



Tűzfal üzemeltetés DevNet alapokon



Papp Ádám

Rendszermérnök

papp.adam@getcon.hu

+36-20-495-9289

Tartalomjegyzék

- 1 **Célkitűzés: tűzfal egy ideális világban**
- 2 **Kihívás: migrációs és üzemeltetési nehézségek**
- 3 **Megoldás: DevNet szerepe a securityben**
- 4 **Esettanulmányok: migráció, elemzés, konszolidáció**
- 5 **Összefoglalás**

Célkitűzés: tűzfal egy ideális világban

Célkitűzés



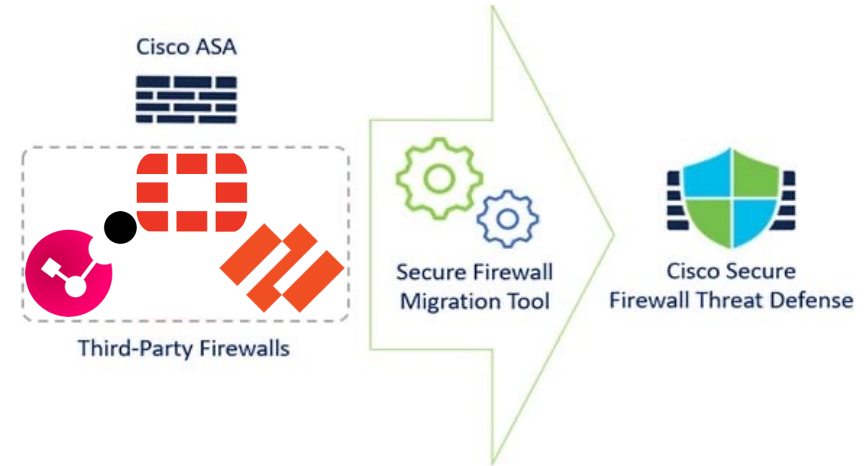
Tűzfal egy ideális világban



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



LABOR	Labor_Meraki2	3	
LABOR	Labor_Meraki3	3	
SRV	gcgitlab01	H	

1000 rules per page 1-1000 of 8115 << 1 /9 >>

Biztos van rá valami
Cisco tool!



Akkor gyorsan
összekattintjuk!

Nehézségek – üzemeltetés



Alkalmazás üzemeltető

Honnan tudjam mit és hogyan csinál a tűzfal?!

Honnan tudjam hogyan működik az alkalmazás?!

Alkalmazás térkép?!



Hálózat üzemeltető

Csak menjen, bármi áron!

Kész van már?
Tegnapra kell!

És mi hasznosat csináltál 2 napig!?



