VPN – Virtual Private Networks

Matej Kovačič

Jožef Stefan Institute
Ljubljana, Slovenia

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

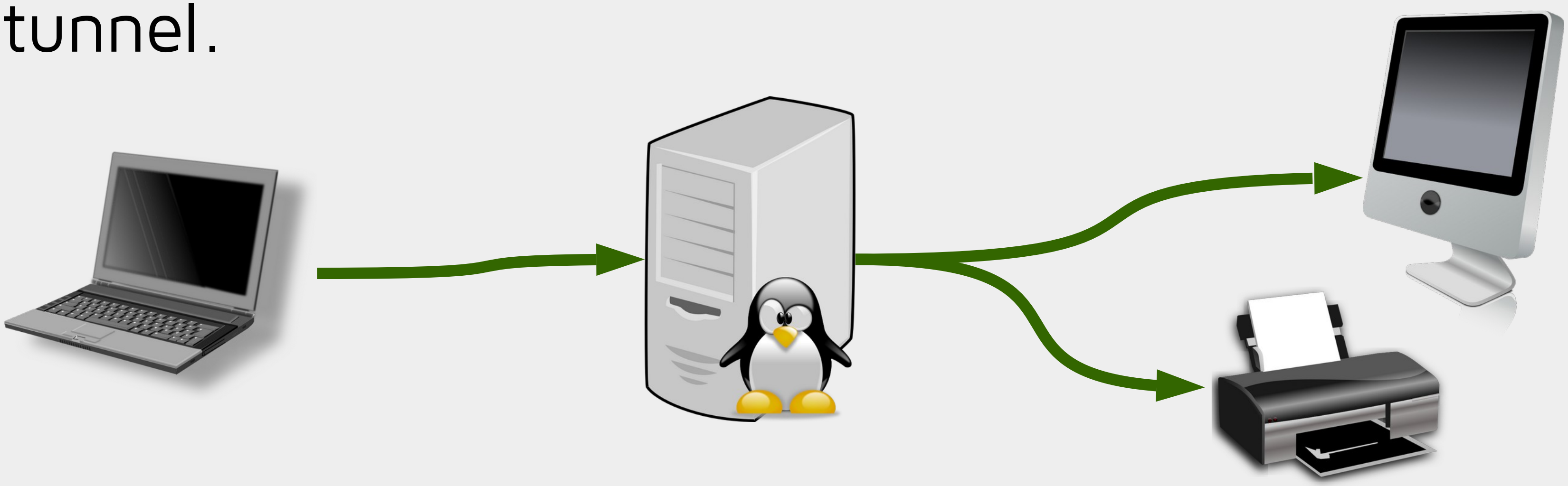
IRCAI
International Research Centre
on Artificial Intelligence
under the auspices of UNESCO

Personal blog:
https://telefoncek.si

VPN basics

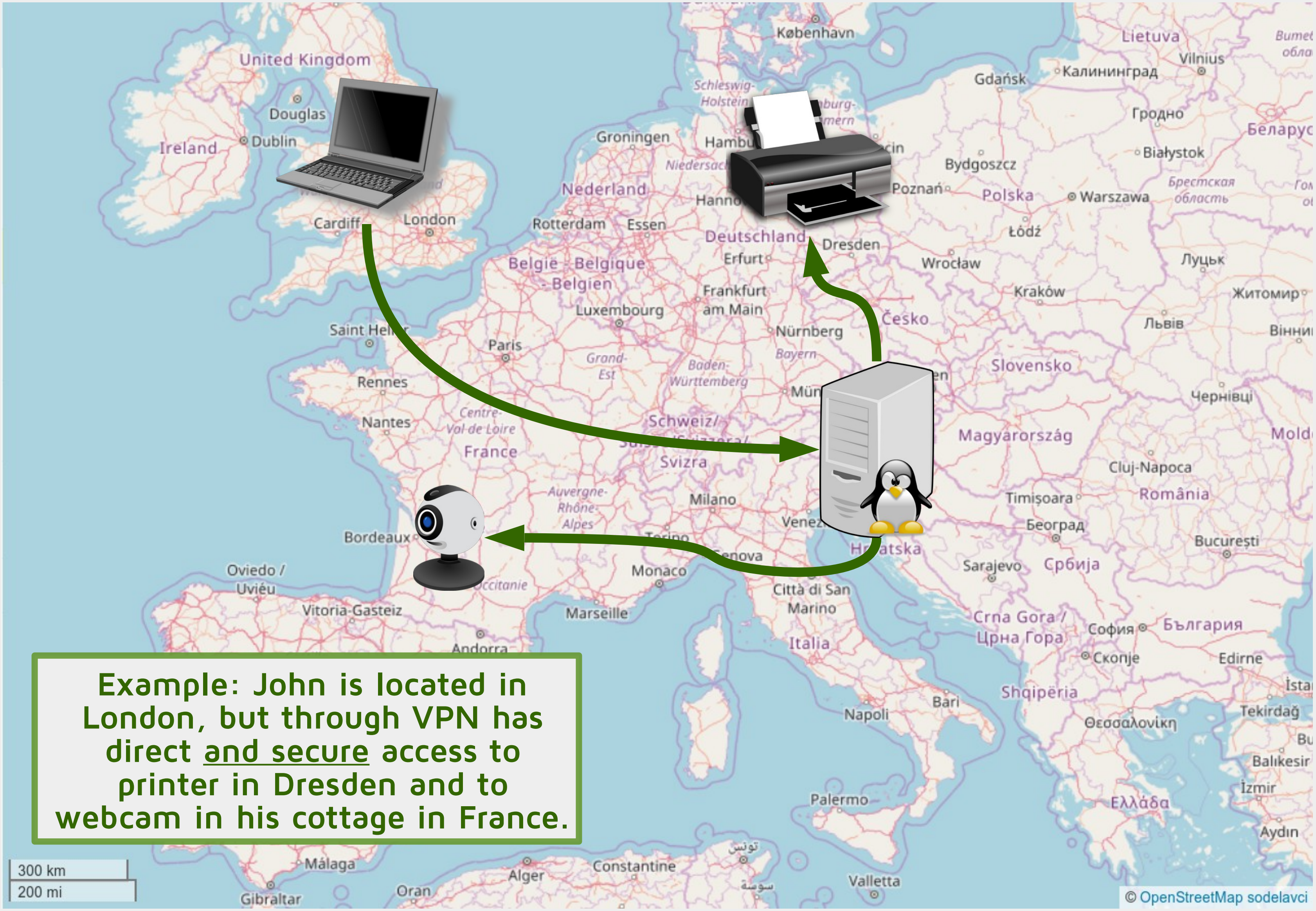
What is VPN?

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.

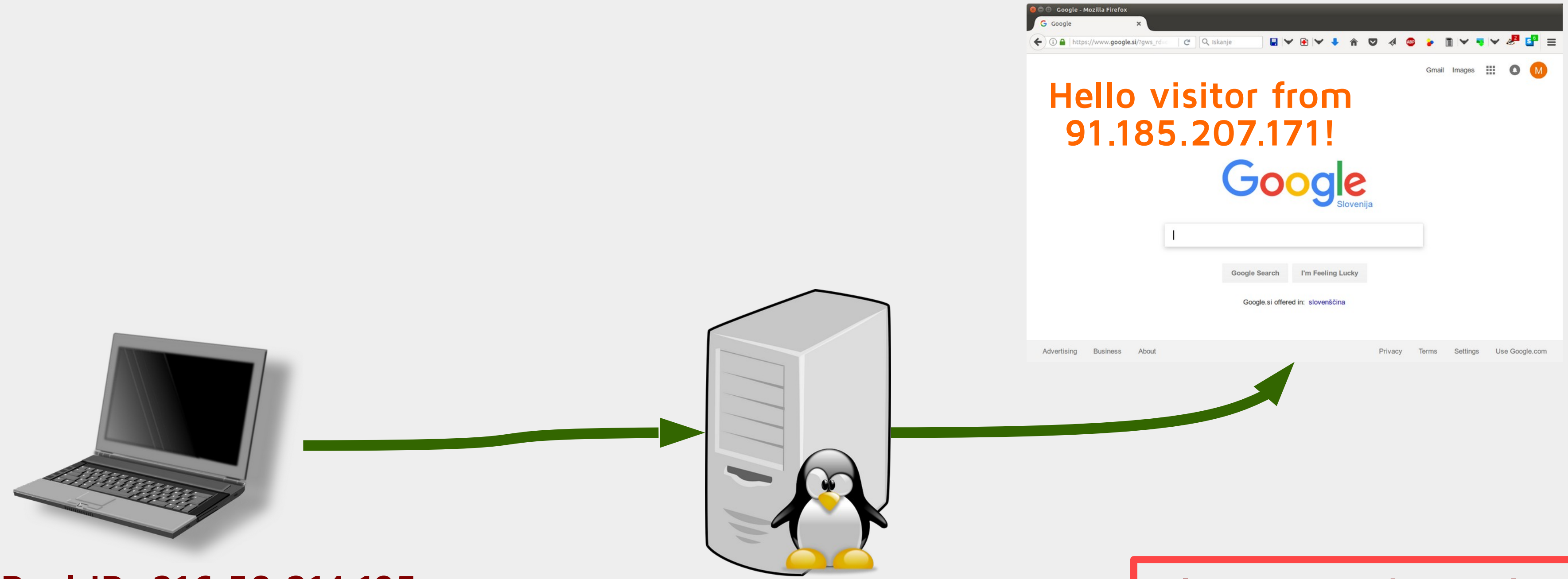
Access to remote networks or devices



Example: John is located in London, but through VPN has direct <u>and secure</u> access to printer in Dresden and to webcam in his cottage in France.

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.



