

ISACA KONFERENCIA 2026

Csere István

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

2026.06.02.

Előzmények

Dolgozni bárhol



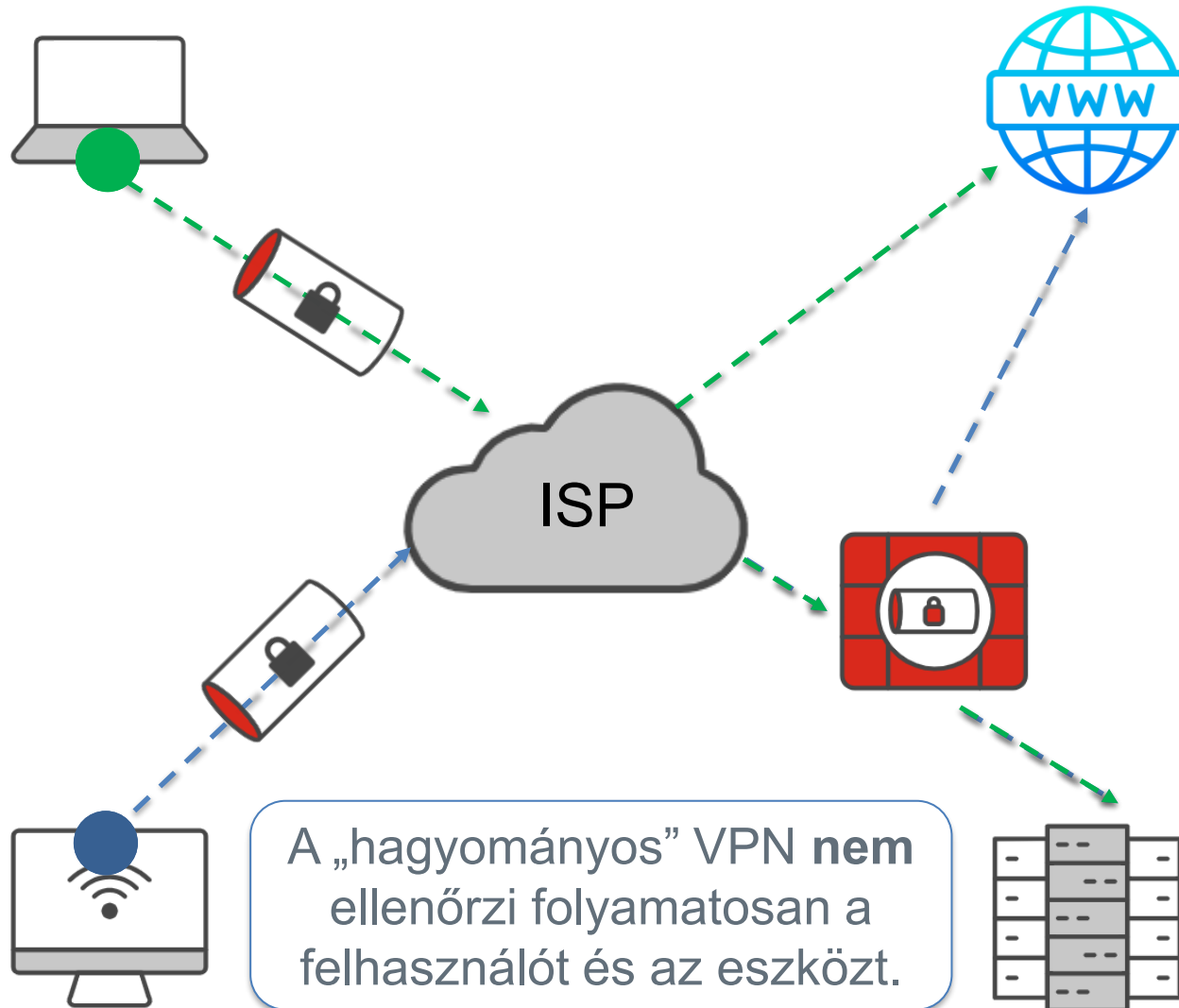
Megnövekedett rizikó – a felhasználók egy része a vállalati hálózaton kívül dolgozik

