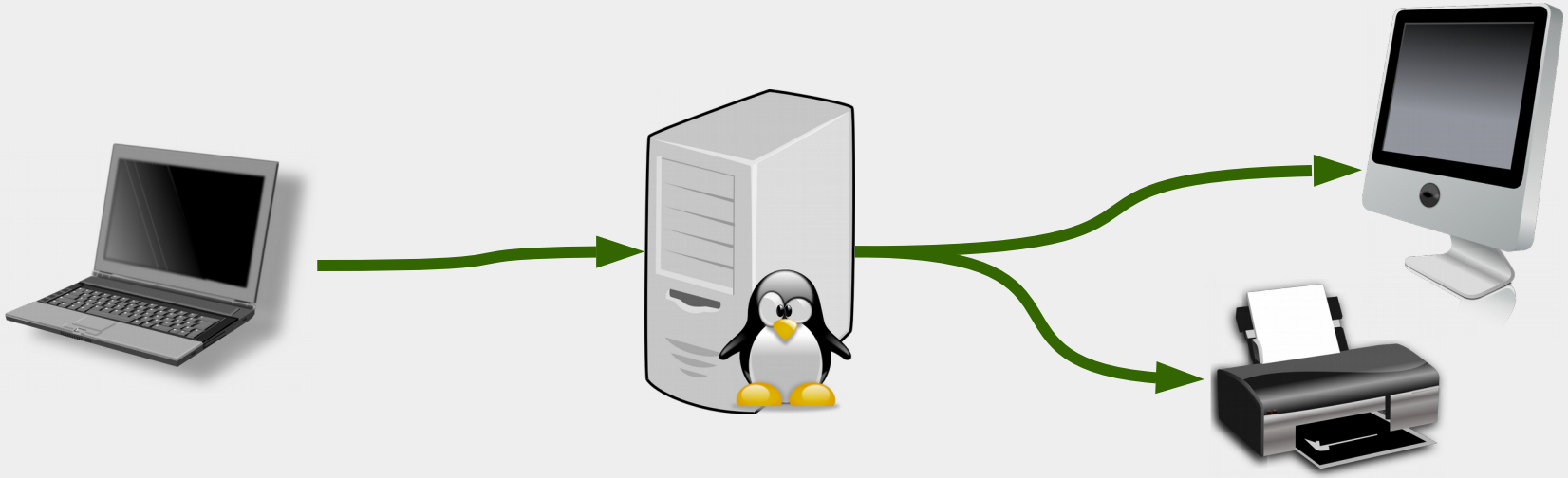
VPN Freedom Hacking

Matej Kovačič
matej.kovacic@telefoncek.si

Kaj?

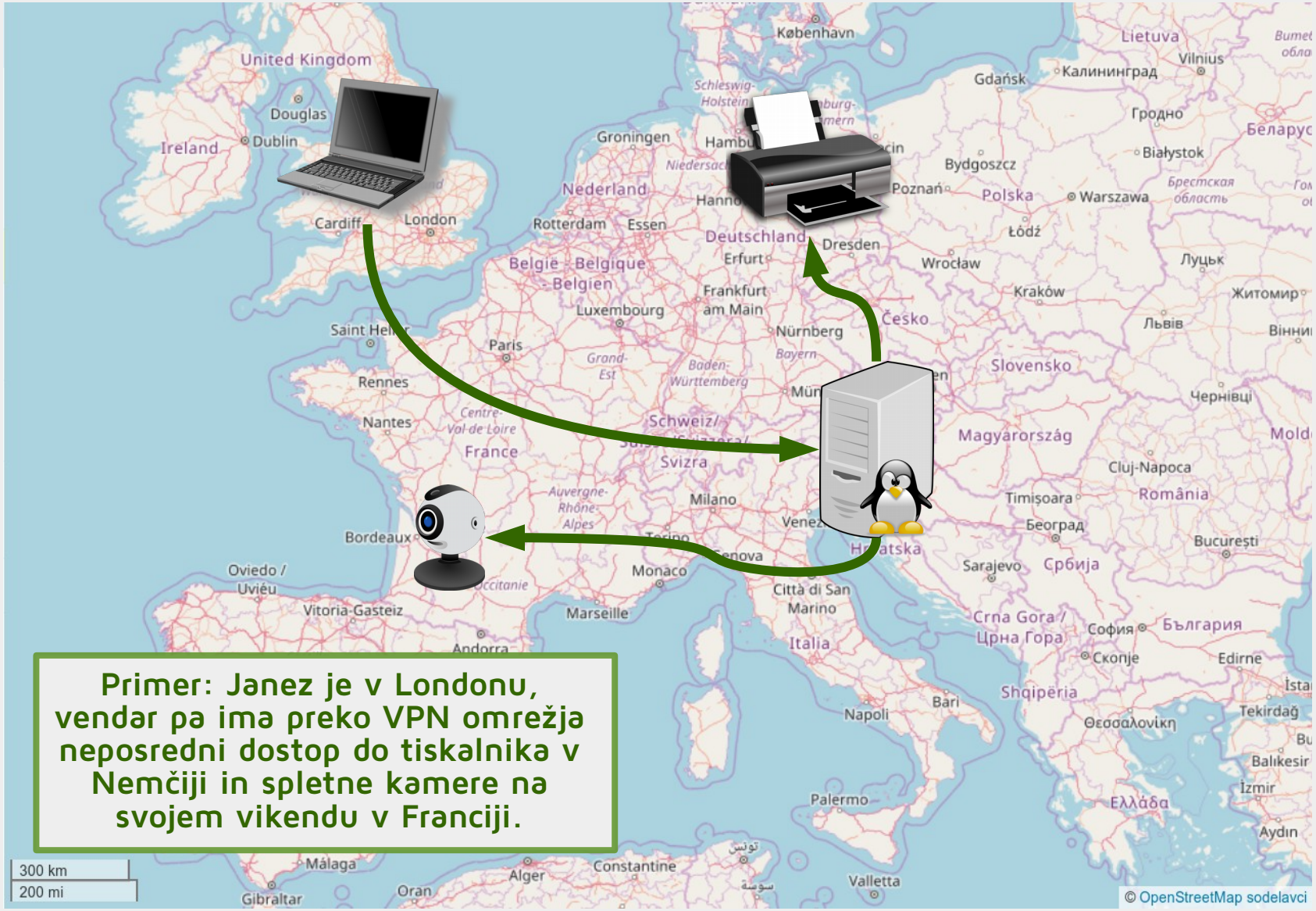
Kaj je VPN

VPN ali *virtual private network* je način povezave računalnika ali omrežja z oddaljenim računalnikom ali omrežjem preko (šifriranega) tunela.



