GetCon

MEGBÍZHATÓ KAPCSOLAT

Tűzfal üzemeltetés DevNet alapokon

Papp Ádám

Rendszermérnök

papp.adam@getcon.hu

+36-20-495-9289

Tartalomjegyzék

GetCon
MEGBÍZHATÓ KAPCSOLAT

Célkitűzés: tűzfal egy ideális világban

Célkitűzés

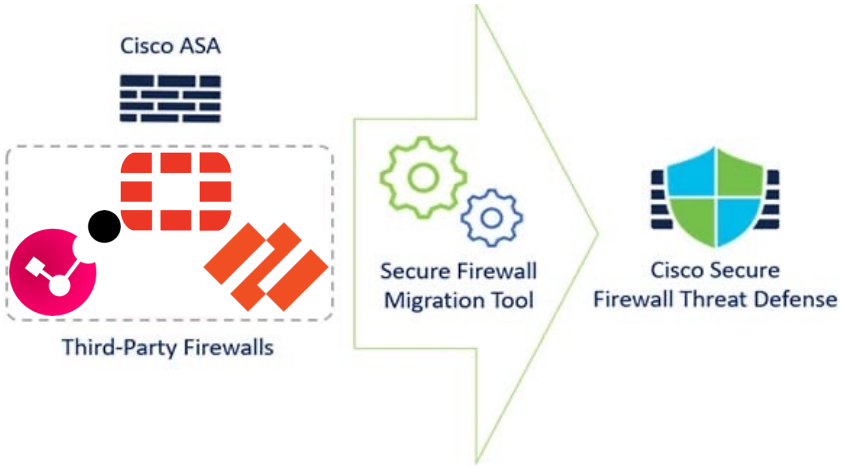
GetCon
MEGBÍZHATÓ KAPCSOLAT

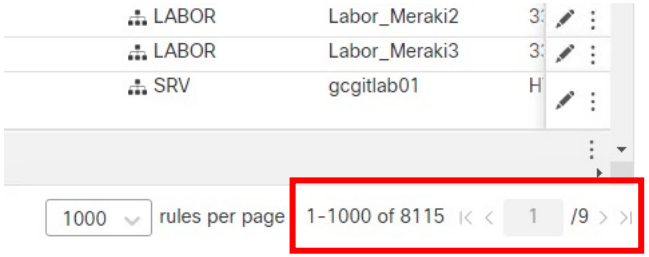
Tűzfal egy ideális világban

Kihívás: migrációs és üzemeltetési nehézségek

Nehézségek - Migráció

- Firepower Migration Tool
  - nem tökéletes
  - nem támogat bármilyen tűzfalat
- Terjedelmes konfiguráció
- Korábbi tűzfal más elven működik mint a Cisco





Nehézségek – üzemeltetés

Alkalmazás üzemeltető

Honnan tudjam mit és hogyan csinál a tűzfal?!

Alkalmazás térkép?!

Honnan tudjam hogyan működik az alkalmazás?!

Hálózat üzemeltető

Csak menjen, bármi áron!