Előzmények

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



Hagyományos kliens VPN megközelítés



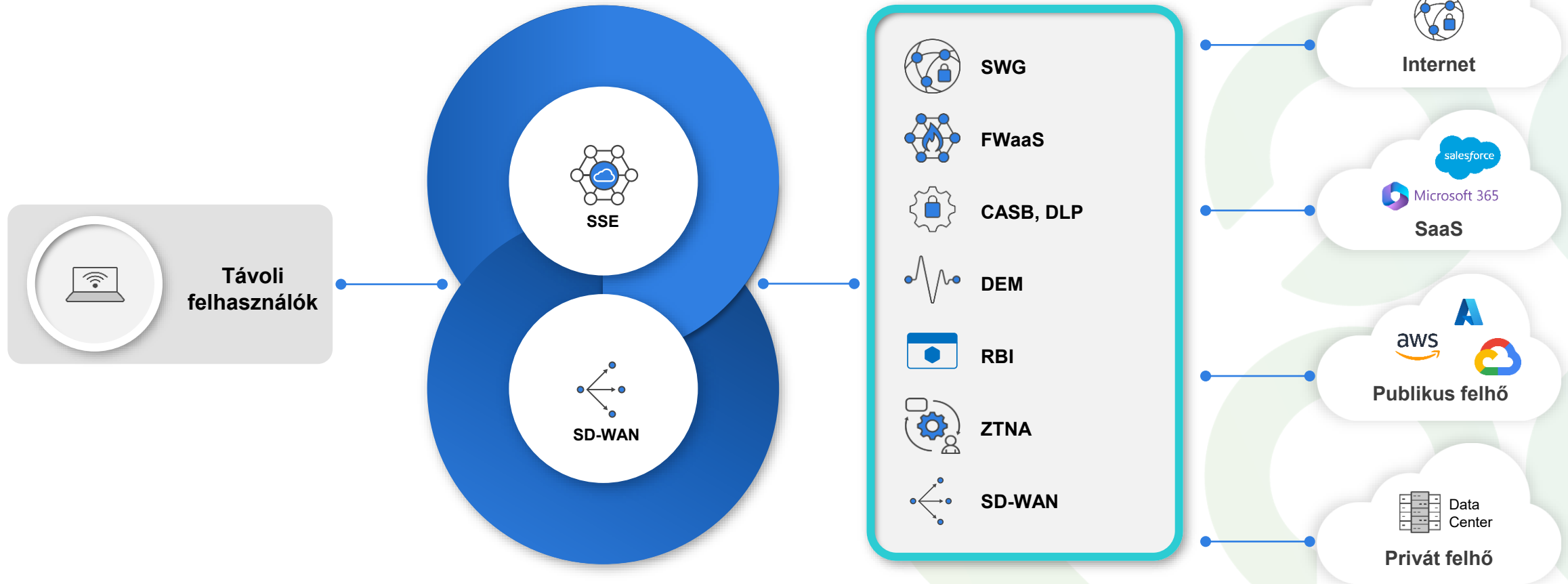
Full tunneling

- VPN eszköz túlterhelése
 - Távolság

Split tunneling

- Láthatóság hiánya
- Ellenőrizetlen internet kapcsolat

Konceptió



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.



Kihívások - „Honnan” jöttünk?

