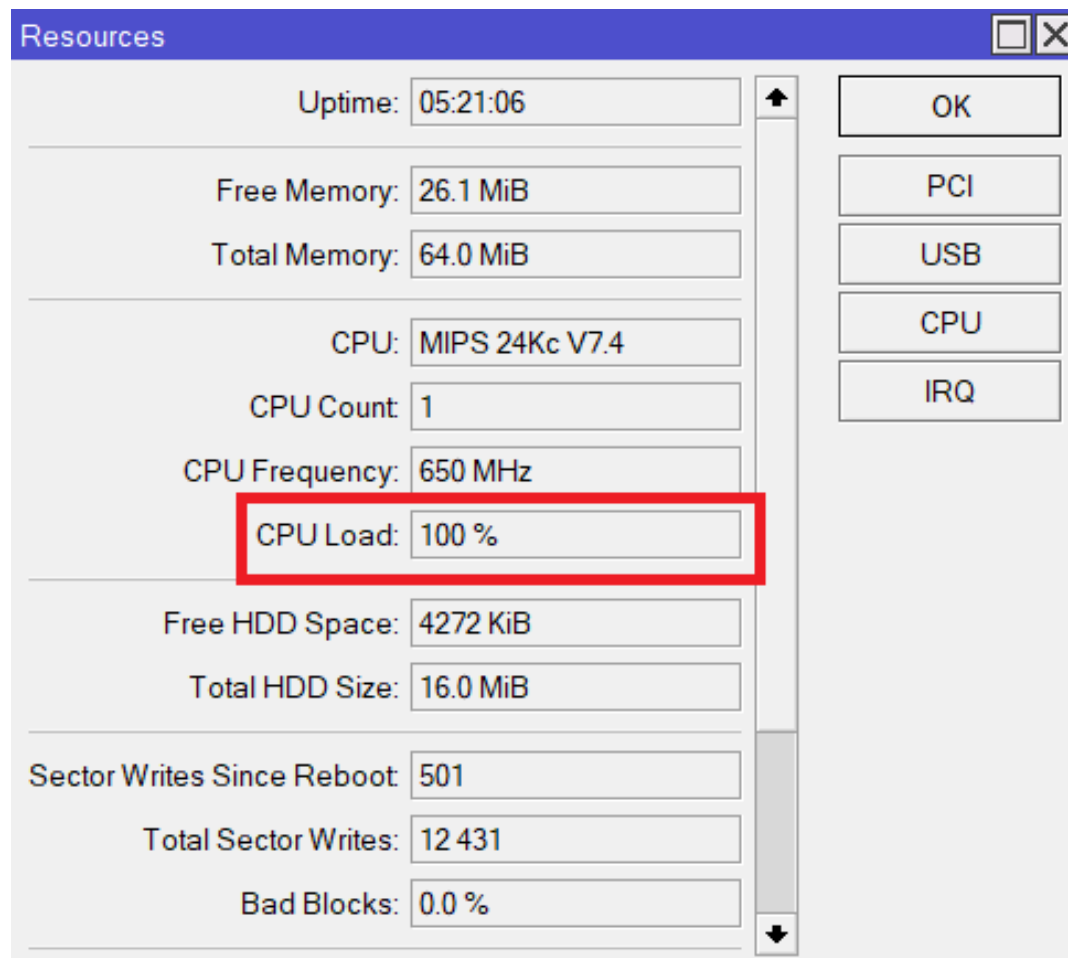
Мikrotik Тест скорост на трансфер

Скорости на трансфер:

MAP2nD

CPU Intensive: 100%

Tx:5.6Mbps



The screenshot shows the 'Resources' window in Mikrotik WinBox. The window title is 'Resources' and it has standard window controls (minimize, maximize, close). The main area displays various system statistics in a list format. The 'CPU Load' field is highlighted with a red rectangular border and shows '100 %'. Other fields include Uptime (05:21:06), Free Memory (26.1 MiB), Total Memory (64.0 MiB), CPU (MIPS 24Kc V7.4), CPU Count (1), CPU Frequency (650 MHz), Free HDD Space (4272 KiB), Total HDD Size (16.0 MiB), Sector Writes Since Reboot (501), Total Sector Writes (12 431), and Bad Blocks (0.0 %). On the right side of the window, there is a vertical stack of buttons: OK, PCI, USB, CPU, and IRQ.

