



# VPN Freedom Hacking

(CC) 2019, Matej Kovačič  
matej.kovacic@telefoncek.si

# Privacy and surveillance

---

Arendt and Habermas pointed out two aspects of the private: personal space - space of intimacy, and space which enables associations of individuals and their action.

Privacy is a limit on (government or corporate) power - the more someone knows about us, the more power they can have over us.

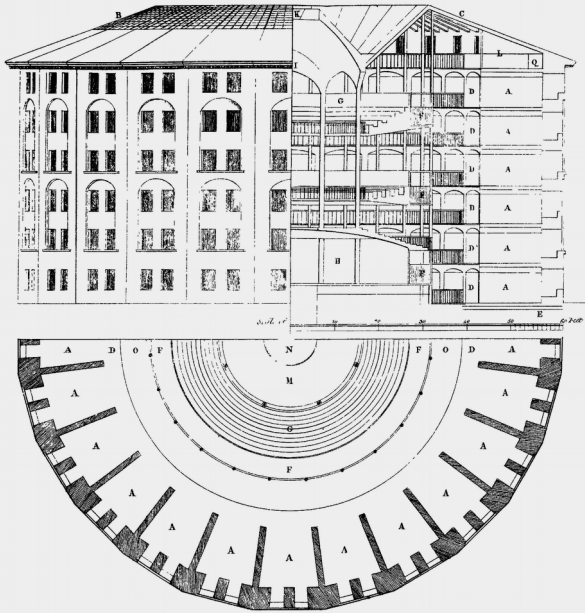
Privacy is linked with freedom and autonomy (control over our lives).

Privacy is key to freedom of thought and also key to protecting speaking unpopular messages. Privacy helps protect our ability to associate with other people and engage in political activity.

Therefore privacy today is a value, a precondition of human freedom and emancipation.

# Privacy and surveillance

---



The idea of surveillance as a means of executing power over individuals was first introduced by Bentham in his work describing the idea of prison Panopticon. Surveillance and control could be directed in two ways: against individual or against authority (government). The idea of the control of the state authority has been introduced in 1791 in Bentham's essay *Of Publicity*.

His idea has been directed against non-transparency and secrecy of authority, but today is often used as an argument against privacy of individuals. It came to the conversion of the principle of transparency, and the consequence is that individuals who want to protect their privacy are often faced with allegations of hiding and consecutive immorality. "To be good citizens ... is to be measurable and predictable consumers" (Gareth Palmer).

# Privacy and surveillance

---

Is internet a “technology of freedom” or is panopticism already built-in it?

We cannot overlook the close connection between surveillance and technology. Information technology has a high significance for national security, freedom and democracy.

Today technology today is designed for surveillance. The technologies of surveillance are widespread and are socially acceptable. (Personal) information today has a great value; the information society is a surveillance society.

We live in a society which, on the one hand, recognizes individuality and privacy, but on the other, we are also witnessing an increase in surveillance. With use of technology, individuals are becoming more and more transparent.

# Eavesdropping

The image shows two windows from a network analysis tool. The top window is Wireshark, displaying a list of network packets. The bottom window is a VoIP RTP Player, showing an audio waveform corresponding to the selected packet in Wireshark.

**Wireshark - sip.pcap**

Filter: sip

No.	Time	Source	Destination	Protocol	Info
69	14.865457	153.5	212.1	SIP/XML	Request: PUBLISH sip: [redacted]@212.1
72	16.867222	153.5	212.1	SIP/XML	Request: PUBLISH sip: [redacted]@212.1
82	23.453253	153.5	212.1	SIP/SDP	Request: INVITE sip:015805373@212.1, with
83	23.461385	212.1	153.5	SIP	Status: 100 Trying
84	23.466803	212.1	153.5	SIP	Status: 401 Unauthorized
85	23.475217	153.5	212.1	SIP	Request: ACK sip:015805373@212.1
86	23.530435	153.5	212.1	SIP/SDP	Request: INVITE sip:015805373@212.1 with
87	23.535845	212.1	153.5	SIP	Status: 100 Trying
89	24.572367	212.1	153.5	SIP	Status: 180 Ringing
92	25.651003	153.5	212.1	SIP	Request: CANCEL sip:015805373@212.1
93	25.760161	212.1	153.5	SIP	Status: 200 OK
94	25.769395	212.1	153.5	SIP	Status: 487 Request Cancelled
97	25.985041	153.5	212.1	SIP	Request: ACK sip:015805373@212.1

**Packet 82 Details:**

- Frame 82 (1219 bytes on wire, 1219 bytes captured)
- Ethernet II, Src: [redacted]
- Internet Protocol, Src: [redacted]
- User Datagram Protocol, Src Port: sip (5060), Dst: [redacted]
- Session Initiation Protocol

**Packet 82 Hex:**

```
0000 00 18 73 a3 4e 48 00 15 af e5 25 c8 08 00 45
0010 04 b5 00 00 40 00 40 11 5f 95 99 05 85 5b d4
0020 e4 34 13 c4 13 c4 04 a1 de c4 49 4e 56 49 54
0030
0040
0050
0060 20 32 38 20 4d 61 79 20 32 30 30 39 20 31 32
0070 32 36 3a 35 31 20 47 4d 54 0d 0a 43 53 65 71
0080 20 31 20 49 4e 56 49 54 45 0d 0a 56 69 61 3a
```

File: "/media/MATEJ/sip.pcap" 31 KB 00:00:32

**VoIP RTP Player - sip\_govor.pcap**

Duration: 11.76 Drop by jitter Buff: 0(0.0%) Out of Seq: 0(0.0%)

Duration: 12.04 Drop by jitter Buff: 0(0.0%) Out of Seq: 1(0.2%)

Jitter buffer [ms]: 50

Buttons: Decode, Play, Pause, Stop, Zapri

# Censorship




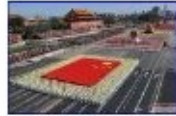








http://images.google.cn/images?gbv=2&hl=zh-CN&sa=1&q=tiananmen+square+...

Google 图片  搜索图片 高级

使用了 SafeSearch 功能。(了解更多) 屏蔽图片

图片 打开百度... 获得约 214 条结果, 以下是第 1-20 条 (用时 0.05 秒)

**Tian'an Men Square**  
hotels.english.ctrip.com Book Hotel Rooms with Confidence. The Best Values for Beijing Hotels.

 <b>Tiananmen</b> 450 x 263 - 374k - bmp chinadaily.com.cn	 <b>the vast Tiananmen</b> 420 x 272 - 37k - jpg anti-cnn.com	 <b>Tiananmen</b> 450 x 250 - 49k - jpg chinadaily.com.cn	 <b>historic Tiananmen</b> 650 x 425 - 95k - jpg junshi.xilu.com
 <b>English is very</b> 300 x 300 - 19k - jpg hi.baidu.com	 <b>only at Tiananmen</b> 450 x 300 - 68k - jpg eol.cn	 <b>Tiananmen</b> 650 x 358 - 36k 2008.sina.com.cn 查找相关图片	 <b>the Tiananmen</b> 500 x 334 - 72k - jpg 2008.cn.yahoo.com
			













http://images.google.co.uk/images?hl=en&source=hp&q=tiananmen%20square%20...

Google images  Search images Advanced Image S...

SafeSearch: Moderate

Images Show options... Results 1 - 20 of about 506,000 (0.23 sec)

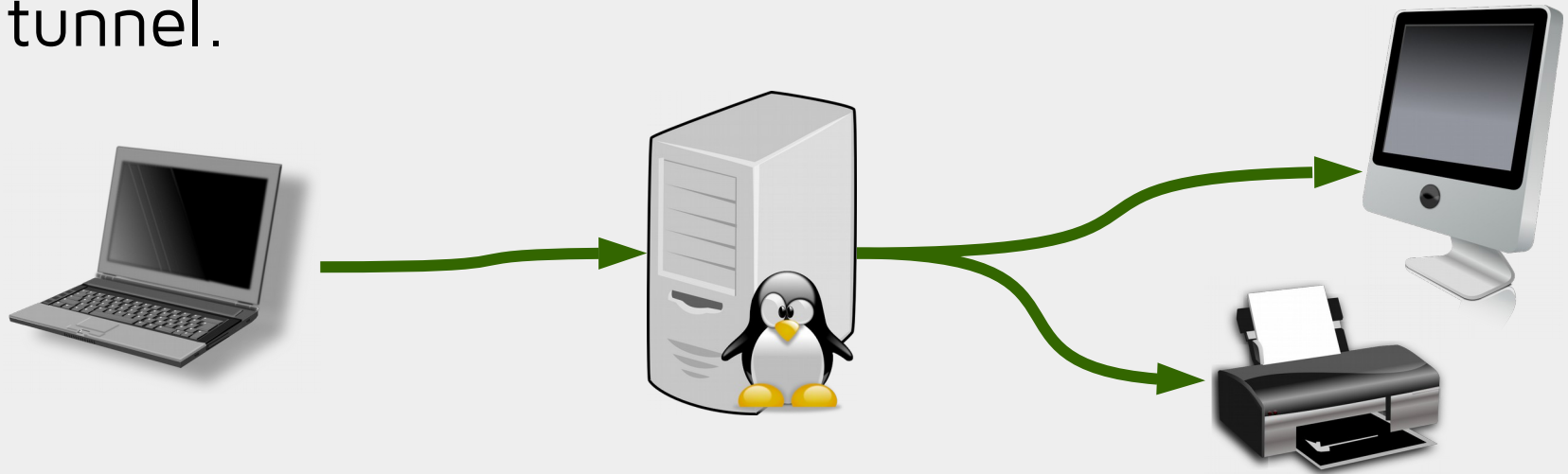
**Tiananmen Square Posters**  
www.AllPosters.co.uk Choose from over 500,000 Posters and Prints. Find your favourite!