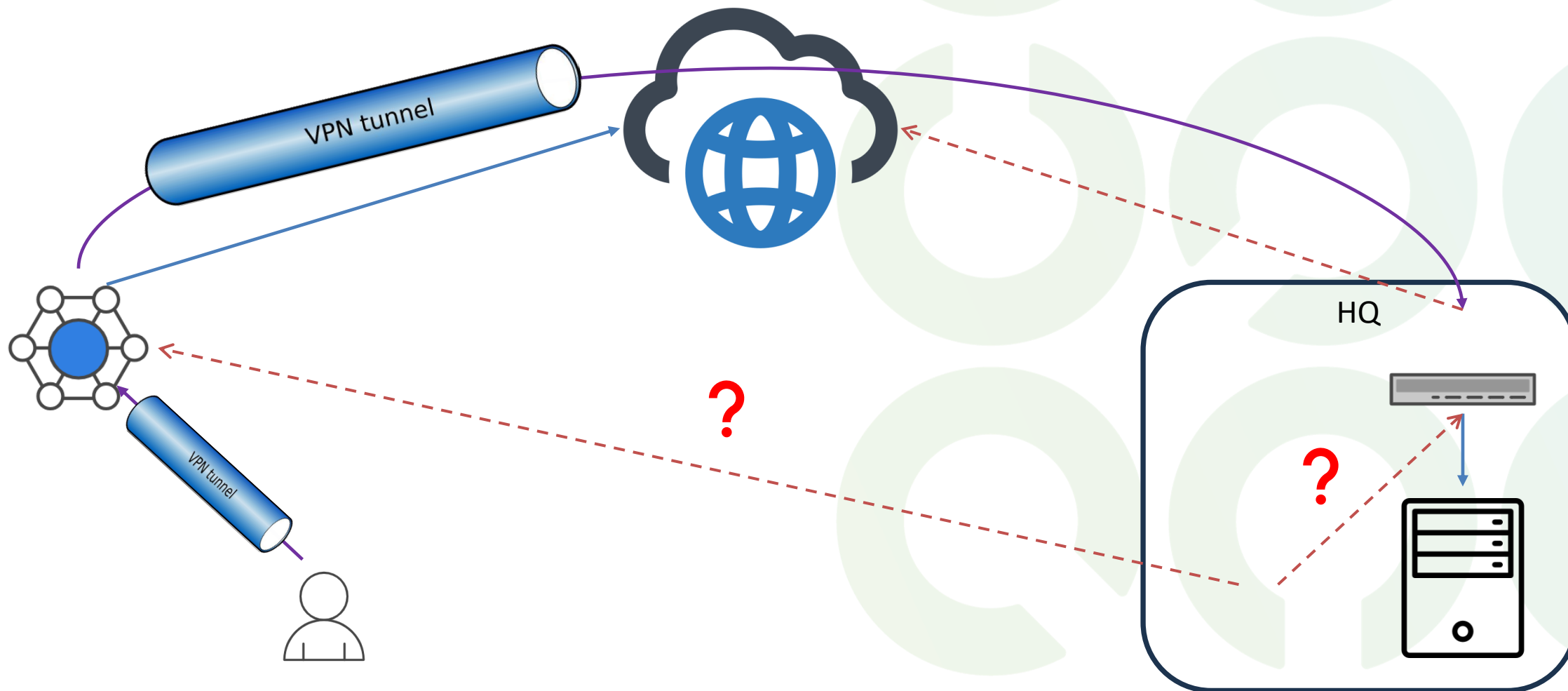
Földrajzilag
legközelebbi PoP



- Nem érünk el geofencing-elte 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.



Kihívások - Távol, vagy az irodában?



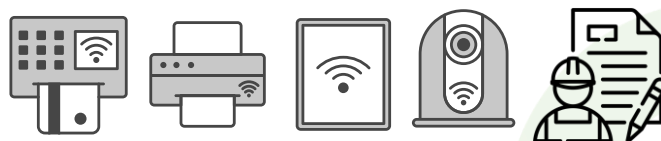
Kihívások

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

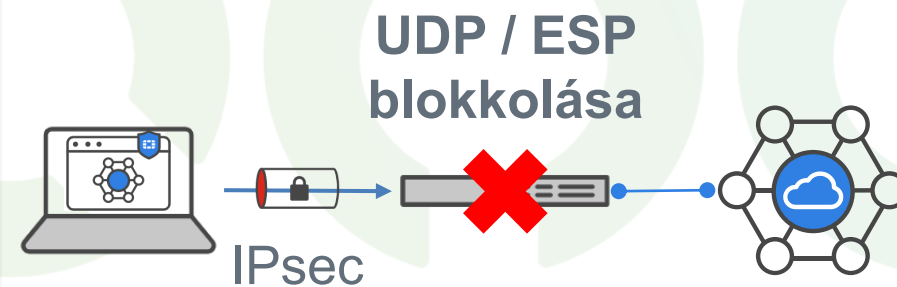
Nem lehet beállításokat végrehajtani a kliensen