Uptime:	05:21:06
Free Memory:	26.1 MiB
Total Memory:	64.0 MiB
CPU:	MIPS 24Kc V7.4
CPU Count:	1
CPU Frequency:	650 MHz
CPU Load:	100 %
Free HDD Space:	4272 KiB
Total HDD Size:	16.0 MiB
Sector Writes Since Reboot:	501
Total Sector Writes:	12 431
Bad Blocks:	0.0 %



Wireguard

IOS, Windows, Linux client

1. Microsoft – 32/64bit.
2. IOS, MacOS – app/play store: WireGuard.
3. Android - Play Store: WireGuard.
4. Linux.

<https://www.wireguard.com/install/>



Wireguard

Windows client

Microsoft – добавяне на тунел:

[Interface]

PrivateKey = WINDOWS PRIVATE KEY

Address = VPN ADDRESS

DNS = 1.1.1.1, 1.0.0.1

[Peer]

PublicKey = YOUR_SERVER_PUBLIC_KEY

AllowedIPs = 0.0.0.0/0

Endpoint = YOUR_SERVER_WAN_IP:13431



Wireguard

Windows client

Microsoft – добавяне на тунел:

[Interface]

PrivateKey = WINDOWS PRIVATE KEY

Address = 10.200.100.3/24

DNS = 1.1.1.1, 1.0.0.1

[Peer]

PublicKey = NVfis+JyU6JX69bYNzoo1EpFg8G8gOvdWi/CC997qGU=

AllowedIPs = 0.0.0.0/0

Endpoint = 1.1.1.1:13431



Wireguard

Windows client

Edit tunnel

Name: Mikrotik

Public key: (unknown)

[Interface]
PrivateKey = WINDOWS PRIVATE KEY
Address = 10.200.100.3/24
DNS = 1.1.1.1, 1.0.0.1

[Peer]
PublicKey = ILLsWsEb59v8DaIV2n5HNwCk39U2LIz6yiFKamRbvFk=
AllowedIPs = 0.0.0.0/0
Endpoint = 1.1.1.1:13431

Save Cancel



Wireguard

Windows client

Microsoft – добавяне на тунел:

Block untunneled traffic (kill-switch)

*Маркирайки Block untunneled traffic осигурява рутирание на целия трафик през VPN тунела, добавяйки правила в Windows Firewall.



Wireguard

Windows client R1

R1
Interface

Interface <wireguard-win>

General | Status | Traffic

Name: wireguard-win

Type: Wireguard

MTU: 1420

Actual MTU: 1420

Listen Port: 13431

Private Key: [REDACTED]