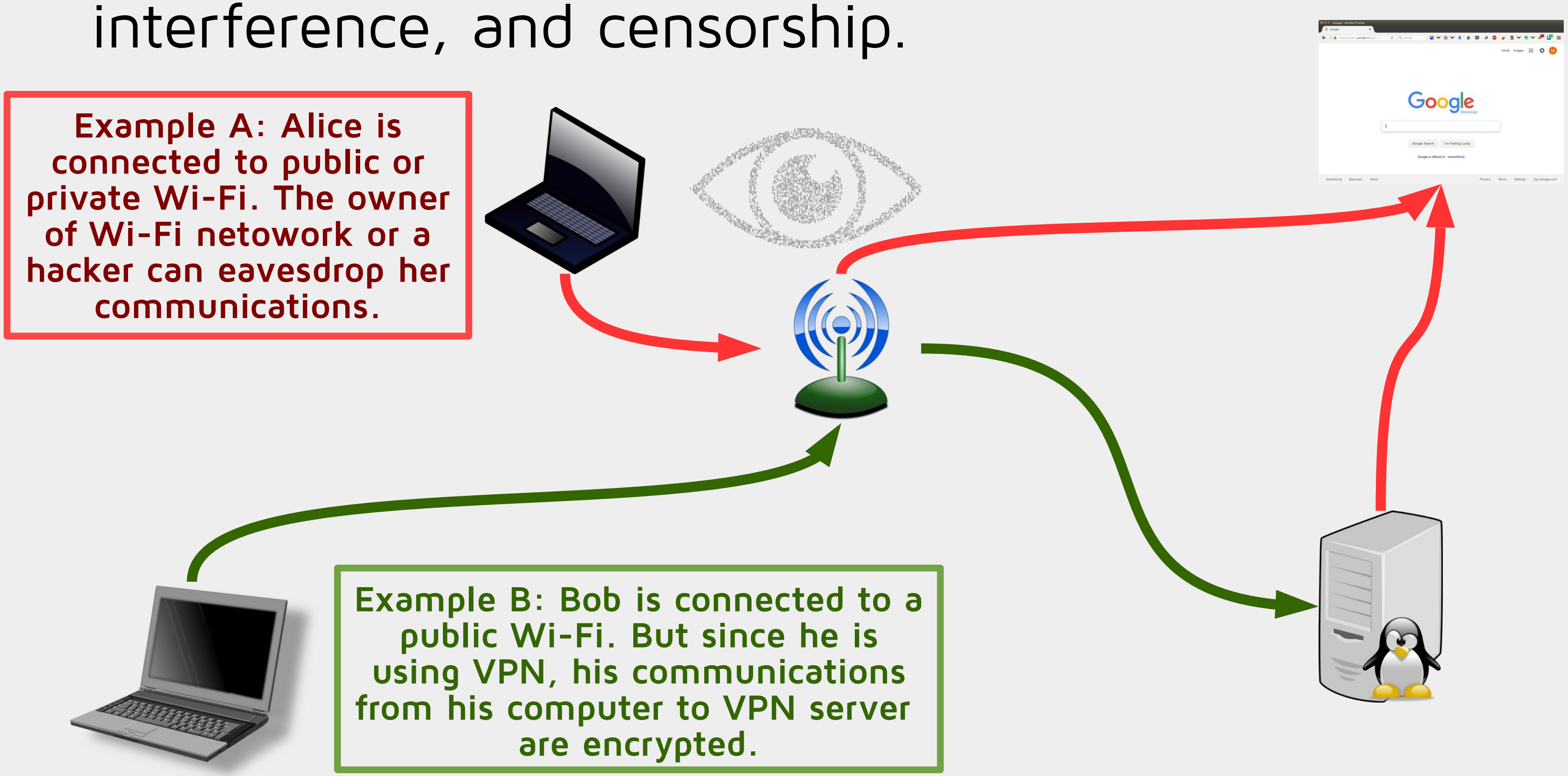
Real IP: 216.58.214.195

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

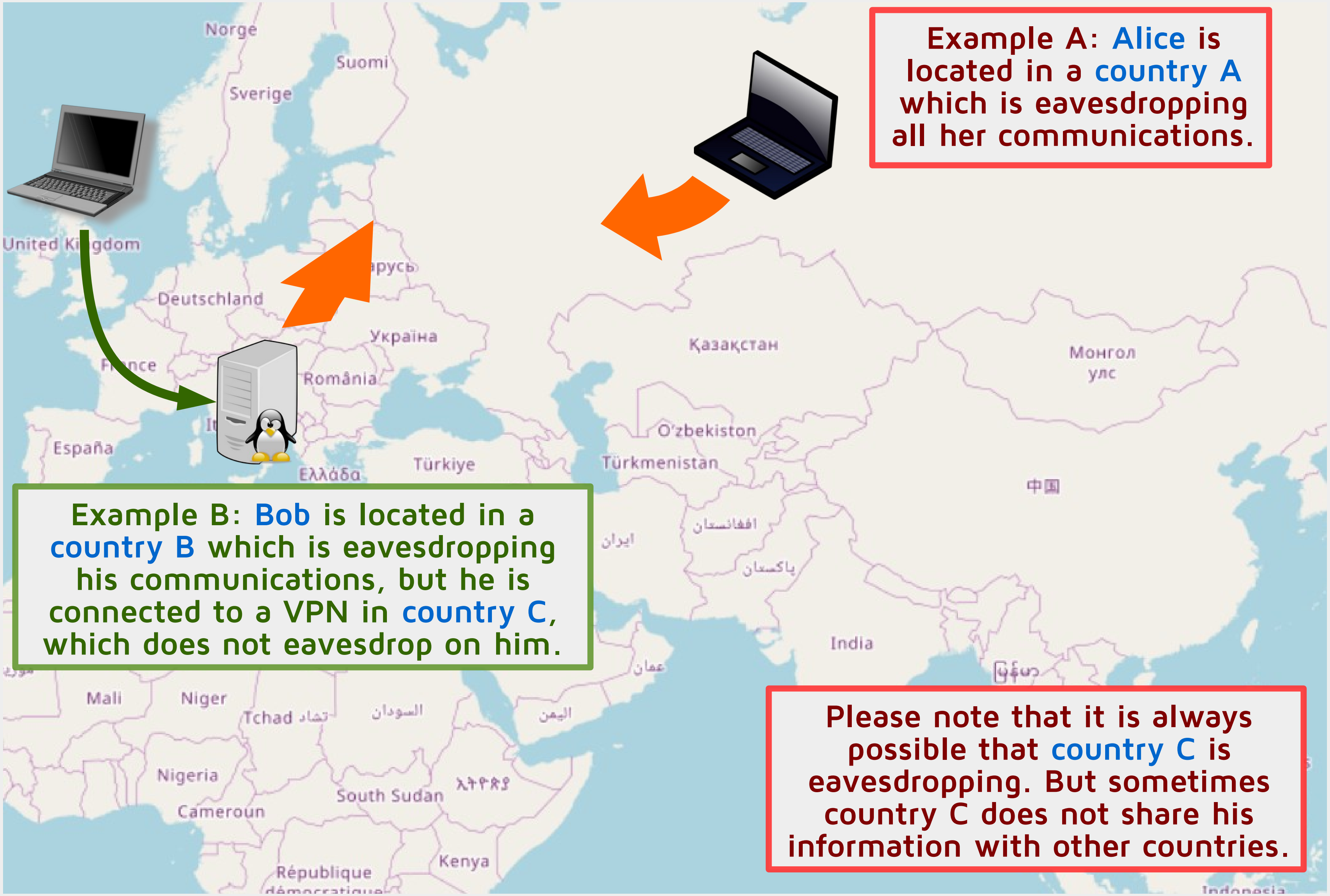
Since VPN establishes a secure tunnel between two or more devices, VPNs are often used to protect network traffic from snooping, interference, and censorship.



Example A: Alice is connected to public or private Wi-Fi. The owner of Wi-Fi netowork 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



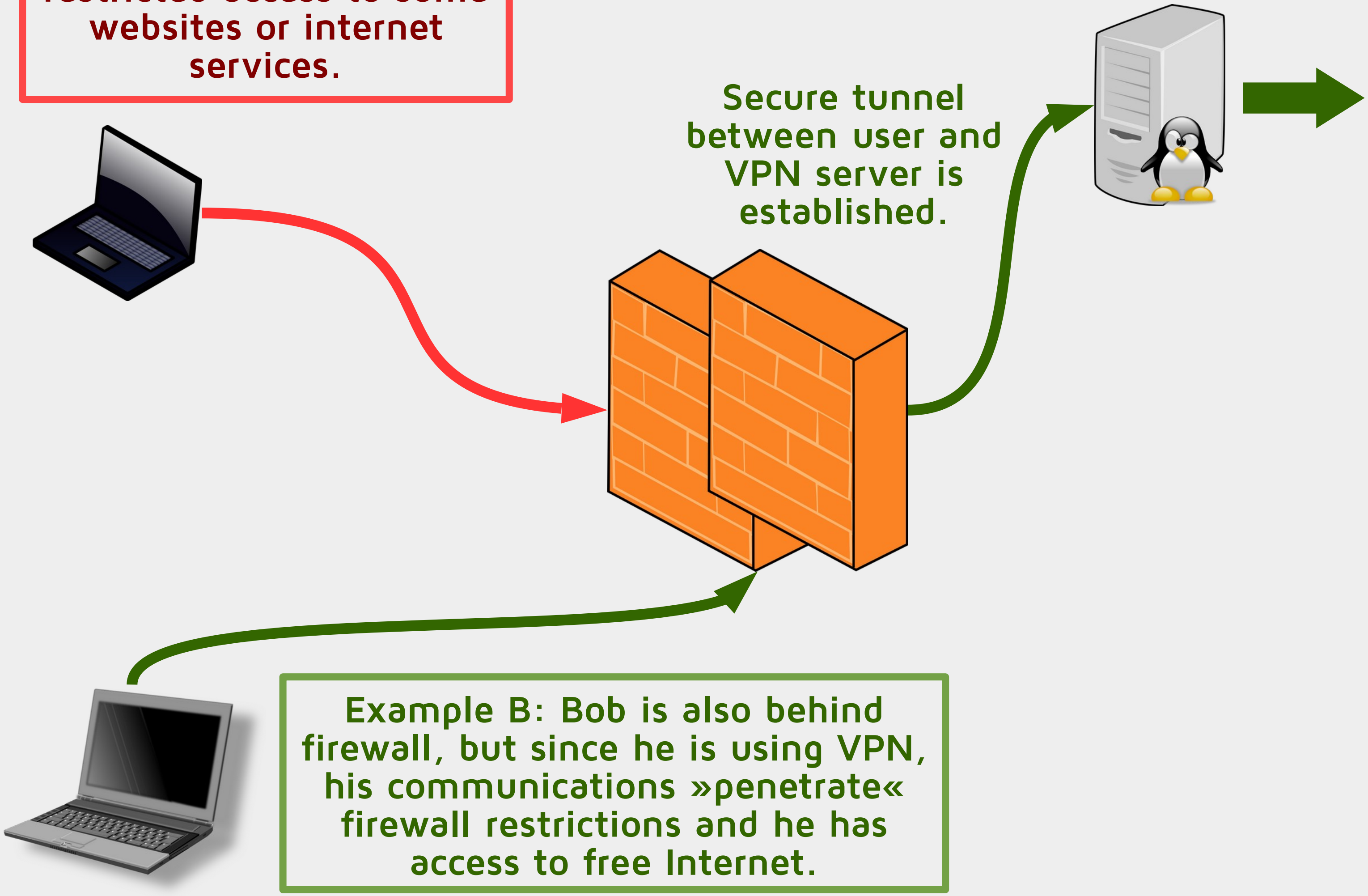
Example A: Alice is located in a country A which is eavesdropping all her communications.

Example B: Bob is located in a country B which is eavesdropping his communications, but he is connected to a VPN in country C, which does not eavesdrop on him.

Please note that it is always possible that country C is eavesdropping. But sometimes country C does not share his information with other countries.