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

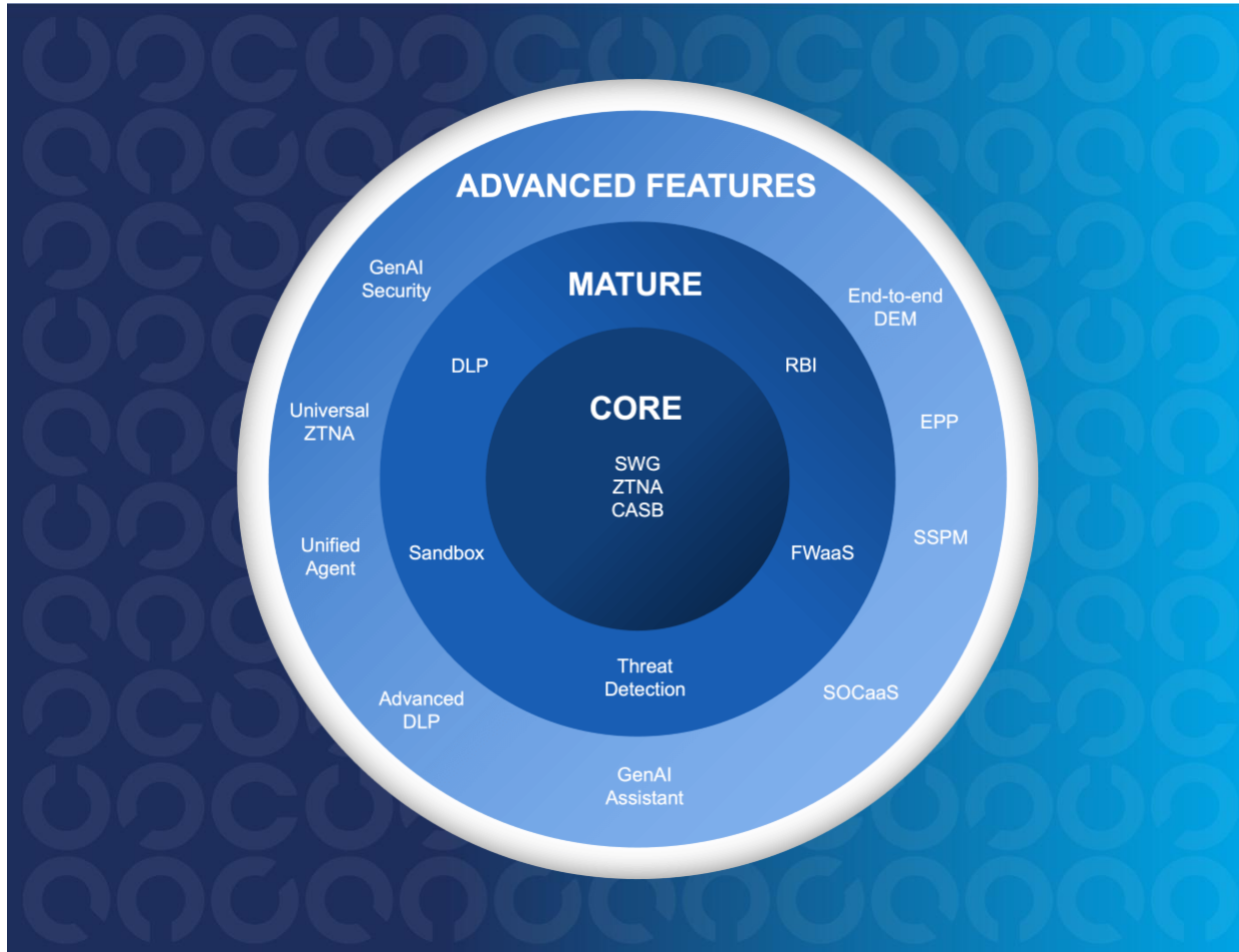


IPsec VPN korlátozása

- 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



Megoldások FortiSASE-val



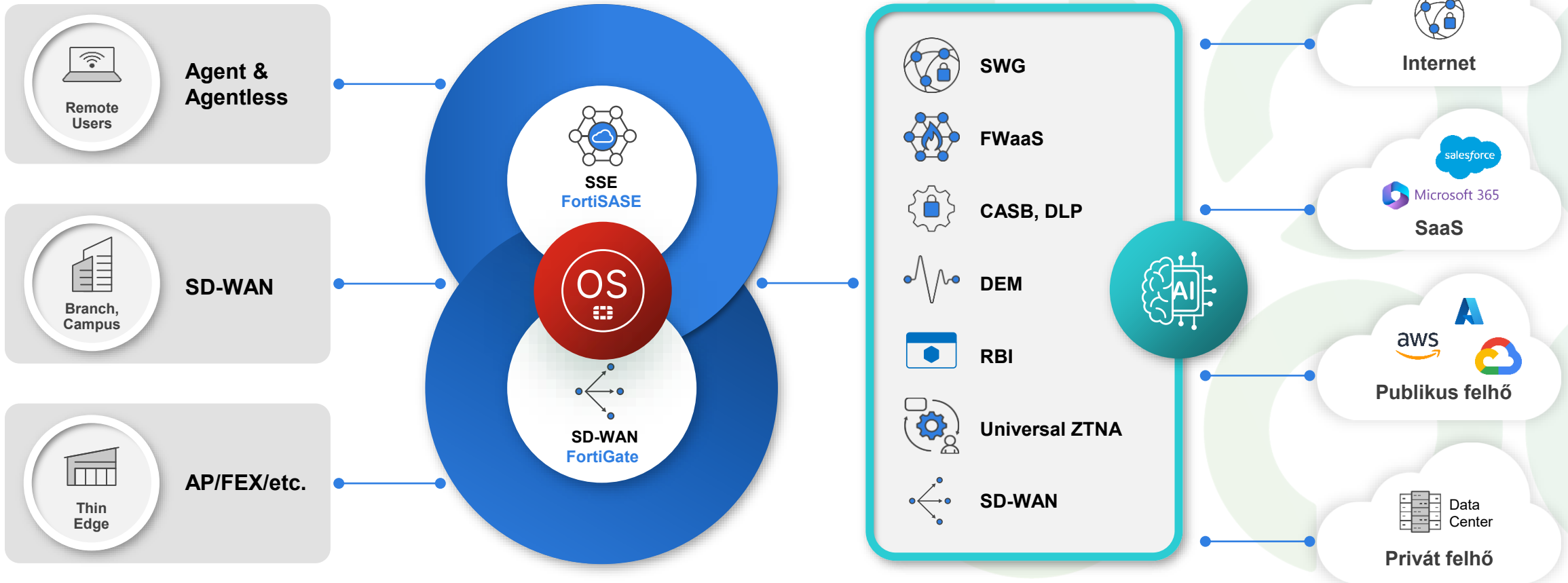
FORTINET



ISACA[®]
Budapest Chapter

Fortinet SASE koncepció

Egységes SASE



FORTINET


Egységes
menedzsment

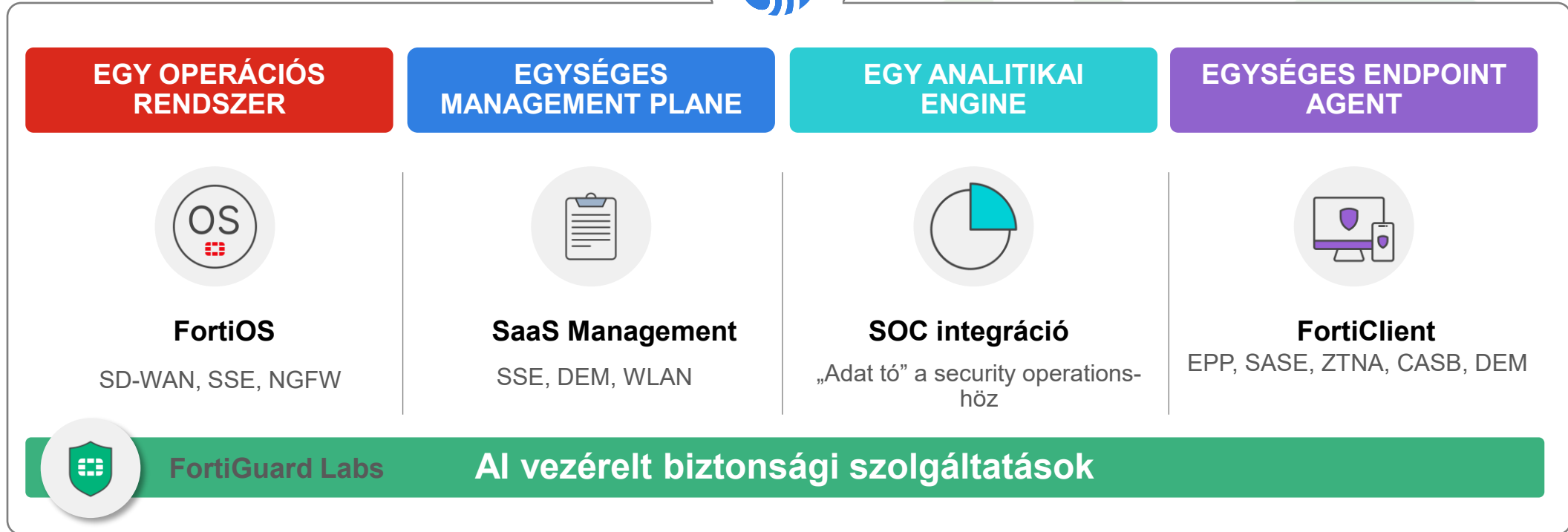

Egységes
Data Lake



ISACA[®]
Budapest Chapter

Megoldások – Egy gyártós (Single Vendor) SASE

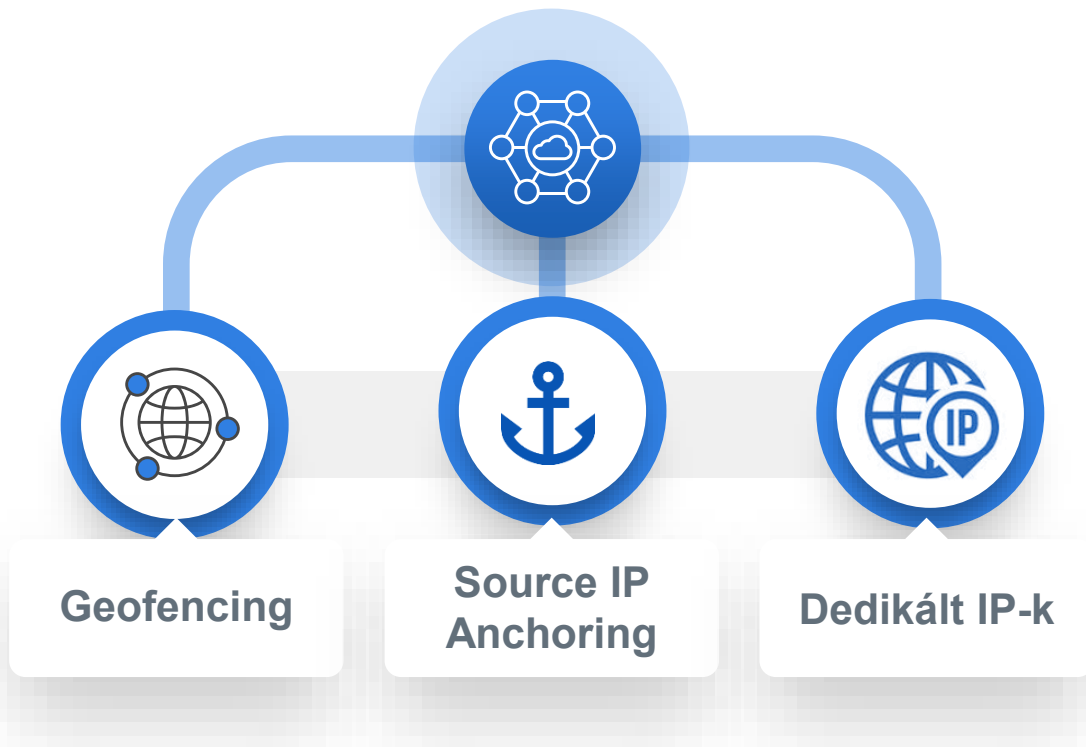
Kihívás: Multi Vendor SASE



- 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

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 megfelelés biztosításához.



Dedikált IP-k

Fenntartott IP-címek, amelyek engedélyezési listára (whiteliste) 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