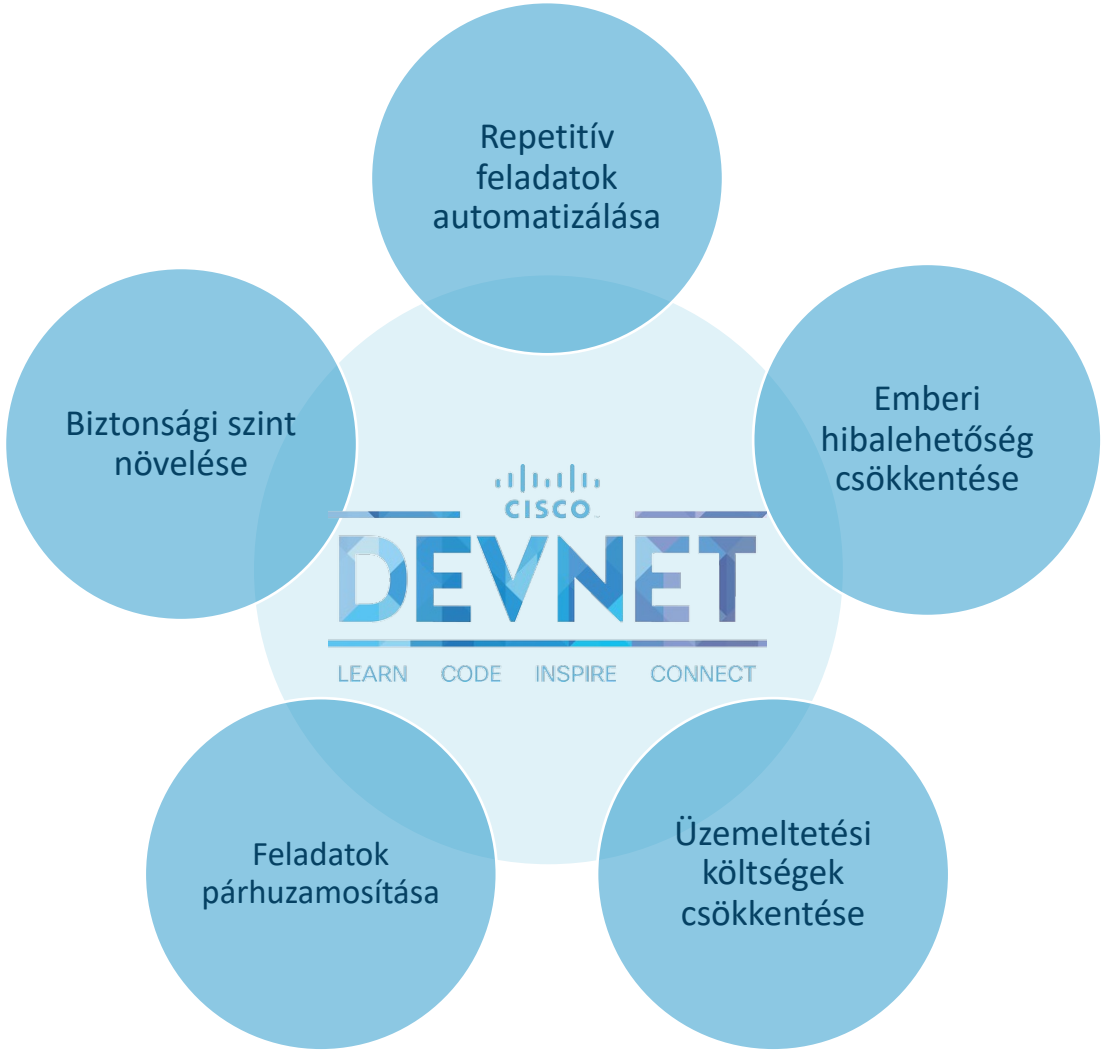
Kész van már? Tegnapra kell!

És mi hasznosat csináltál 2 napig!?

