

# 3 hónap: 3 use case WireGuard-dal

Szabó Endre

Hackerspace Budapest Online Meetup

2020. június 28.

Mi nem célja az előadásnak?

Mi nem célja az előadásnak?

- ▶ Ez nem WireGuard endorsement. YMMV.

# Az előadás terjedelme

Mi nem célja az előadásnak?

- ▶ Ez nem WireGuard endorsement. YMMV.

Mi a célja az előadásnak?

Mi nem célja az előadásnak?

- ▶ Ez nem WireGuard endorsement. YMMV.

Mi a célja az előadásnak?

- ▶ Évek alatt kialakult best-practice-ok kivonatos bemutatása.
- ▶ Otthoni VPN környezetem bemutatása.

## IP-címzés általánosságban

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,



**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

- ▶ AMPRNet™ 44.128.0.0/16 teszt célú hálózatát lenyúltam,

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

- ▶ AMPRNet™ 44.128.0.0/16 teszt célú hálózatát lenyúltam,
- ▶ minden site-nak van egy „ $x < 64$ ” azonosítószáma (`site_id`),

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

- ▶ AMPRNet™ 44.128.0.0/16 teszt célú hálózatát lenyúltam,
- ▶ minden site-nak van egy „ $x < 64$ ” azonosítószáma (`site_id`),
- ▶ (ebből kalkulálódik egy /22 méretű IP subnet minden site-nak),

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

- ▶ AMPRNet™ 44.128.0.0/16 teszt célú hálózatát lenyúltam,
- ▶ minden site-nak van egy „ $x < 64$ ” azonosítószáma (`site_id`),
- ▶ (ebből kalkulálódik egy /22 méretű IP subnet minden site-nak),
- ▶ és egy ENSZ LOCODE alapú azonosító stringje (`site_code`),

**Site:** minden, fizikailag elkülönülő telephelyen lévő eszközök összessége. Ez lehet:

- ▶ valódi helyi hálózat (lakás),
- ▶ VPS,
- ▶ vagy egy-egy kiemeltebb road-warrior is.

Általános jellemzők:

- ▶ AMPRNet™ 44.128.0.0/16 teszt célú hálózatát lenyúltam,
- ▶ minden site-nak van egy „ $x < 64$ ” azonosítószáma (`site_id`),
- ▶ (ebből kalkulálódik egy /22 méretű IP subnet minden site-nak),
- ▶ és egy ENSZ LOCODE alapú azonosító stringje (`site_code`),
- ▶ (ebből származtatódnak a hostnevek prefixei).

# **1. USE CASE: SITE TO SITE VPN**



# Site to Site VPN jellemzők

Jellemzők:

- ▶ Full mesh VPN

# Site to Site VPN jellemzők

Jellemzők:

- ▶ Full mesh VPN
- ▶ Automatikus deploy Ansible-lel

# Site to Site VPN jellemzők

Jellemzők:

- ▶ Full mesh VPN
- ▶ Automatikus deploy Ansible-lel
- ▶ Teljes 0.0.0.0/0 hirdetve minden végponton

# Site to Site VPN jellemzők

Jellemzők:

- ▶ Full mesh VPN
- ▶ Automatikus deploy Ansible-lel
- ▶ Teljes 0.0.0.0/0 hirdetve minden végponton
- ▶ SNAT Internet felé minden, tunnelből érkező forgalomra

# Site to Site VPN jellemzők

Jellemzők:

- ▶ Full mesh VPN
- ▶ Automatikus deploy Ansible-lel
- ▶ Teljes 0.0.0.0/0 hirdetve minden végponton
- ▶ SNAT Internet felé minden, tunnelből érkező forgalomra

Hátrány:

# Site to Site VPN jellemzők

## Jellemzők:

- ▶ Full mesh VPN
- ▶ Automatikus deploy Ansible-lel
- ▶ Teljes 0.0.0.0/0 hirdetve minden végponton
- ▶ SNAT Internet felé minden, tunnelből érkező forgalomra

## Hátrány:

- ▶ WireGuard crypto-routing és DynDNS miatt minden site felé egy dedikált tunnel interface jelenléte szükséges.

# Site to Site VPN route optimalizálás

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest



# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.
- ▶ Natívan, kernelspace-ben, netfilter DNAT+SNAT kombóval.