Protection from blocking

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

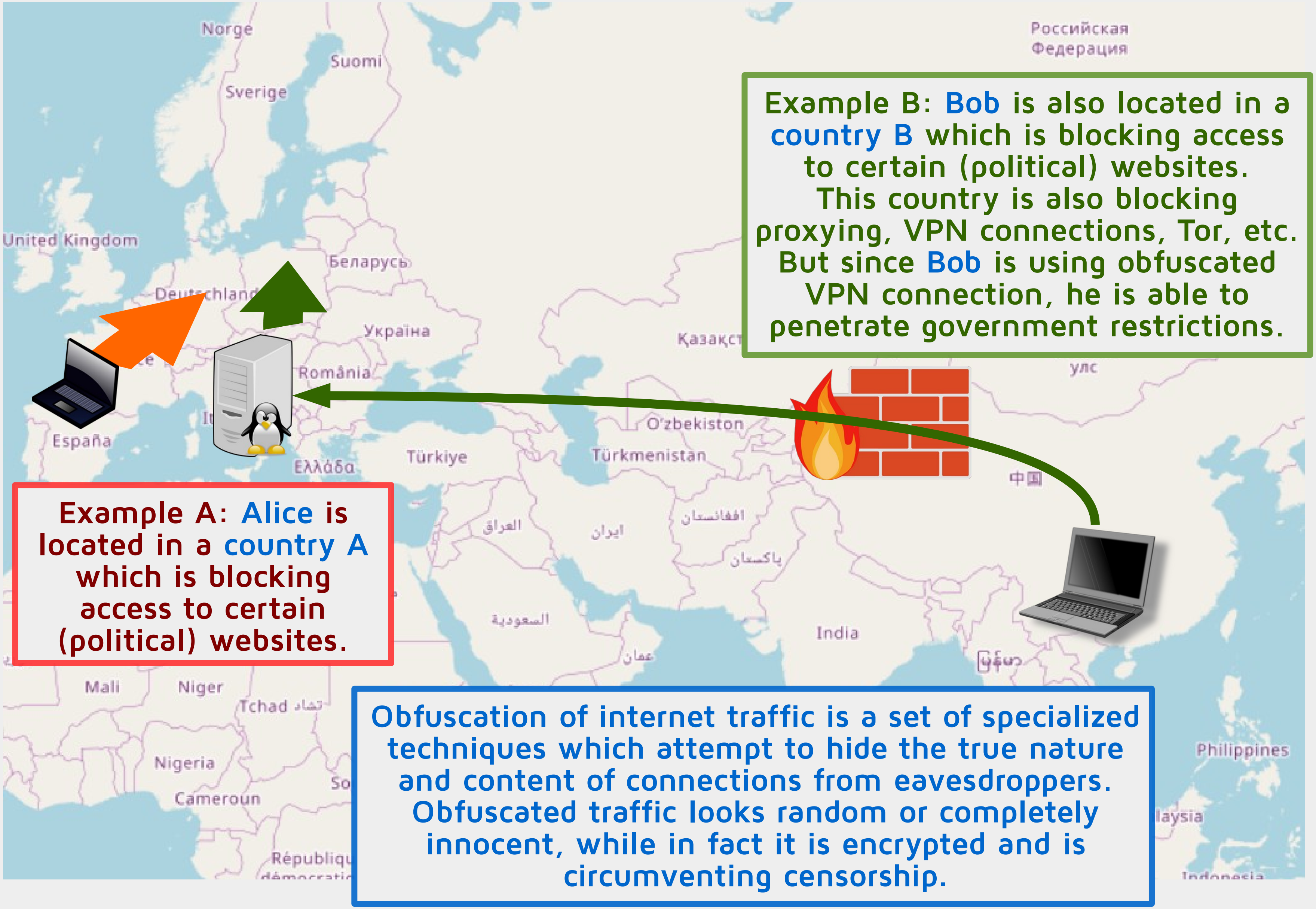


Secure tunnel between user and VPN server is established.

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 cenzorship



Example B: Bob is also located in a country B which is blocking access to certain (political) websites. This country is also blocking proxying, VPN connections, Tor, etc. But since Bob is using obfuscated VPN connection, he is able to penetrate government restrictions.

Example A: Alice is located in a country A which is blocking access to certain (political) websites.

Obfuscation of internet traffic is a set of specialized techniques which attempt to hide the true nature and content of connections from eavesdroppers. Obfuscated traffic looks random or completely innocent, while in fact it is encrypted and is circumventing censorship.

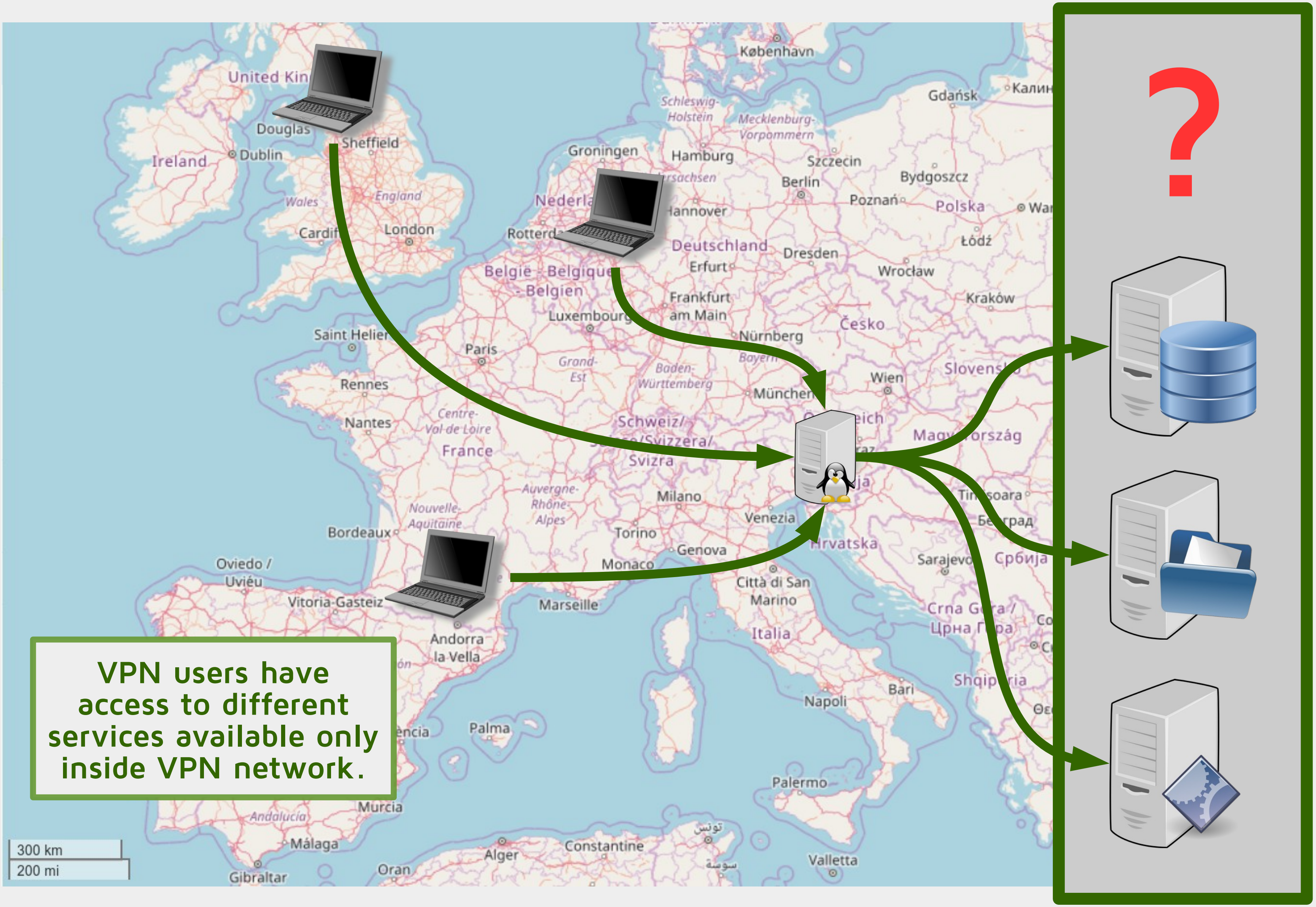
Additional services

Additional services

Additional services inside VPN network:

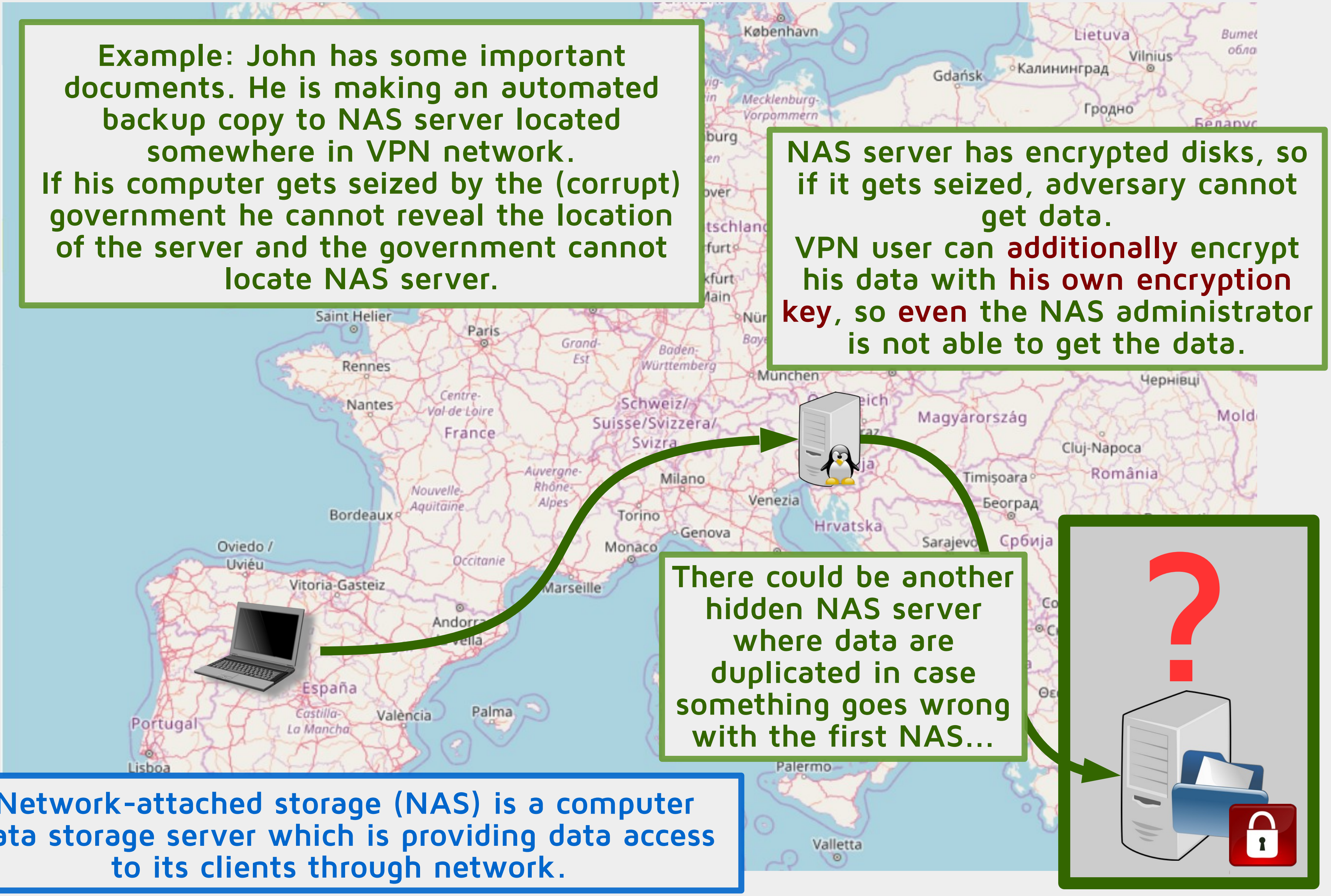
- hidden services (NAS, internal websites (accessible only inside VPN network),...);
- private bridges to other networks (for instance secure remote access to your home network);
- notifications (infrastructure monitoring);
- intrusion detection;
- blocking unwanted domains;
- ...

Hidden services



VPN users have access to different services available only inside VPN network.