 <b>Tiananmen</b> 600 x 408 - 68k - jpg ramblingsofpassion... Find similar images	 <b>Tiananmen Square</b> 400 x 267 - 96k - jpg facsimilemagazine.com Find similar images	 <b>Populism, Plutocracy</b> 264 x 400 - 31k - jpg thechnadesk... Find similar images	 <b>Tiananmen by</b> 1600 x 1173 - 278k - jpg aroundtheedges...
 <b>Tiananmen</b> 480 x 275 - 27k - jpg waranyou.com	 <b>The Tiananmen</b> 688 x 462 - 99k - jpg learningwitheldisc... Find similar images	 <b>Tiananmen Square</b> 300 x 393 - 25k - jpg kakeytechnology.com	 <b>on Tiananmen</b> 755 x 471 - 204k - gif cnd.org Find similar images
			

## What is VPN?

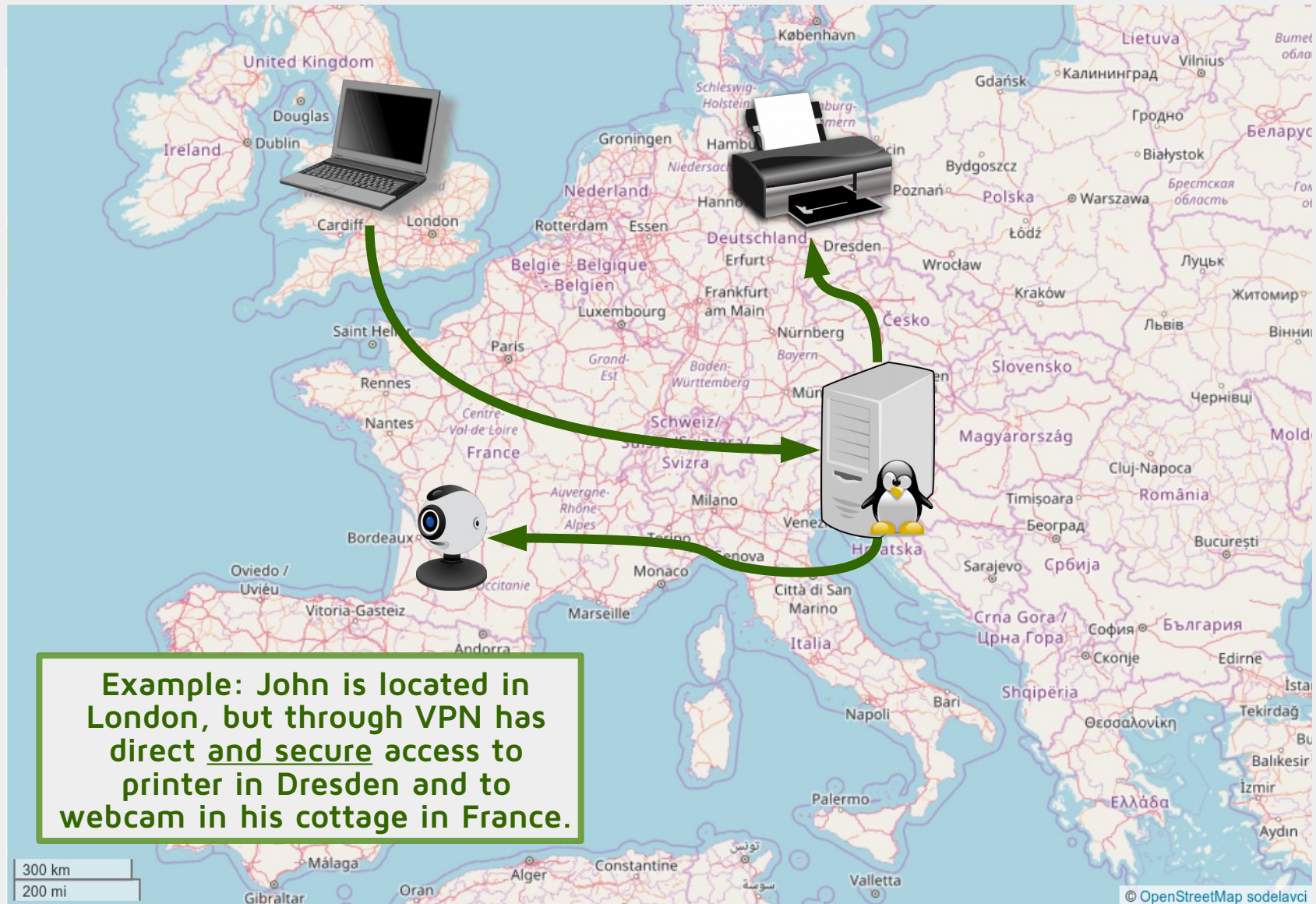
---

A virtual private network or VPN is a way of connecting a computer to a remote network or remote computer through secure (encrypted) tunnel.



Through secure tunnel user can have direct access to the remote network, remote computers or other remote devices regardless of their physical location.

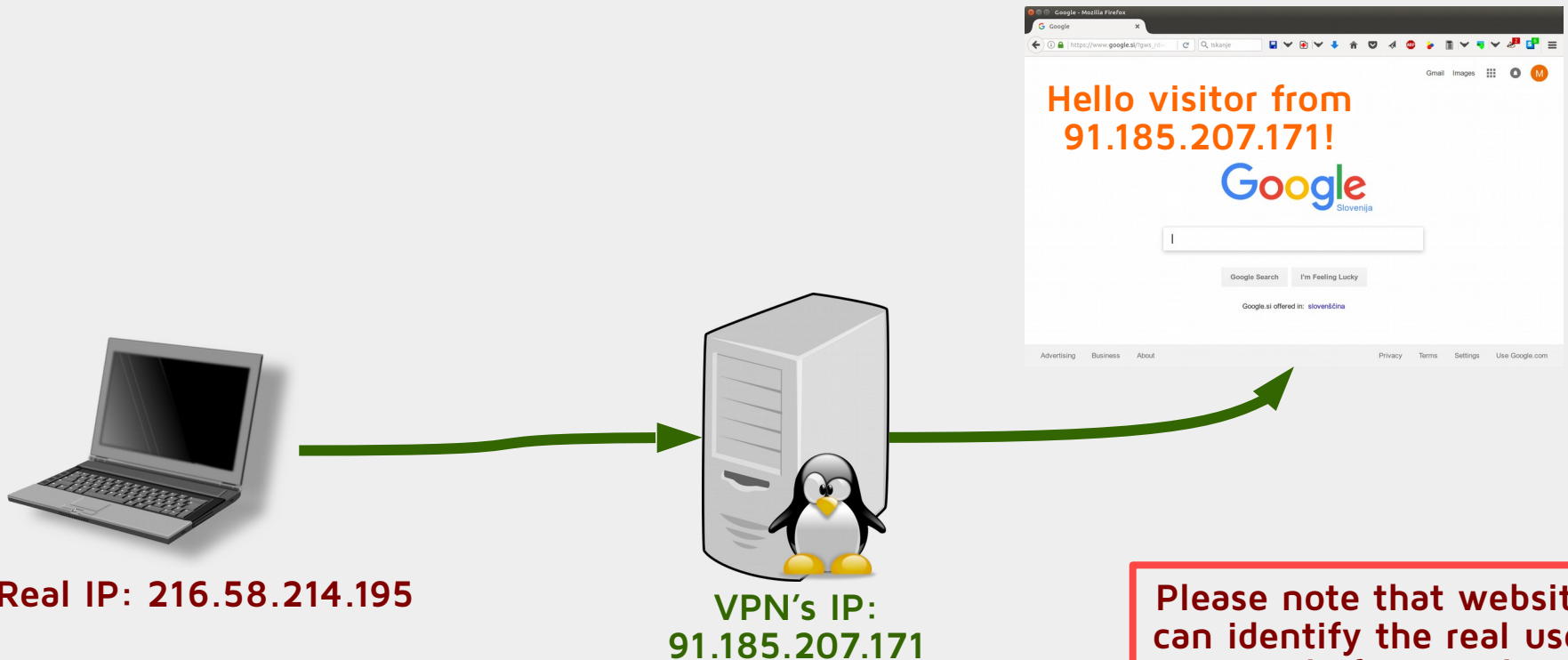
# Access to remote networks or devices





# Hiding real IP address

If user is using VPN server as a gateway to the internet, website he is visiting does not see his real IP address, but IP address of VPN server.



Real IP: 216.58.214.195

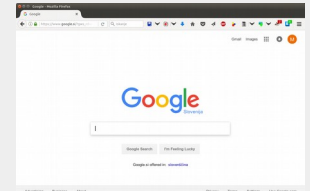
VPN's IP:  
91.185.207.171

**Please note that website can identify the real user not only from IP, but also from cookies and with other measures.**

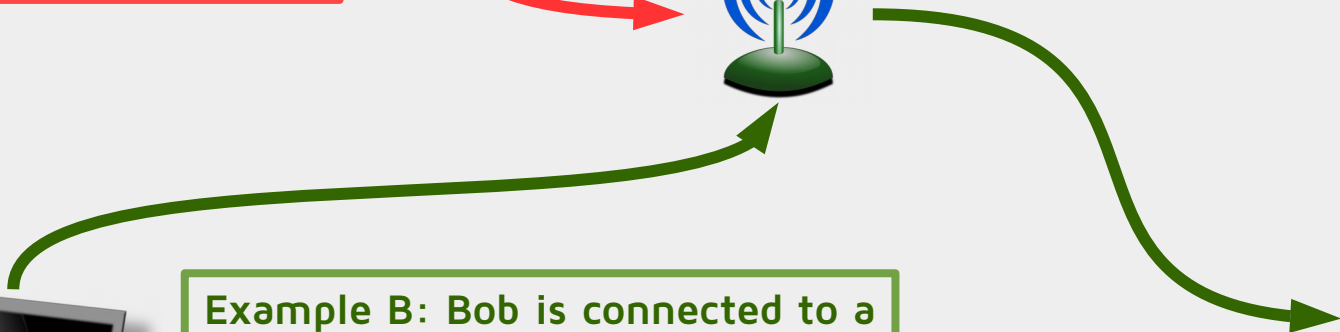
# Protection from hacker's snooping

Since VPN establishes a secure tunnel between two or more devices, VPNs are often used to protect network traffic from snooping, interference, and censorship.

**Example A:** Alice is connected to public or private Wi-Fi. The owner of Wi-Fi network or a hacker can eavesdrop her communications.



**Example B:** Bob is connected to a public Wi-Fi. But since he is using VPN, his communications from his computer to VPN server are encrypted.