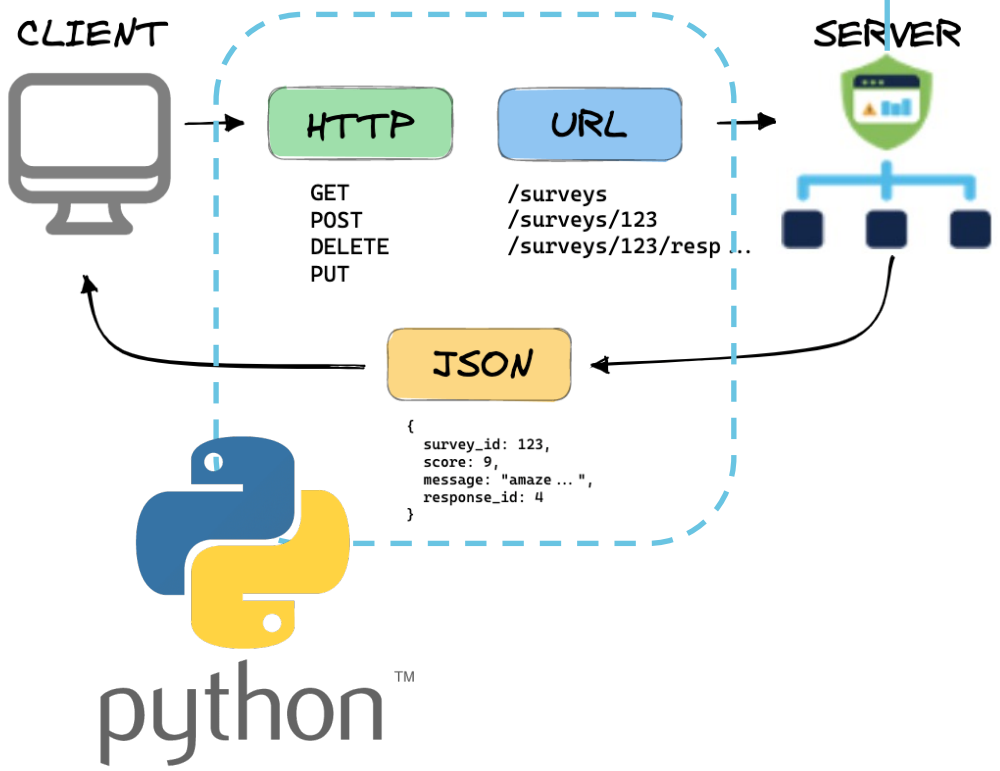
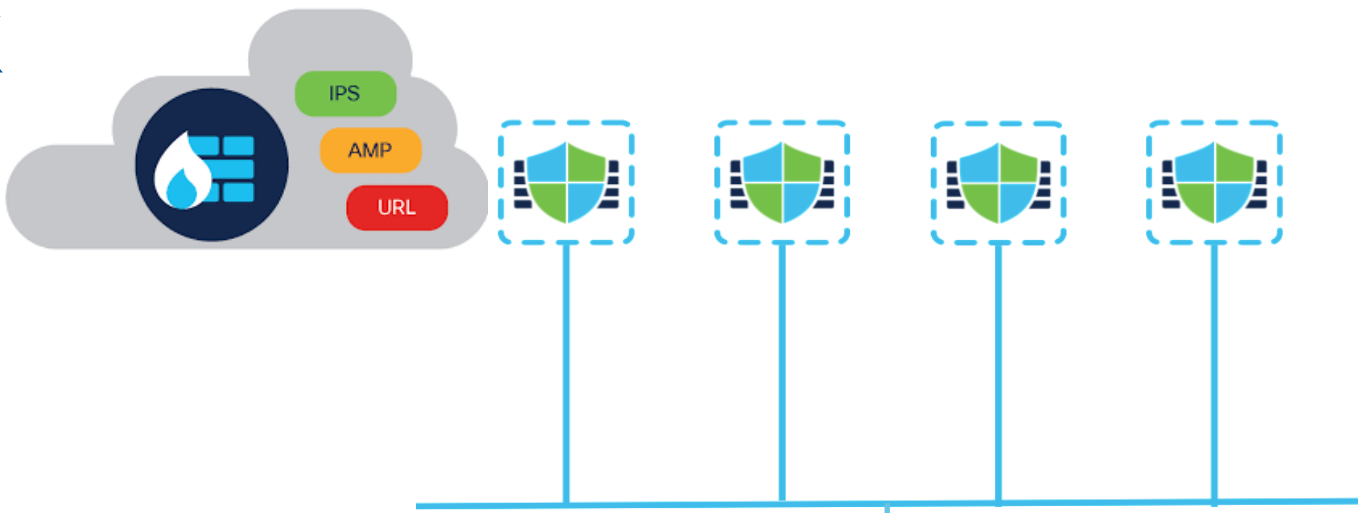
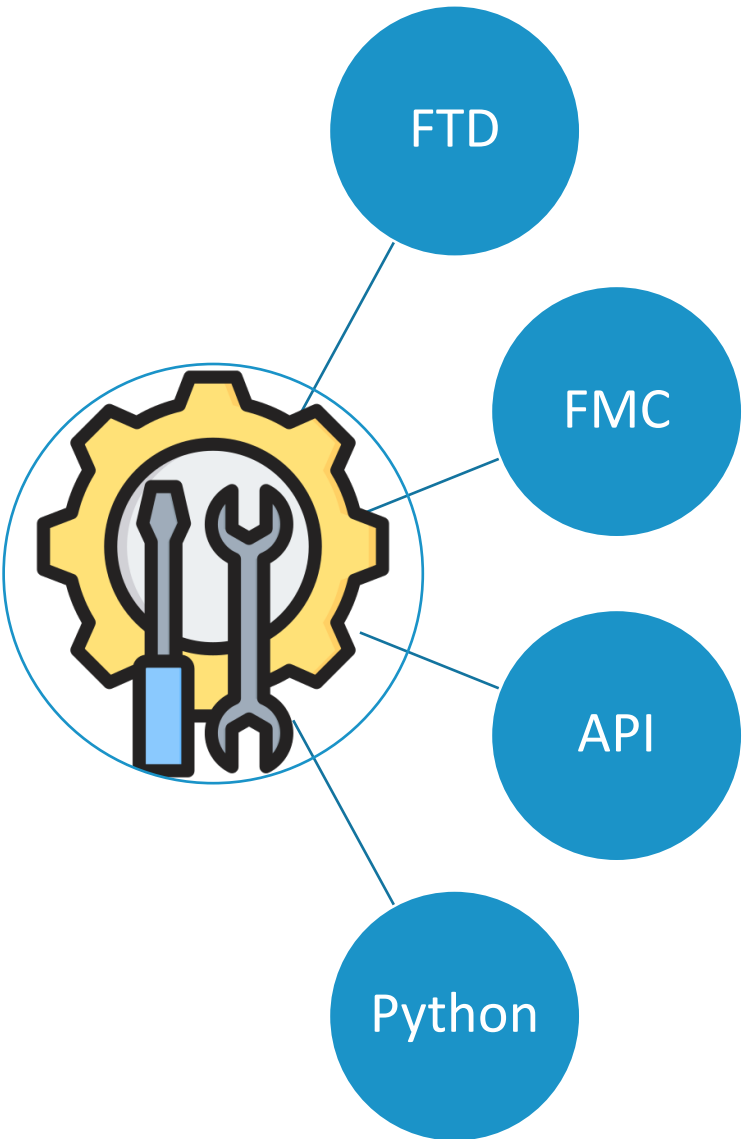
Megoldás: DevNet szerepe a securityben

