Ubuntu server kao router gateway (i kao VPN klijent za sve uređaje na mreži)

written by js | 2022-10-09

Tema

Konfiguriranje Ubuntu servera da bude ruter umjesto rutera. Po želji: konfiguriranje Ubuntu servera da bude VPN klijent za sve uređaje u LAN-u.

Preduvjeti

Instaliran i konfiguriran Ubuntu server s dvije mrežne kartice:

- `%ethEXTERNAL%` (spojena na ruter ISP providera, IP adresa npr. `192.161.1.2/16`; interface u stvarnosti ima neki kretenski naziv tipa "eth1s5")
- `%ethINTERNAL%`(spojena na switch u LAN-u na kojega su spojena sva računala u lokalnoj mreži; IP adresa npr. `10.100.100.100/8`; stvarni naziv NIC-a je kretenski kao i onaj gore)

SysCtl

- `nano /etc/sysctl.conf`

Dodaj ili promijeni:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=0
# DISABLE IPV6 - Ako želiš
net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=1
```

Primijeni pravila:

- `sysctl -p`

IPtables

- `iptables --table nat --append POSTROUTING --out-interface %ethEXTERNAL% -j MASQUERADE`
- `iptables --append FORWARD --in-interface %ethINTERNAL% -j ACCEPT`
- `iptables-save`

Klijenti

Sada svim računalima i mobitelima u LAN-u rekonfiguriraj postavke mrežne kartice i stavi da im je gateway IP adresa 192.168.1.2

Naravno, to možeš napraviti i DHCP serverom, no to je tema za drugu priču.

Wireguard

Ako želiš da tu Ubuntu bude i VPN klijent putem kojega svi na mreži idu "van":

- `apt install wireguard-tools resolvconf net-tools -y`

Generiraj konfiguracijski fajl na web stranicama svoga VPN providera i spremi to kao datoteku
`/etc/wireguard/wg0.conf`. Sadržaj:

```
[Interface]
PrivateKey = blablaserkenjprivatekey=
ListenPort = 56396
MTU = 1292
DNS = 1.1.1.1
Address = 10.11.12.13/24
[Peer]
PublicKey = +blablaserkenjpublickey=
AllowedIPs = 0.0.0.0/0
Endpoint = 123.234.123.234:1443
PersistentKeepalive = 25
```

IPtables za Wireguard

- `iptables -t nat -A POSTROUTING -o wg0 -j MASQUERADE`
- `iptables-save`

Rute

Dodaj neke rute za koje želiš da idu putem tvog ISP-a, a ne putem VPN-a (dodaj u ovo banke i sl.):

- `ip route add to 85.209.12.20  via 192.168.1.1    # gov.hr`
- `ip route add to 89.249.109.24 via 192.168.1.1    # e-predmet.pravosudje.hr`
- `ip route add to 185.20.29.73  via 192.168.1.1    # e-porezna.porezna-uprava.hr`
- `ip route add to 91.194.242.66 via 192.168.1.1    # mycheckout.eway2pay.com`
- `ip route add to 66.254.114.41 via 192.168.1.1    # golematorebabe.hr`

Napomena:`192.168.1.1` je adresa routera kojega ti je poklonio tvoj dragi ISP.

Razno

Ovo NEĆE raditi automatski nakon boota, pa se neke radnje mora provesti ručno nakon restarta. Detalje za taj dio ću staviti naknadno.

Ovo NIJE killswitch konfiguracija. Ako padne Wireguard – komunikacija će se nastaviti "normalnim" kanalom. Trenutačno nemam blagog pojma kako napraviti killswitch – dopisat ću kad pokradem s Neta.

Nakon svega ovoga za svaki slučaj na Windows mašinama napravi `netsh winhttp reset proxy` jer postoji mogućnost (vjerojatnost, čak) da moroni iz multibilijunske firme nisu bili u stanju detektirati promjenu i nastupanje novog rutera umjesto rutera, nego će prdit da nemaš internet u jednoj Office applikaciji, a uredno biti prijavljeni na Microsoft account u drugoj ili čak u istoj.

ubuntu server router vpn client xubuntu xserver xrouter xvpn xclient gateway xgateway