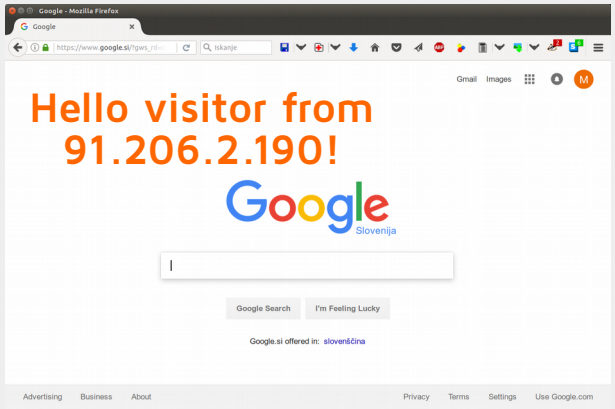
Skozi varni tunel ima uporabnik povezavo do oddaljenega omrežja, oddaljenih računalnikov ali drugih oddaljenih naprav, ne glede na njihovo fizično lokacijo.

Dostop do oddaljenih omrežij ali naprav

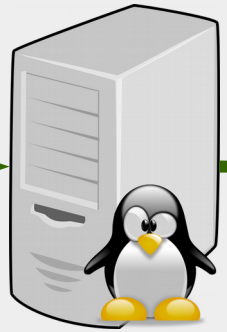


VPN omogoča »skrivanje« IP naslova

Če uporabnik VPN uporablja kot prehod za dostop do interneta, obiskana spletna stran ne vidi njegovega pravega IP naslova, pač pa IP naslov VPN strežnika.