Example: hidden NAS server



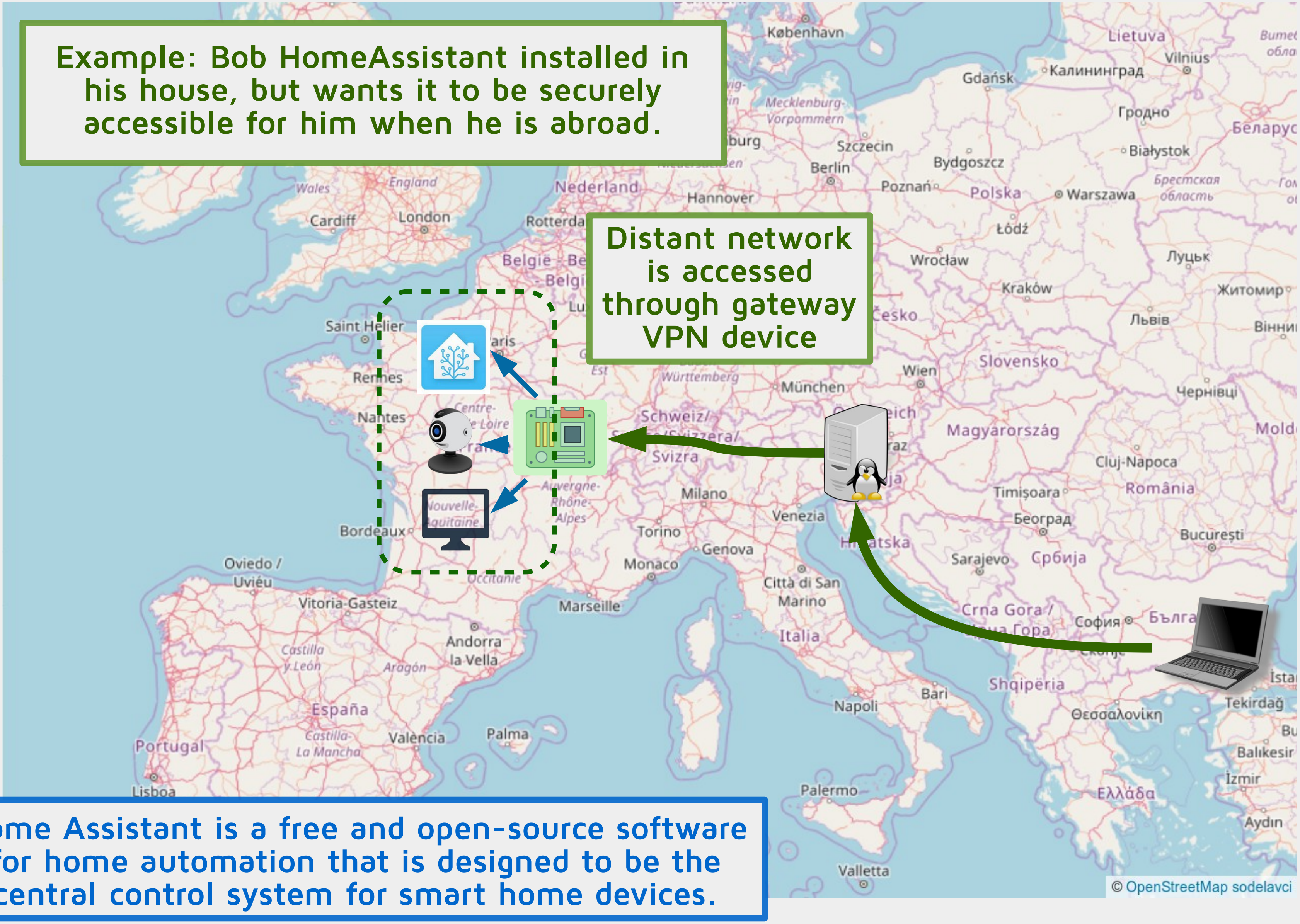
Example: John has some important documents. He is making an automated backup copy to NAS server located somewhere in VPN network.
If his computer gets seized by the (corrupt) government he cannot reveal the location of the server and the government cannot locate NAS server.

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.

Private bridges to distant networks



Example: Bob HomeAssistant installed in his house, but wants it to be securely accessible for him when he is abroad.

Distant network is accessed through gateway VPN device

© OpenStreetMap sodelavci

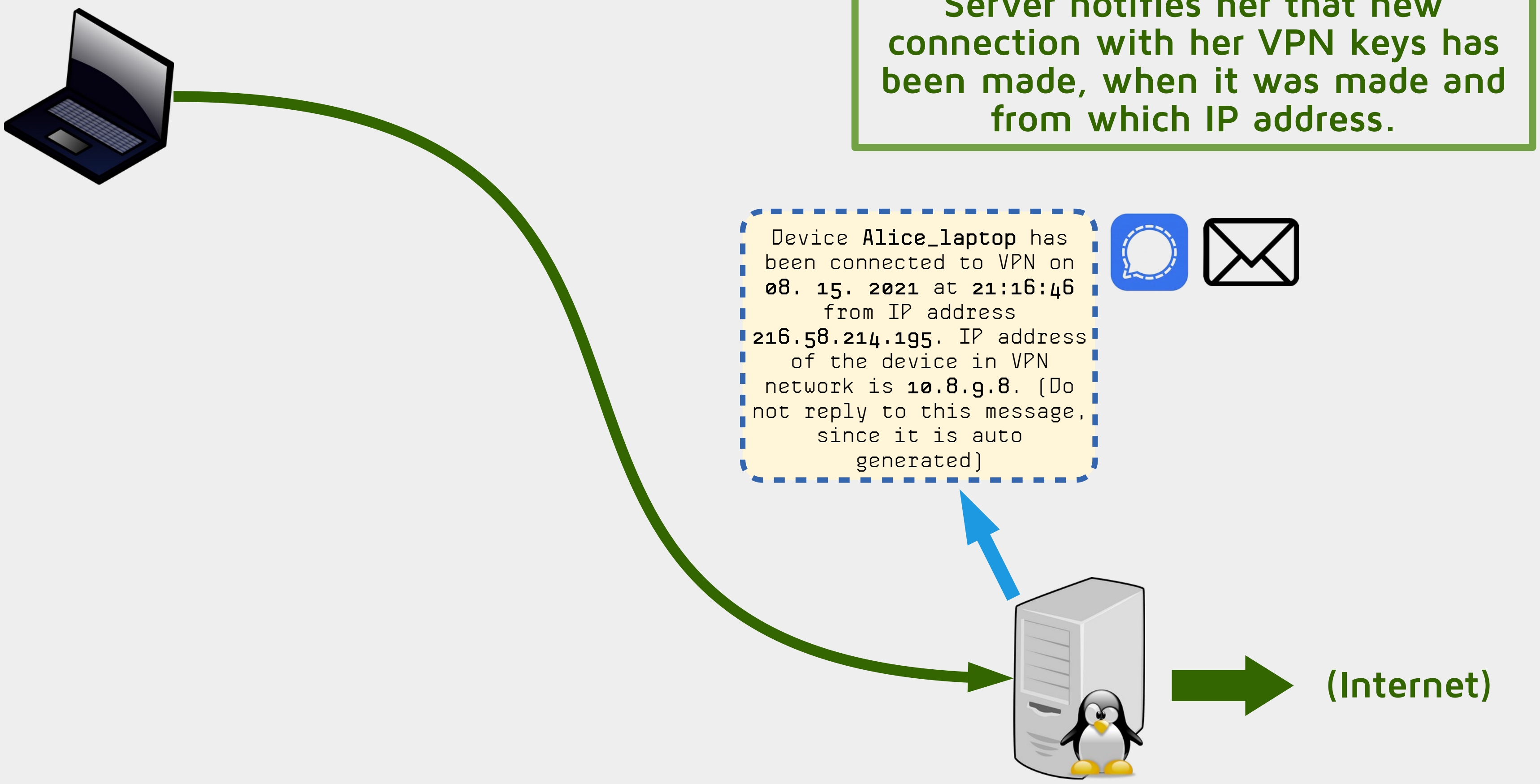
Home Assistant is a free and open-source software for home automation that is designed to be the central control system for smart home devices.

Connection notifications

Connection notifications could be useful for infrastructure monitoring and to detect when and where VPN keys have been used.

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.

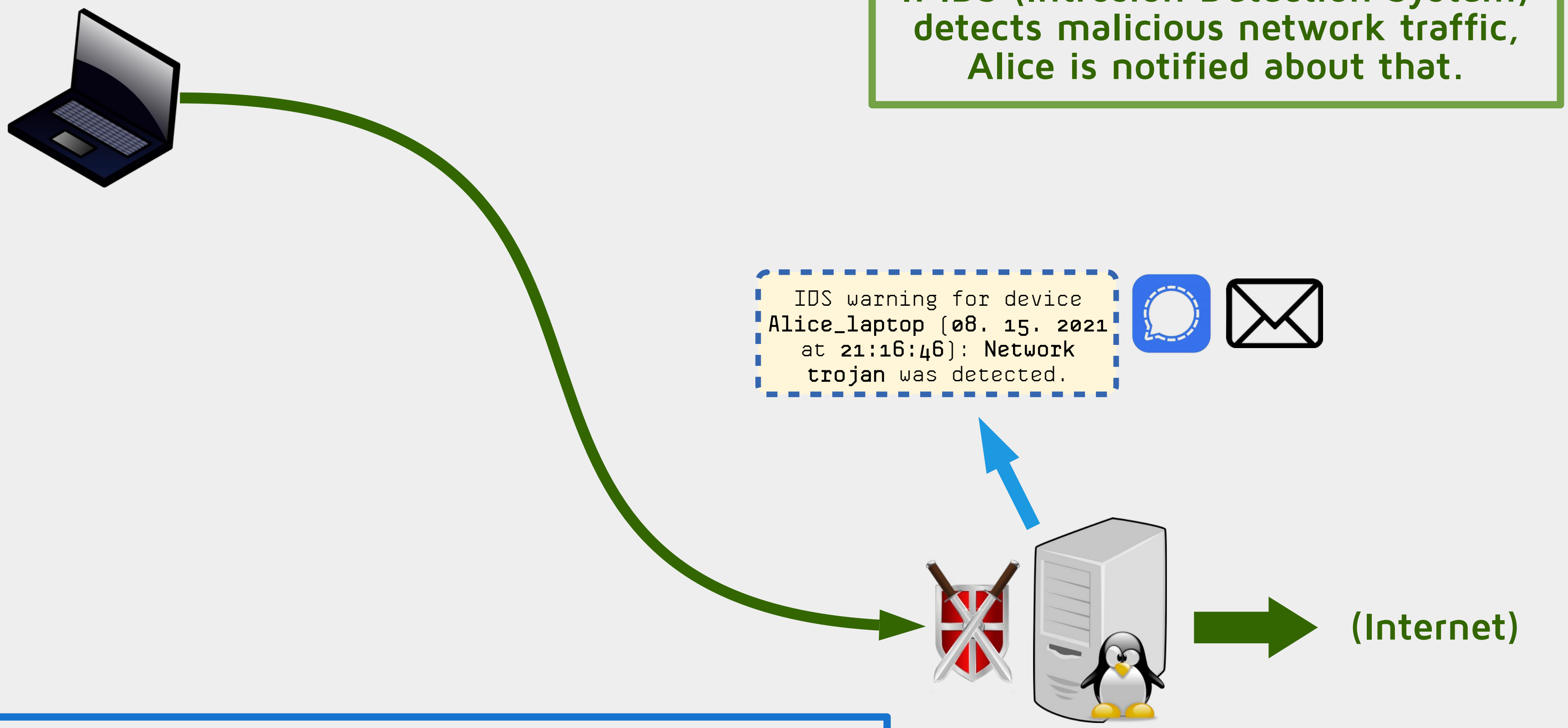


Device **Alice_laptop** has been connected to VPN on **08. 15. 2021** at **21:16:46** from IP address **216.58.214.195**. IP address of the device in VPN network is **10.8.9.8**. (Do not reply to this message, since it is auto generated)

Intrusion detection

Example: Alice is journalist and has been targeted by government malware.