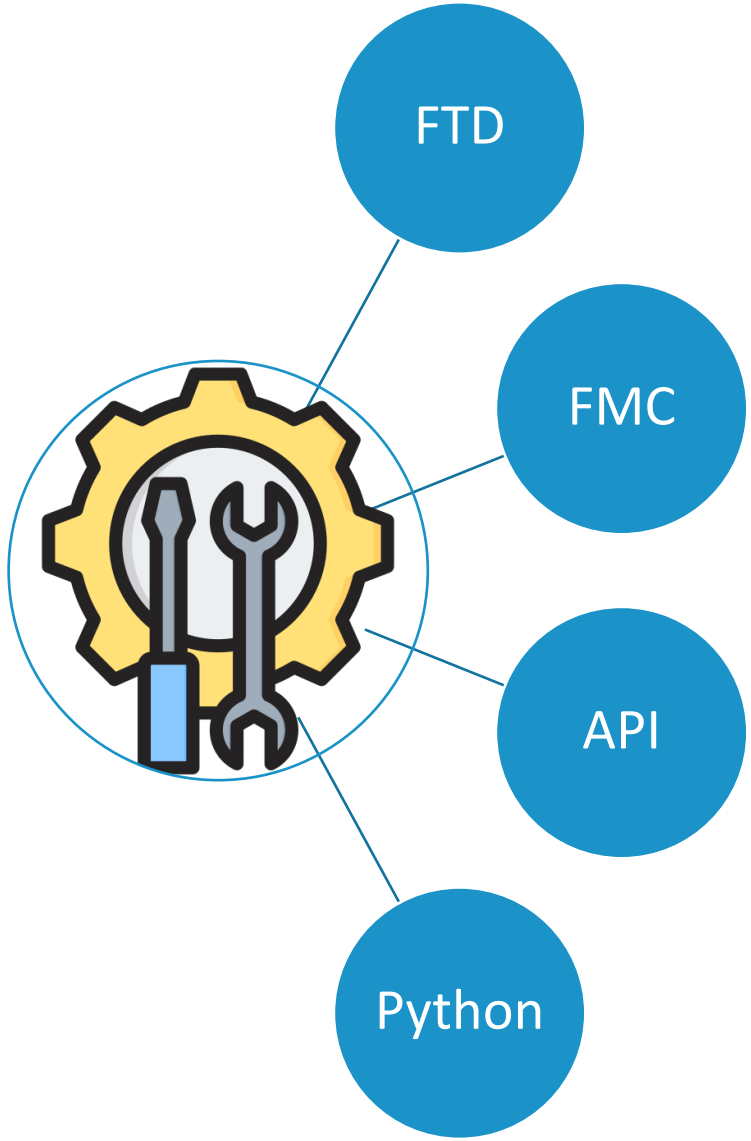
Megoldás: DevNet szerepe a securityben

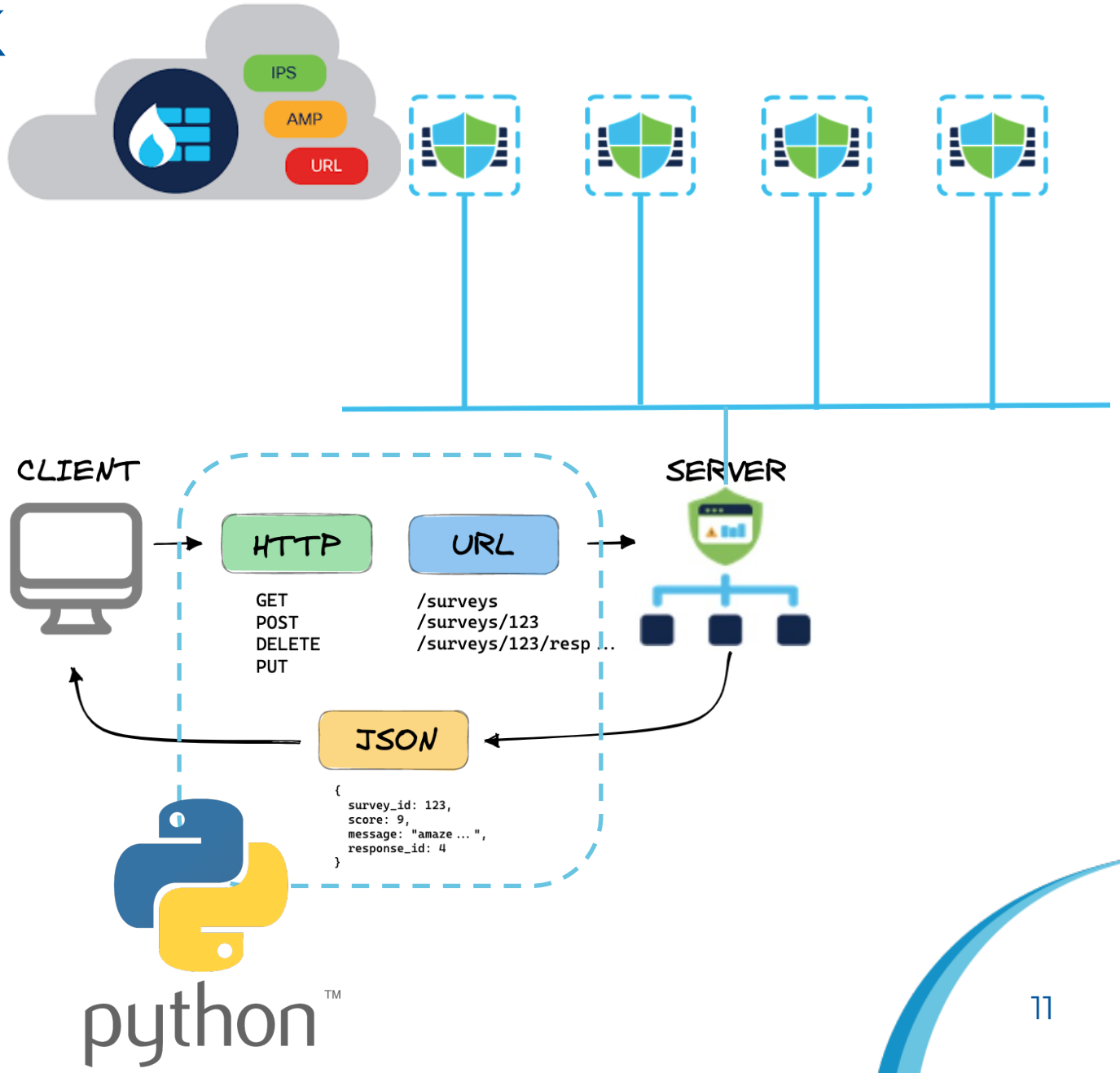
Mi az a DevNet? Miért jó?