Pravi IP naslov:
216.58.214.205

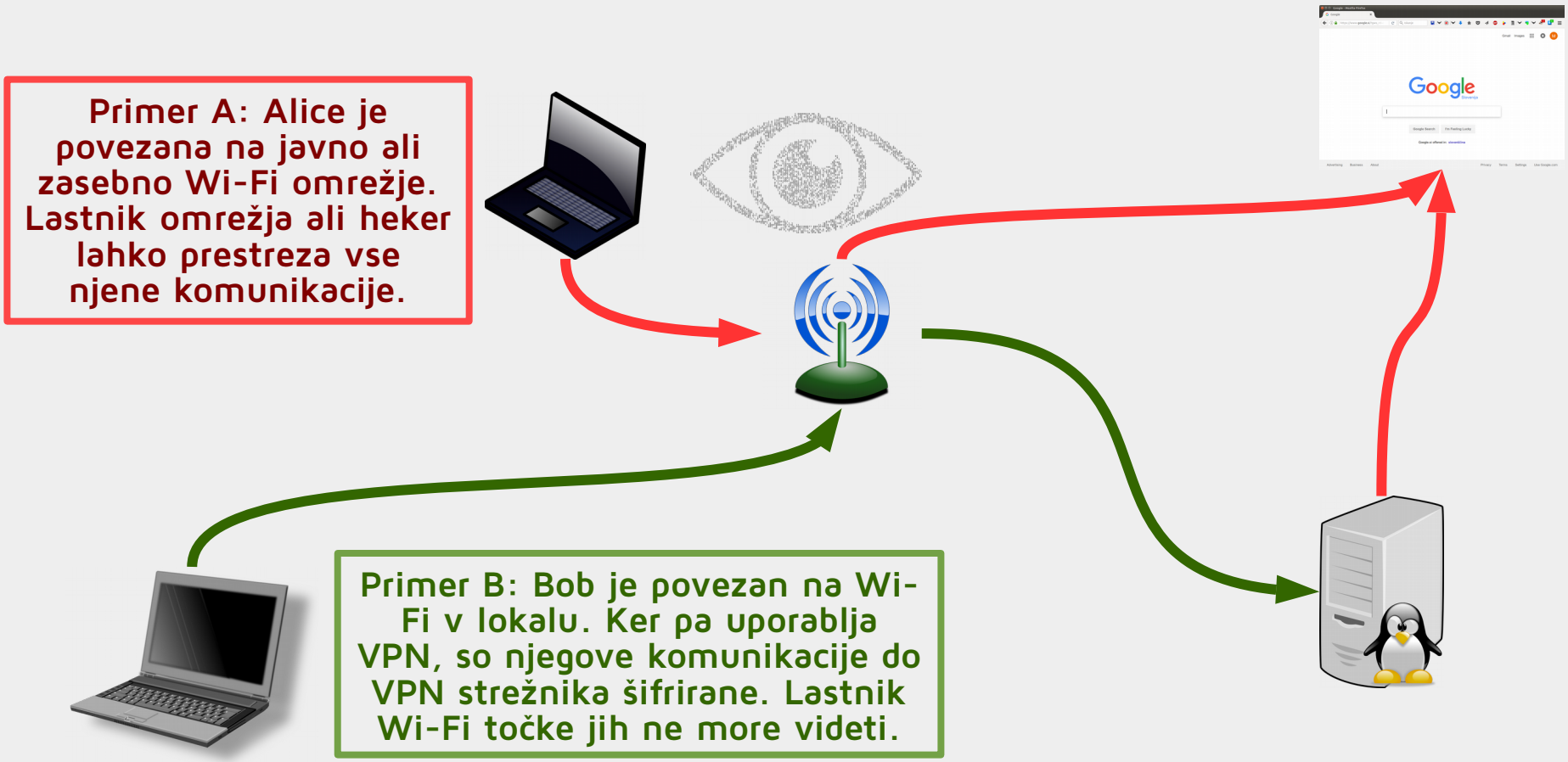


IP VPN-ja:
91.206.2.190

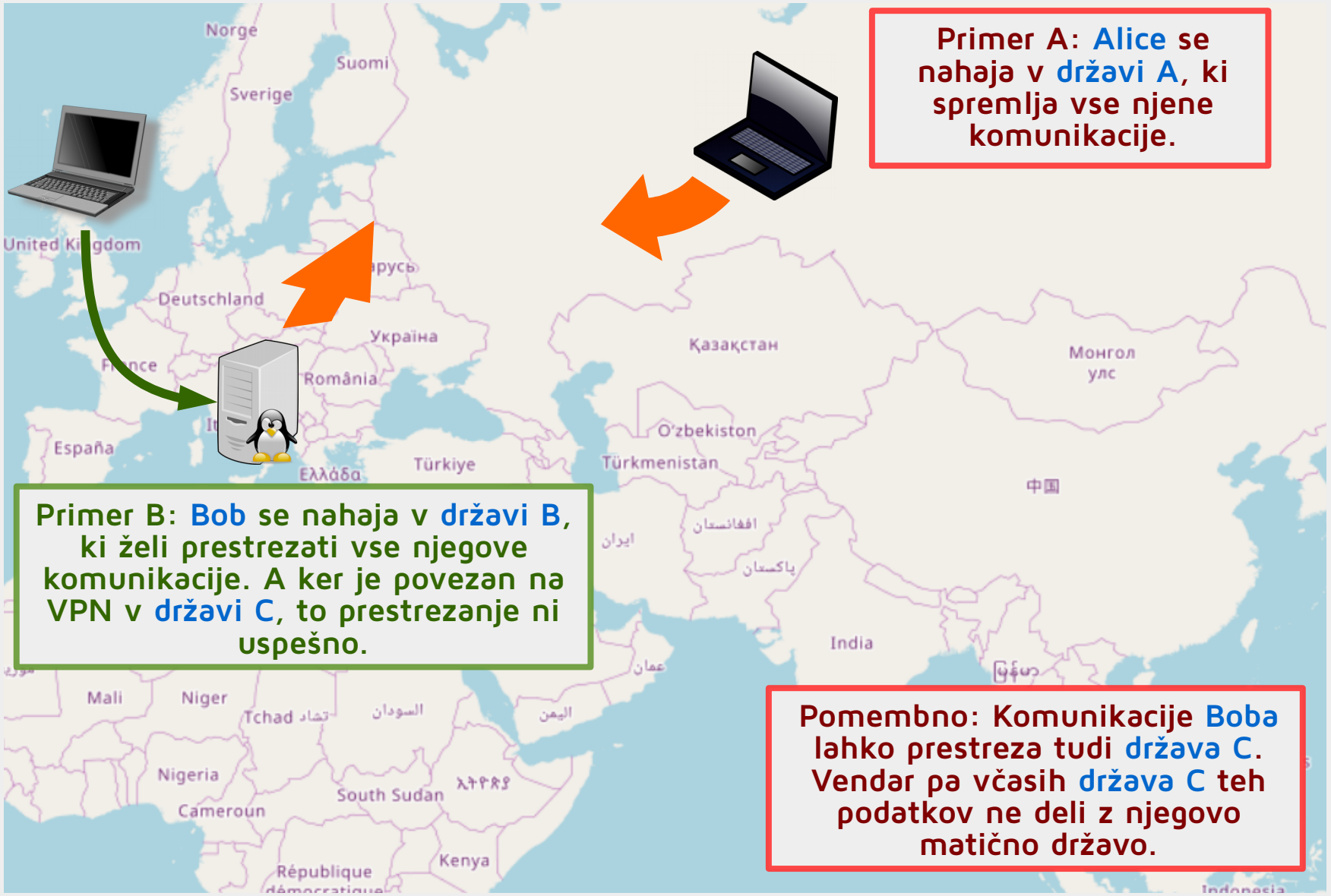
Pomembno: spletna stran lahko uporabnika identificira ne samo na podlagi IP naslova, pač pa tudi s spletnimi piškotki in drugimi mehanizmi.

Zaščita pred prestrezanjem

Ker VPN ustvari varni tunel med dvema napravama, ga je mogoče uporabiti za zaščito pred prestrezanjem, poseganjem v promet in cenzuro.



Zaščita pred državnim prestrezanjem



Primer A: Alice se nahaja v državi A, ki spremlja vse njene komunikacije.

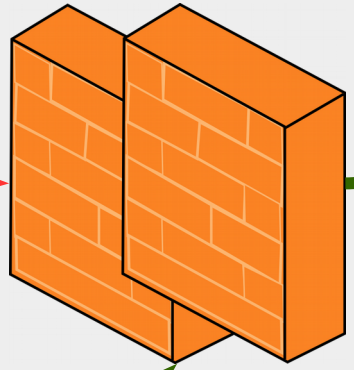
Primer B: Bob se nahaja v državi B, ki želi prestrezati vse njegove komunikacije. A ker je povezan na VPN v državi C, to prestrezanje ni uspešno.

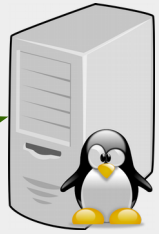
Pomembno: Komunikacije Boba lahko prestreza tudi država C. Vendar pa včasih država C teh podatkov ne deli z njegovo matično državo.

Zaščita pred blokadami

Primer A: Alice se nahaja za požarnim zidom, ki ji omejuje dostop do določenih spletnih strani ali storitev interneta.

Med uporabnikom in VPN strežnikom je vzpostavljen varen tunel.

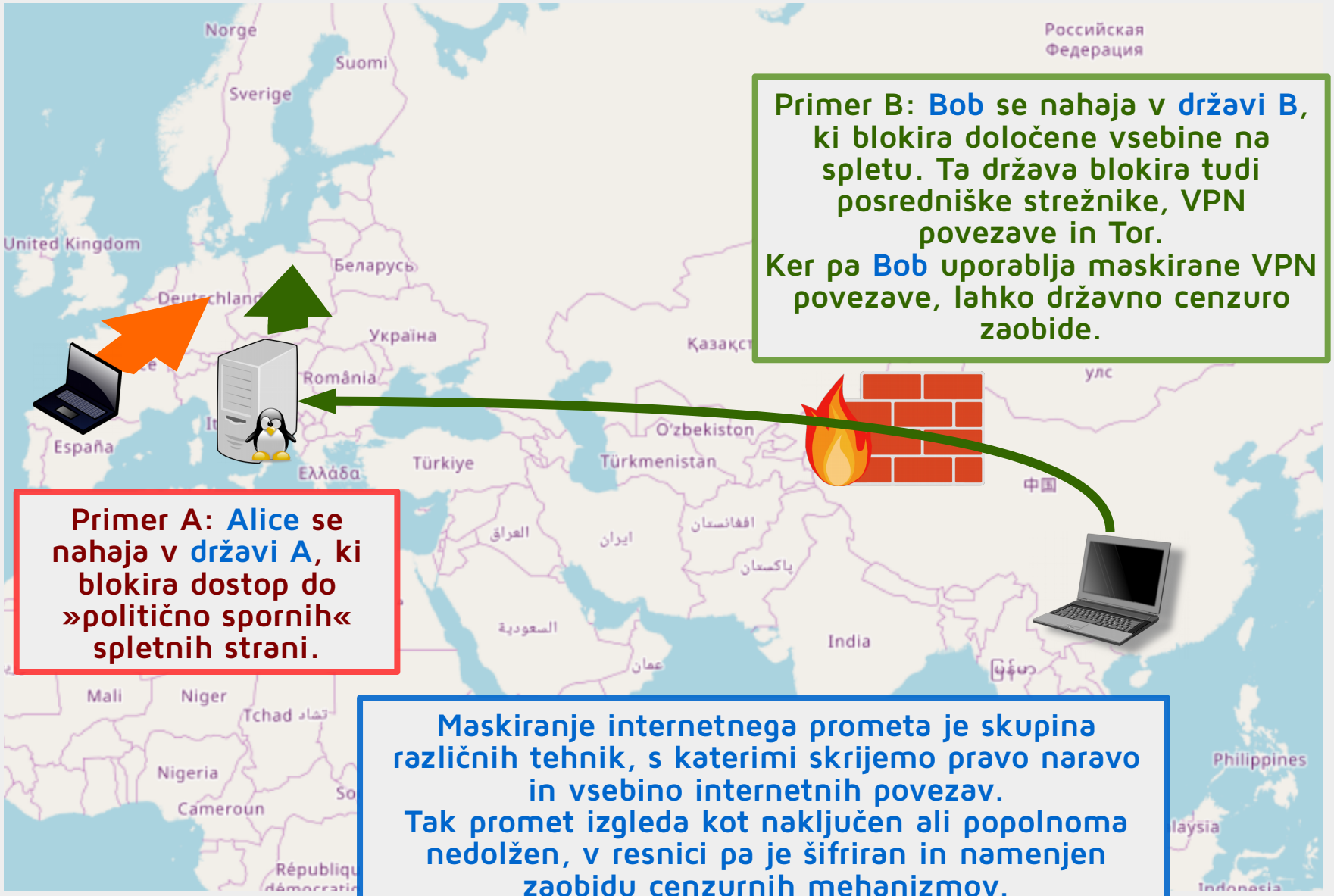




Uporabnik ima neoviran dostop do interneta.

