ISACA KONFERENCIA 2026

Csere István

"Dolgozni bárhonnan" 2026-ban. Kiberbiztonsági kihívások - megoldások

2026.06.02.

ISACA
Budapest Chapter

Előzmények

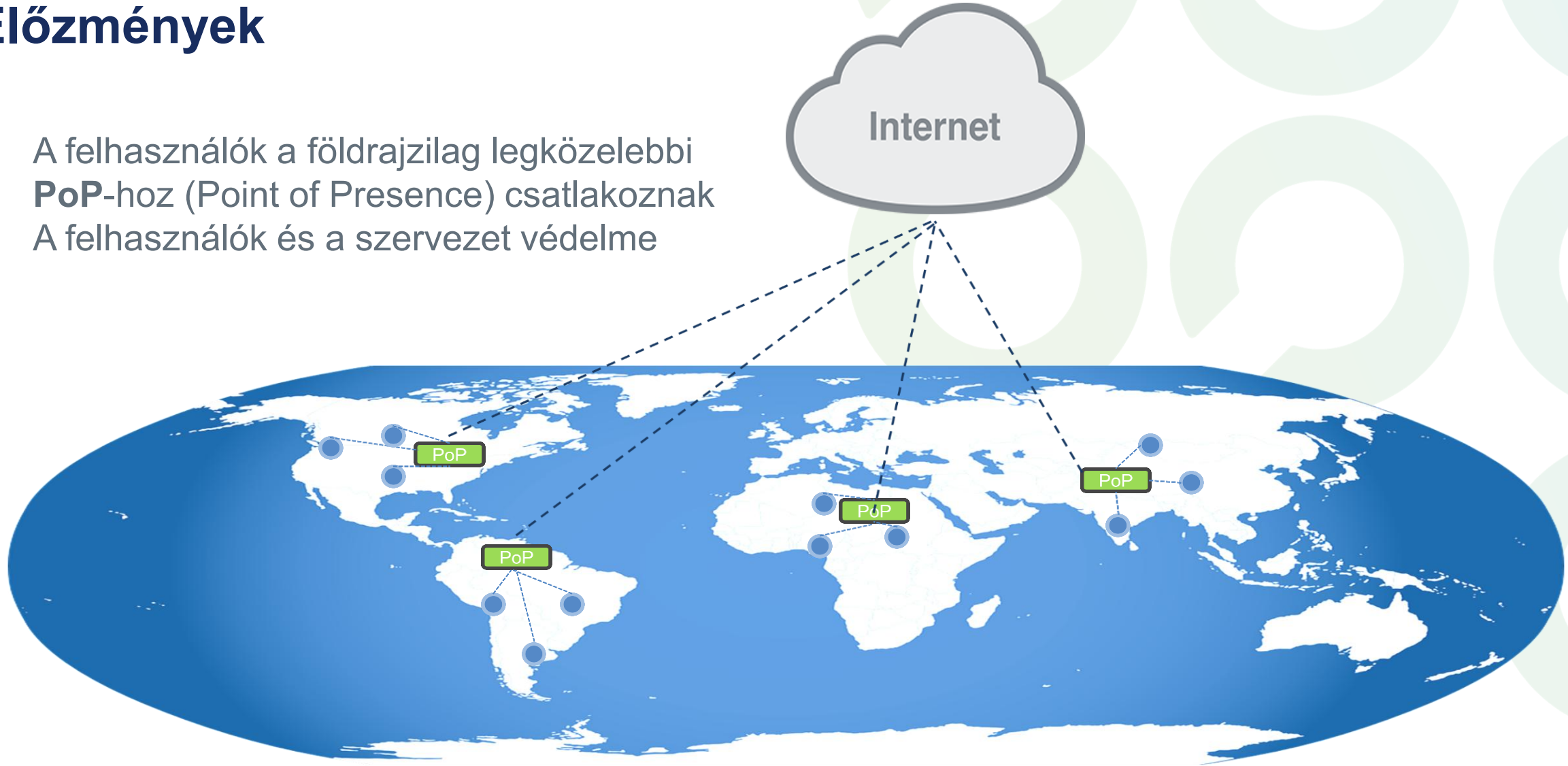
Dolgozni bárhonnan

Megnövekedett rizikó – a felhasználók egy része a vállalati hálózaton kívül dolgozik