Developing & *Networking* → **DevNet** ≈ hálózat automatizáció



Felhasznált eszközök

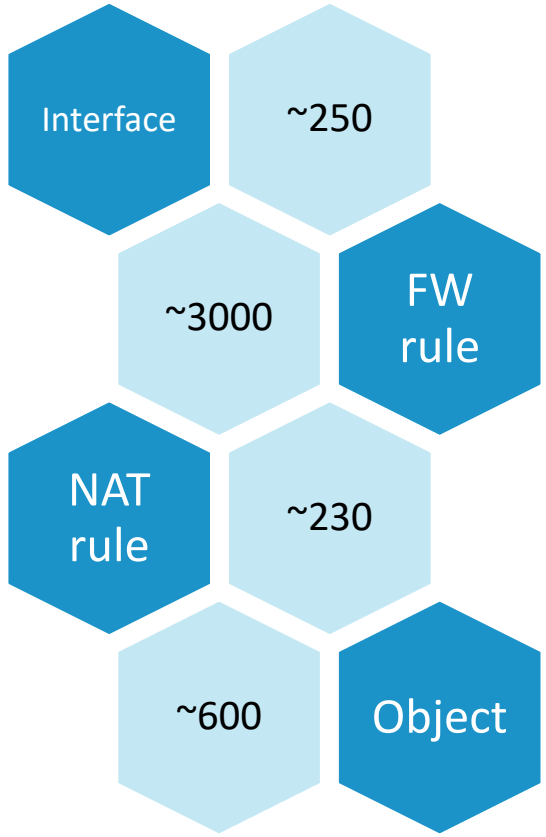




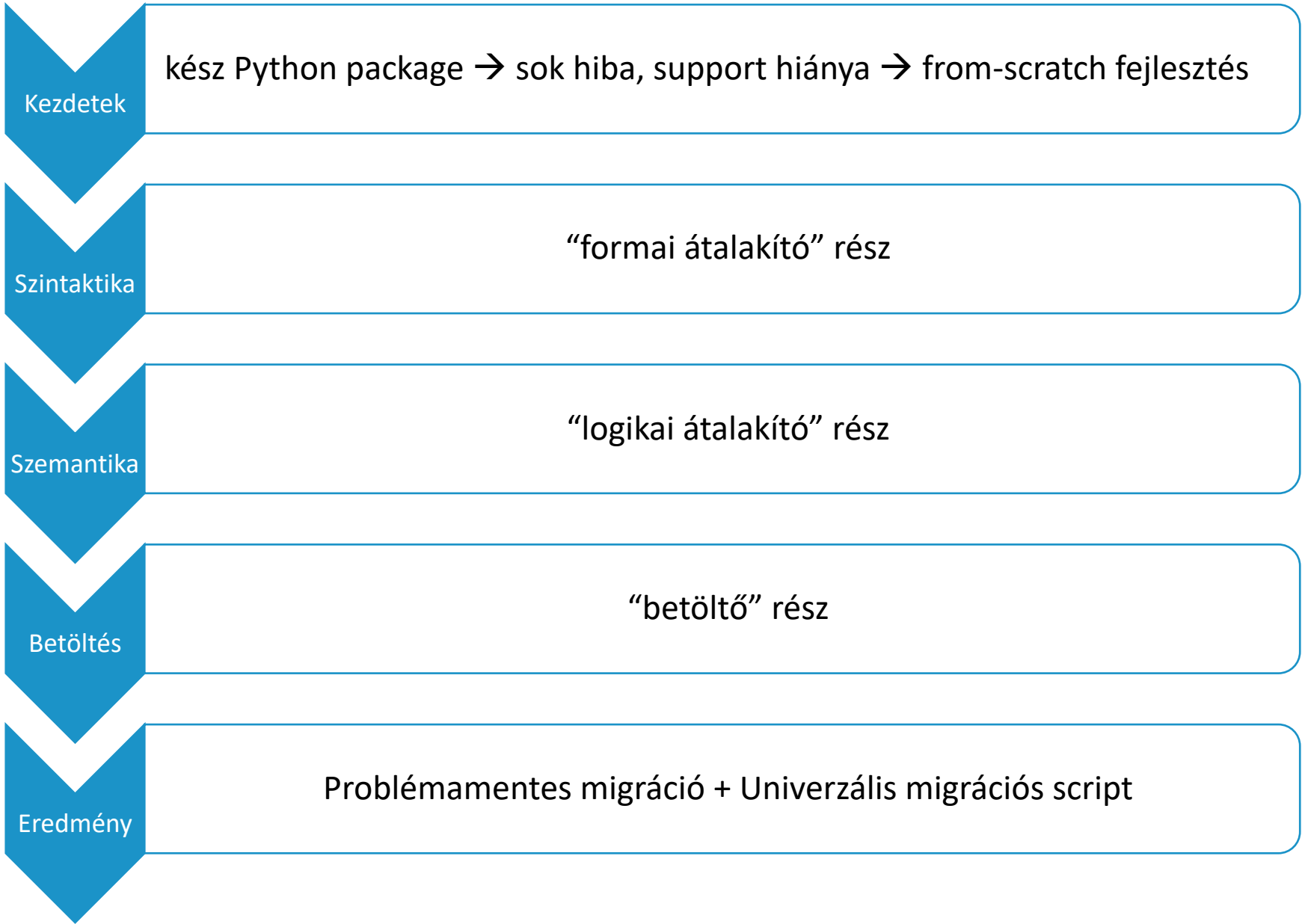
Case study 1: tűzfal migrációk

Case study 1a: pfSense migráció

- **Ügyfél:** több kulturális intézményt összefogó kiterjedt szervezet
- **Típus:** pfSense
- **Funkciók:** internet edge és belső FW, VPN koncentrátor (all-in-one)