Primer B: Tudi Bob se nahaja za požarnim zidom. A ker uporablja VPN, lahko njegove komunikacije »prebijejo« požarni zid, zato ima neoviran dostop do interneta.

Zaščita pred državno cenzuro

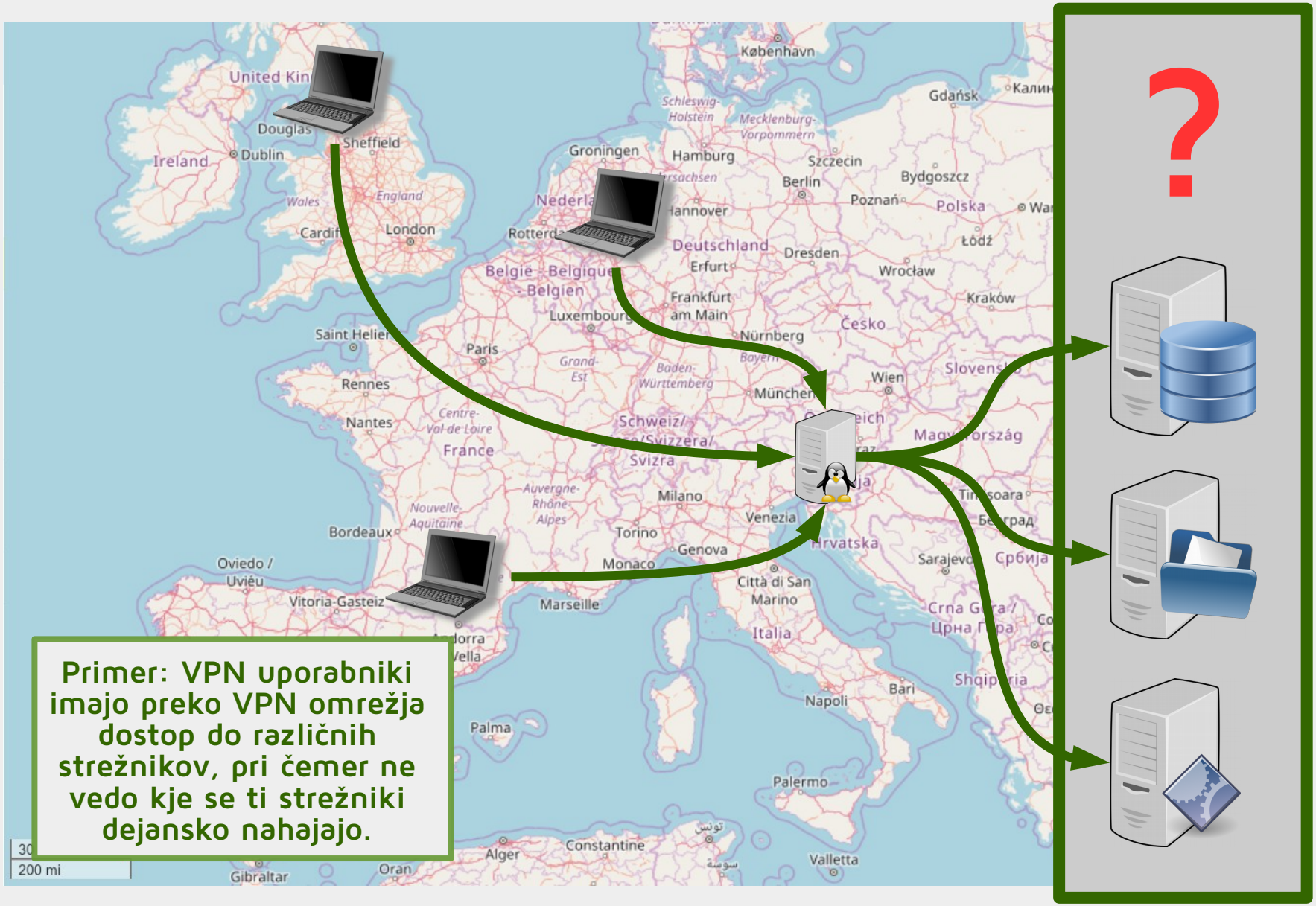


Primer A: Alice se nahaja v državi A, ki blokira dostop do »politično spornih« spletnih strani.

Primer B: Bob se nahaja v državi B, ki blokira določene vsebine na spletu. Ta država blokira tudi posredniške strežnike, VPN povezave in Tor.
Ker pa Bob uporablja maskirane VPN povezave, lahko državno cenzuro zaobide.

Maskiranje internetnega prometa je skupina različnih tehnik, s katerimi skrijemo pravo naravo in vsebino internetnih povezav.
Tak promet izgleda kot naključen ali popolnoma nedolžen, v resnici pa je šifriran in namenjen zaobidu cenzurnih mehanizmov.

Skrite storitve



Primer skrite storitve: skriti NAS strežnik

Primer: Janez je novinar in je pridobil pomembne dokumente, ki razkrivajo korupcijo v vladi. Njegov računalnik samodejno izdeluje varnostne kopije dokumentov na NAS strežnik, ki se nahaja nekje v VPN omrežju. Če skorumpirana država Janezov računalnik zaseže, kopija dokumentov ostane na NAS strežniku.

NAS strežnik ima šifrirane diske. Če napadalec strežnik zaseže, ne more pridobiti podatkov.
VPN uporabnik svoje podatke **dodatno** šifrira s **svojim lastnim šifrirnim ključem**. Zato do podatkov ne more **niti** skrbnik NAS sistema.

V omrežju se morda nahaja še en skriti NAS strežnik, kamor se podatki inkrementalno kopirajo za primer, da pride do težav pri prvem NAS-u...

NAS (Network-attached storage) je strežnik namenjen hrambi podatkov in varnostnih kopij odjemalcev preko omrežja.

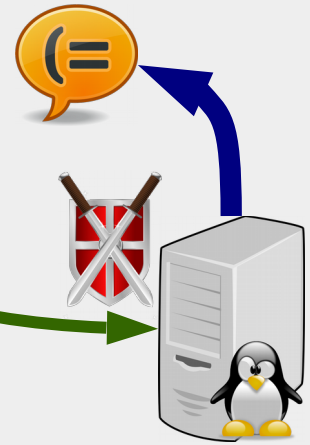
Primer skrite storitve: Intrusion Detection

Primer: novinarka Alice je tarča državnih trojancev. Njen računalnik je tarča NSA-jevega Quantum Insert napada (gre za različico MITM napada).

VPN strežnik s privoljenjem Alice analizira ves njen VPN promet. IDS (Intrusion Detection System) zazna vzorec Quantum Insert napada in Alice o tem obvesti preko aplikacije Signal.

Alice si lahko ogleda tudi »netflow« analizo svojih omrežnih povezav.