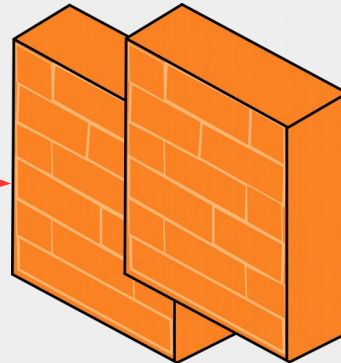
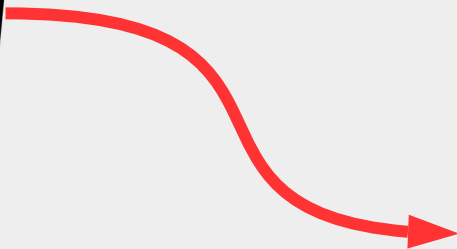


# Protection from government snooping



# Protection from blocking

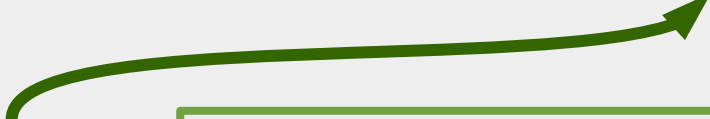
**Example A: Alice is behind firewall and has restricted access to some websites or internet services.**



**Secure tunnel between user and VPN server is established.**

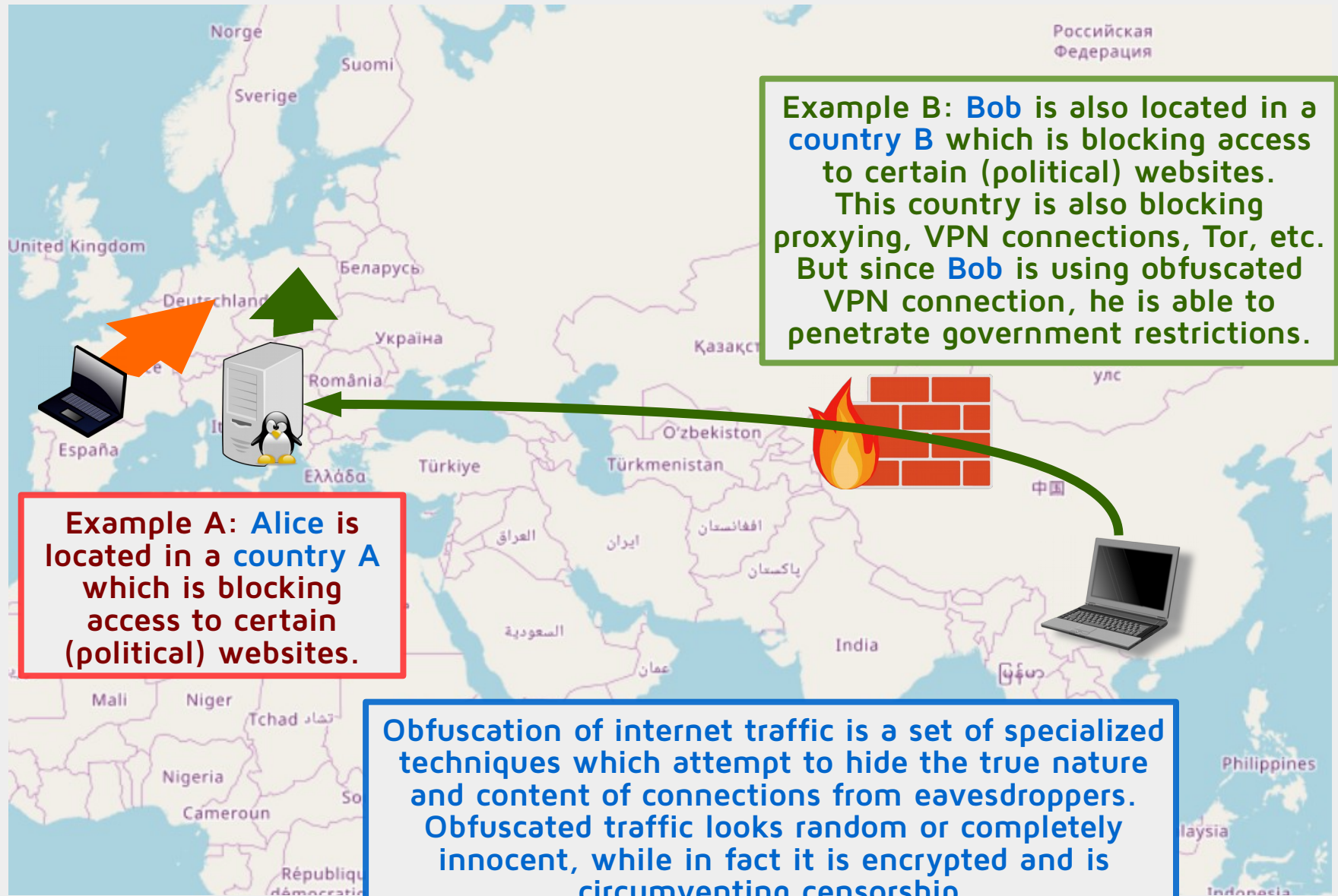


**User has unrestricted access to Internet.**

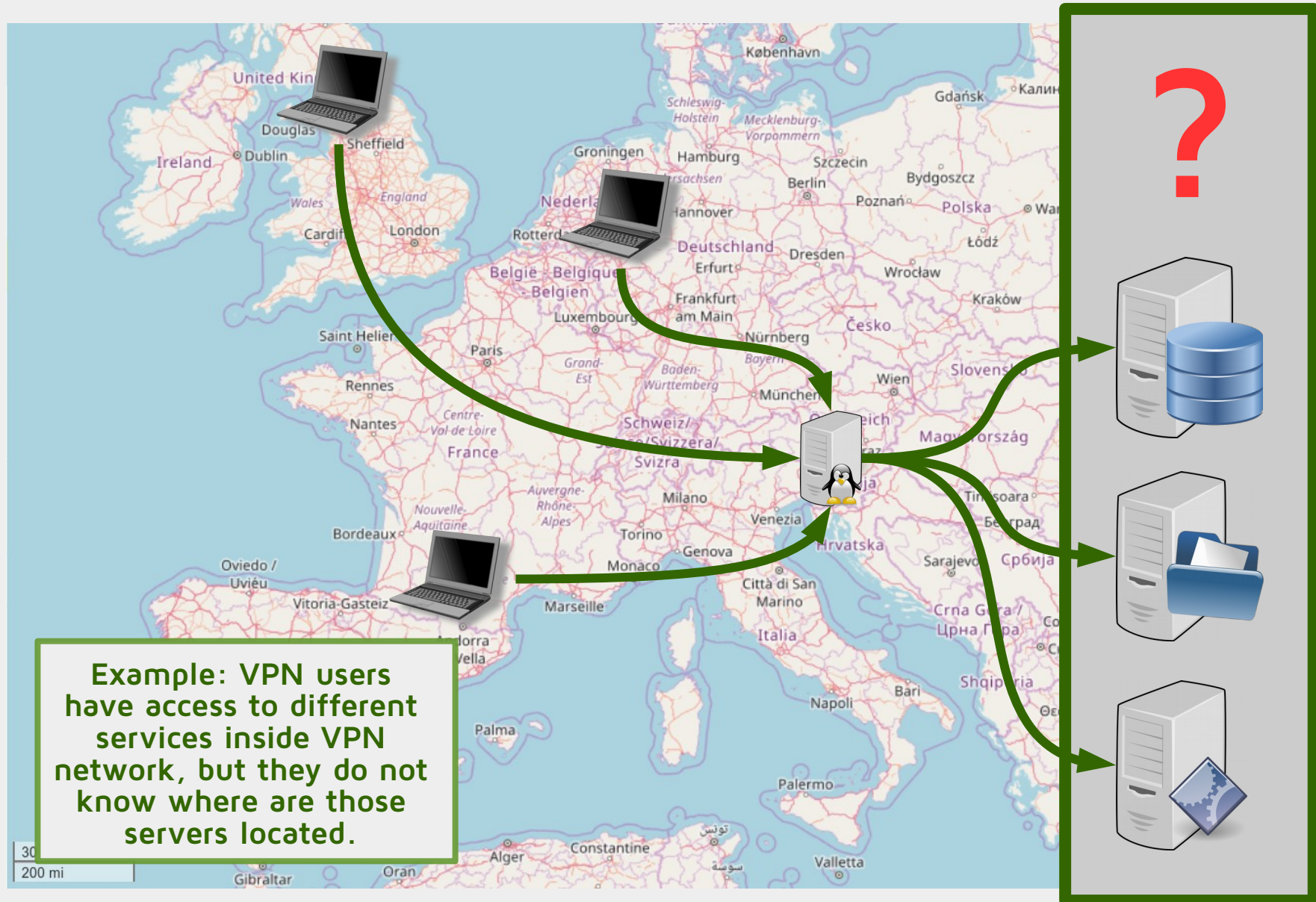


**Example B: Bob is also behind firewall, but since he is using VPN, his communications »penetrate« firewall restrictions and he has access to free Internet.**