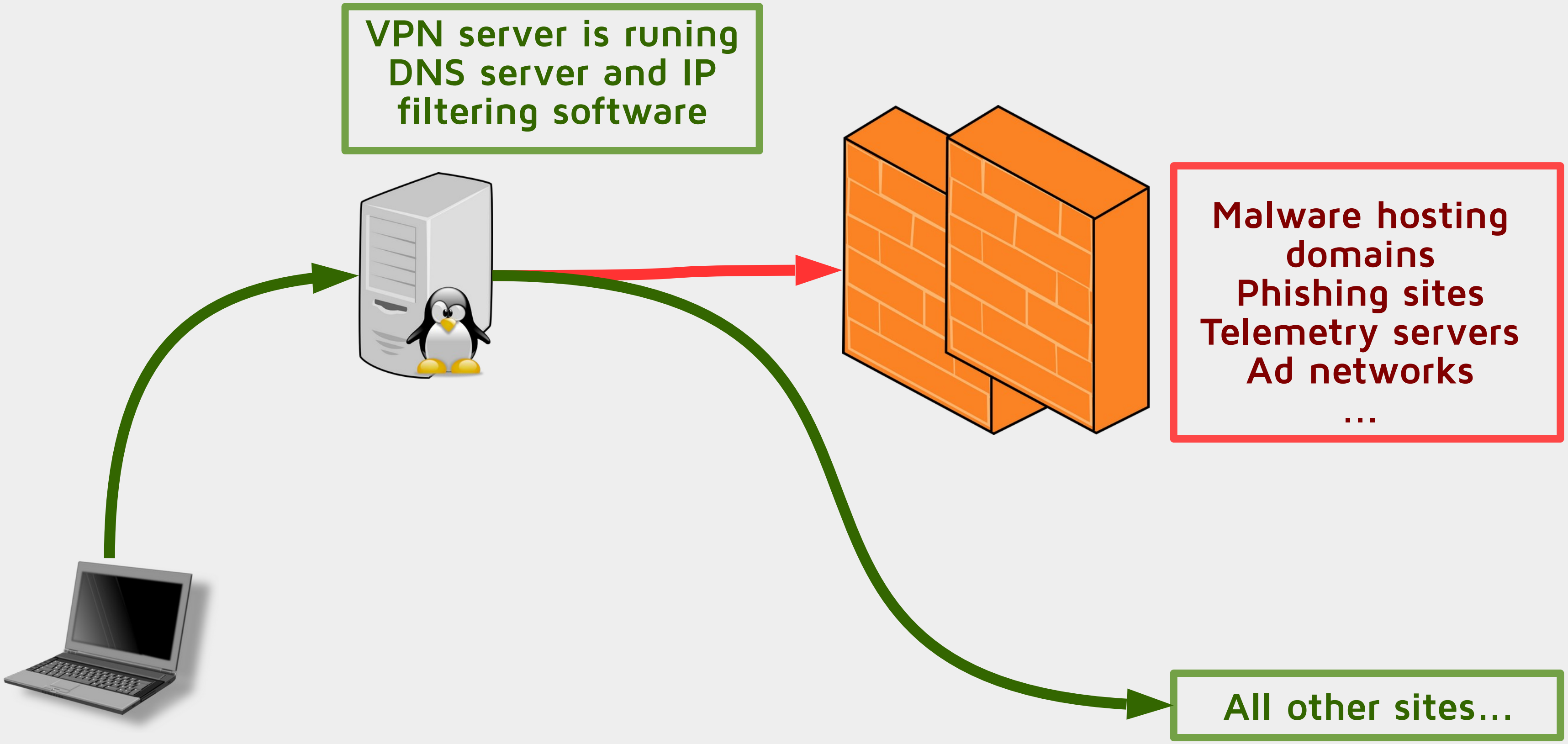
VPN server is analysing all Alice's traffic (with her consent!).
If IDS (Intrusion Detection System) detects malicious network traffic, Alice is notified about that.



IDS warning for device Alice_laptop (08. 15. 2021 at 21:16:46): Network trojan was detected.

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

Blocking unwanted domains



VPN server is runing DNS server and IP filtering software

Malware hosting domains
Phishing sites
Telemetry servers
Ad networks
...

All other sites...

Blocking telemetry servers and ad networks can save bandwith and speed up internet connection.

Security

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.).

Why your own infrastructure?

A study from 2021 analysing different VPN products has shown:

- A lot of these products are owned/operated by the same company (for at least of 101 VPN products researchers found out that they are owned or operated by only 23 companies).
- VPN service providers are not transparent with users regarding their owners and parent companies' locations.
- Up to 30% of VPNs have connections with or were owned by Chinese firms.
- VPN services are located in different "privacy unfriendly" countries including China, Hong Kong, Pakistan, UAE, USA, UK, Switzerland...

Source: VPN pro, https://vpnpro.com/. Jan Youngren. Hidden VPN owners unveiled: 101 VPN products run by just 23 companies. April 19th, 2021.

Why your own infrastructure?

Why is this a problem?

- **China**: high level of surveillance and cyber spying, sponsors cyber attacks on foreign officials, government can ask for encryption keys, data, etc., China is leading active »war« against VPN services, VPN owners need a license to operate in China, VPN applications are not available on the Chinese Android and iOS application stores,...
- **Pakistan**: government can access any data without a warrant and data can be freely handed over to foreign institutions.

Why your own infrastructure?

Why is this a problem?

- **USA**: founding member of the *Five Eyes alliance*, a major surveillance state, NSA invests heavily in backdooring encryption technology, FBI can access any data by secret subpoenas (NSLs),...
- **UK**: founding member of the *Five Eyes alliance* and has surveillance legislation that gives law enforcement strong surveillance power (*Investigatory Powers Act*, or *Snooper's Charter*, introduced in 2016).

Why your own infrastructure?

Why is this a problem?

- **Switzerland**: Swiss strong privacy laws are a myth. Swiss *Federal Act on the Surveillance of Post and Telecommunications* and *Federal Intelligence Service Act* are introducing full and unlimited surveillance of all electronic communication. Data protection laws in Switzerland are in many cases not applicable to surveillance measures by secret services, police authorities and public prosecutors. Surveillance measures in Switzerland are approved behind closed doors by Compulsory Measures Courts and there is no effective supervision of the security authorities. Regarding intelligence cooperation, Switzerland has several bilateral agreements with EU and is bound by a *Mutual Legal Assistance Treaty* with the United States.

More info: Martin Steiger. 2019. ProtonMail voluntarily offers Assistance for Real-Time Surveillance. https://archive.is/VwyL5

Why your own infrastructure?

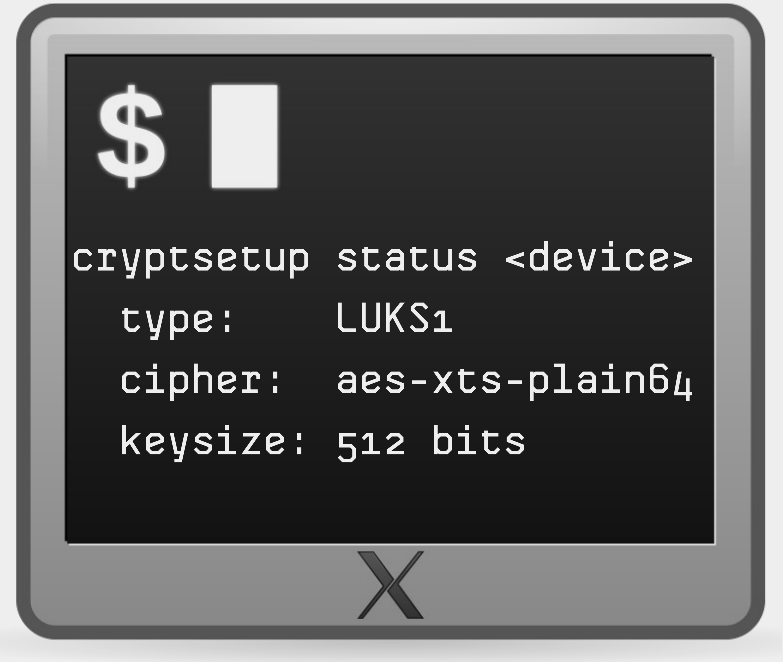
Transparency and trust are vital in the VPN industry.

- Who is the operator of exit points (VPN gateways to the internet) and how user's data is handled there.
- Where are VPN servers and exit points located (country, legislation)?
- How trustworthy is the ISP of VPN provider?
- Is VPN infrastructure well protected and maintained regularly?
- How transparent and secure is VPN software/hardware on user's endpoint?

Full disk encryption

Machine should have hard disks fully encrypted, so when machine is booted, system administrator needs to enter the password to unlock the disks.

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



```
cryptsetup status <device>
  type:    LUKS1
  cipher:  aes-xts-plain64
  keysize: 512 bits
```

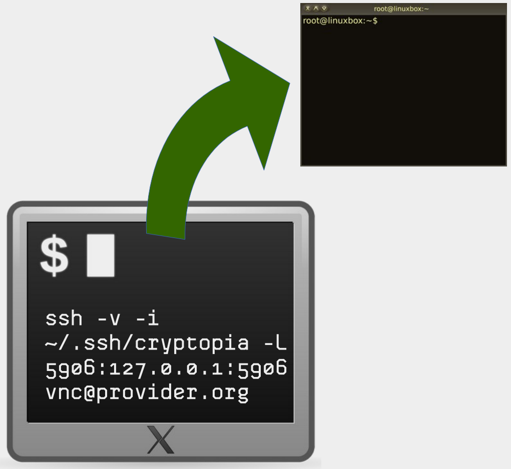
Only after that, machine is booted.

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

Remote management console access

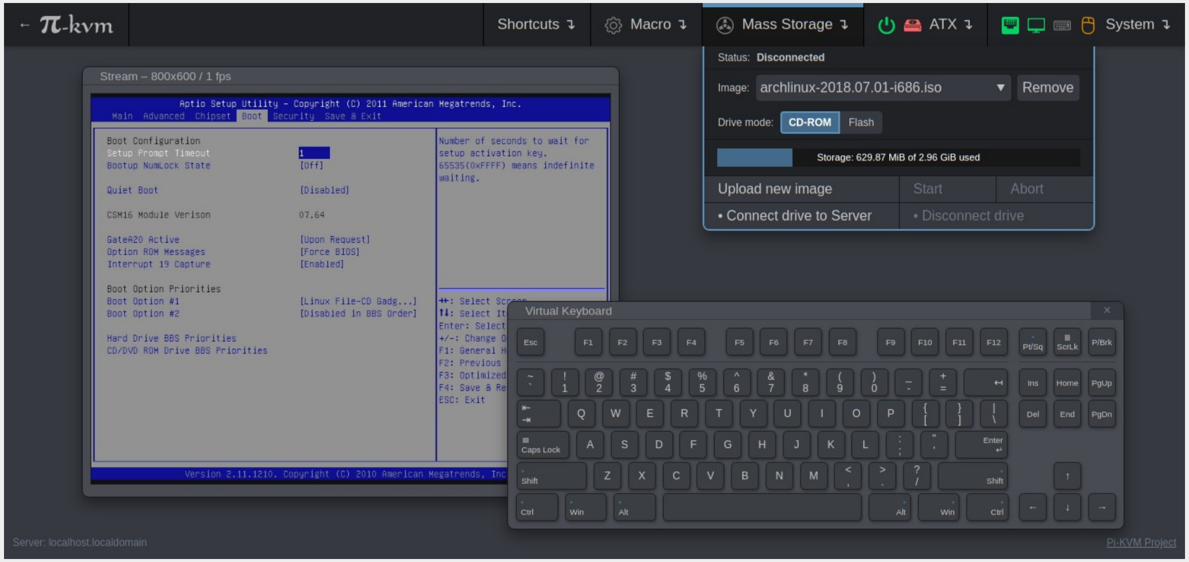
Machine could accessible through remote access management console:

- Virtual VNC console accessible through encrypted reverse SSH tunel.
- PiKVM accessible through VPN.



```
root@linuxbox:~
root@linuxbox:~$
```

```
$ 

ssh -v -i
~/.ssh/cryptopia -L
5906:127.0.0.1:5906
vnc@provider.org
```



```
          Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
   Main  Advanced  Chipset  Boot  Security  Save & Exit

   Boot Configuration                                 Number of seconds to wait for
   Setup Prompt Timeout          1                    setup activation key.
   Bootup NumLock State          [Off]                65535(0xFFFF) means indefinite
                                                      waiting.
   Quiet Boot                    [Disabled]

   CSM16 Module Verison          07.64

   GateA20 Active                [Upon Request]
   Option ROM Messages           [Force BIOS]
   Interrupt 19 Capture          [Enabled]

   Boot Option Priorities                             ++: Select Screen
   Boot Option #1                [Linux File-CD Gadg...]  ↑↓: Select It
   Boot Option #2                [Disabled in BBS Order]  Enter: Select
                                                      +/-: Change O
   Hard Drive BBS Priorities                          F1: General H
   CD/DVD ROM Drive BBS Priorities                    F2: Previous
                                                      F3: Optimized
                                                      F4: Save & Re
                                                      ESC: Exit

          Version 2.11.1210. Copyright (C) 2010 American Megatrends, Inc
```

Status: **Disconnected**

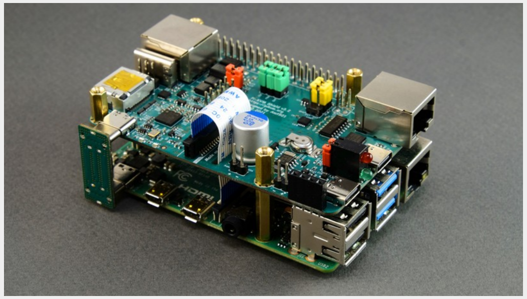
Image: archlinux-2018.07.01-i686.iso ▼ Remove

Drive mode: **CD-ROM** Flash

Storage: 629.87 MiB of 2.96 GiB used

Upload new image | Start | Abort

• Connect drive to Server | • Disconnect drive



Zero trust policy for access

Machine should have access controls enabled. Zero trust policy for any access should be implemented.

Access allowed from a trusted IP addresses only, additional mechanisms to limit brute force authentication attempts (from trusted IP addresses!) are also desirable.

VPN server

There are several VPN servers available. General advice:

- Regarding cryptography, open source software is usually better choice (open source software is more transparent, security through obscurity principle does not work).
- Software should have been independently security reviewed (being open source does not ensure security review).

VPN server

General advice:

- Security settings and cryptographic configuration should be hardened (ensure the use of secure cryptographic protocols and algorithms (TLS 1.3, 4096 Diffie-Hellman parameters, long prime numbers, TLS and HMAC authentication, additional checks for cryptographic keys, etc.).
- Cryptographic keys should be off-site generated.
- Prevent DNS leaking (and use DNS over HTTP/TLS).
- What security measures should be implemented inside VPN network (routing, access control,...)?

Endpoint device security

VPN user’s endpoint device cannot be easily trusted.

General advice:

- Be aware that cryptographic material on end-user's devices is hard to protect and could be stolen/abused.
- Consider implementing multi-factor authentication.
- Authentication through identity provider has positive and negative aspects.
- Deauthorize users (i.e. employees,...) who are not authorized for VPN use any more.

Network traffic obfuscation

Traffic obfuscation

Traffic obfuscation means hiding the type of network traffic which is exchanged between two endpoints.

Traffic obfuscation helps information hiding in communication networks – it hides the type of the network traffic (network protocol) exchanged between network entities.

Traffic obfuscation can prevent detection of VPN use and VPN blocking.

Port sharing

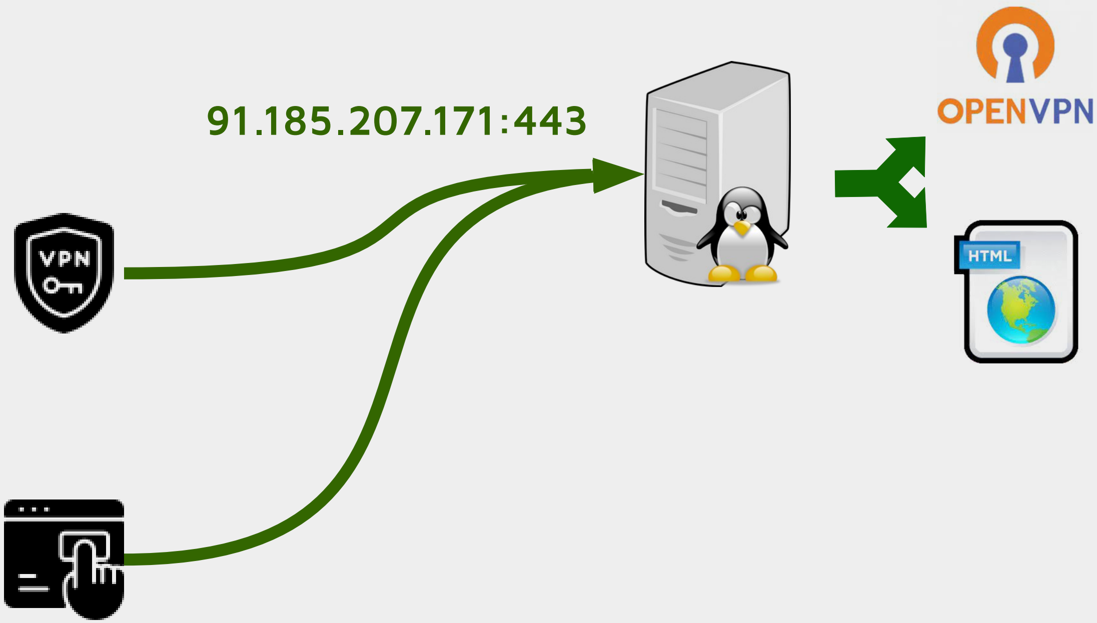
TCP tunnel is a technology that aggregates and transfers packets sent between end hosts as a single TCP connection.

Port sharing technique allows multiple listeners to listen on the same combination of port and IP address.

Firewalls are generally configured to block TCP traffic on all ports except for a few well-known entry points.

However, this technique is not effective if deep packet inspection is being used.

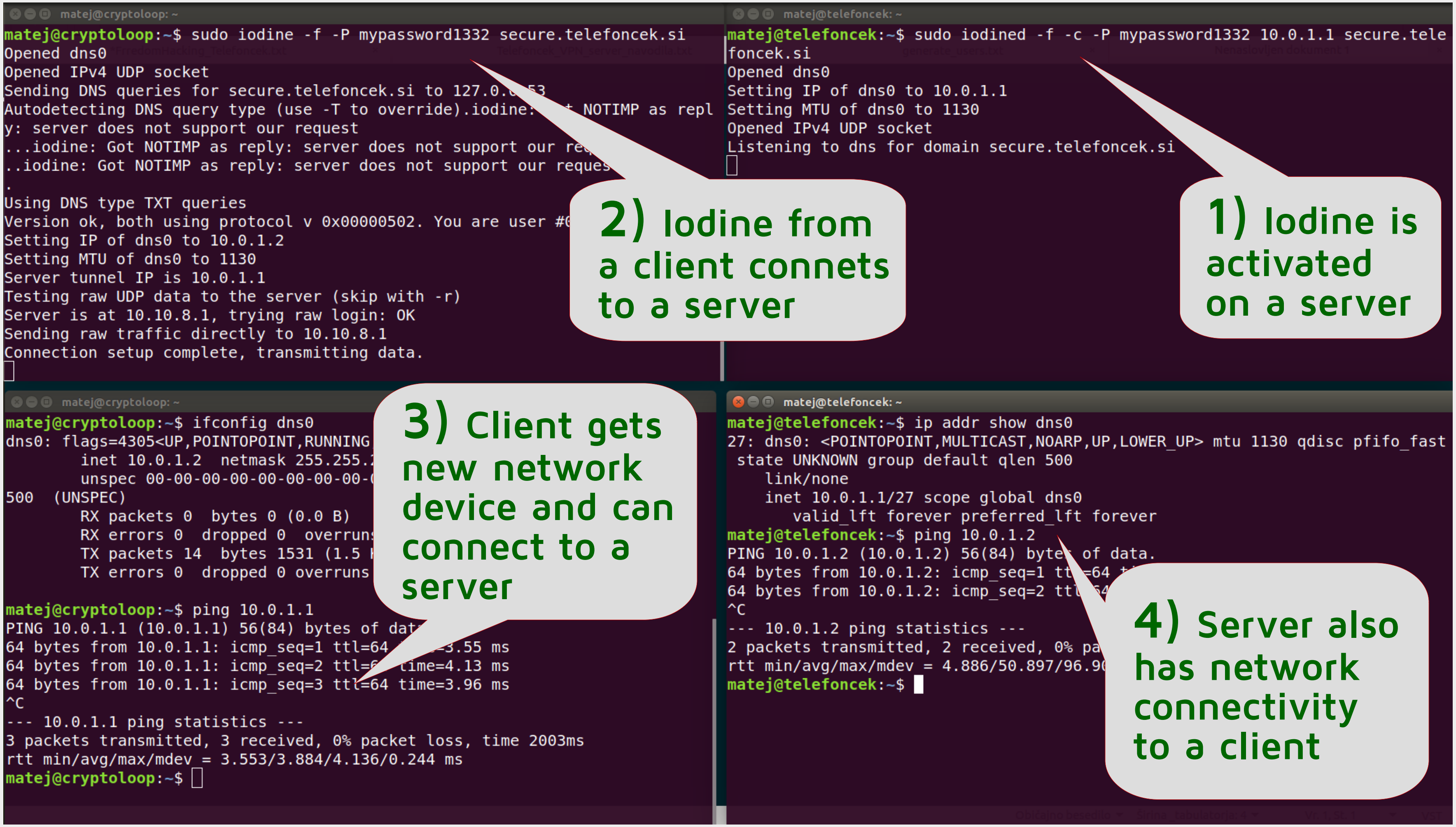
Port sharing



VPN connection (from VPN client) and HTTPS connection (from browser) are established to the same IP and the same port.

When run in TCP server mode, OpenVPN can share port with another application, such as an HTTPS server. If OpenVPN senses a connection to its port which is using a non-OpenVPN protocol, it will proxy the connection to the server at HTTPS server.

TCP over DNS (Iodine)



```
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.  53
Autodetecting DNS query type (use -T to override).iodine:   t NOTIMP as repl
y: server does not support our request
...iodine: Got NOTIMP as reply: server does not support our re
..iodine: Got NOTIMP as reply: server does not support our reques
.
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@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@cryptoloop:~$ ifconfig dns0
dns0: flags=4305<UP,POINTOPOINT,RUNNING
        inet 10.0.1.2  netmask 255.255.2
        unspec 00-00-00-00-00-00-00-00-0
500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns
        TX packets 14  bytes 1531 (1.5 K
        TX errors 0  dropped 0 overruns

matej@cryptoloop:~$ ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of dat
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64    =3.55 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=6  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:~$ 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) byte  of data.
64 bytes from 10.0.1.2: icmp_seq=1 tt =64 t
64 bytes from 10.0.1.2: icmp_seq=2 ttl 64
^C
--- 10.0.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% pa
rtt min/avg/max/mdev = 4.886/50.897/96.90
matej@telefoncek:~$
```

1) Iodine is activated on a server

2) Iodine from a client connets to a server

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

4) Server also has network connectivity to a client

TCP traffic is obfuscated as DNS traffic with special software (Iodine). First connection with Iodine is established, then we tunnel OpenVPN connection inside it.