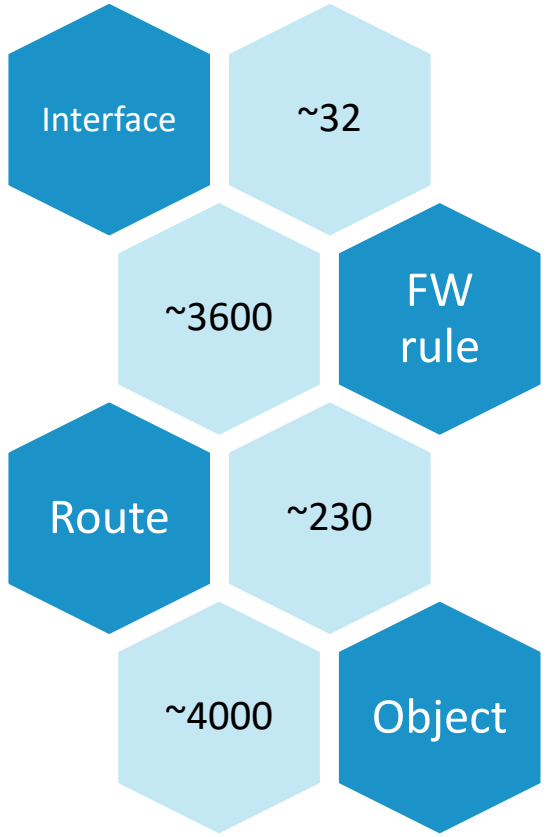
Case study 1a: pfSense migráció



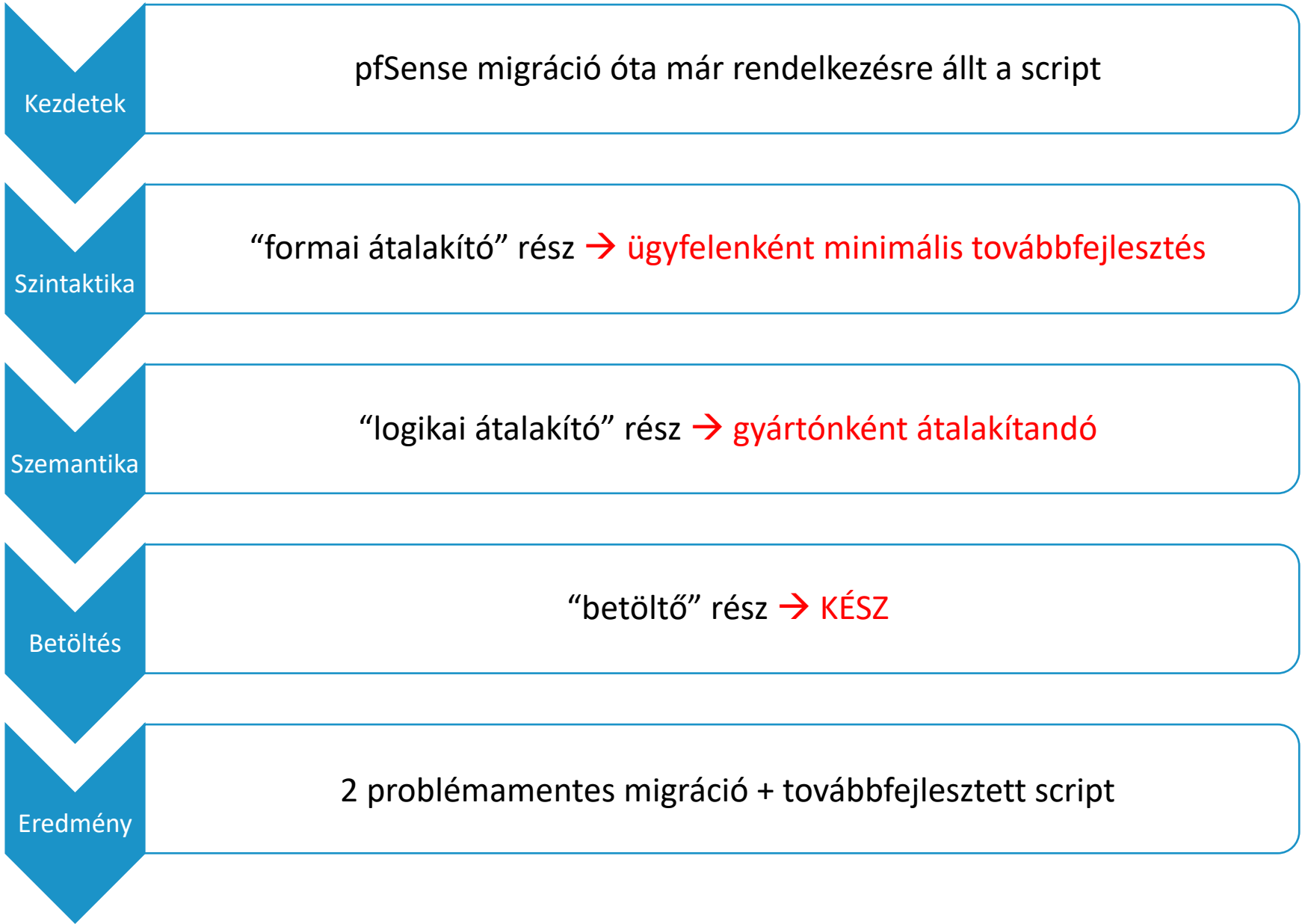
GetCon
MEGBÍZHATÓ KAPCSOLAT

Case study 1b: iptables migráció

- **Ügyfél:** erősen kritikus kormányzati szerv
- **Típus:** iptables
- **Funkciók:** 2 backend (belső) tűzfalpár



Case study 1b: iptables migráció