ISACA Budapest Chapter

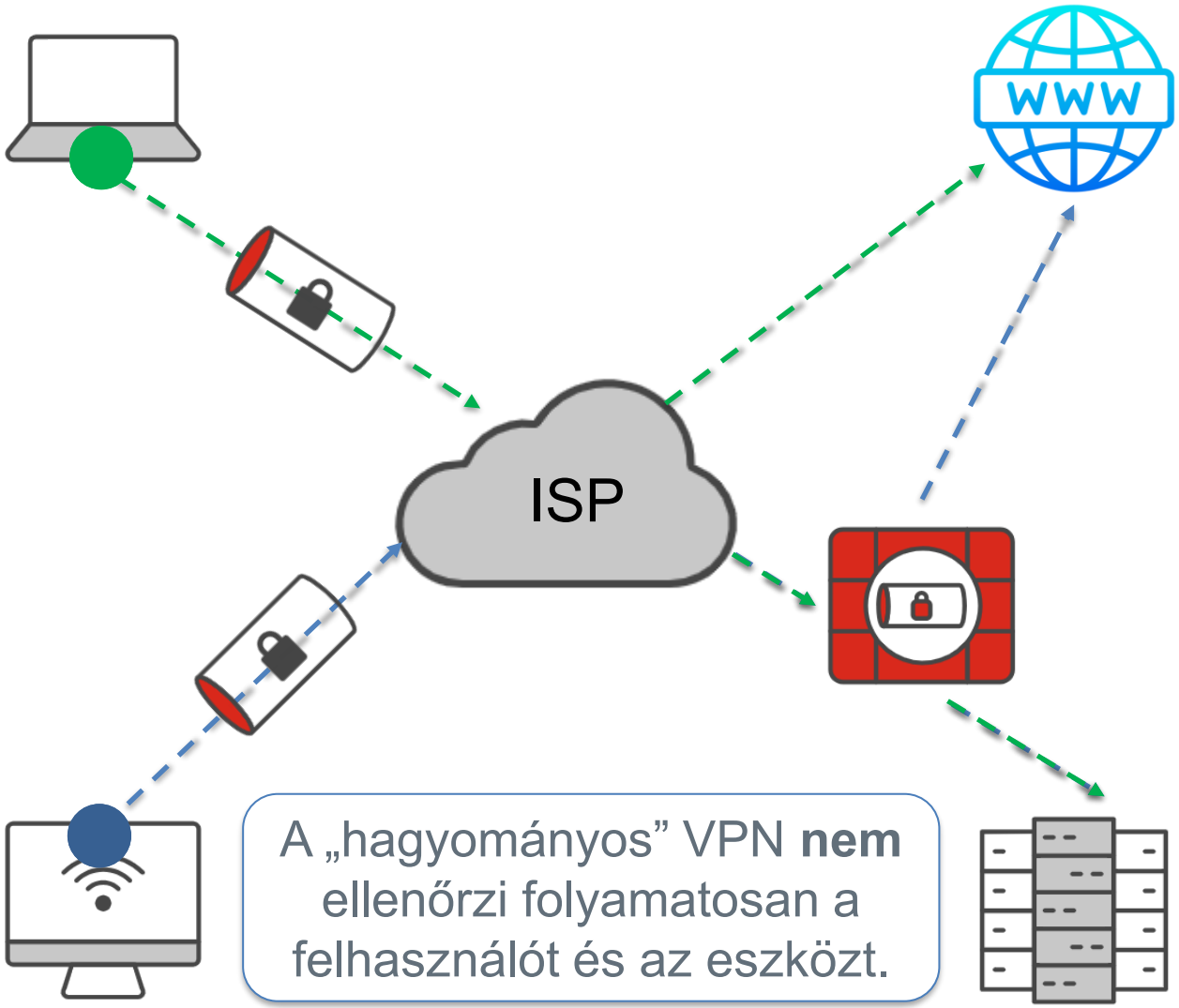
Előzmények

- A felhasználók a földrajzilag legközelebbi **PoP**-hoz (Point of Presence) csatlakoznak
- A felhasználók és a szervezet védelme



ISACA
Budapest Chapter

Hagyományos kliens VPN megközelítés



A „hagyományos” VPN **nem** ellenőrzi folyamatosan a felhasználót és az eszközt.