Mi az a DevNet? Miért jó?

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



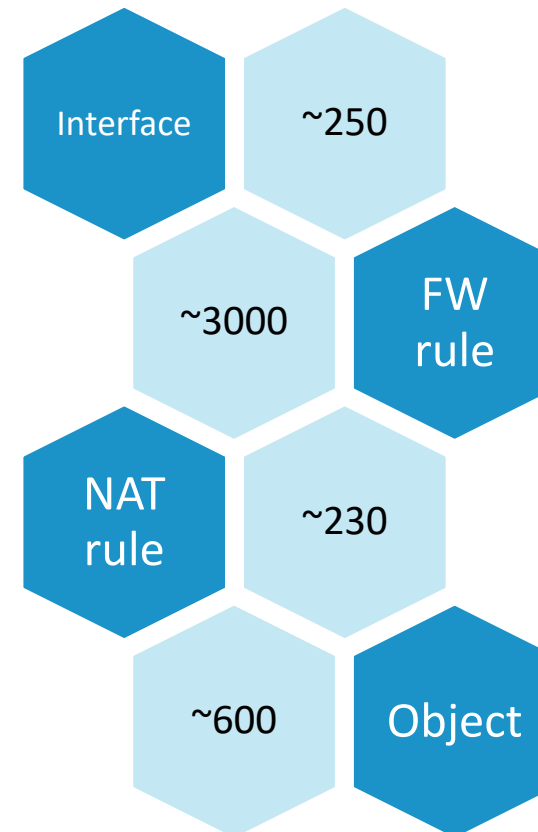
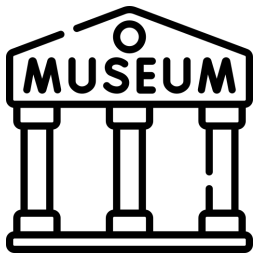
Felhasznált eszközök