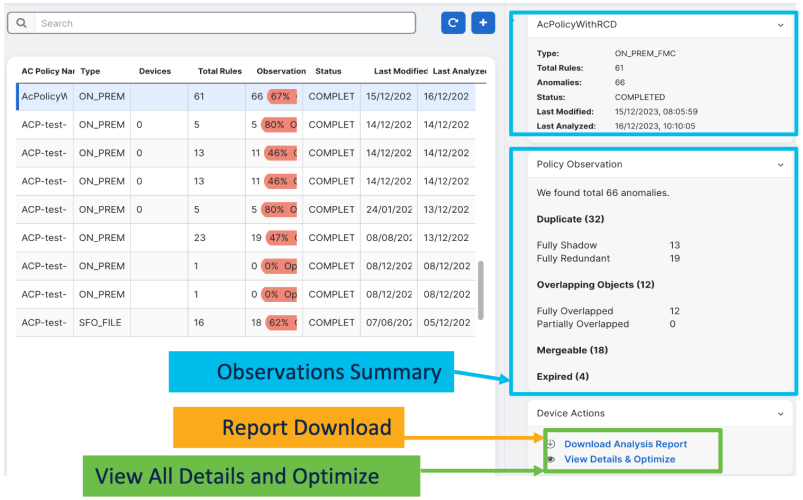


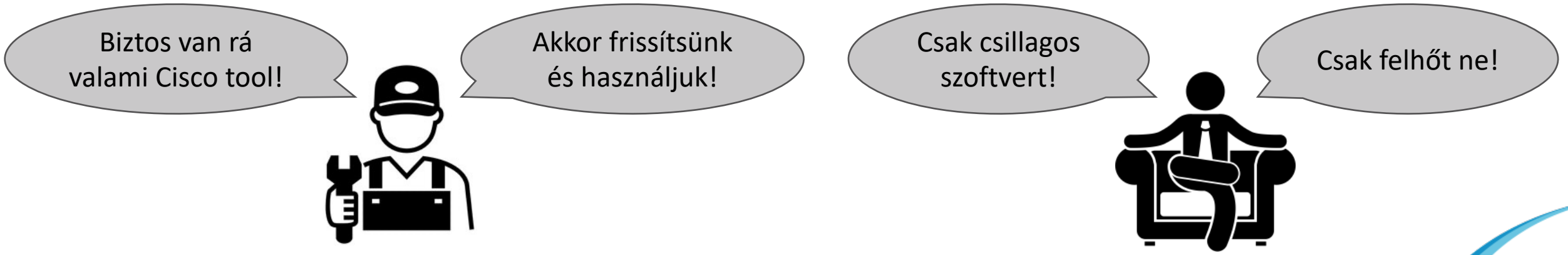
GetCon
MEGBÍZHATÓ KAPCSOLAT

Case study 2: szabályrendszer elemzés

Szabálylrendszer elemzés

- Korábban nem létező feature
- FMC 7.6+: Policy Analyzer & Optimizer (PAO)
- Hátrányok:
  - túl friss szoftver, jelenleg nem ajánlott verzió
  - aktív felhő kapcsolat szükséges