# Protection from government censorship



# Hidden services



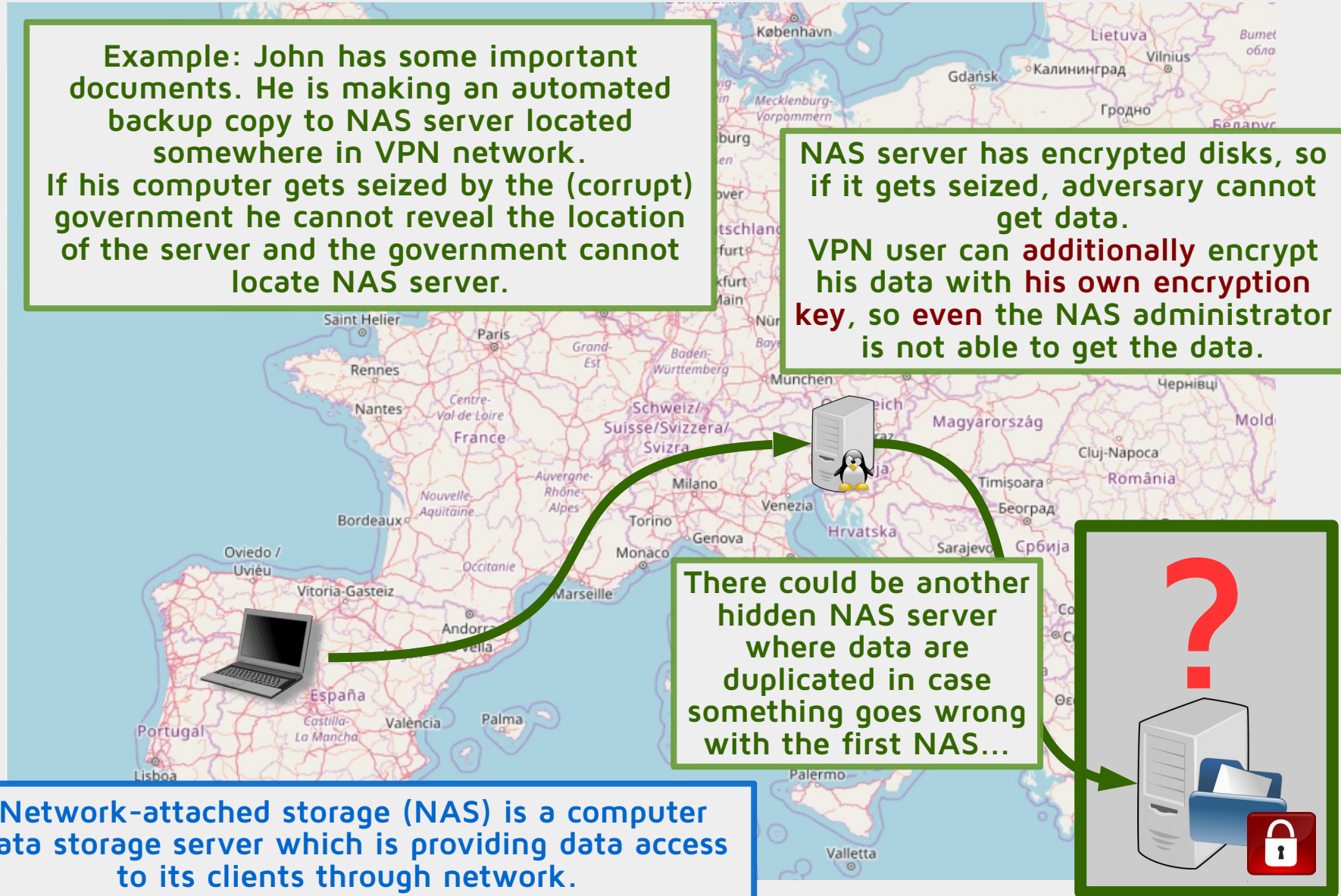
# Example: Hidden NAS server

Example: John has some important documents. He is making an automated backup copy to NAS server located somewhere in VPN network. If his computer gets seized by the (corrupt) government he cannot reveal the location of the server and the government cannot locate NAS server.

NAS server has encrypted disks, so if it gets seized, adversary cannot get data. VPN user can **additionally** encrypt his data with **his own encryption key**, so **even** the NAS administrator is not able to get the data.

There could be another hidden NAS server where data are duplicated in case something goes wrong with the first NAS...

Network-attached storage (NAS) is a computer data storage server which is providing data access to its clients through network.



# Connection notifications

Example: Alice is journalist and her laptop was stolen. Since she is not using password, attacker is able to connect to VPN using her keys...

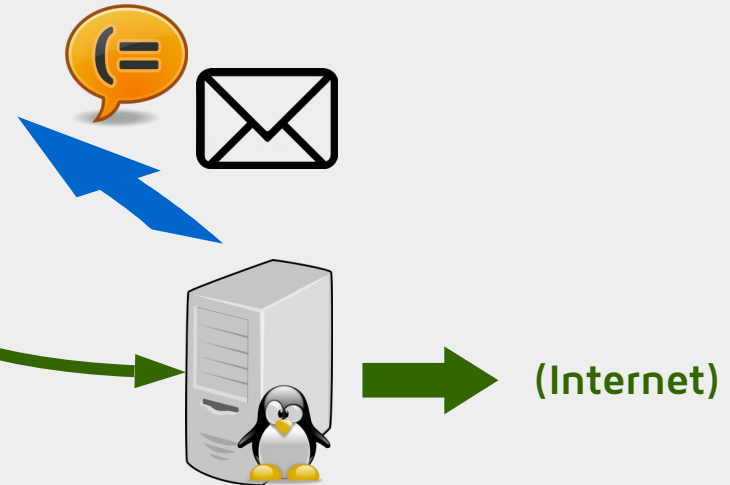


When VPN server detects connection, Alice is notified about that via e-mail and Signal message.

Server notifies her that new connection with her VPN keys has been made, when it was made and from which IP address.

Regarding user connection and user disconnection to VPN notifications, there are four options:

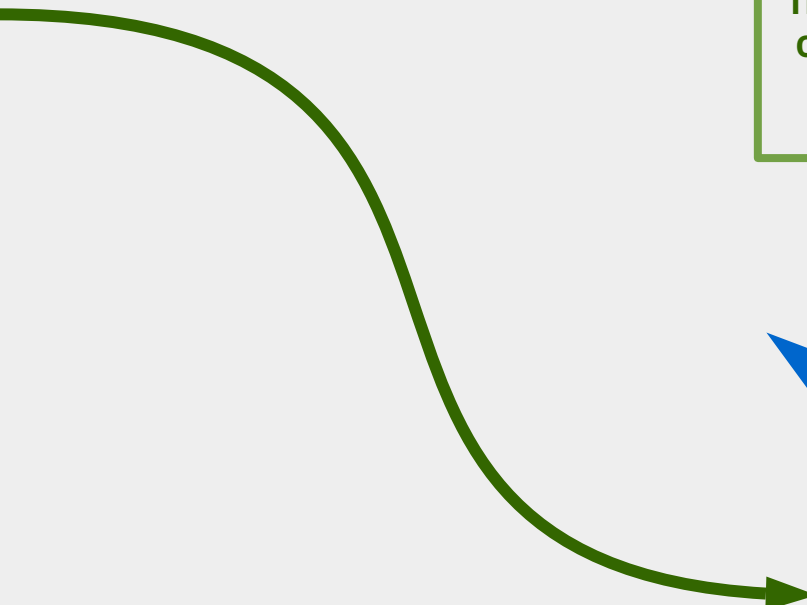
- there are absolutely no notifications for a given user account;
- user connects and disconnects could be **logged to a database** on the server, user can **receive an e-mail** or user can **receive a Signal message**.



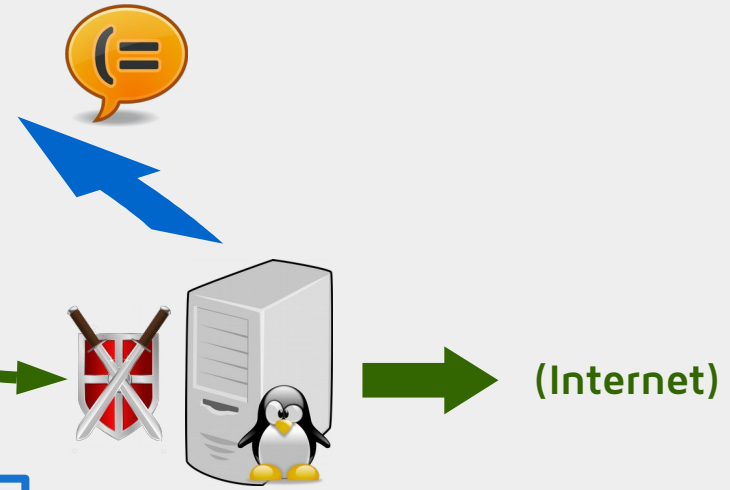


# Intrusion detection (*not implemented yet*)

Example: Alice is journalist and has been targeted by government malware. Her computer has been targeted with NSA's Quantum Insert attack.



VPN server is analysing all Alice's traffic (with her consent!). If IDS (Intrusion Detection System) detects Quantum Insert pattern in Alice's network traffic, Alice is notified about that.



Intrusion Detection System (IDS) is a network security technology used for detecting attacks against a target application or computer.

## Additional services

---

It is possible to have additional services inside VPN network. For example:

- hidden NAS (for secure backups);
- internal websites (accessible only inside VPN network);
- private bridges to other networks (for instance secure remote access to your home network);
- secure access to remote (private) printers;
- etc.

## Why your own infrastructure?

---

Research of VPN apps for Android from 2016  
(University of New South Wales and the University of Berkeley):

- they tested 283 VPN apps from Google Play Store;
- 18 percent of the apps **failed to encrypt** users' traffic;
- 38 per cent of the apps **injected malware or malvertising**;
- over 82 per cent of apps **requested to access sensitive data** such as user accounts and text messages;
- three quarters of the apps used third-party user tracking libraries, majority of them had several security issues (for instance did not prevent DNS leaking, etc.)

# Secure VPN configuration



## The Machine

---

Server is running in virtual machine. Host machine and network is outside our administration, but is regularly maintained.