Full tunneling

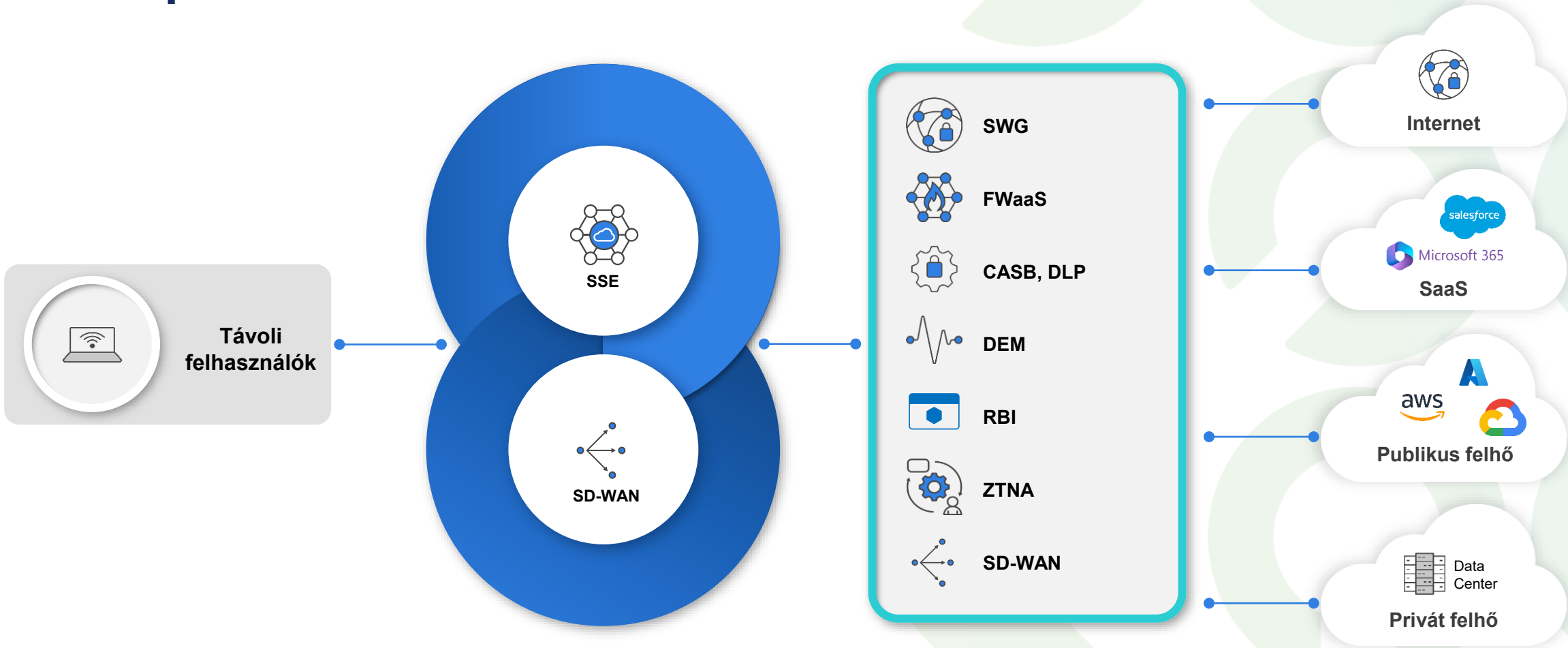
- VPN eszköz túlterhelése
- Távolság

Split tunneling

- Láthatóság hiánya
- Ellenőrízetlen internet kapcsolat

ISACA Budapest Chapter

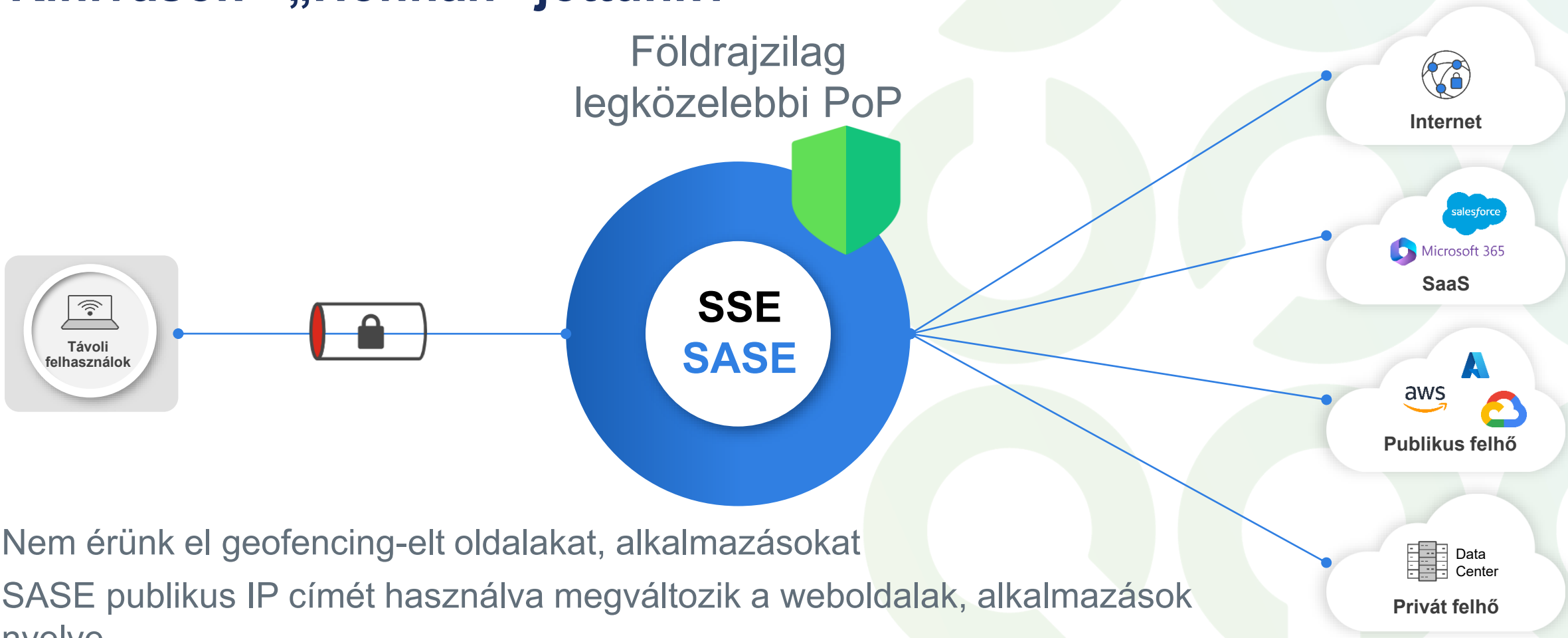
Koncepció



2019-ben a Gartner vezette be a SASE fogalmát, és úgy határozta meg, mint a hálózatbiztonsági funkciók (azaz felhőalapú biztonsági szolgáltatások) és az SD-WAN képességek kombinációját.

ISACA® Budapest Chapter

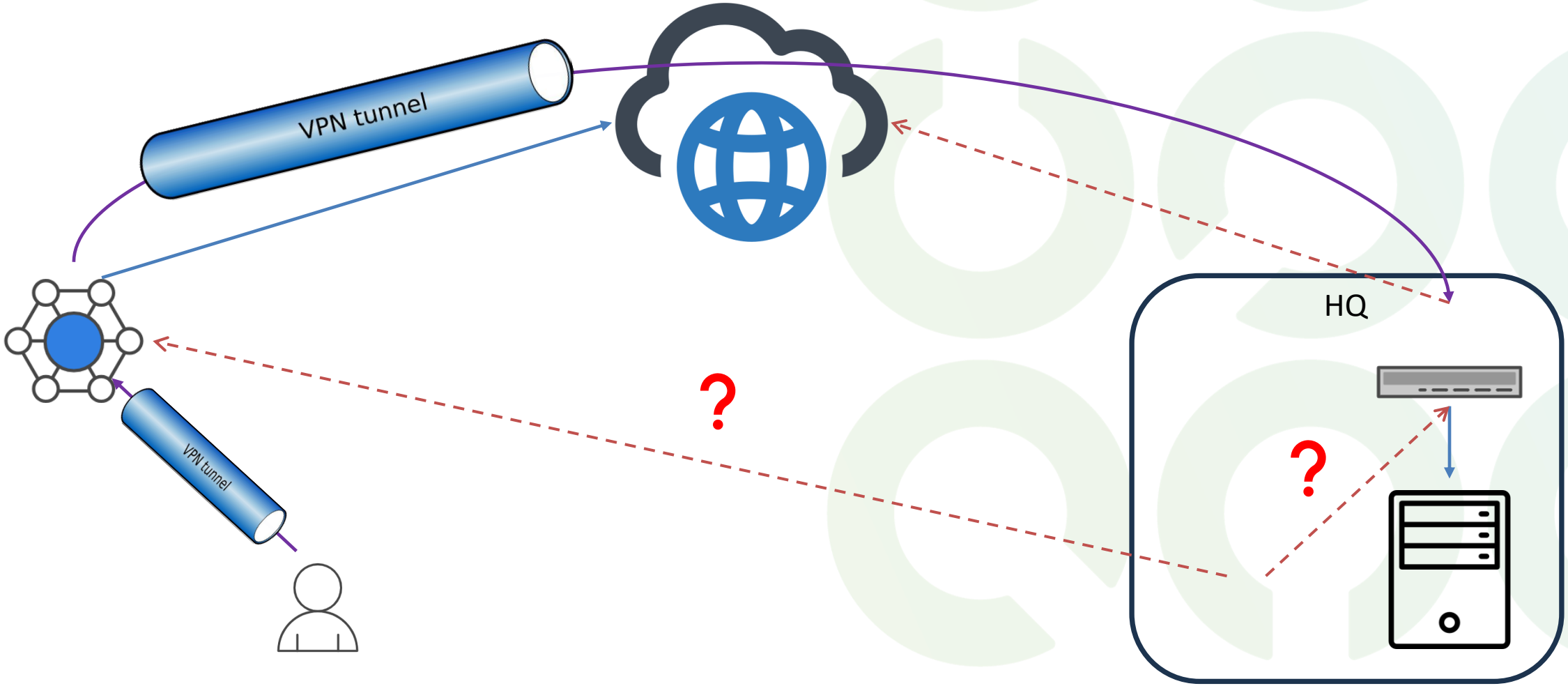
Kihívások - „Honnan” jöttünk?



- Nem érünk el geofencing-elt oldalakat, alkalmazásokat
- SASE publikus IP címét használva megváltozik a weboldalak, alkalmazások nyelve
- Egyes országoknak speciális biztonsági ellenőrzési követelményeik vannak.
  - A felhasználó tartózkodási országa alapján a helyi jogszabályoknak megfelelő szabályzatot kell alkalmazni.

ISACA®
Budapest Chapter

Kihívások - Távol, vagy az irodában?