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.
- ▶ Natívan, kernelspace-ben, netfilter DNAT+SNAT kombóval.
- ▶ A forgalom útja így: Bécs - Budapest (- Budapest)

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.
- ▶ Natívan, kernelspace-ben, netfilter DNAT+SNAT kombóval.
- ▶ A forgalom útja így: Bécs - Budapest (- Budapest)
- ▶ Eredmény: 18 msec RTT.

Hátrány:

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.
- ▶ Natívan, kernelspace-ben, netfilter DNAT+SNAT kombóval.
- ▶ A forgalom útja így: Bécs - Budapest (- Budapest)
- ▶ Eredmény: 18 msec RTT.

Hátrány:

- ▶ Dinamikus című végpontok között initiatort kell kinevezni.

# Site to Site VPN route optimalizálás

Nemzetközi forgalom optimalizálásra is lehetőség van.

A probléma:

- ▶ Bécsi UPC és DIGI között a forgalom: Bécs - Frankfurt - Bukarest - Budapest
- ▶ 38 msec RTT.

A megoldás:

- ▶ Forgalom elirányítása kevesebb hop-on keresztül, BGP nélkül.
- ▶ Egyik budapesti VPS-en terminálás nélküli, same-interface tükrözés.
- ▶ Natívan, kernelspace-ben, netfilter DNAT+SNAT kombóval.
- ▶ A forgalom útja így: Bécs - Budapest (- Budapest)
- ▶ Eredmény: 18 msec RTT.

Hátrány:

- ▶ Dinamikus című végpontok között initiatort kell kinevezni.
- ▶ SPoF bevezetése. :)



**2. USE CASE:**

**ROAD WARRIOR VPN**

# Road warrior VPN jellemzők

Jellemzők:

- ▶ Ansible-lel segített

# Road warrior VPN jellemzők

Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása
- ▶ Szerver oldalon proxy ARP lehetősége

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása
- ▶ Szerver oldalon proxy ARP lehetősége

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása
- ▶ Szerver oldalon proxy ARP lehetősége

## Namespace használat macerái:

- ▶ Nincs network manager ami támogatná ezt a setup-ot.



# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása
- ▶ Szerver oldalon proxy ARP lehetősége

## Namespace használat macerái:

- ▶ Nincs network manager ami támogatná ezt a setup-ot.
- ▶ Még a `wg-quick` sem támogatja, de patch-et küldtem.

# Road warrior VPN jellemzők

## Jellemzők:

- ▶ Ansible-lel segített
- ▶ Teljes 0.0.0.0/0 hirdetve minden koncentrátoron
- ▶ Jobb kliensek párhuzamosan több tunnelt is tudnak használni
- ▶ Kliens oldalon network namespacing kihasználása
- ▶ Szerver oldalon proxy ARP lehetősége

## Namespace használat macerái:

- ▶ Nincs network manager ami támogatná ezt a setup-ot.
- ▶ Még a `wg-quick` sem támogatja, de patch-et küldtem.
- ▶ Default namespace helyi hálózatra macerásan tud szolgáltatni.

# **3. USE CASE: MAGYAR FIX IP-CÍM**

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú
- ▶ Egy tunnelezett, budapesti IP-címmel rendelkező kijáratú

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú
- ▶ Egy tunnelezett, budapesti IP-címmel rendelkező kijáratú
- ▶ Snowflake network bridge

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú
- ▶ Egy tunnelezett, budapesti IP-címmel rendelkező kijáratú
- ▶ Snowflake network bridge
- ▶ PVLAN és WiFi client isolation alapú `fwmark`



Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú
- ▶ Egy tunnelezett, budapesti IP-címmel rendelkező kijáratú
- ▶ Snowflake network bridge
- ▶ PVLAN és WiFi client isolation alapú `fwmark`
- ▶ RPDB rule `fwmark` alapján

Szükség volt egy magyar IP-cím Bécsbe routolására.

Helyi hálózati jellemzők:

- ▶ Két WiFi SSID itthon:
- ▶ Egy natív, bécsi UPC kijáratú
- ▶ Egy tunnelezett, budapesti IP-címmel rendelkező kijáratú
- ▶ Snowflake network bridge
- ▶ PVLAN és WiFi client isolation alapú `fwmark`
- ▶ RPDB rule `fwmark` alapján

Hátrány:

- ▶ Nincs.