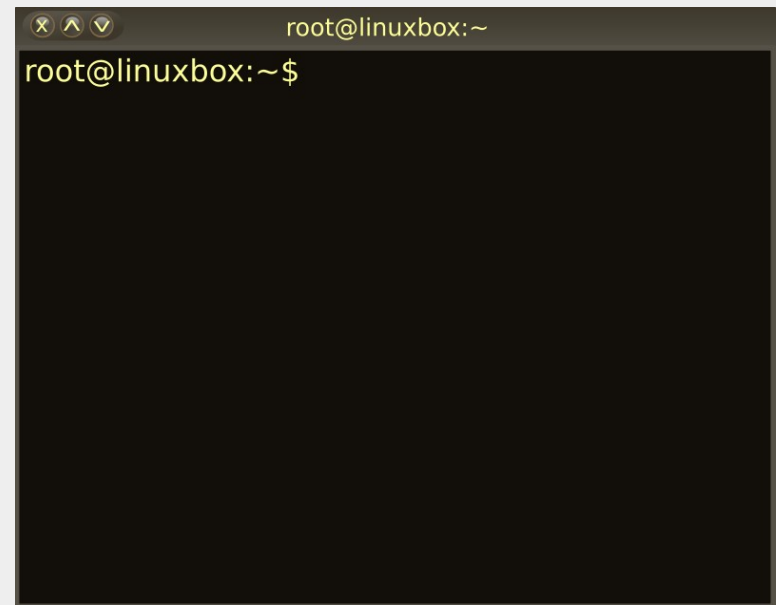
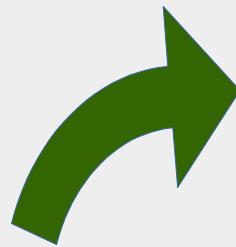
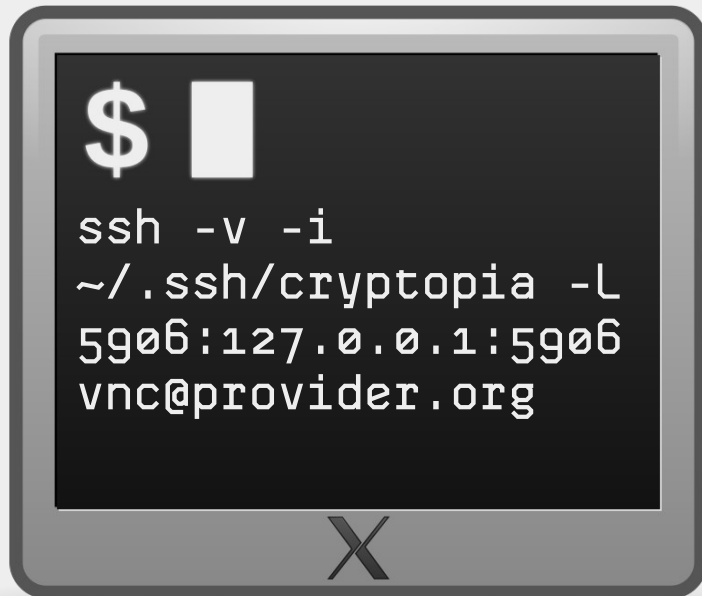
Server is running under fully patched Debian operating system. Debian is Linux distribution which takes security very seriously and has many security mechanisms already built-in.



## Remote console

---

Machine is accessible through virtual VNC console, which is accessible through encrypted reverse SSH tunnel.

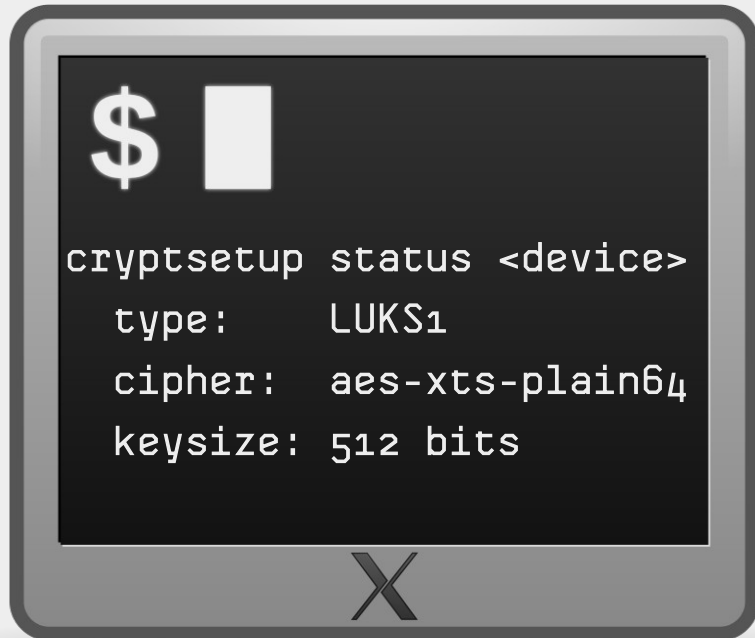


## Full disk encryption

---

All hard disks are fully LUKS encrypted, so when machine is booted, system administrator needs to login to virtual VNC console and enter the password to unlock the disks.

```
Please unlock disk sda5_crypt: *****
```



Only after that, machine is booted.

If machine is seized, data on a disk cannot be gathered unless disks are unlocked.

## Hardened SSH

---

Machine has SSH enabled for remote administration. SSH configuration is hardened.



Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

```
/ssh/ssh_host_ed25519_key  
Login no  
Includes yes  
PermitEmptyPasswords no  
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,  
aes128-gcm@openssh.com,aes256-ctr,aes128-ctr  
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.  
com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-  
ripemd160  
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,  
ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-  
exchange-sha256
```



## Firewall and brute force protection

---

Machine has also firewall, which allows access to SSH from a list of trusted IP addresses only.



We are additionally using mechanisms to limit brute force authentication attempts to SSH (from trusted IP addresses!).

## Website

---

Machine is running website with a lot of legitimate content.

All content is static, i.e. there is no server side scripting and no database in backend, which greatly reduces the possible attack surface.

Web server is configured in such a way that all web browsers are automatically redirected from HTTP to secure HTTPS connection.



https://



## Website

---

Web server is also serving several security headers, which restrict modern browsers from running into easily preventable vulnerabilities.

We are continuously running security tests on our website in order to maintain the highest level of its security.



<https://observatory.mozilla.org/analyze.html?host=yourhost.org>

## OpenVPN

---

Server is running carefully configured OpenVPN server. We have implemented:

- use of highly secure cryptographic protocols and algorithms (TLS 1.2+, 4096 Diffie-Hellman parameters, long prime numbers, TLS authentication, HMAC authentication, additional checks for cryptographic keys, etc.);
- all cryptographic keys are off-site generated;
- clients inside VPN network can see each other, but have static IP addresses;
- we are running our own DNS server which is serving DNS requests for VPN clients (to prevent DNS leaking).

## OpenVPN has been security reviewed

---

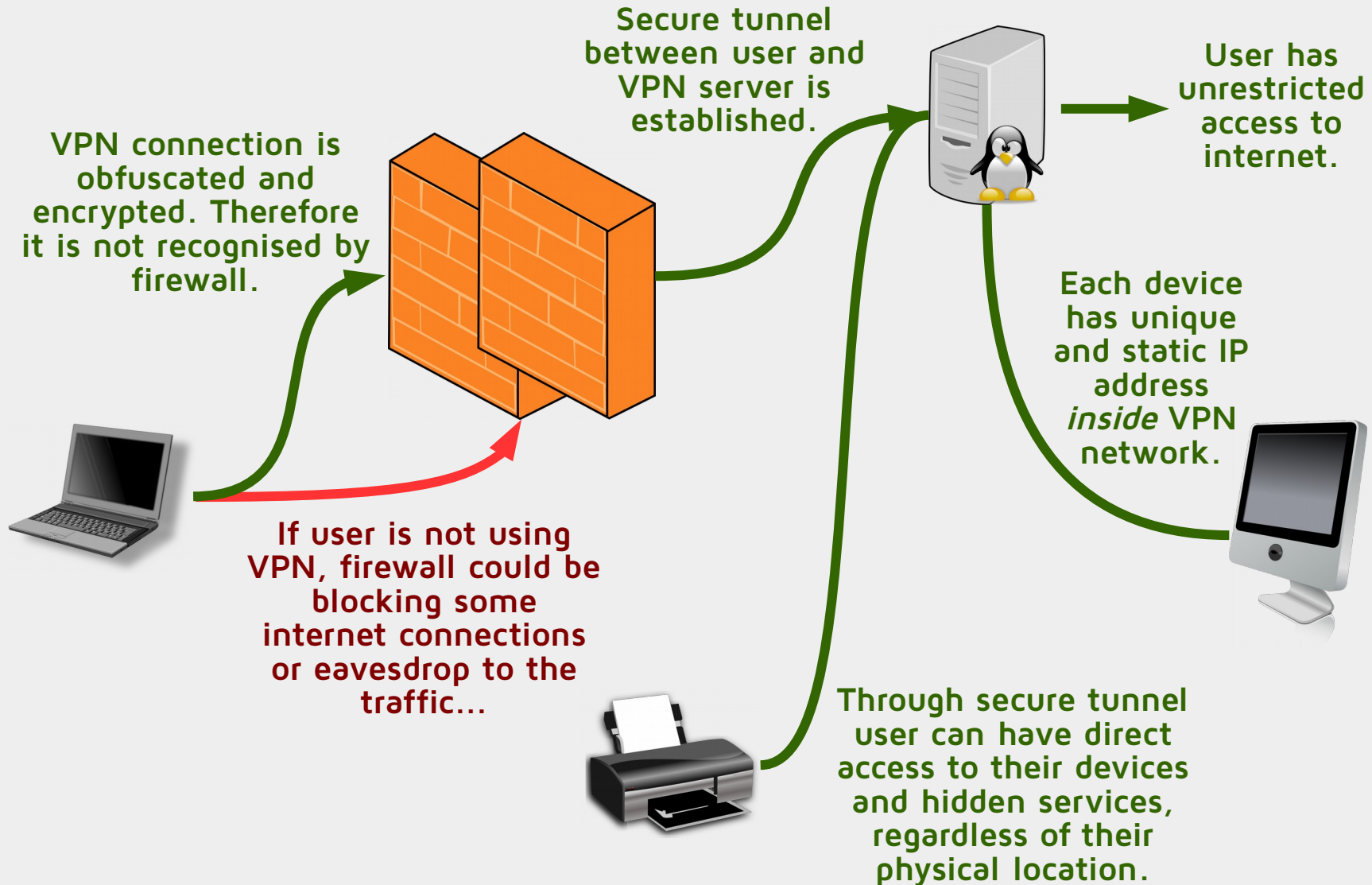
A security review led by from reputable expert on cryptography dr. Matthew Green from Johns Hopkins University has audited OpenVPN 2.4's code from December 2016 till February 2017.

The review found “no major vulnerabilities”.

Another security audit has been run by QuarksLab in the beginning of 2017.

Security audit found two bugs, but both were fixed before the report has been published.

# OpenVPN - Basic setup



## OpenVPN – Blocking and censorship resistance

---

VPN server is also trying to hide VPN traffic:

- all communication are fully encrypted and are going over TCP protocol;
- we are using port sharing technique – OpenVPN and HTTPS web server are running on the same IP address and on the same port.

This enables us to penetrate many firewalls, prevent traffic blocking and additionally hides VPN traffic among HTTPS traffic.

However, attacker which would use deep packet inspection would be able to identify VPN traffic. That is why we are actively developing advanced traffic obfuscation techniques.