ISACA
Budapest Chapter

Kihívások

Multi Vendor SASE

- Több megoldást, dashboard-ot kell kezelni
- Hibakezelés
  - Több csapattal kell dolgozni
  - Több felületen, több hibajegyet kell kezelni.
  - Felelősség áthárítás
- Fluktuáció
- Integrációs nehézségek

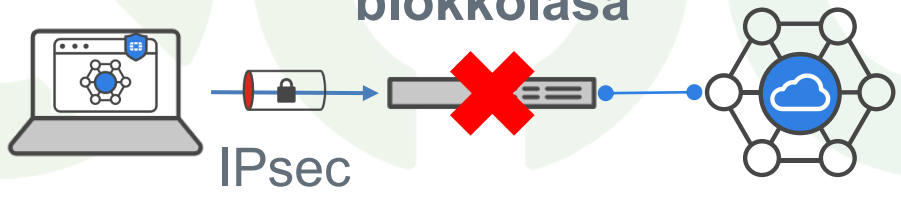
Nem lehet beállításokat végrehajtani a kliensen

- IoT, OT eszközök
- Nincs admin jogunk az eszközön
  - Vendég, contractor

IPsec VPN korlátozása

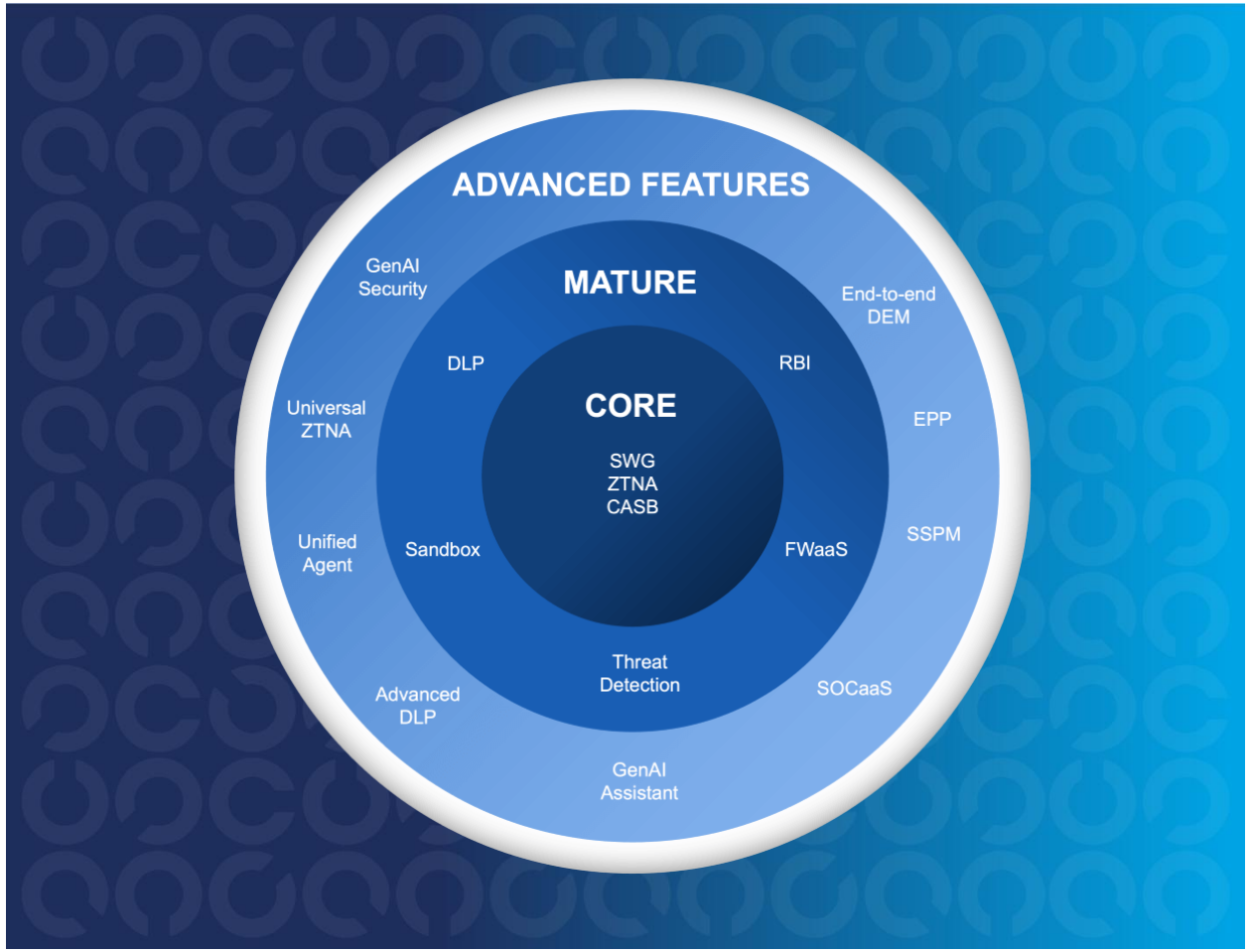
- Nyilvános WiFi hálózatokon sok helyen tiltják az IPsec-hez szükséges UDP 500 / 4500 portokat vagy az ESP-t
- Országos szintű korlátozás
- Szolgáltatói problémák vagy korlátozás

UDP / ESP blokkolása



ISACA Budapest Chapter

Megoldások FortiSASE-val



FORTINET

HRP

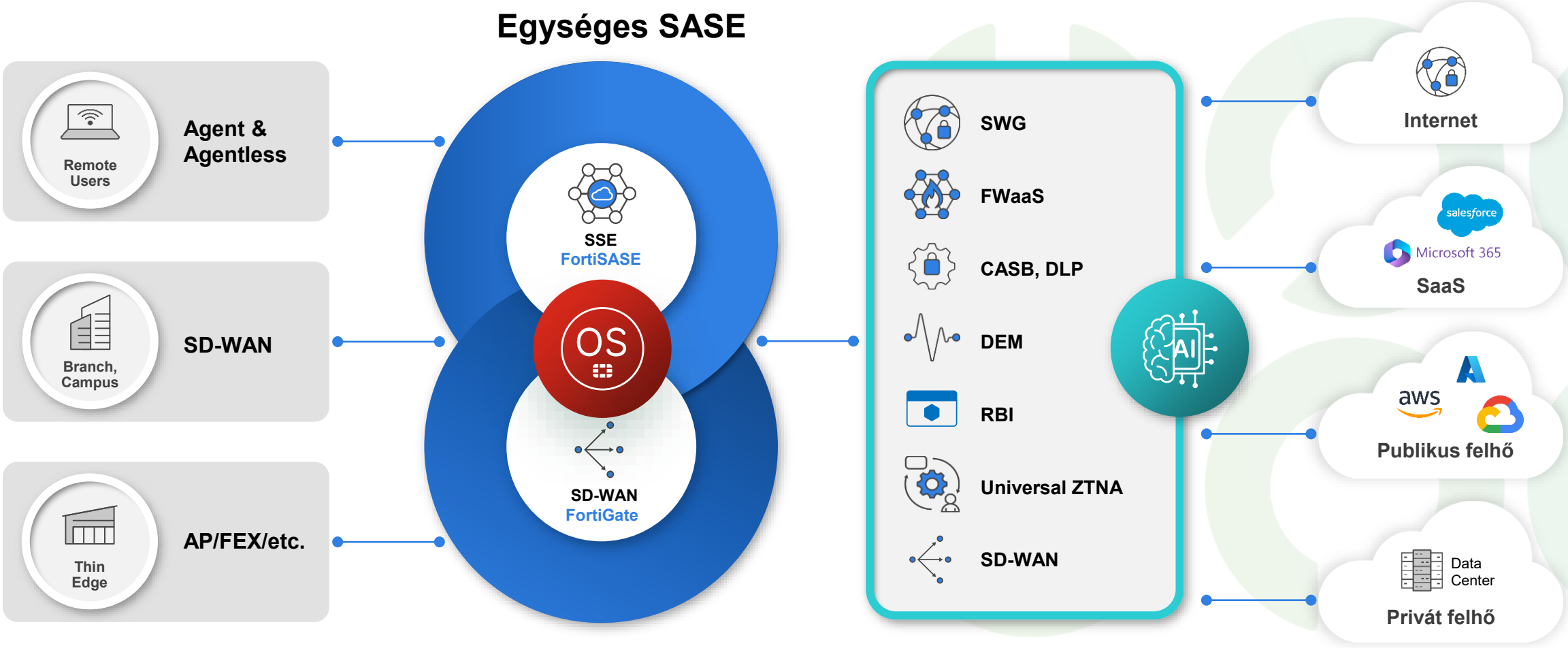
FORTINET ENGAGE Distributor Specialization SASE