Case study 2: szabályrendszer elemzés

- GetCon saját fejlesztés!
- Paraméterezhető integrált Python software.
- https://github.com/GetCon-Hungary/fmc-analyser

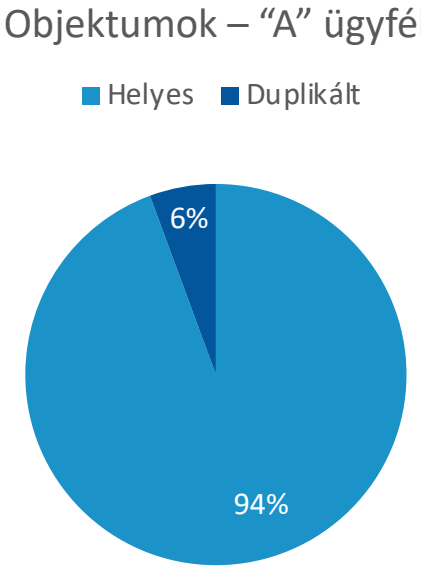
	Name	Duplicated	Reversed	Merge Candidates
108	alf_7			alf_8
109	alf_8			alf_7
110	alf_9			alf_10
111	alf_10			alf_9
112	alf_284	alf_321		alf_285, alf_321, alf_322
113	alf_285	alf_322		alf_284, alf_321, alf_322
114	alf_286	alf_323		alf_287, alf_323, alf_324
115	alf_287	alf_324		alf_286, alf_323, alf_324
116	alf_321	alf_284		alf_284, alf_285, alf_322
117	alf_322	alf_285		alf_284, alf_285, alf_321

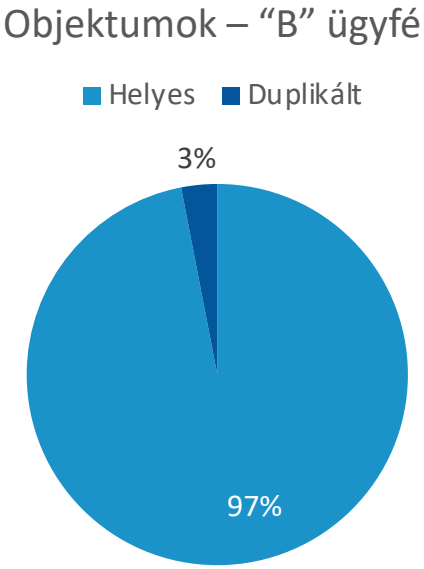
Akkor ezt most le kell fejlesztenem magamnak?

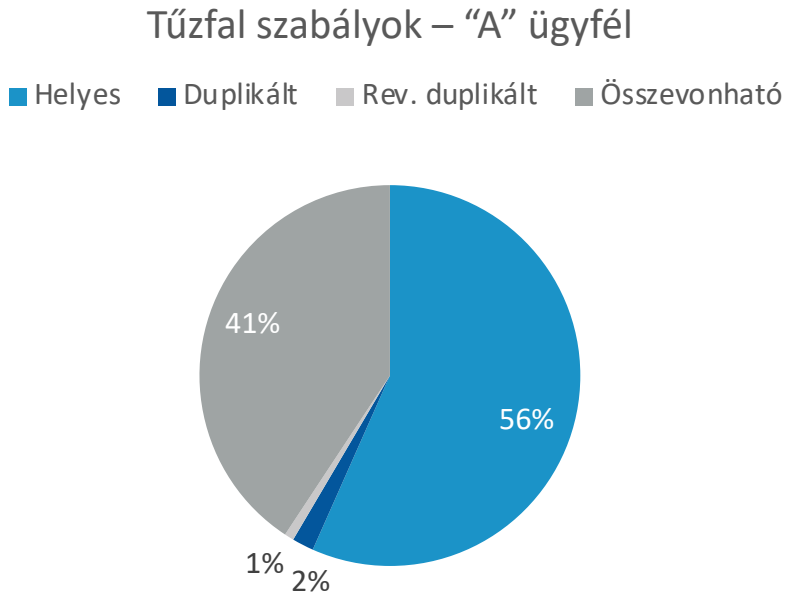
Biztosan egy vagyonba kerül!