	Name	Profile Group	Source	Security Posture Tag	User	Destination	Schedule	Action
System defined								
<input type="checkbox"/>	FortiClient logging exemption	Default Internet Access	All Agent Device Traffic		All users	FAZ_PUBLIC_DOMAIN	always	Ac
<input type="checkbox"/>	Threat Feed Deny		all		All users	none	always	De
<input type="checkbox"/>	Botnet Deny		all		All users	Botnet-C&C.Server	always	De
<input type="checkbox"/>	Captive portal access exemption		All Edge Device Traffic		No captive portal authentication required	Captive Portal	always	Ac
<input type="checkbox"/>	Captive portal DNS traffic exemption	Edge device captive portal	All Edge Device Traffic		No captive portal authentication required	All Internet Traffic	always	Ac
Custom								
<input type="checkbox"/>	Allow-All	Default Internet Access	all		All users	All internet Traffic	always	Ac
<input type="checkbox"/>	Users in Italy	Italian Profile	Italy		All users	All internet Traffic	always	Ac
<input type="checkbox"/>	Users in France	French Profile	France		All users	All internet Traffic	always	Ac
<input type="checkbox"/>	Users in Poland	Polish Profile	Poland		All users	All internet Traffic	always	Ac
<input type="checkbox"/>	Implicit Deny		all		All users	All internet Traffic	always	De

Megoldások – Thin Edge eszközök

Kihívás: Nem lehet beállításokat végrehajtani a kliensen



Kisebb helyszínek biztosítása

Kisebb fiókirodák, ideiglenes helyszínek



IoT, OT és agent nélküli eszközök

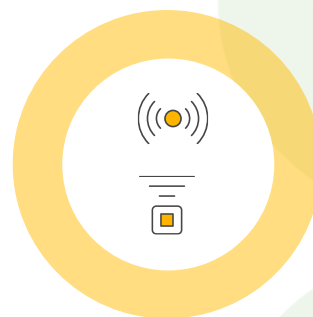
Olyan eszközökre, amikre nem telepíthető agent. (pl. IoT/OT, ATM)



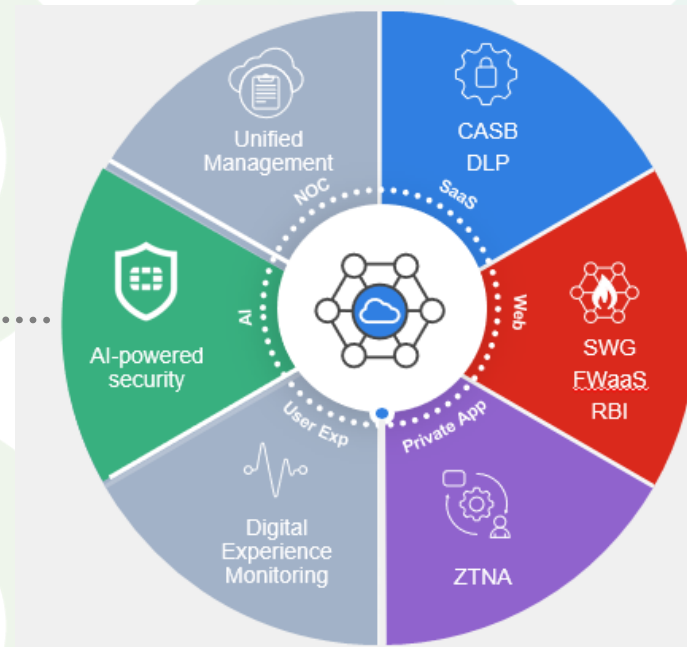
Központi láthatóság és menedzsment

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)