FORTINET ENGAGE Distributor Specialization OPERATIONAL TECHNOLOGY

FORTINET Authorized Training Center

ISACA® Budapest Chapter

Fortinet SASE koncepció



FORTINET

ISACA Budapest Chapter

Megoldások – Egy gyártós (Single Vendor) SASE

Kihívás: Multi Vendor SASE

- Egy gyártó
- Egy operációs rendszer
- Egy menedzsment felület

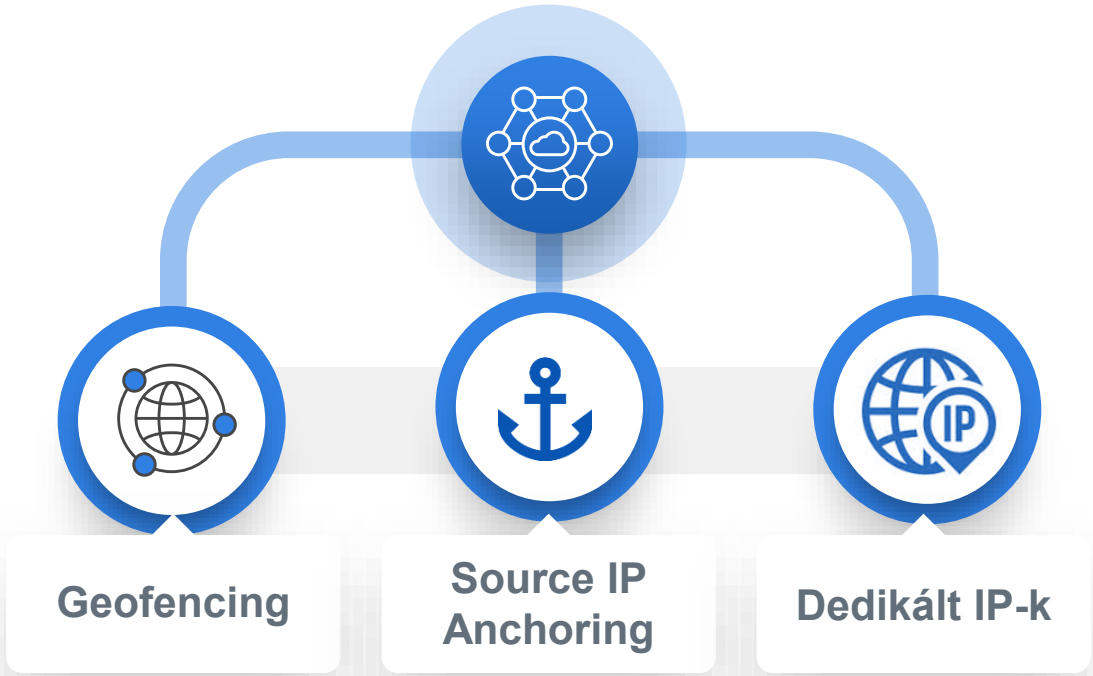
- Egyszerűbb üzemeltetés
- Egy hibajegy nyílik probléma esetén
- Nincs felelősség áthárítás a support csapatok között

- Egy gyártós fejlesztés – nincsenek integrációs nehézségek

ISACA Budapest Chapter

Megoldások – Forrás IP rögzítése, Dedikált IP-k

Kihívás: „Honnan” jöttünk?



Geofencing

Szabályozza, hogy mely országokból csatlakozhatnak távoli felhasználók a FortiSASE-hez.

Source IP Anchoring

Biztosítja, hogy a felhasználótól vagy eszköztől származó forgalom egy állandó, kijelölt IP-címről származónak tűnjön, függetlenül a tényleges fizikai vagy hálózati helyzetétől. Ideális a szabályozási megfelelőség biztosításához.