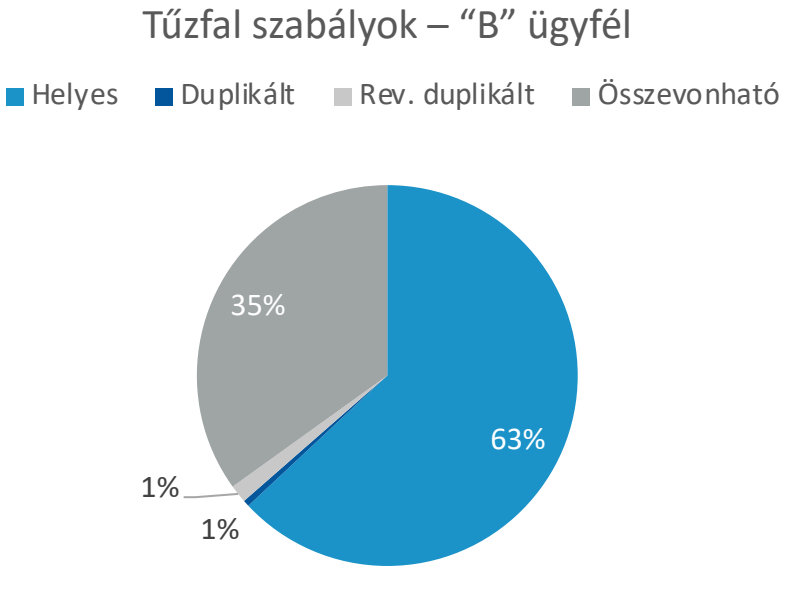
GetCon
MEGBÍZHATÓ KAPCSOLAT

Case study 2: szabályrendszer elemzés







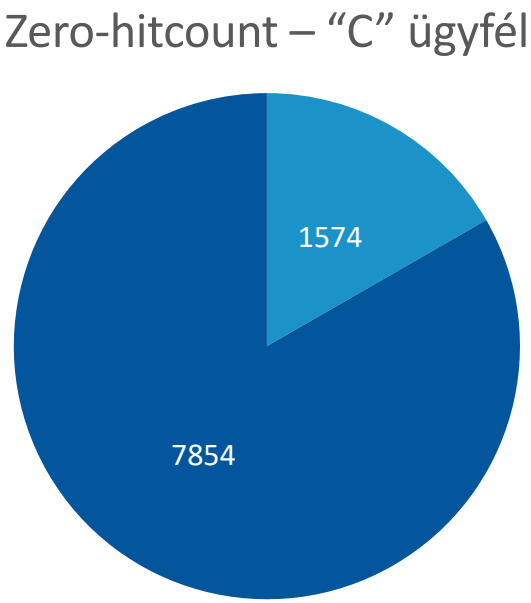


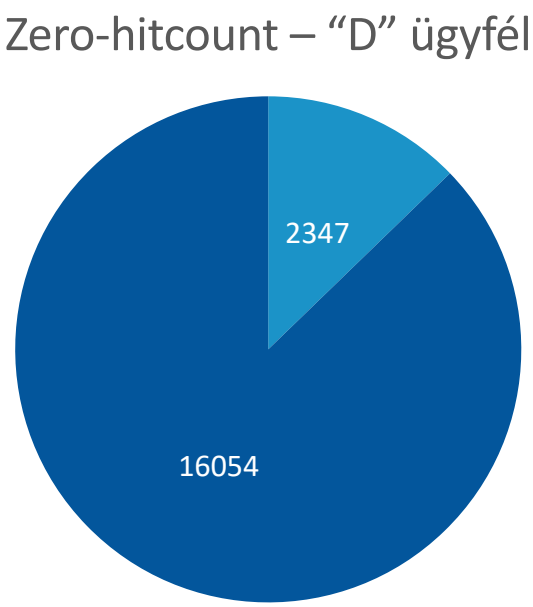
GetCon
MEGBÍZHATÓ KAPCSOLAT

Case study 3: szabályrendszer konszolidáció

Case study 3: szabályrendszer konszolidáció

- Többszörösen migrált, régóta használt tűzfalak
- Sosem/régóta nem használt szabályok
- Szabályok legyűjtése, letiltása, majd törlése
- Táblázatos riport a módosításokról
- Eredmények: **82,69-87,25% (!)**





Összefoglalás

Összefoglalás

- Migráció: sokszor megkerülhetetlen a DevNet.
- Üzemeltetés: könnyíti, humán erőforrást szabadít fel, biztonsági szintet kövel.
- Nincs license vagy eszköz bekerülési költsége.

Bármi megoldható, ami nem, arra ott a DevNet.

Fejlesztési lehetőségek

GetCon
MEGBÍZHATÓ KAPCSOLAT

Köszönöm a figyelmet!

Papp Ádám

Rendszermérnök

papp.adam@getcon.hu

+36-20-495-9289