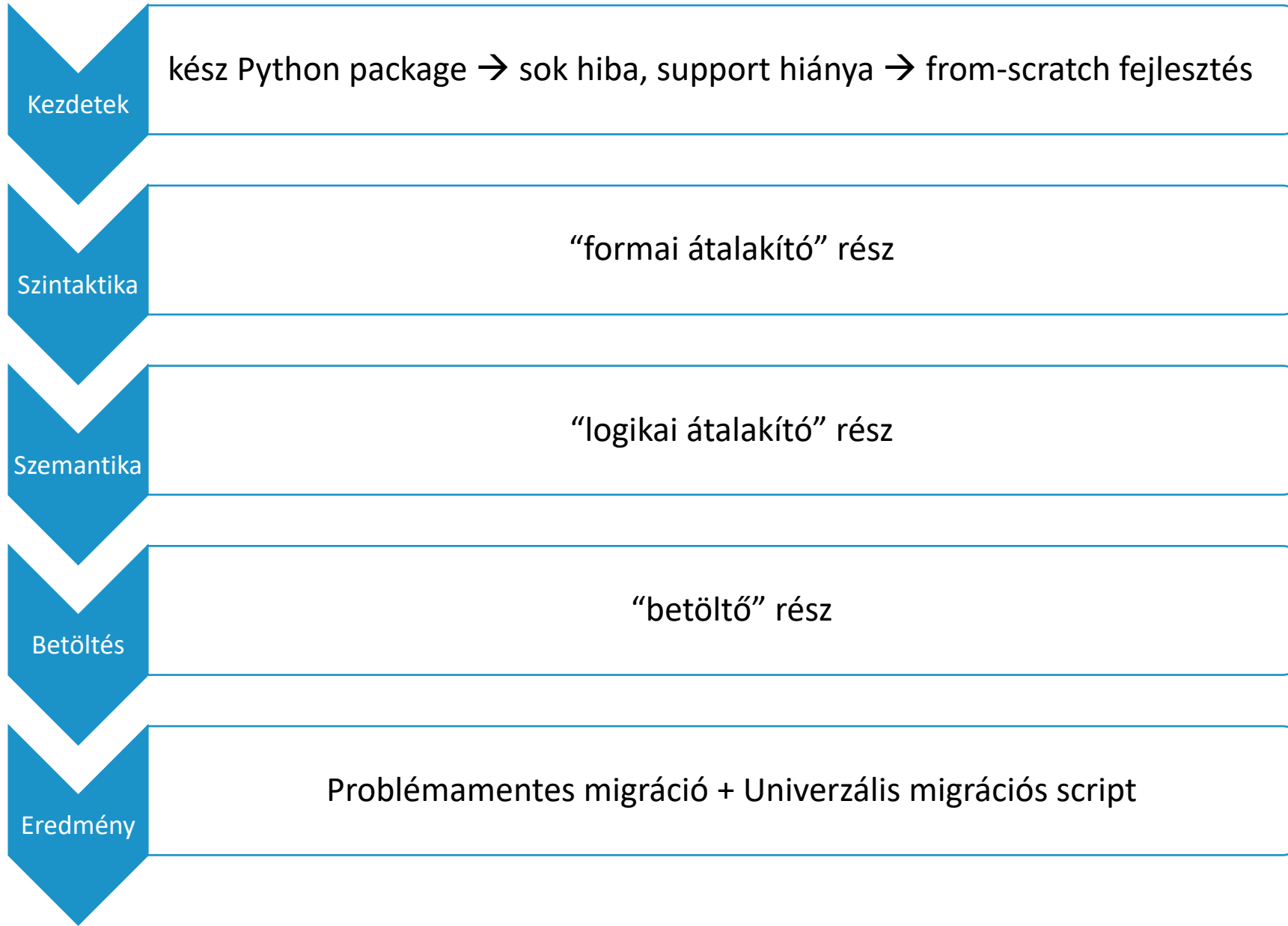
Case study 1: tűzfal migrációk

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)