Dedikált IP-k

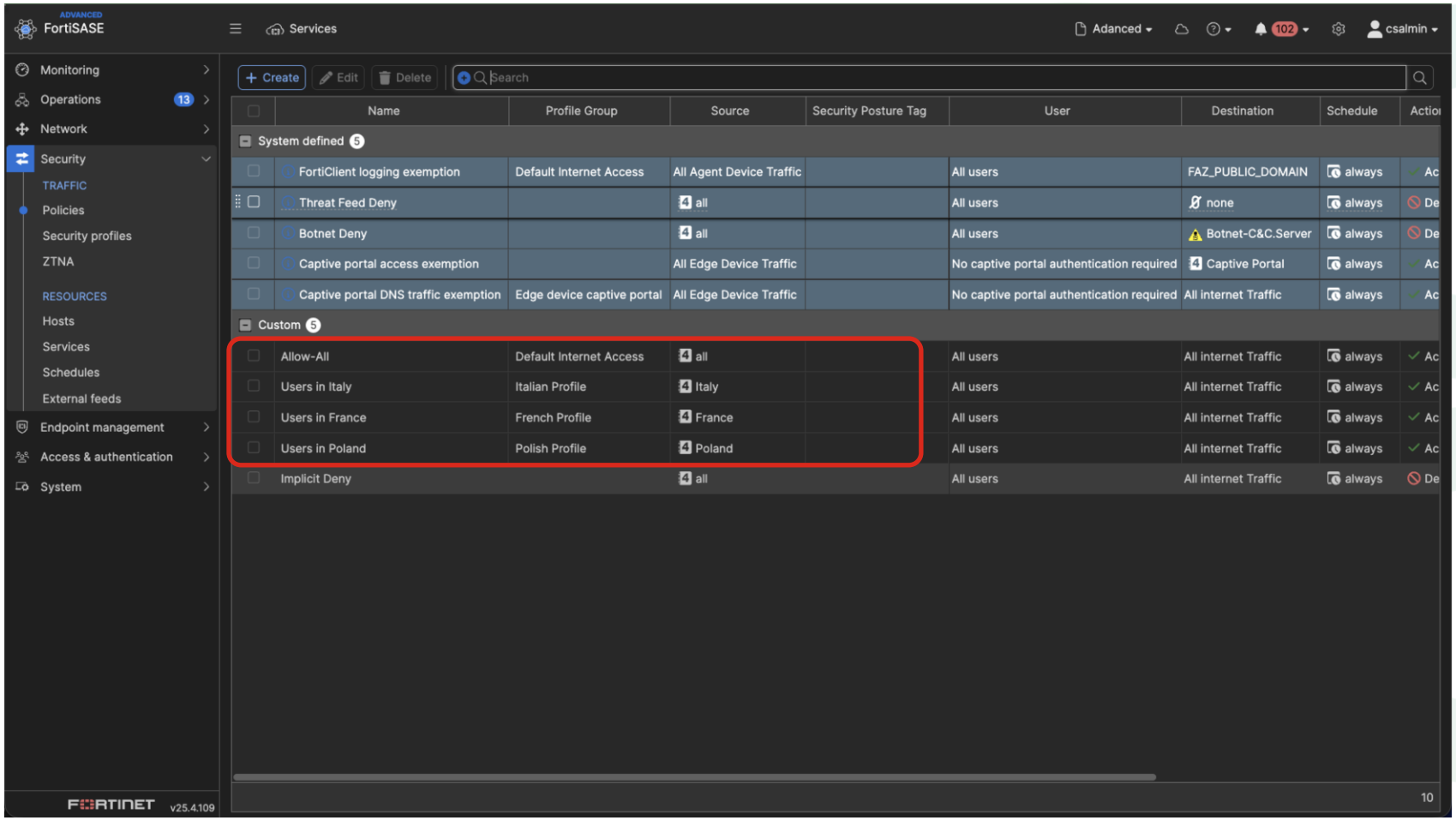
Fenntartott IP-címek, amelyek engedélyezési listára (whitelistre) tehetők, hogy a POP-ból érkező hozzáférést biztosítsák a SaaS alkalmazásokhoz.

ISACA Budapest Chapter

Megoldások – Helyi jogszabályoknak megfelelés

Kihívás: „Honnan” jöttünk?

- A FortiSASE 25.4.c verziója bevezette a földrajzi alapú biztonsági szabályzási lehetőséget.
- A felhasználó helyétől függően különböző szabálykészletek alkalmazhatók



ISACA Budapest Chapter

Megoldások – Thin Edge eszközök

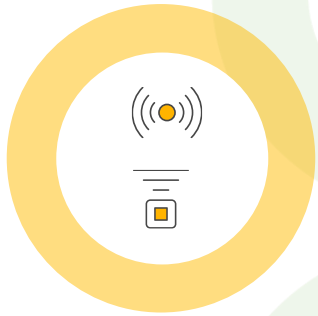
Kihívás: Nem lehet beállításokat végrehajtani a kliensen

Kisebb helyszínek biztosítása
Kisebb fiókirodák, ideiglenes helyszínek

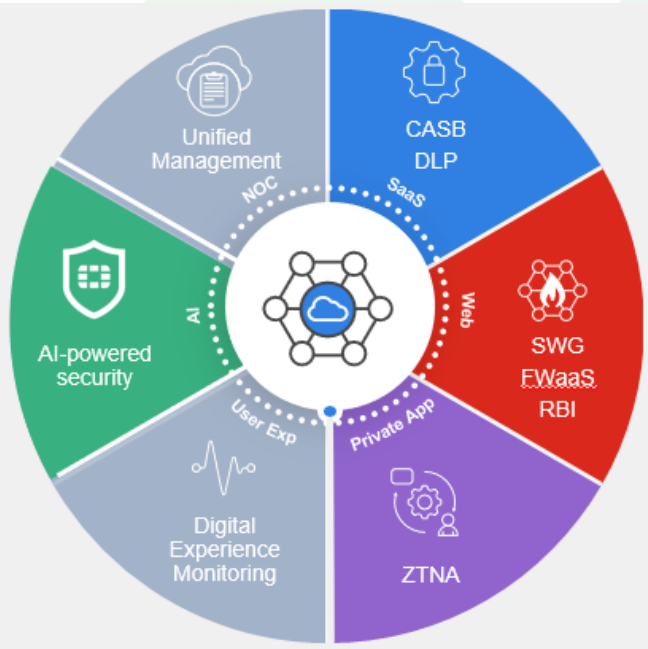
IoT, OT és agent nélküli eszközök
Olyan eszközökre, amikre nem telepíthető agent. (pl. IoT/OT, ATM)

Központi láthatóság és menedzsment
Egységes kezelés és átláthatóság minden végponton, rugalmas telepítési lehetőségekkel.

FortiAP, FortiExtender, FortiGate, FortiBranchSASE, FortiSwitch integráció a FortiSASE-val



Thin Edge
(Home office, Retail, ATM, IoT/OT)