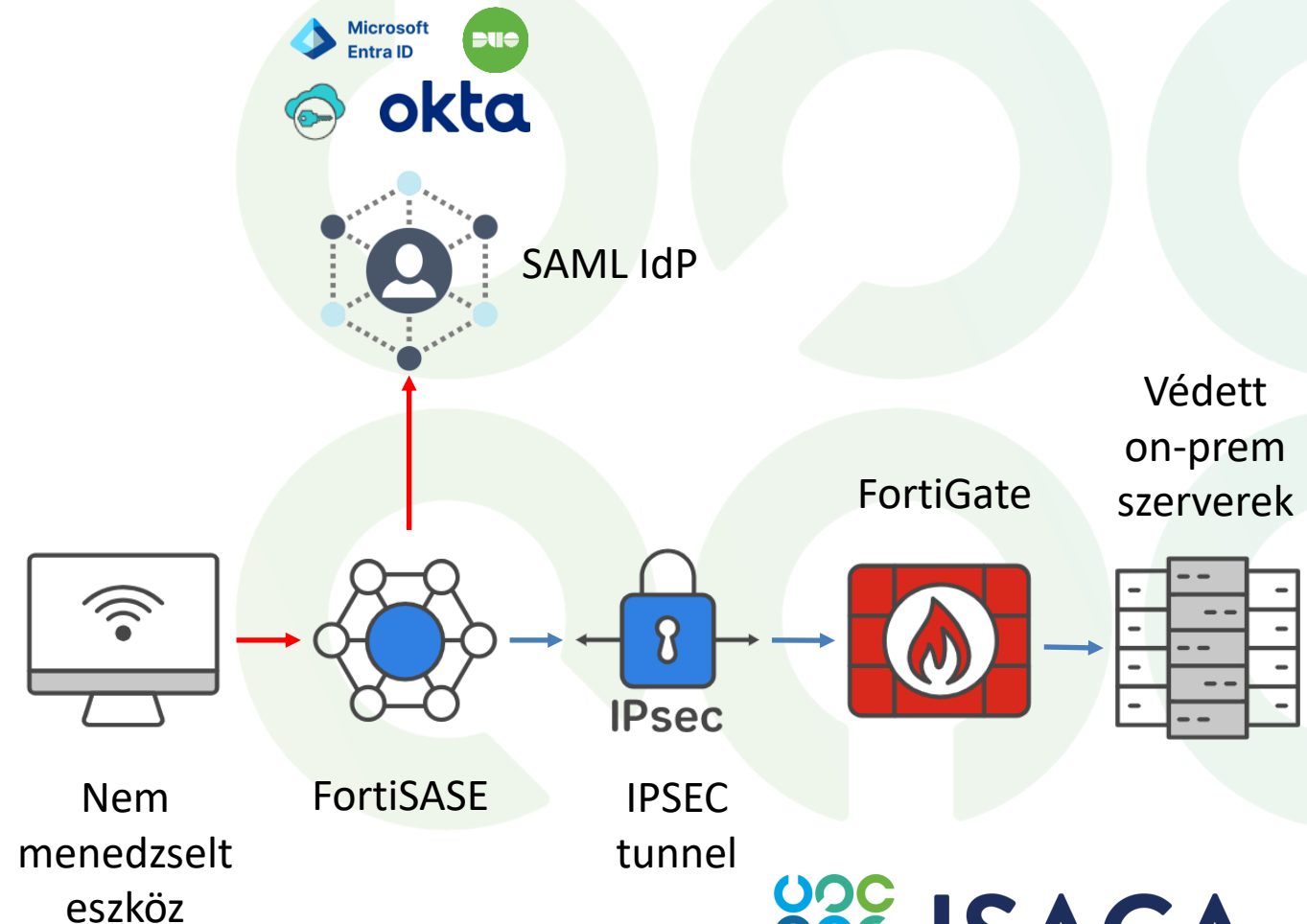


ISACA
Budapest Chapter

Megoldások – Agentless ZTNA

Kihívás: Nem lehet beállításokat végrehajtani a kliensen

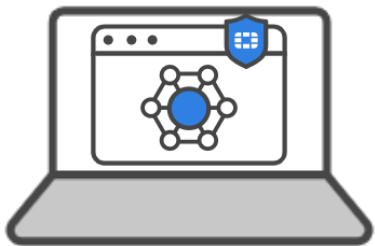
- Nem menedzselhető eszközzel rendelkező felhasználónak (szerződéses, külsős alvállalkozó) biztosít biztonságos hozzáférést.
- Az alkalmazások egy webfelületről indíthatóak
- Felhasználó azonosítás: Hitelesítést kényszerít ki egy SAML IdP felé a távoli felhasználó webböngészőjéből.
- A FortiSASE ZTNA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