VPN over websocket

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";
}
```

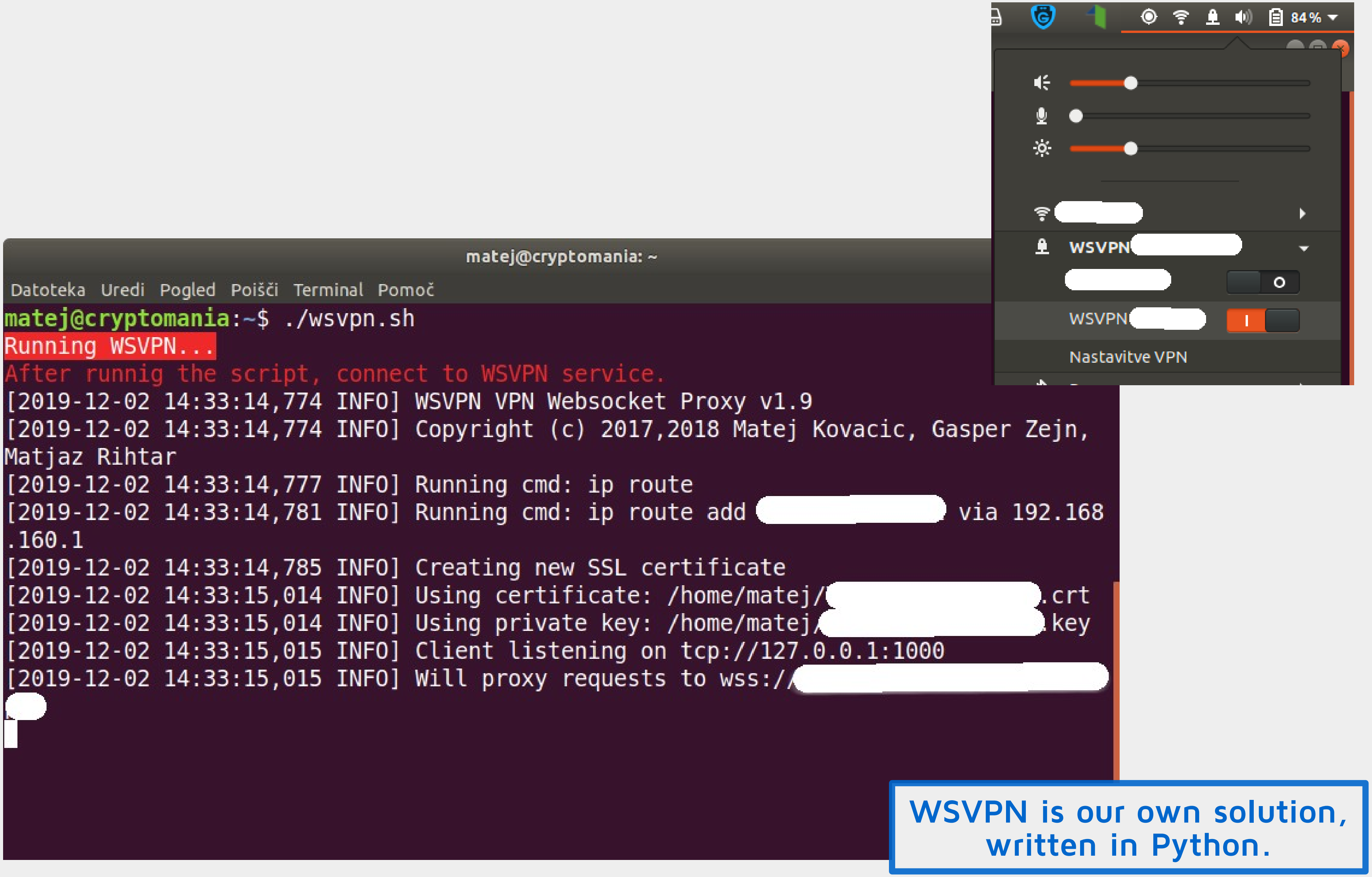
WSVPN (Websocket VPN)

```
screen python wsvpn-1.g.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.g.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.g
[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
```

WSVPN is our own solution, written in Python. Some commercial providers are now offering similar solutions, that wrap OpenVPN in a WebSocket

WSVPN (Websocket VPN)