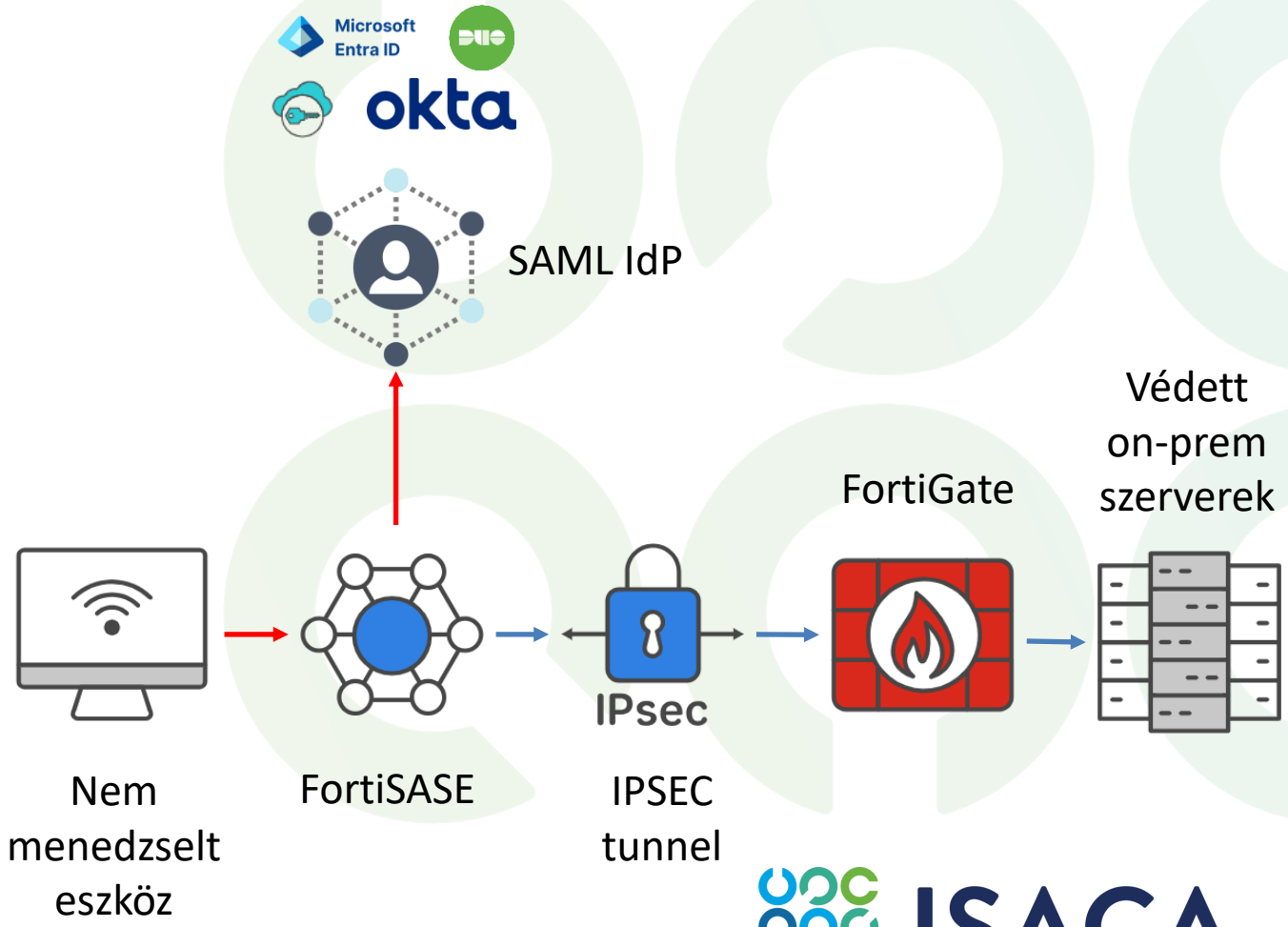


ISACA Budapest Chapter

Megoldások – Agentless ZTNA

Kihívás: Nem lehet beállításokat végrehajtani a kliensen

- Nem menedzselhető eszközzel rendelkező felhasználónak (szerződéses, külsős alvállalkozó) biztosít biztonságos hozzáférést.
- Az alkalmazások egy webfelületről indíthatóak
- Felhasználó azonosítás: Hitelesítést kényszerít ki egy SAML IdP felé a távoli felhasználó webböngészőjéből.
- A FortiSASE ZTNA alkalmazás gateway-ként működik a HTTPS forgalmon és reverse proxy-ként funkcionálva védi a privát, web alapú alkalmazásokat
- Geolokációs korlátozások hozzáadhatóak

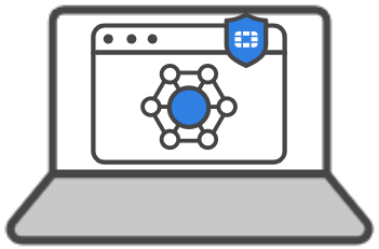


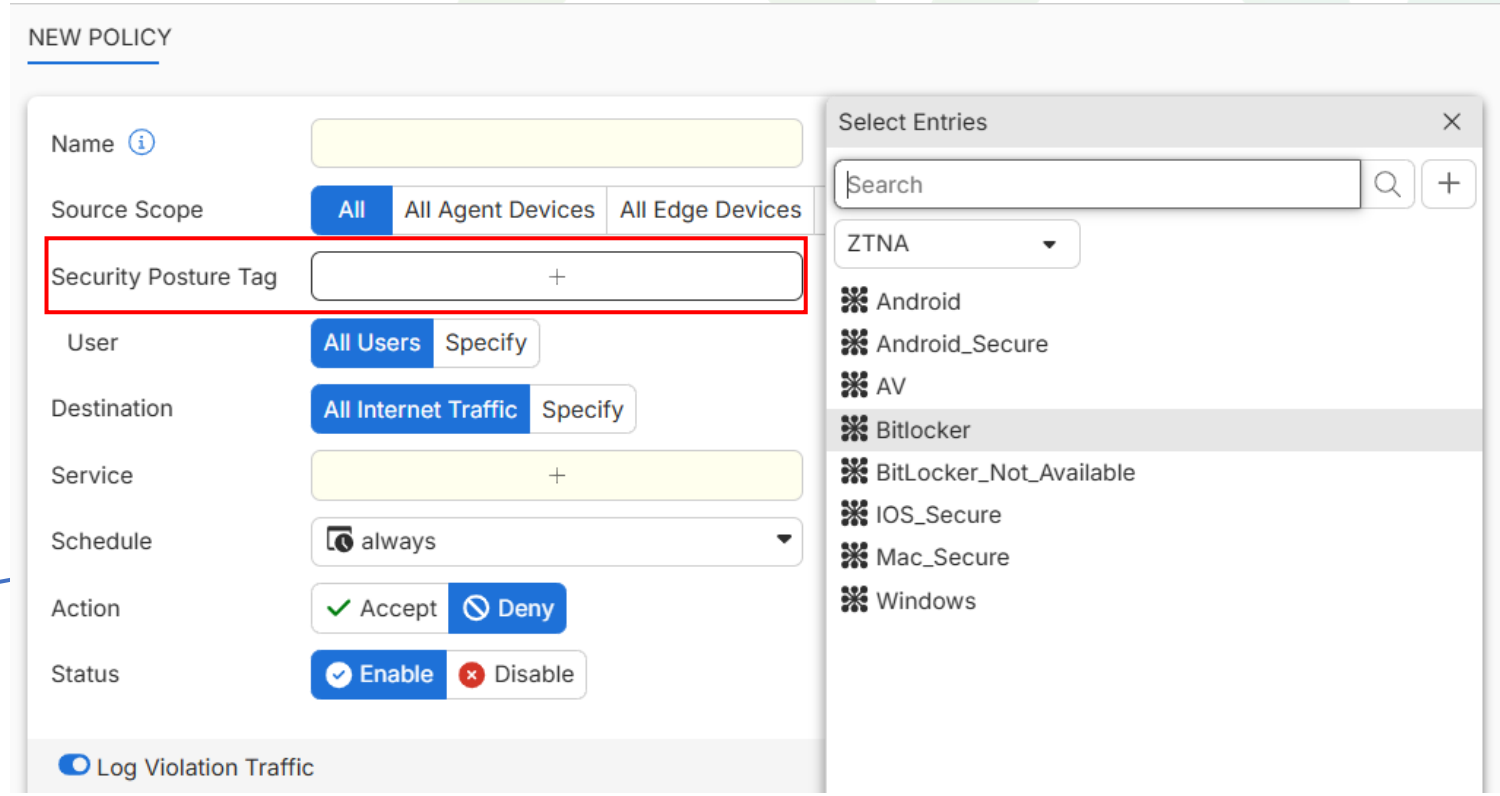
ISACA Budapest Chapter

Megoldások – ZTNA – Eszköz állapot ellenőrzése

Kihívás: Hagyományos kliens VPN, „megbízunk benned, ha már bent vagy”