Public Key: ILlswsEb59v8DaIV2n5HNwCk39U2Llz6yiFKamRbvFk=

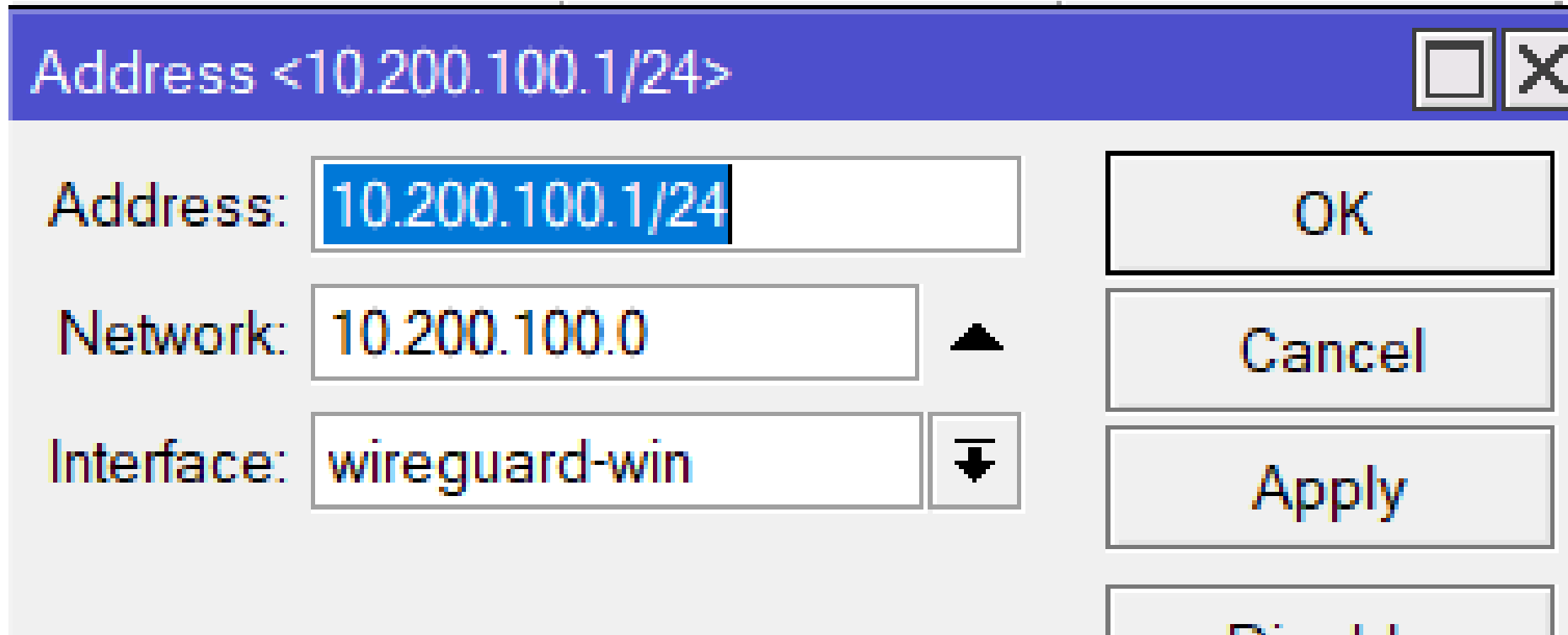
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch



Wireguard

Windows client R1

R1
Address



A screenshot of a Windows dialog box titled "Address <10.200.100.1/24>". The dialog box has a blue title bar with a minimize button and a close button. It contains three input fields: "Address:" with the value "10.200.100.1/24", "Network:" with the value "10.200.100.0", and "Interface:" with the value "wireguard-win". To the right of the "Network:" and "Interface:" fields are up and down arrow buttons. On the right side of the dialog box, there are four buttons: "OK", "Cancel", "Apply", and "Dismiss".



Wireguard

Windows client R1

R1 Peer

Wireguard Peer <h6FWDWxRjzYXyX1DsKFwdQ3wzxcCzzS9ZEMqG+f/T0l=> X

Interface:	wireguard-win	▼	OK
Public Key:	h6FWDWxRjzYXyX1DsKFwdQ3wzxcCzz!		Cancel
Endpoint:	1.1.1.2	▲	Apply
Allowed Address:	10.200.100.3/32	◆	Comment
Preshared Key:		▼	Copy
Persistent Keepalive:	00:00:30	▲	Remove



Wireguard

Windows client R1

R1
Interface
port

```
numbers: 1
[admin@R1 Elsinor] > interface/wireguard/peer print
0 interface=wireguard1 public-key="xSrUE4DpUQvQJtJB4TVQosNO1MzlFoY+s/5SqqswBwU="
  endpoint=1.1.1.2:13231 allowed-address=10.200.200.2/32,10.0.2.0/24
  persistent-keepalive=30 rx=47.5KiB tx=120.6KiB last-handshake=47m16s

1 interface=wireguard-win
  public-key="h6FWDWxRjzYXyX1DsKFwdQ3wzxxCzzS9ZEMqG+f/T0I="
  endpoint=1.1.1.2:13431 allowed-address=10.200.100.3/32
  persistent-keepalive=30 rx=25.9KiB tx=46.9KiB last-handshake=25m30s
[admin@R1 Elsinor] > █
```



Wireguard

Mikrotik Тест скорост на трансфер



Скорости на трансфер:

R1: MAP2nD

CPU Intensive: 100%

Tx:5.6Mbps

Win10 i5 8600

Processes Performance App history Startup Users Details Services							
Name	Status	47% CPU	43% Memory	2% Disk	97% Network	0% GPU	GPU engine
>  bttest.exe (32 bit)		22.5%	2.7 MB	0 MB/s	0 Mbps	0%	
>  WireGuard: Fast, Modern, Secure VPN Tunnel		20.6%	38.1 MB	0 MB/s	92.1 Mbps	0%	





Благодаря за вниманието!