Alice je po Signalu obveščena tudi vedno, ko se katera od njenih naprav poveže v VPN omrežje in ko se VPN povezava prekine.
S tem olajšamo zaznavo nepooblaščene uporabe VPN storitve z njenimi ključi ali jo opozorimo na izpad povezave.



(internet)

Intrusion Detection System (IDS) je sistem za zaznavanje vdorov, ki zaznava nepooblaščene aktivnosti v informacijskem sistemu ali sumljive vzorce omrežnega prometa.

Kako?

Strežnik

Strežnik(i) tečejo v virtualnem stroju. Gostiteljskega sistema ne upravljamo sami, a je redno vzdrževan.

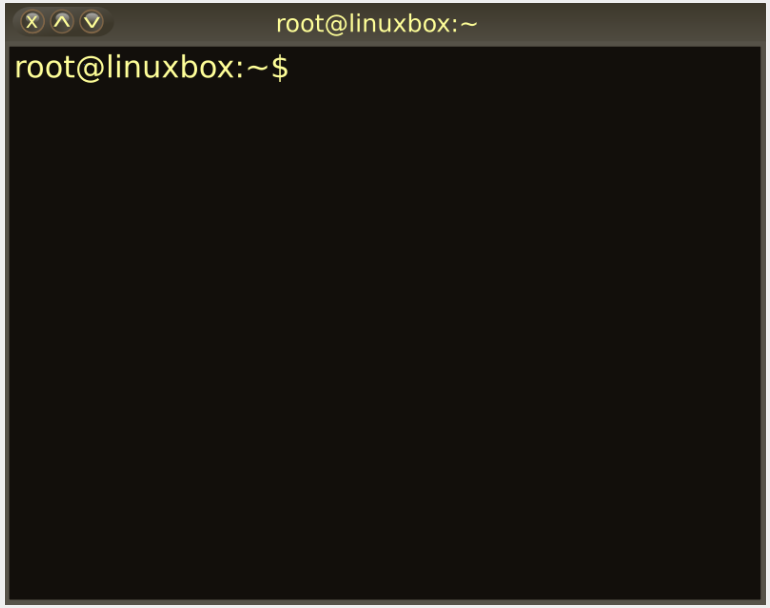
Strežnik teče pod posodobljenim Debian Stretch operacijskim sistemom.

Zakaj Debian?

> »*Debian takes security very seriously. We handle all security problems brought to our attention and ensure that they are corrected within a reasonable timeframe.*«

Oddaljena konzola

Strežnik je dostopen preko virtualne VNC konzole, ki je dostopna preko šifriranega reverznega SSH tunela.



Šifrirani diski

Vsi diski so šifrirani z LUKS. Ko se strežnik ponovno zažene, se mora skrbnik nanj naajprej povezati preko virtualne konsole in vnesti geslo za odklep diskov.

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

Šele nato se strežnik sploh zažene.

Če je strežnik kompromitiran, do podatkov na disku ni mogoče priti brez gesla.

Ojačan SSH in požarni zid

Strežnik uporablja tim. ojačane SSH nastavitve. Požarni zid dovoljuje SSH dostope le iz izbranih IP naslovov.

Tudi pri teh naslovih uporabljamo dodatne mehanizme za omejevanje napadov z grobo silo.