- A FortiClient minden végponti információt megoszt a FortiSASE-val és folyamatosan szinkronizálja az aktuális biztonsági állapotát (posture) a FortiSASE-ból
- A ZTNA kritériumok alapján „megcímkézi” a végpontokat
- A ZTNA címkéket tudjuk használni a szabályrendszereinkben

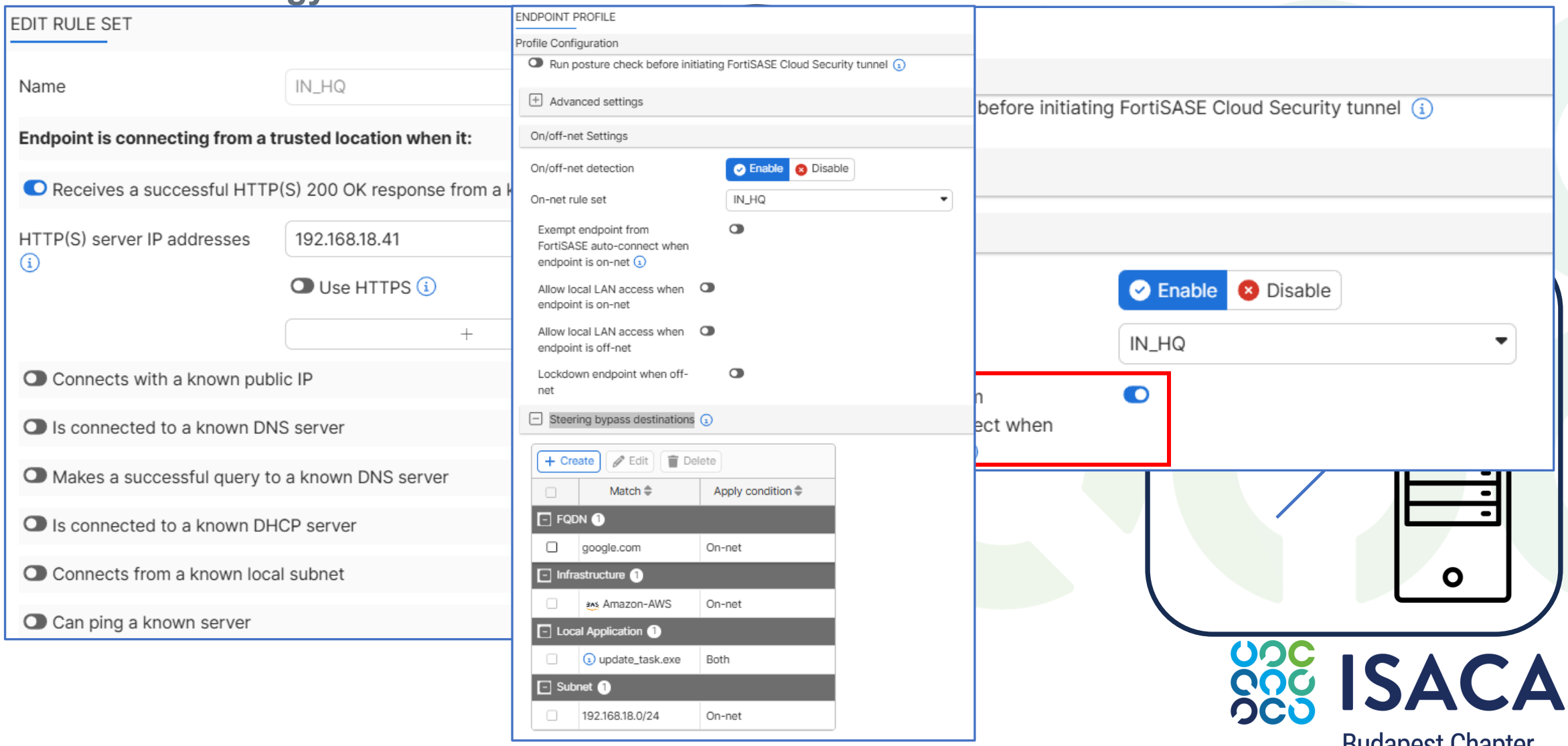




ISACA Budapest Chapter

Megoldások – Azonosítjuk a környezetünket

Kihívás: Távol vagy az irodában?

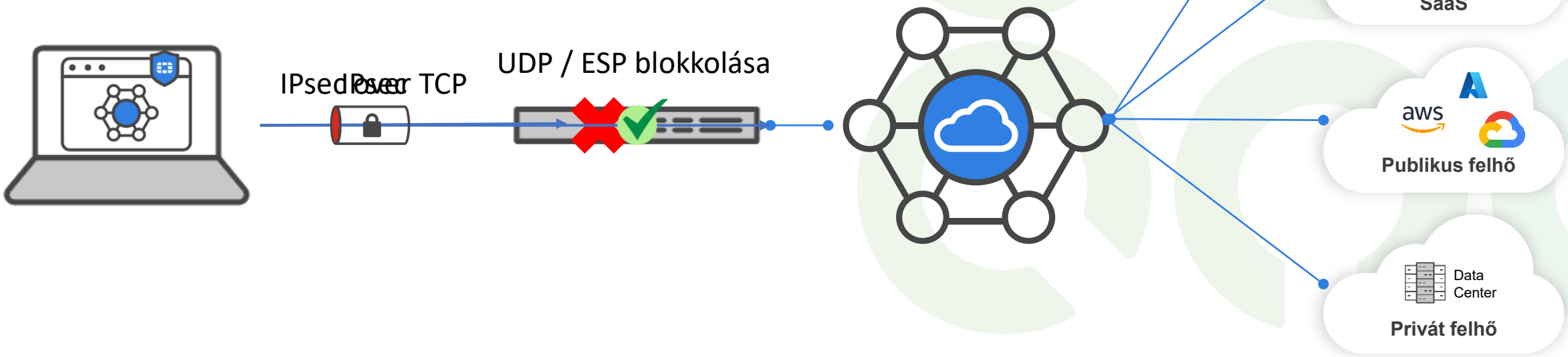


ISACA Budapest Chapter

Megoldások – IPsec over TCP

Kihívás: IPsec VPN korlátozása

- Ha nem sikerül UDP-n felépíteni a kapcsolatot, van lehetőség IPsec over TCP-n (TCP port 443) keresztül létrehozni a kapcsolatot másodlagosan
- FortiClient 7.4.5+ szükséges



ISACA Budapest Chapter

KÖSZÖNÖM A FIGYELMET!