## Traffic obfuscation

---

We have implemented and tested two traffic obfuscation technologies.

We are using traffic obfuscation in order to prevent government censors to detect someone is using VPN traffic, and then blocking VPN connections.

One obfuscation technology is Iodine, which tunnels VPN connection over DNS protocol.

Another approach was developed by us and is using HTTPS protected websockets.



# Iodine (TCP over DNS)

```
matej@cryptoloop:~$ sudo iodine -f -P mypassword1332 secure.telefoncek.si
Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for secure.telefoncek.si to 127.0.0.53
Autodetecting DNS query type (use -T to override).iodine: Got NOTIMP as repl
y: server does not support our request
...iodine: Got NOTIMP as reply: server does not support our request
..iodine: Got NOTIMP as reply: server does not support our request
.
Using DNS type TXT queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 10.0.1.2
Setting MTU of dns0 to 1130
Server tunnel IP is 10.0.1.1
Testing raw UDP data to the server (skip with -r)
Server is at 10.10.8.1, trying raw login: OK
Sending raw traffic directly to 10.10.8.1
Connection setup complete, transmitting data.
█

matej@cryptoloop:~$ ifconfig dns0
dns0: flags=4305<UP,POINTOPOINT,RUNNING
    inet 10.0.1.2 netmask 255.255.255.255
    unspec 00-00-00-00-00-00-00-00-00-00-00-00
500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0
    TX packets 14 bytes 1531 (1.5 KiB)
    TX errors 0 dropped 0 overruns 0

matej@cryptoloop:~$ ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data:
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=3.55 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=4.13 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=3.96 ms
^C
--- 10.0.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.553/3.884/4.136/0.244 ms
matej@cryptoloop:~$ █

matej@telefoncek:~$ sudo iodined -f -c -P mypassword1332 10.0.1.1 secure.tele
foncek.si
Opened dns0
Setting IP of dns0 to 10.0.1.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Listening to dns for domain secure.telefoncek.si
█

matej@telefoncek:~$ ip addr show dns0
27: dns0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1130 qdisc pfifo_fast
state UNKNOWN group default qlen 500
    link/none
    inet 10.0.1.1/27 scope global dns0
        valid_lft forever preferred_lft forever
matej@telefoncek:~$ ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data:
64 bytes from 10.0.1.2: icmp_seq=1 ttl=64 time=4.886 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=64 time=5.087 ms
^C
--- 10.0.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 4.886/50.897/96.904/0.244 ms
matej@telefoncek:~$ █
```

1) Iodine is activated on a server

2) Iodine from a client connects to a server

3) Client gets new network device and can connect to a server

4) Server also has network connectivity to a client

When we have covert connection with Iodine established, we run OpenVPN connection inside it.

## WebSockets

---

WebSocket is a protocol for creating a fast two-way channel between a web browser and a server.

HTTPS encrypted WebSocket connections look like ordinary HTTPS traffic.

However, inside WebSocket channel we can open OpenVPN channel...

```
location /vpn/ {
    proxy_pass http://127.0.0.1:2000;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
}
```

## WSVPN (WebSocket VPN)

---

```
screen python wsvpn-1.9.py -m server -l  
ws://127.0.0.1:2000/vpn/ -u localhost:8081  
-d
```

```
[2018-12-02 18:02:45,655 INFO] Connecting to upstream ws://localhost:8081/  
[2018-12-02 18:02:45,657 INFO] Connected to upstream  
[2018-12-02 18:02:45,658 INFO] Start upstream loop  
[2018-12-02 18:02:52,727 INFO] WS client disconnected  
[2018-12-02 18:02:54,540 WARNING] WS client disconnected  
[2018-12-02 18:02:54,542 WARNING] Upstream disconnected
```

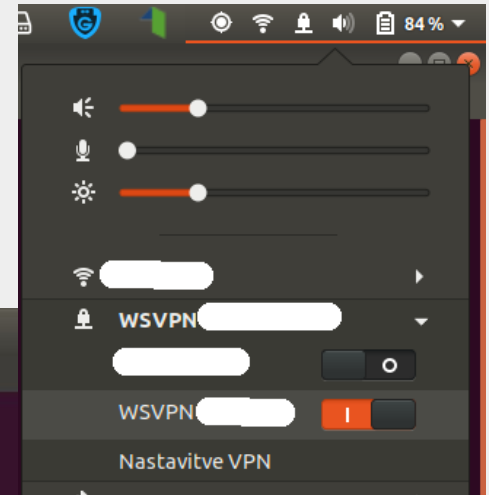


```
sudo python wsvpn-1.9.py -m client -l  
127.0.0.1:1000 -u wss://x.x.x.x:443/vpn/ -r
```

```
[2018-12-18 10:50:39,554 INFO] WSVPN VPN Websocket Proxy v1.9  
[2018-12-18 10:50:39,554 INFO] Copyright (c) 2017,2018 M***, G***, M***  
[2018-12-18 10:50:39,556 INFO] Running cmd: ***  
[2018-12-18 10:50:39,561 INFO] Running cmd: ***  
[2018-12-18 10:50:39,566 INFO] Creating new SSL certificate  
[2018-12-18 10:50:39,639 INFO] Using certificate: ./localhost.crt  
[2018-12-18 10:50:39,639 INFO] Using private key: ./localhost.key  
[2018-12-18 10:50:39,640 INFO] Client listening on tcp://127.0.0.1:1000  
[2018-12-18 10:50:39,640 INFO] Will proxy requests to wss://x.x.x.x:443/vpn/
```

# WSVPN (WebSocket VPN)

```
matej@cryptomania: ~  
Datoteka Uredi Pogled Poišči Terminal Pomoč  
matej@cryptomania:~$ ./wsvpn.sh  
Running WSVPN..  
After running the script, connect to WSVPN service.  
[2019-12-02 14:33:14,774 INFO] WSVPN VPN Websocket Proxy v1.9  
[2019-12-02 14:33:14,774 INFO] Copyright (c) 2017,2018 Matej Kovacic, Gasper Zejn,  
Matjaz Rihtar  
[2019-12-02 14:33:14,777 INFO] Running cmd: ip route  
[2019-12-02 14:33:14,781 INFO] Running cmd: ip route add [redacted] via 192.168  
.160.1  
[2019-12-02 14:33:14,785 INFO] Creating new SSL certificate  
[2019-12-02 14:33:15,014 INFO] Using certificate: /home/matej/[redacted].crt  
[2019-12-02 14:33:15,014 INFO] Using private key: /home/matej/[redacted].key  
[2019-12-02 14:33:15,015 INFO] Client listening on tcp://127.0.0.1:1000  
[2019-12-02 14:33:15,015 INFO] Will proxy requests to wss://[redacted]
```



## WSVPN device

---

User first needs to run WSVPN software, which opens HTTPS encrypted websocket connection to the server, and then run VPN client.

This is a little unhandy for most users.

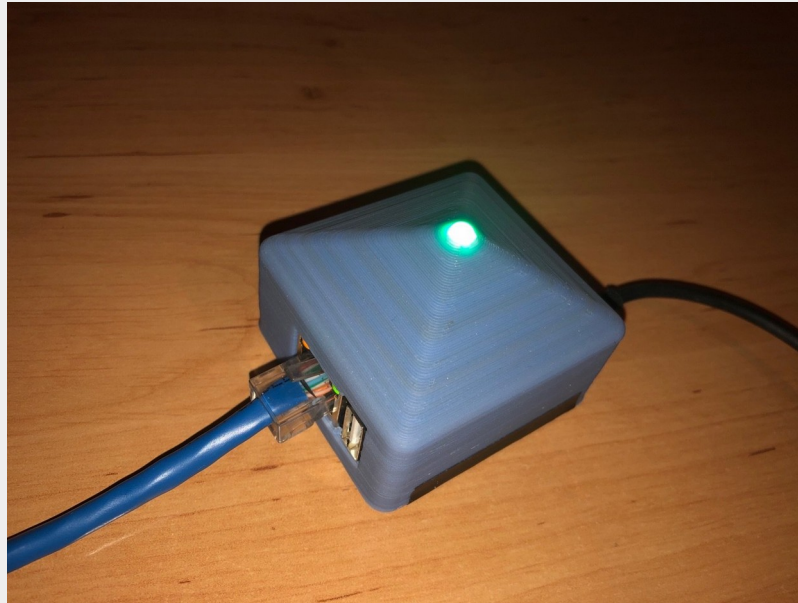
Therefore we developed a small hardware device (based on OrangePi), which acts as a WiFi access point.

When device is connected to the network, it automatically connects itself to our VPN server through obfuscated connection. This is indicated by the small green diode on the top of the device.