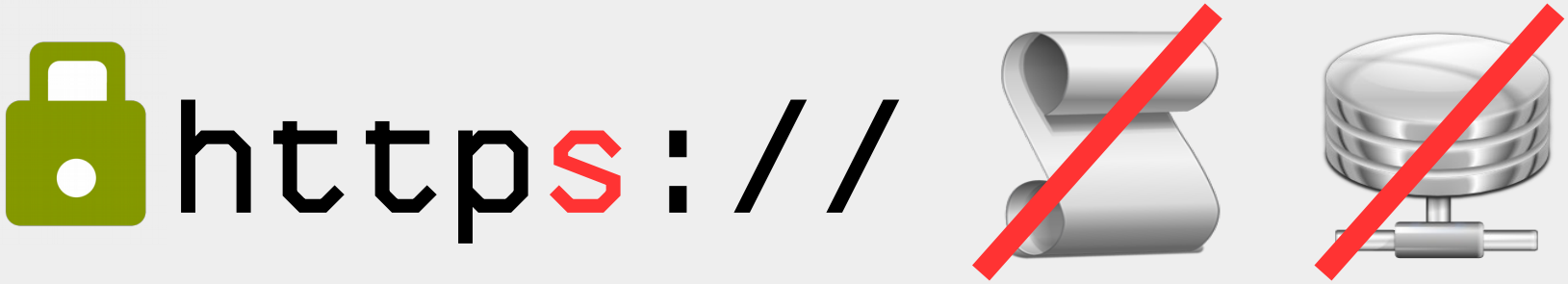
```
HostKey /etc/ssh/ssh_host_ed25519_key
PermitRootLogin no
StrictModes yes
PermitEmptyPasswords no
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,
aes128-gcm@openssh.com,aes256-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.
com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-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

Spletna stran

Na strežniku teče spletna stran z veliko količino legitimne vsebine.

Vsebina je statična, kar pomeni, da ni omogočeno izvajanje strežniških skript, niti na strežniku ne teče baza podatkov. To dodatno zmanjšuje možnosti za uspešen napad.

Vsa spletna vsebina je strežena izključno preko kvalitetnih HTTPS povezav.



OpenVPN

Na strežniku teče OpenVPN strežnik. Med drugim ima implementirano:

- varne kriptografske protokole in algoritme (TLS 1.2+, 4096 Diffie-Hellman parametri, dolga praštevila, TLS overjanje, HMAC overjanje, dodatne kontrole kriptografskih ključev, itd.);
- vsi kriptografski ključi so ustvarjeni na ločeni napravi (tim. *off-site*);
- odjemalci znotraj VPN omrežja se med seboj vidijo, a imajo statične IP naslove;
- uporabljamo lasten DNS strežnik za preprečevanje DNS uhajanja in zagotavljanje tim. skritih storitev.

OpenVPN – maskiranje prometa

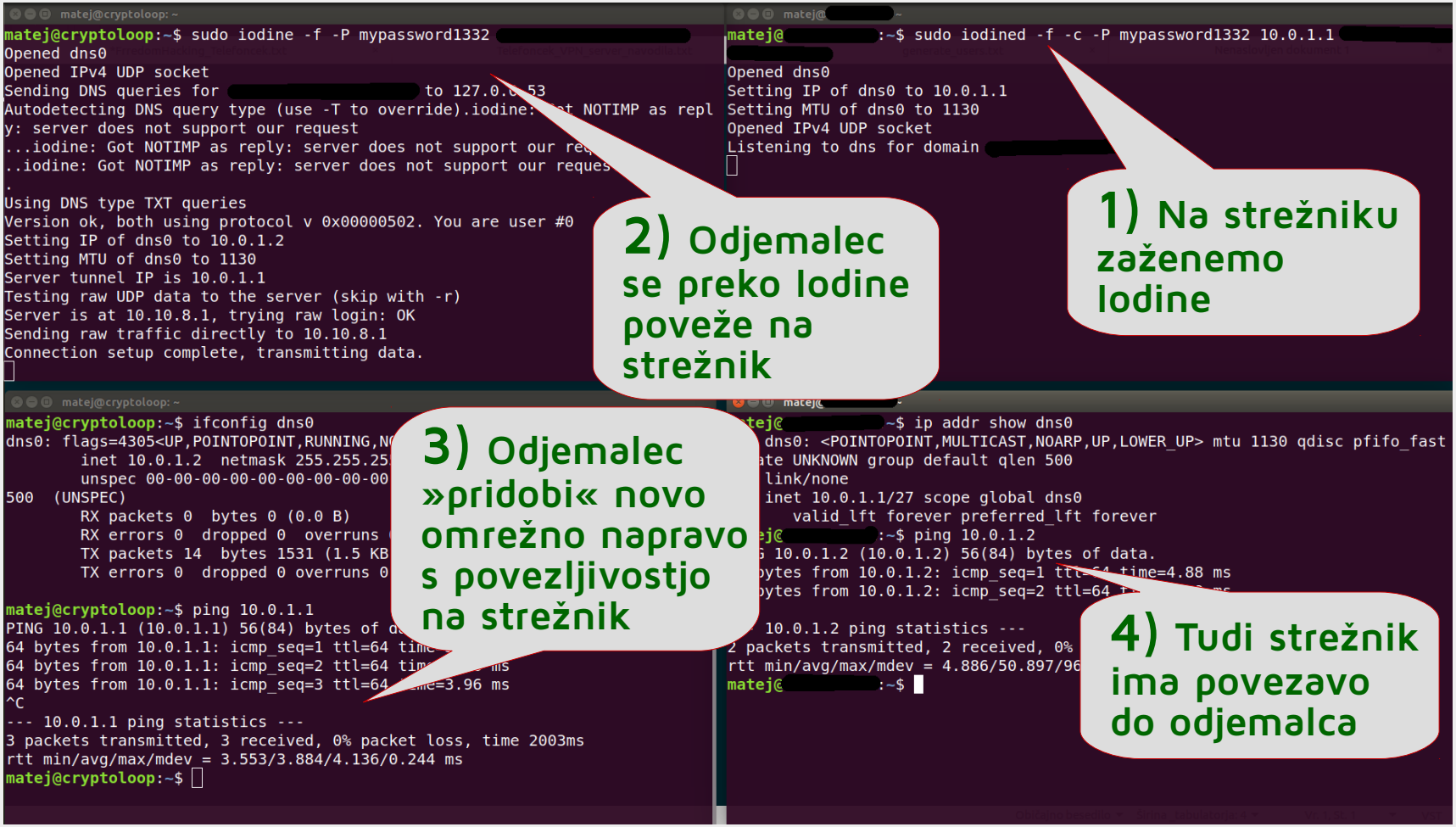
VPN strežnik skruša maskirati VPN promet:

- vse povezave so šifrirane in potekajo preko TCP protokola;
- uporabljamo tehniko "deljenja vrat" (angl. *port sharing*) – OpenVPN in HTTPS spletni strežnik sta dosegljiva na istem IP naslovu na istih TCP vratih (TCP/443).

S pomočjo te tehnike lahko prebijemo mnogo požarnih zidov. Dodatno nam pomaga dejstvo, da je na strežniku dostopna legitimna HTTPS vsebina.

Vendar pa napadalec, ki uporablja DPI tehnike, lahko zazna VPN promet. Zato smo pričeli z implementacijo dodatnih maskirnih tehnik.

Iodine (TCP preko DNS)



Na strežniku teče Iodine, ki nam omogoča vzpostavitev prikrite povezave preko DNS zahtevkov. Preko te povezave nato vzpostavimo šifriran tunel.

WebSockets

WebSocket je komunikacijski protokol, ki omogoča dvosmerne komunikacijske kanale preko ene same TCP povezave.

HTTPS šifrirane WebSocket povezave izgledajo povsem legitimne in jih je težko ločiti od spletnega prometa.

Vendar pa znotraj njih lahko prikrito teče OpenVPN promet...

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

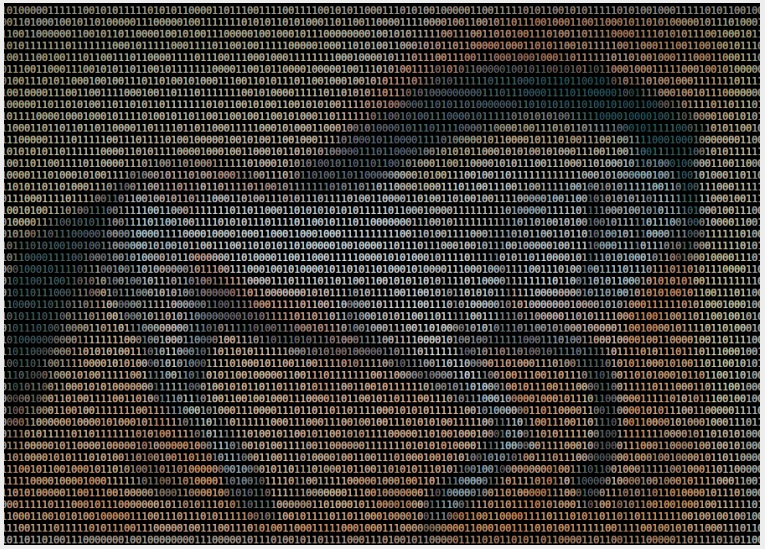
WebSockets

```
chisel server --port 8080 --auth
freedom:hacker --socks5&

2017/10/26 22:00:14 server: SOCKS5 Enabled
2017/10/26 22:00:14 server: Fingerprint
b8:ad:7e:25:61:8a:f6:e1:f6:e8:ce:56:e4:85:d3:c5
2017/10/26 22:00:14 server: User authenication enabled
2017/10/26 22:00:14 server: Listening on 8080...
```