```
matej@cryptomania:~$ ./wsvpn.sh
Running WSVPN...
After runnig 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]
[redacted]
```

WSVPN is our own solution, written in Python.

WSVPN device

Traffic obfuscation generally needs special software to be installed on a client.

We have developed a hardware device based on small ARM board, which acts as a WiFi access point.

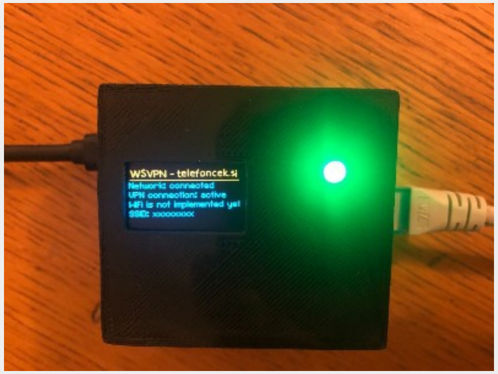
When device is connected to the network, it automatically connects itself to VPN server through obfuscated connection. This is indicated by the small green diode on the top of the device.

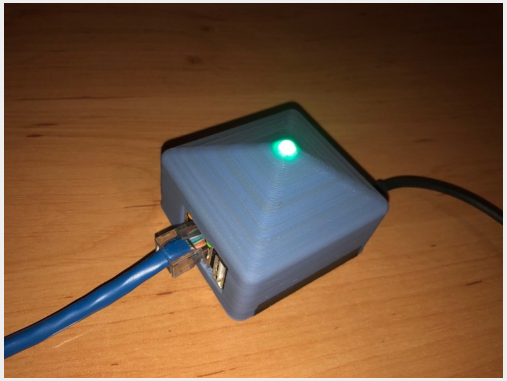
User then connects to WSVPN device via WiFi, and all user’s network traffic is then automatically routed to VPN server.

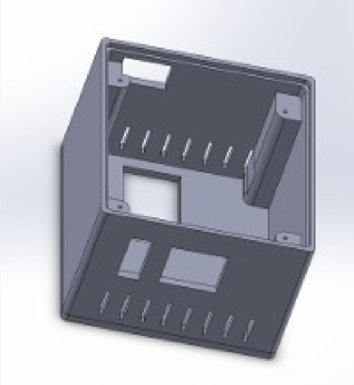
Therefore, no additional software is needed.

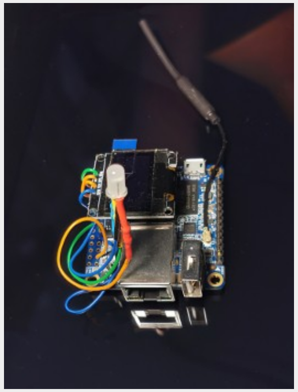
WSVPN device

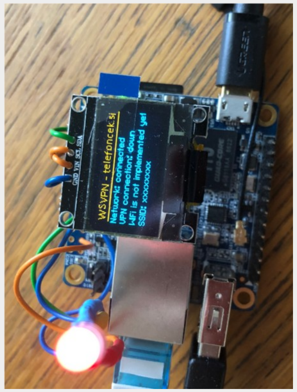
We have developed and tested several ARM based devices (OrangePi, RaspberryPi,...) with additional hardware (LED diode, OLED display).

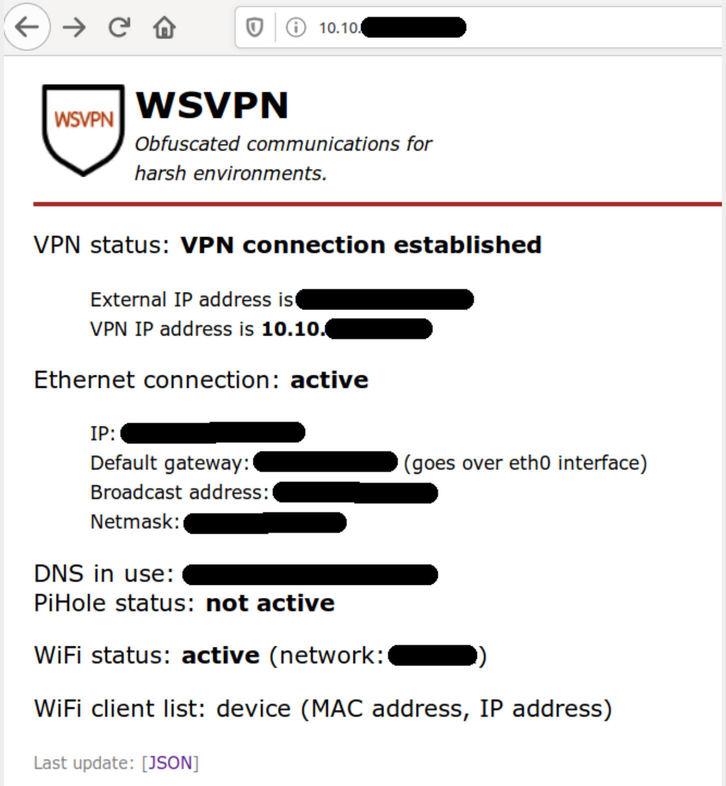












WSVPN

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]

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 is some political event, connection to VPN server can not be possible at all (even HTTP connection to the “tainted” server was not working).

After:

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

WSVPN – testing in Uzbekistan and Moscow

Before:

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

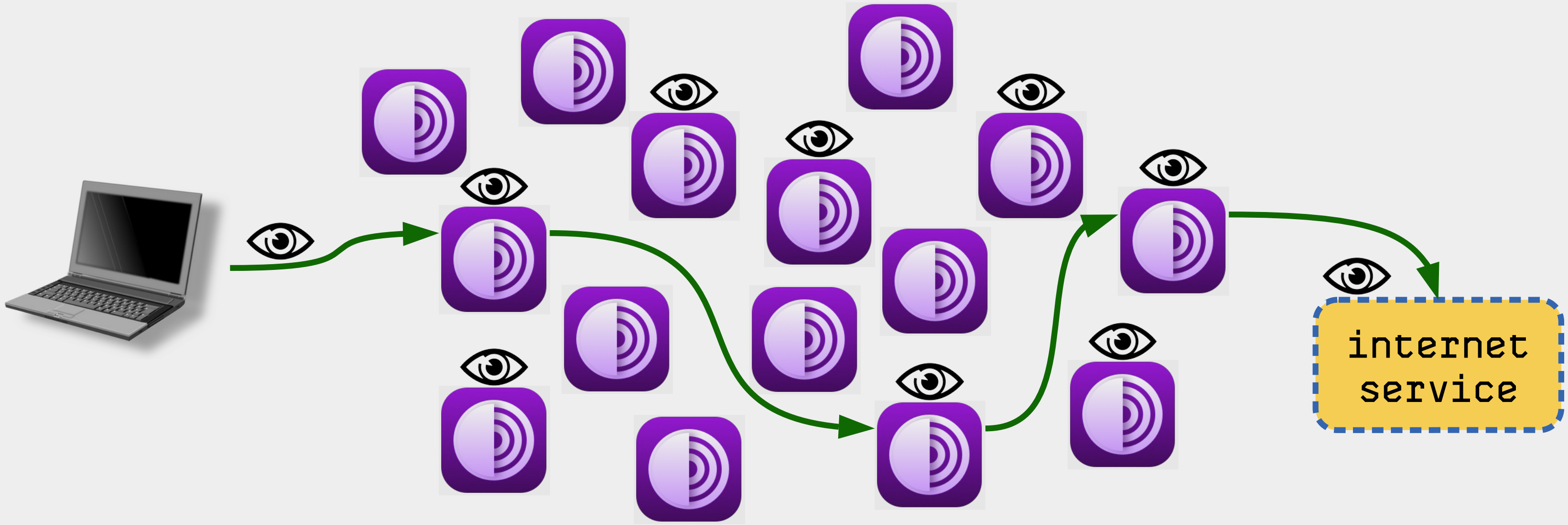
After

- VPN connection is 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).

Netflow data analysis

Netflow data reveals traffic flow and volume across the network. It can show which server is communicating with another.

This data can be used for tracking traffic through VPNs or Tor network.



More info: Dr. Neal Krawetz. Tor 0day: Finding IP Addresses. Tuesday, September 15th, 2020. https://www.hackerfactor.com/blog/index.php?/archives/896-Tor-0day-Finding-IP-Addresses.html

Netflow data analysis

Tor's network security is based on a shell game. With enough users and enough path shuffling, this theoretical God's eye view should be able to see lots of people using the Tor network and lots of exit traffic, but cannot associate entrance traffic with exit traffic.

...

If you are downloading small files, like typical web traffic, then you look like everyone else. But if you download something large, like a video, ISO image, or large audio file, then someone with the God's eye view can see the route as a large amount of traffic flows down one path, easily associating your network address to the exit traffic.

Dr. Neal Krawetz, Tor Oday: Finding IP Addresses.

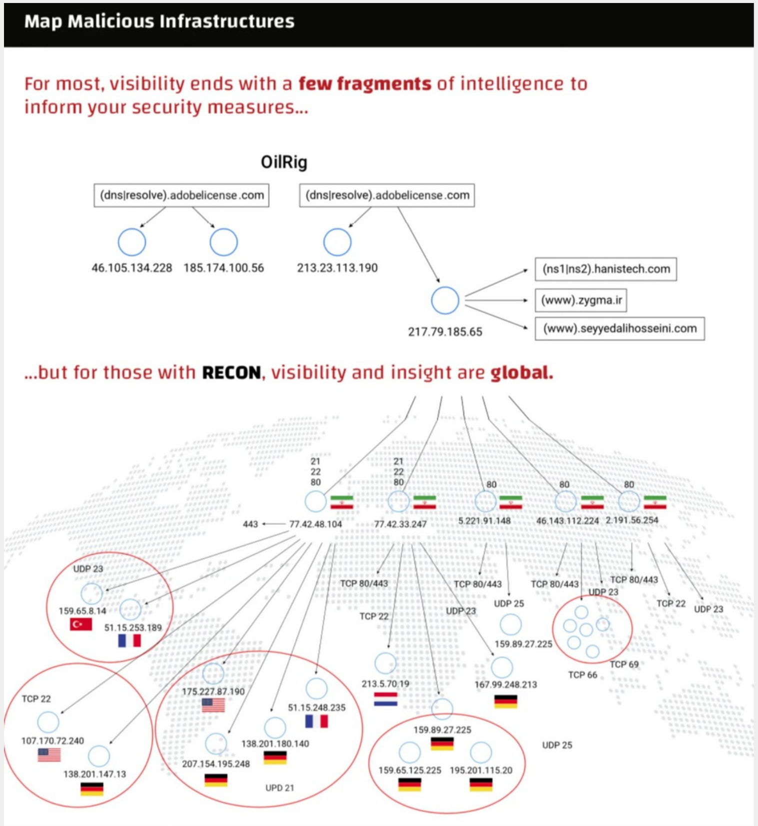
Netflow data analysis

> *For hidden services, it's even easier ... If I upload a file to your service, then the file upload must complete before the back-end file processing begins. This means, if your adversary has a God's eye view and wants to find your hidden service, then they just need to upload a large file to your hidden service. They don't even need to use your specific upload page; any web page will work and it doesn't matter if the upload fails after it completes.*
>
> Dr. Neal Krawetz, Tor Oday: Finding IP Addresses.

Netflow data analysis

Netflow data are also being offered for commercial purposes.

These data could also be combined with phone location data.



Map Malicious Infrastructures

For most, visibility ends with a **few fragments** of intelligence to inform your security measures...

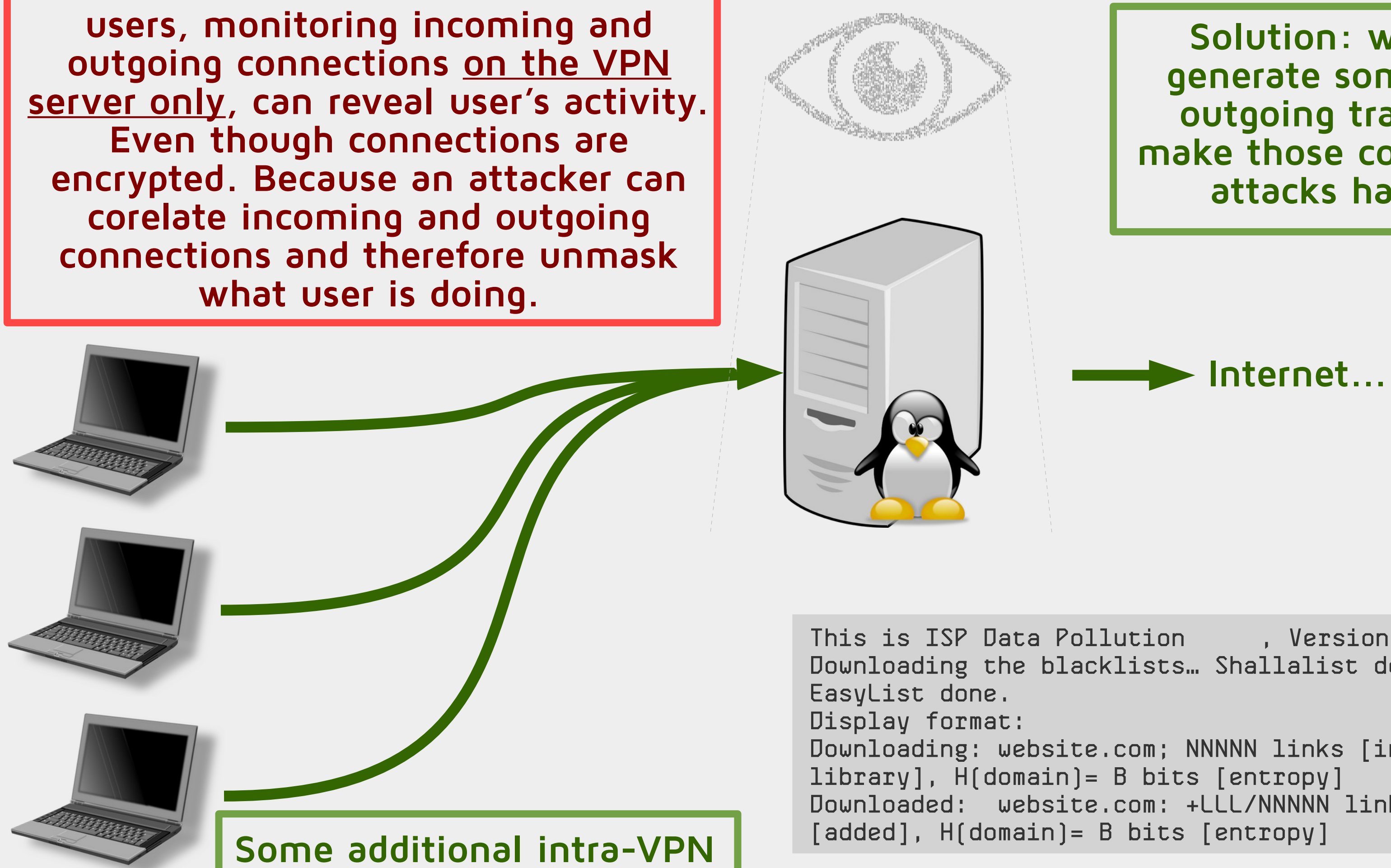
...but for those with **RECON**, visibility and insight are **global.**

A section of Team Cymru's marketing material for its Pure Signal Recon product. Image: Team Cymru.

Joseph Cox. 2021. How Data Brokers Sell Access to the Backbone of the Internet. August 24th, 2021. https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

Network polluting

If there are few concurrent VPN users, monitoring incoming and outgoing connections <u>on the VPN server only</u>, can reveal user's activity. Even though connections are encrypted. Because an attacker can corelate incoming and outgoing connections and therefore unmask what user is doing.



Solution: we can generate some fake outgoing traffic to make those correlation attacks harder.

Some additional intra-VPN traffic can also be generated to make correlation attacks harder.

```
This is ISP Data Pollution      , 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]
```

P2P VPN

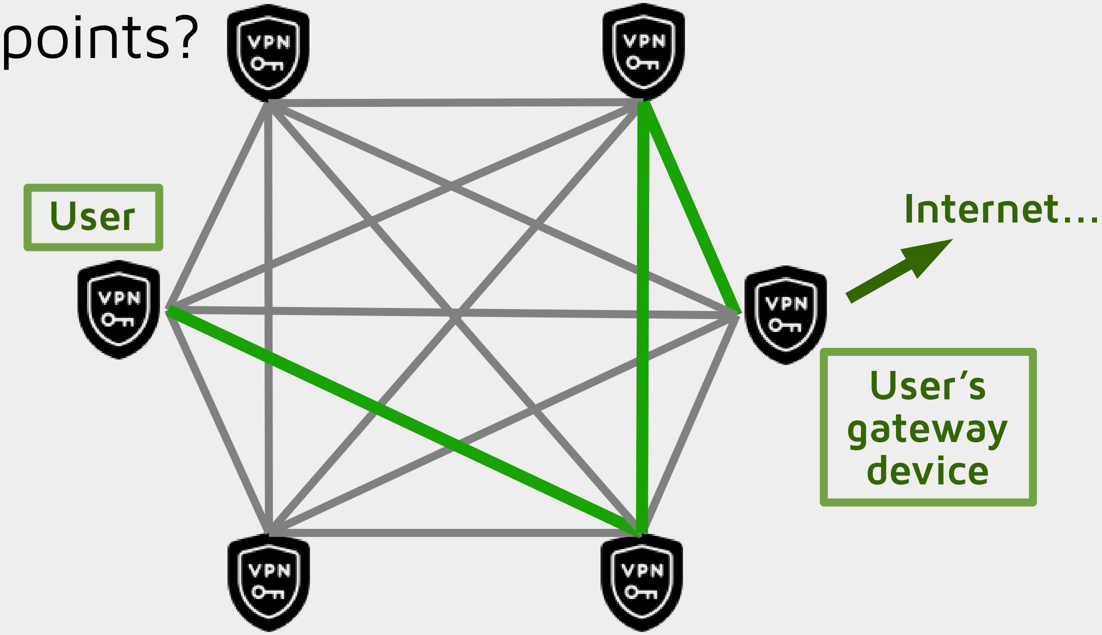
The idea comes from (WiFi) mesh networks, Tor network and Magic wormhole...

Prototype implementation: BadVPN.

Some commercial VPN providers are offering VPN exit points on US residential IP addresses in order to avoid geoblocking by Netflix...

Problem: trusting endpoints?

Client connects user into VPN network.
Clients relay network traffic to other clients.
Client connects to user's gateway, where user is authenticated and gets the access to internet (or private network behind gateway)



Questions?

Matej Kovačič

Jožef Stefan Institute
Ljubljana, Slovenia

United Nations
Educational, Scientific and
Cultural Organization

IRCAI
International Research Centre
on Artificial Intelligence
under the auspices of UNESCO

Personal blog:
https://telefoncek.si