## WSVPN device

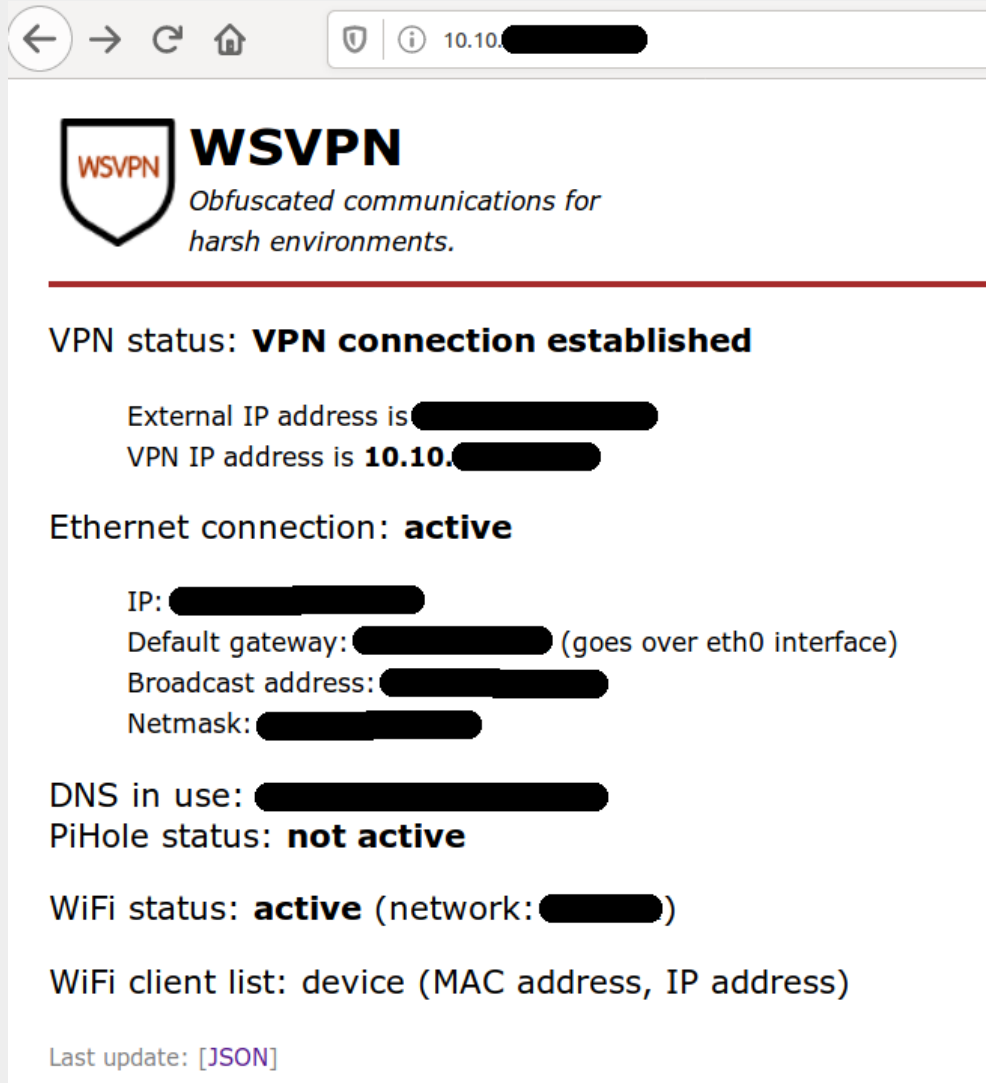
---

User then connects to WSVPN device via WiFi, and all his traffic is then automatically routed to our VPN server.



User therefore does not need any additional software on his/her devices. He or she just connect to WSVPN WiFi and has direct access to the uncensored internet through obfuscated VPN connection.

# WSVPN device



The screenshot shows the WSVPN web interface. At the top, there is a navigation bar with a shield icon and the text "10.10." followed by a redacted IP address. Below the navigation bar is the WSVPN logo and the tagline "Obfuscated communications for harsh environments." A red horizontal line separates the header from the main content. The main content displays the VPN status as "VPN connection established". Below this, it shows the external IP address and the VPN IP address as "10.10." followed by a redacted IP address. The Ethernet connection is shown as "active" with details for IP, default gateway, broadcast address, and netmask. The DNS is in use, and PiHole status is "not active". The WiFi status is "active" with the network name redacted. A WiFi client list is shown with the header "device (MAC address, IP address)". At the bottom, it says "Last update: [JSON]" with a link to the JSON data.

WSVPN  
*Obfuscated communications for harsh environments.*

---

VPN status: **VPN connection established**

External IP address is [REDACTED]  
VPN IP address is **10.10.**[REDACTED]

Ethernet connection: **active**

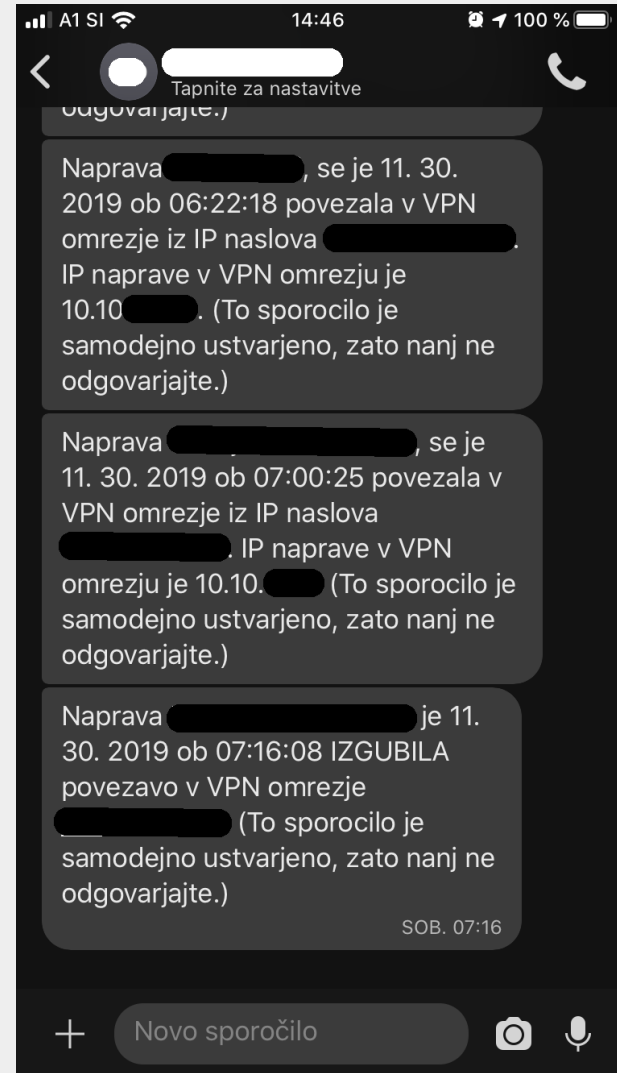
IP: [REDACTED]  
Default gateway: [REDACTED] (goes over eth0 interface)  
Broadcast address: [REDACTED]  
Netmask: [REDACTED]

DNS in use: [REDACTED]  
PiHole status: **not active**

WiFi status: **active** (network: [REDACTED])

WiFi client list: device (MAC address, IP address)

Last update: [\[JSON\]](#)



The screenshot shows a mobile messaging app interface. At the top, there is a status bar with the time "14:46" and battery level "100%". Below the status bar is a header with a back arrow, a circular profile picture, and the text "Tapnite za nastavitve" and "Odgovarjajte.". The main content displays three messages. The first message is from a device named "Naprava [REDACTED]" and says "se je 11. 30. 2019 ob 06:22:18 povezala v VPN omrežje iz IP naslova [REDACTED]. IP naprave v VPN omrežju je 10.10.[REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)". The second message is from the same device and says "se je 11. 30. 2019 ob 07:00:25 povezala v VPN omrežje iz IP naslova [REDACTED]. IP naprave v VPN omrežju je 10.10.[REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)". The third message is from the same device and says "je 11. 30. 2019 ob 07:16:08 IZGUBILA povezavo v VPN omrežje [REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)". At the bottom, there is a text input field with the placeholder "Novo sporočilo" and icons for adding attachments, camera, and voice recording.

14:46 100%

Tapnite za nastavitve  
Odgovarjajte.

Naprava [REDACTED], se je 11. 30. 2019 ob 06:22:18 povezala v VPN omrežje iz IP naslova [REDACTED]. IP naprave v VPN omrežju je 10.10.[REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)

Naprava [REDACTED], se je 11. 30. 2019 ob 07:00:25 povezala v VPN omrežje iz IP naslova [REDACTED]. IP naprave v VPN omrežju je 10.10.[REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)

Naprava [REDACTED] je 11. 30. 2019 ob 07:16:08 IZGUBILA povezavo v VPN omrežje [REDACTED]. (To sporočilo je samodejno ustvarjeno, zato nanj ne odgovarjajte.)

SOB. 07:16

Novo sporočilo

## WSVPN - Testing in China

---

Before:

- China authorities detect VPN connection. Usually they do not block it immediately, but they tend to slow it down, so it is unusable (server pings were above 11.000 ms).
- However, when there was some political event, connection to VPN server has not been possible at all (even HTTP connection was not working).

After:

- VPN connection is working, server pings are around 500 ms.



## WSVPN - Testing in Uzbekistan

---

Before:

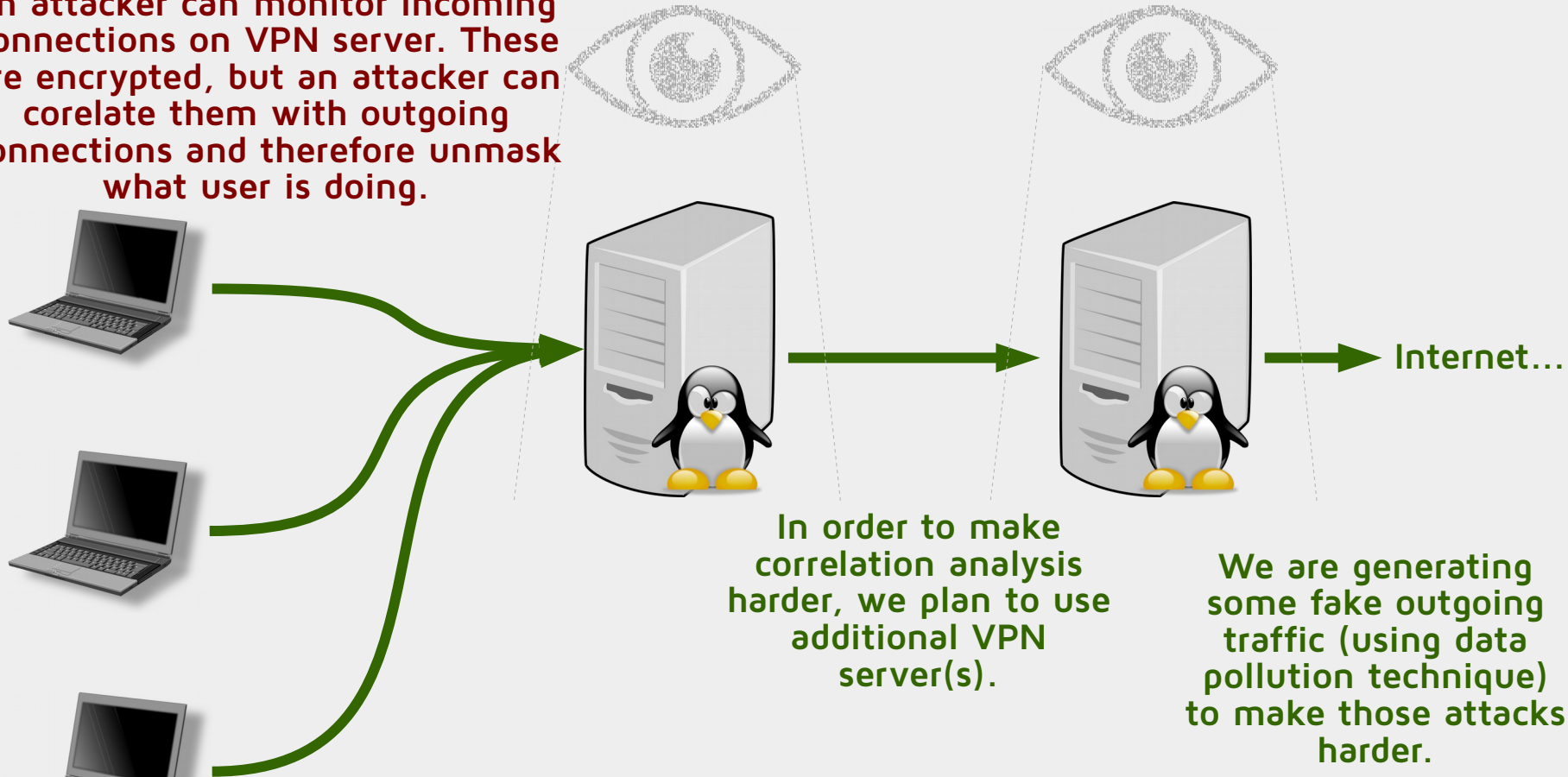
- VPN connection has not been possible, since during the authentication phase, government has been malforming internet traffic.