```
chisel client  --auth freedom:hacker
http://myvpn.si:8080 socks

2017/10/26 22:01:48 client: Connecting to ws://myvpn.si:8080
2017/10/26 22:01:48 client: tunnel#1 127.0.0.1:1080=>socks:
Listening
2017/10/26 22:01:58 client: Retrying in 100ms...
2017/10/26 22:02:09 client: Retrying in 200ms...
2017/10/26 22:02:19 client: Fingerprint
b8:ad:7e:25:61:8a:f6:e1:f6:e8:ce:56:e4:85:d3:c5
2017/10/26 22:02:19 client: Connected (Latency 37.582275ms)
```

Ostale maskirne tehnike

Trenutno poteka aktivno testiranje in razvoj dodatnih maskirnih tehnik. Npr.:



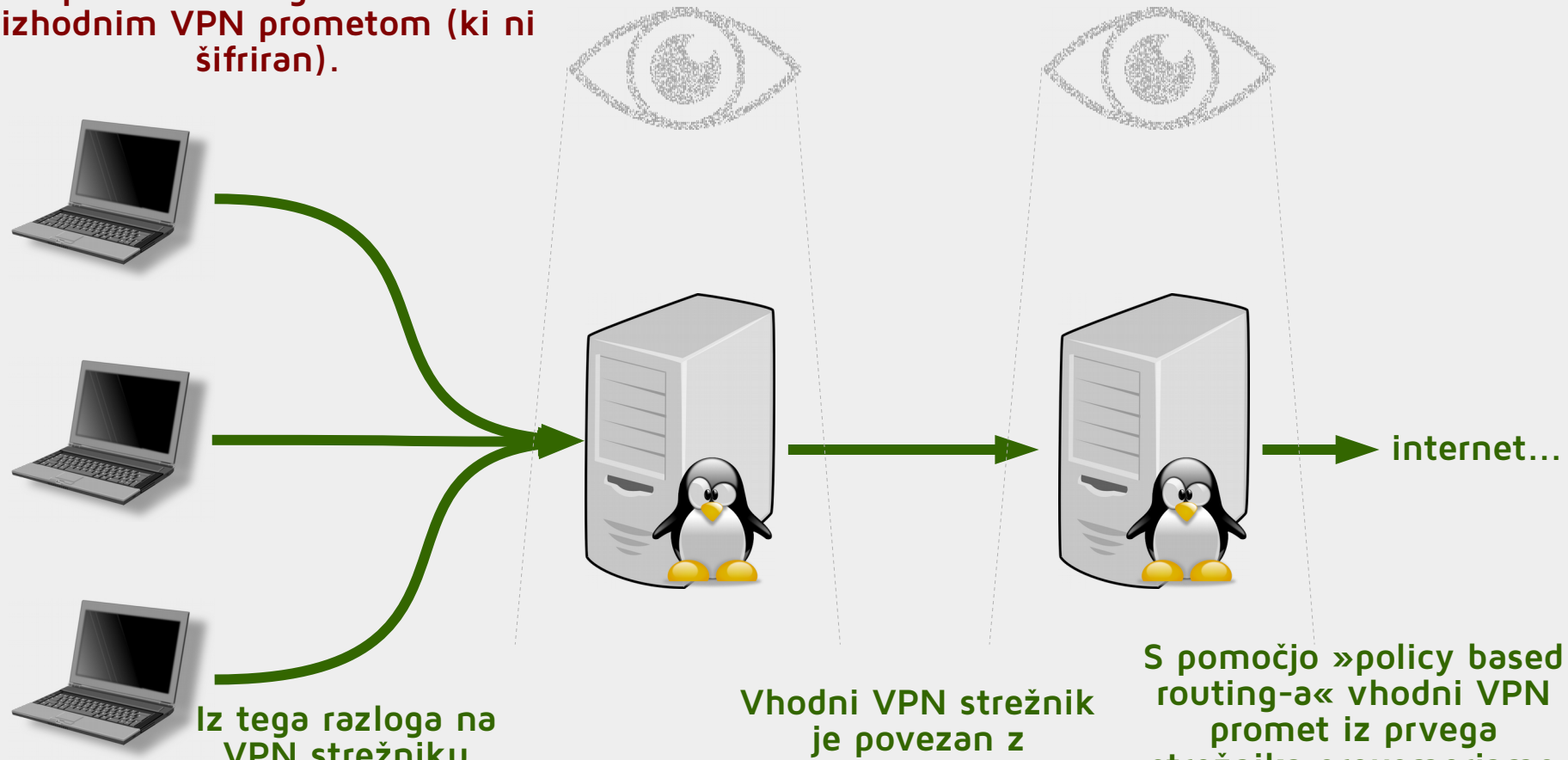
- Stunnel;
- Snowflake (maskiranje prometa preko WebRTC);
- Pluggable transports (Obfsproxy4, meek);
- Domain fronting;
- Dewebsockify.

Cilj je razviti sistem, ki se bo lahko prebil čez praktično katerikoli požari zid.

Odjemalska stran je lahko implementirana na RaspberryPi ali podobni napravi, ki uporabniku služi kot Wi-Fi dostopna točka.

Oteževanje »korelacijskih napadov«

Napadalec lahko z nadzorom prometa VPN strežnika spremlja dohodni (šifriran) VPN promet uporabnika in ga korelira z izhodnim VPN prometom (ki ni šifriran).



Iz tega razloga na VPN strežniku generiramo nekaj dodatnega »intra-VPN« prometa.

Vhodni VPN strežnik je povezan z izhodnim VPN strežnikom.

S pomočjo »policy based routing-a« vhodni VPN promet iz prvega strežnika preusmerjamo do izhodnega, ki se nahaja v drugem omrežju.

Oteževanje »korelacijskih napadov«

Dodatno na strežniku uporabljamo tehnike "onesnaževanja prometa" (tim. *data polluter*), ki generira izmišljeni a veljavni izhodni promet...

```
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]