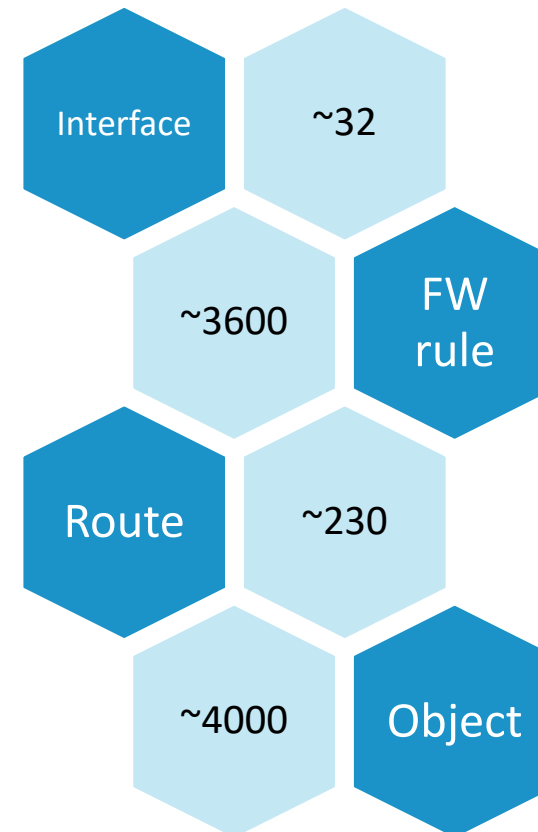


Case study 1a: pfSense migráció

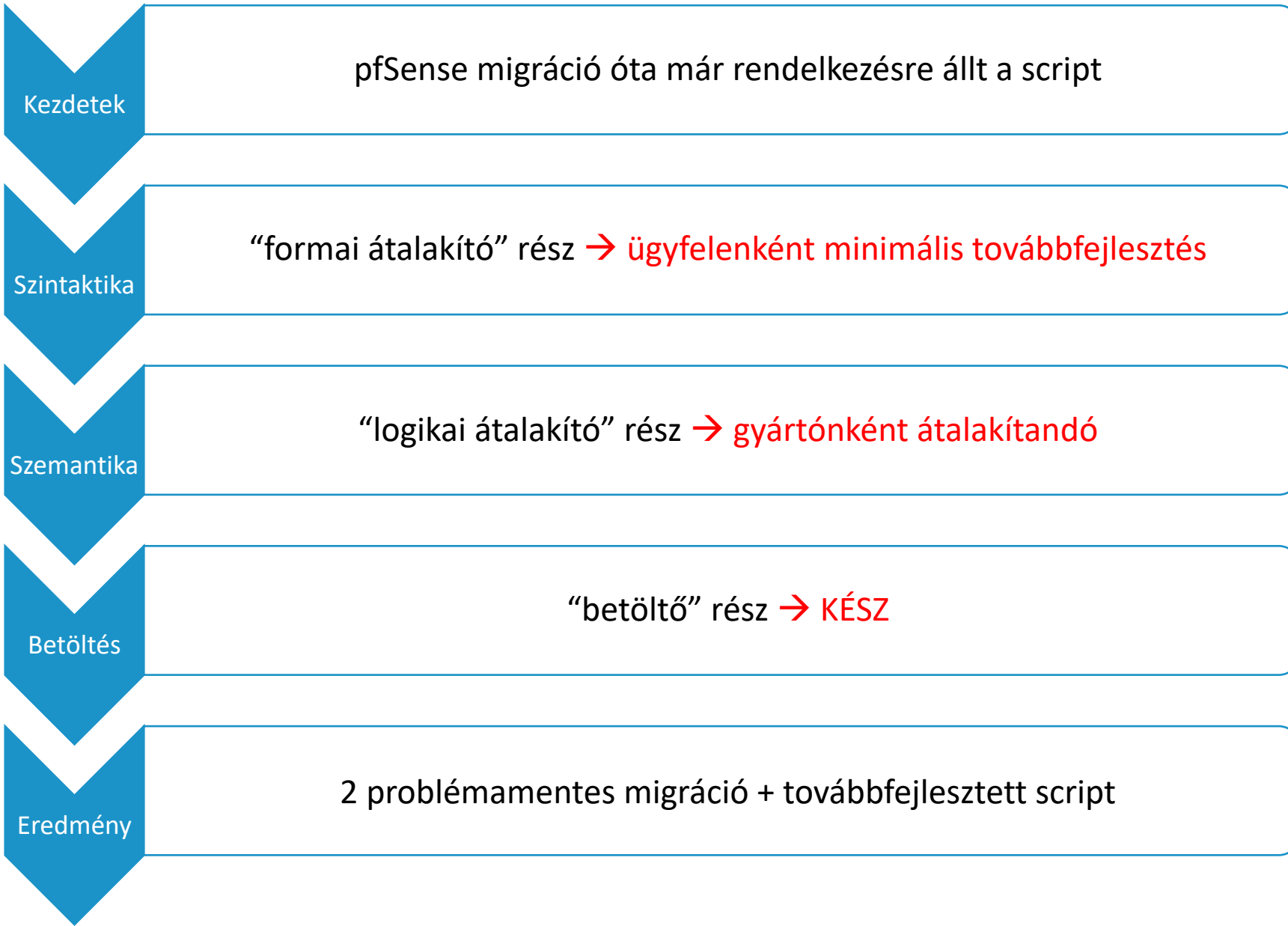


Case study 1b: iptables migráció

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



Case study 1b: iptables migráció



Case study 2: szabályrendszer elemzés

Szabályrendszer elemzés

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

AC Policy Name	Type	Devices	Total Rules	Observation	Status	Last Modified	Last Analyzed
AcPolicyV	ON_PREM		61	66 67%	COMPLET	15/12/202	16/12/202
ACP-test-	ON_PREM	0	5	5 80%	COMPLET	14/12/202	14/12/202
ACP-test-	ON_PREM	0	13	11 86%	COMPLET	14/12/202	14/12/202
ACP-test-	ON_PREM	0	13	11 86%	COMPLET	14/12/202	14/12/202
ACP-test-	ON_PREM	0	5	5 80%	COMPLET	24/01/202	13/12/202
ACP-test-	ON_PREM		23	19 47%	COMPLET	08/08/202	13/12/202
ACP-test-	ON_PREM		1	0 0%	COMPLET	08/12/202	08/12/202
ACP-test-	ON_PREM		1	0 0%	COMPLET	08/12/202	08/12/202
ACP-test-	SFO_FILE		16	18 82%	COMPLET	07/06/202	05/12/202

Observations Summary: 66 anomalies