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-ből
- A ZTNA kritériumok alapján „megcímkézi” a végpontokat
- A ZTNA címkéket tudjuk használni a szabályrendszerünkben



NEW POLICY

Name

Source Scope All All Agent Devices All Edge Devices

Security Posture Tag

User All Users Specify

Destination All Internet Traffic Specify

Service

Schedule

Action Accept Deny

Status Enable Disable

Log Violation Traffic

Select Entries

Search

ZTNA

- ✖ Android
- ✖ Android_Secure
- ✖ AV
- ✖ Bitlocker
- ✖ BitLocker_Not_Available
- ✖ IOS_Secure
- ✖ Mac_Secure
- ✖ Windows

Megoldások – Azonosítjuk a környezetünket

Kihívás: Távol vagy az irodában?

The image shows a screenshot of the FortiSASE configuration interface, divided into three main sections:

- EDIT RULE SET:** Shows the configuration for a rule set named "IN_HQ". The "Endpoint is connecting from a trusted location when it:" section is active, with the option "Receives a successful HTTP(S) 200 OK response from a known server" selected. The "HTTP(S) server IP addresses" field contains "192.168.18.41". Other options like "Use HTTPS", "Connects with a known public IP", "Is connected to a known DNS server", "Makes a successful query to a known DNS server", "Is connected to a known DHCP server", "Connects from a known local subnet", and "Can ping a known server" are all disabled.
- ENDPOINT PROFILE:** Shows the configuration for the "IN_HQ" endpoint profile. The "Run posture check before initiating FortiSASE Cloud Security tunnel" option is enabled. The "On/off-net Settings" section shows "On/off-net detection" is enabled and "On-net rule set" is set to "IN_HQ". Other options like "Exempt endpoint from FortiSASE auto-connect when endpoint is on-net", "Allow local LAN access when endpoint is on-net", "Allow local LAN access when endpoint is off-net", and "Lockdown endpoint when off-net" are all disabled. The "Steering bypass destinations" section is expanded, showing a table of destinations:

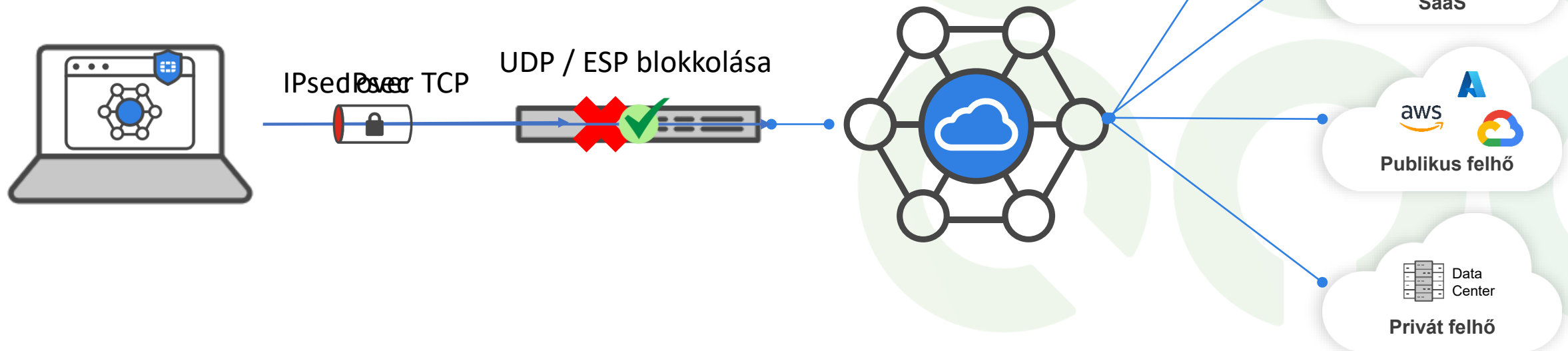
Match	Apply condition
FQDN	
google.com	On-net
Infrastructure	
Amazon-AWS	On-net
Local Application	
update_task.exe	Both
Subnet	
192.168.18.0/24	On-net

The "Steering bypass destinations" section is highlighted with a red box. The "On/off-net detection" toggle is also highlighted with a red box.

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





KÖSZÖNÖM A FIGYELMET!