After

- VPN connection is now working.
- Connecting to VPN with WSVPN device is very easy and requires no additional software and zero configuration from user (except configuration for WiFi access).

# OpenVPN - Advanced setup *(partially implemented)*

If there are few users (or only one), an attacker can monitor incoming connections on VPN server. These are encrypted, but an attacker can correlate them with outgoing connections and therefore unmask what user is doing.



We are generating some additional intra-VPN traffic to make those attacks harder.

In order to make correlation analysis harder, we plan to use additional VPN server(s).

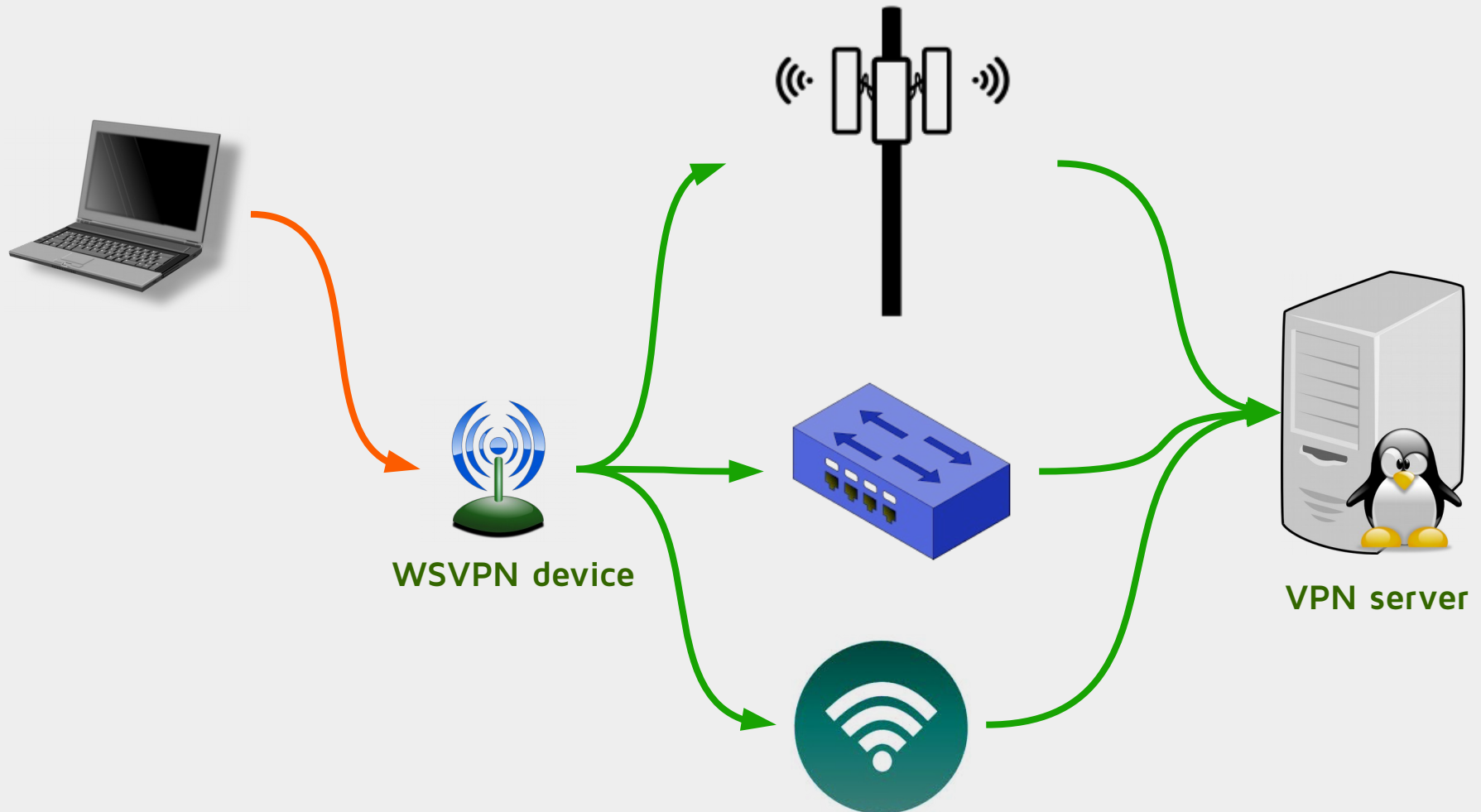
We are generating some fake outgoing traffic (using data pollution technique) to make those attacks harder.

```
This is ISP Data Pollution 3, Version 1.3
Downloading the blacklists... Shallalist done... EasyList
done.
Display format:
Downloading: website.com; NNNNN links [in library],
H(domain)= B bits [entropy]
Downloaded: website.com: +LLL/NNNNN links [added],
H(domain)= B bits [entropy]
```

## Further ideas

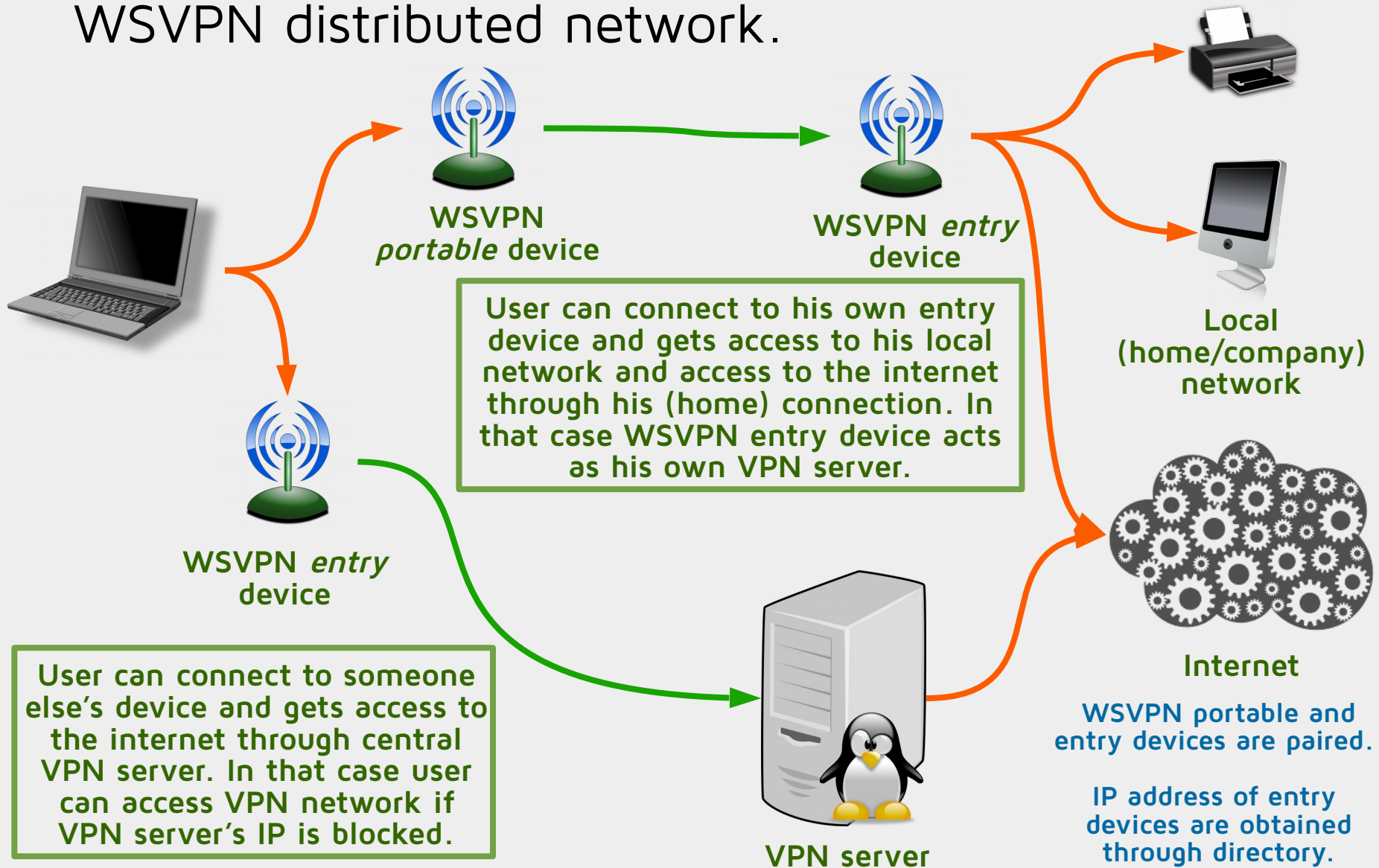
---

WSVPN device should support outgoing connections to ethernet, WiFi and 3G/4G.



## Further ideas

### WSVPN distributed network.



# Questions?



Matej Kovačič  
matej.kovacic@telefoncek.si