http://malazan.wikia.com/wiki/Tattersail:
+157/389 links, H(domain)=2.9 b
```

Zakaj (OpenVPN)?

OpenVPN in varnost

OpenVPN je bil večkrat varnostno pregledan. V pregledu različice 2.4, ki je potekal od decembra 2016 do februarja 2017, in ga je vodil dr. Matthew Green iz Johns Hopkins University, ni bilo najdenih "*nobenih večjih ranljivosti*".

V začetku leta 2017 je pregled opravilo tudi podjetje QuarksLab.

Našli so dve ranljivosti, ki sta bili odpravljeni še pred javno objavo poročila.

Podpora za številne sisteme

OpenVPN je podprt in dejansko deluje na praktično vseh napravah:

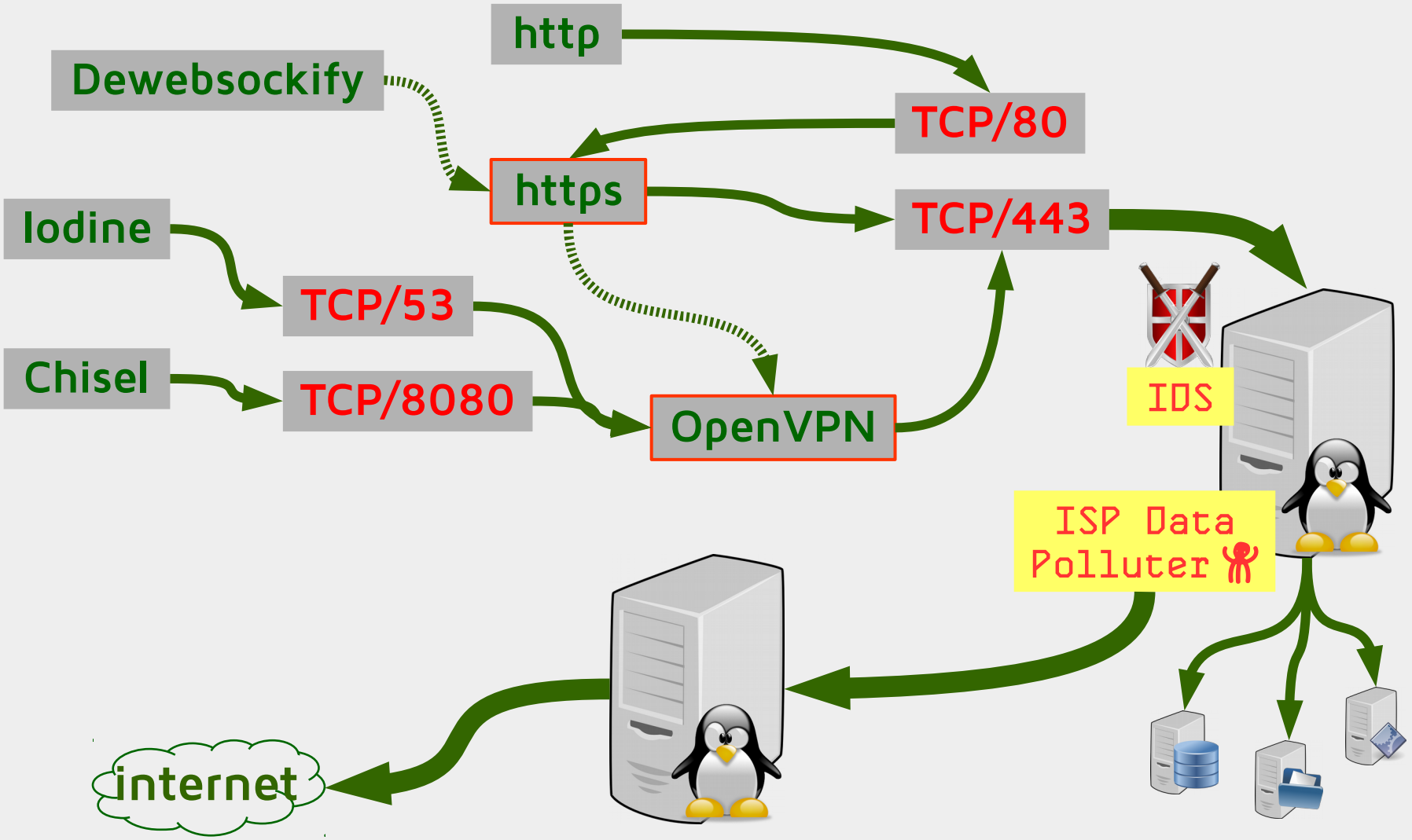
- Windows;
- Linux;
- Mac OS;
- IoT naprave temelječe na Linuxu (ARM);
- Androidni telefoni;
- iPhone.

Zakaj lastna infrastruktura?

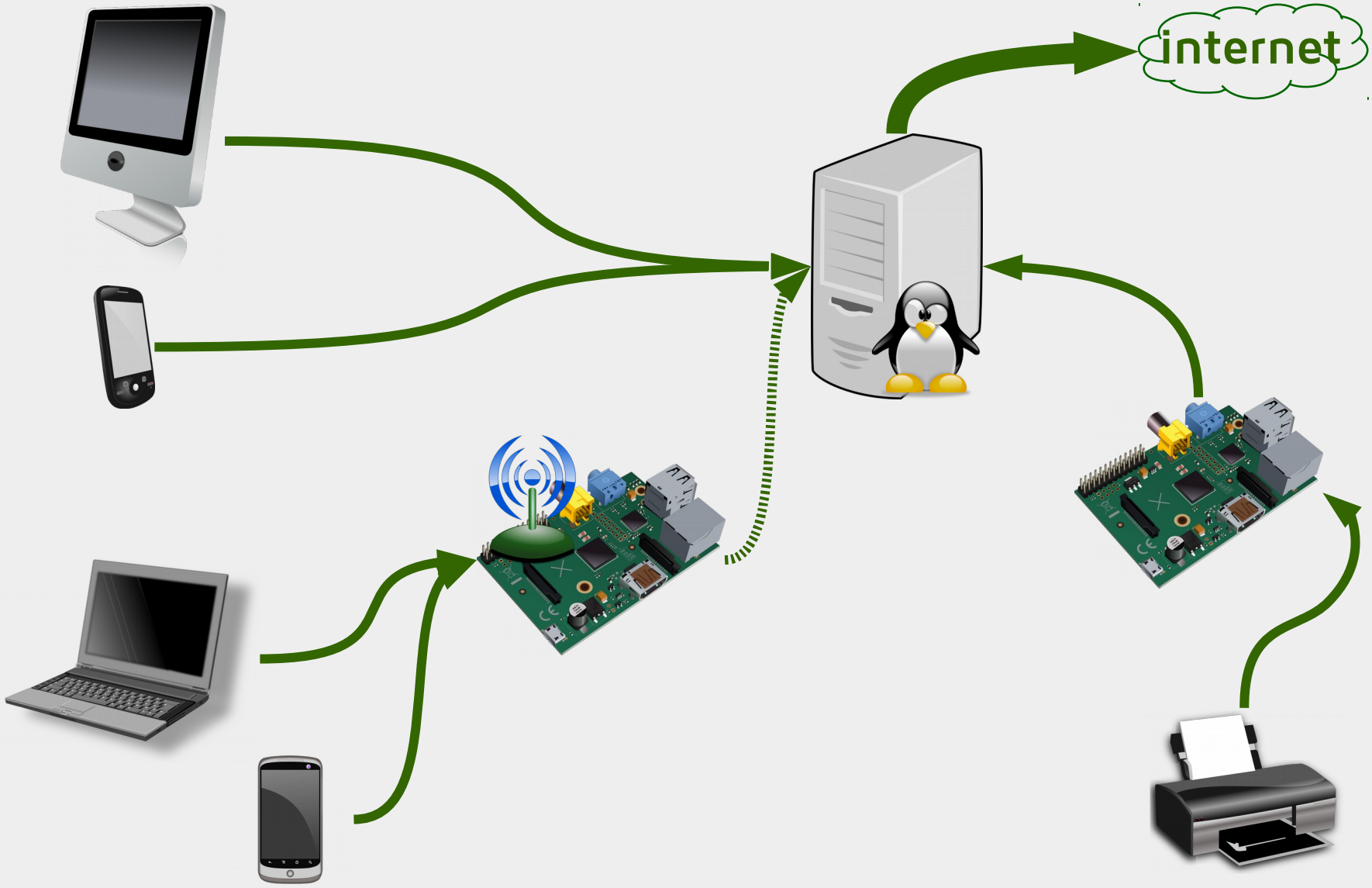
Raziskava VPN aplikacij za Android iz leta 2016 (Univerza Novega Južnega Walesa in Univerza Berkeley):

- testirali so 283 VPN aplikacij iz Google Play Store;
- 18 odstotkov aplikacij prometa sploh **ni šifriralo**;
- 38 odstotkov aplikacij je v promet **vstavljalo** zlonamerno kodo ali reklame;
- več kot 82 odstotkov aplikacij je zahtevalo dostop do osebnih podatkov na telefonu;
- praktično vse aplikacije so imele pomanjkljivosti, pogosto so uporabljale zunanje knjižnice za zbiranje in prodajo osebnih podatkov uporabnikov.

Končna postavitev (strežniški del)



Končna postavitev (uporabniški del)



Vprašanja?

Matej Kovačič
https://telefoncek.si