Duplicate (32): Fully Shadow (13), Fully Redundant (19)

Overlapping Objects (12): Fully Overlapped (12), Partially Overlapped (0)

Mergeable (18): Expired (4)

Device Actions: Download Analysis Report, View Details & Optimize

Biztos van rá valami Cisco tool!



Akkor frissítsünk és használjuk!

Csak csillagos szoftvert!



Csak felhőt ne!

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
118	alf_323	alf_286		alf_286, alf_287, alf_324

Akkor ezt most le kell fejlesztenem magamnak?

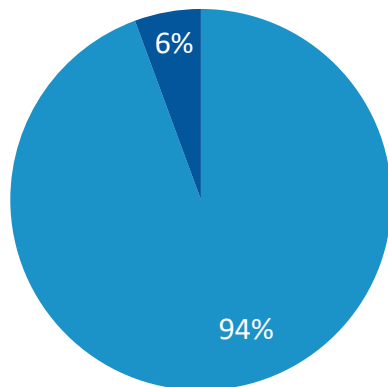


Biztosan egy vagyomba kerül!

Case study 2: szabályrendszer elemzés

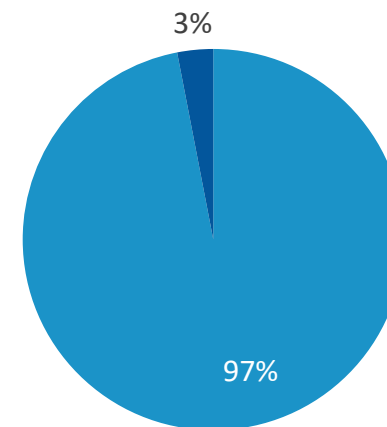
Objektumok – “A” ügyfél

■ Helyes ■ Duplikált



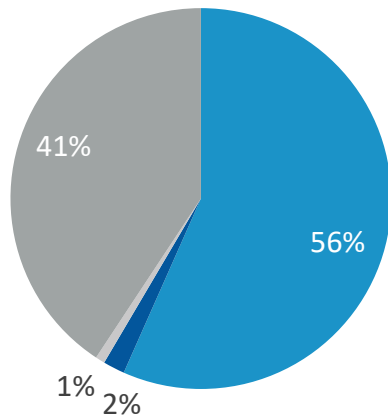
Objektumok – “B” ügyfél

■ Helyes ■ Duplikált



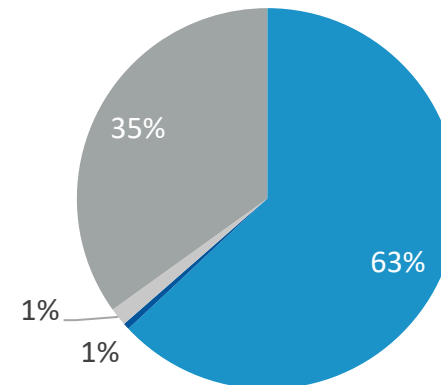
Tűzfal szabályok – “A” ügyfél

■ Helyes ■ Duplikált ■ Rev. duplikált ■ Összevonható



Tűzfal szabályok – “B” ügyfél

■ Helyes ■ Duplikált ■ Rev. duplikált ■ Összevonható

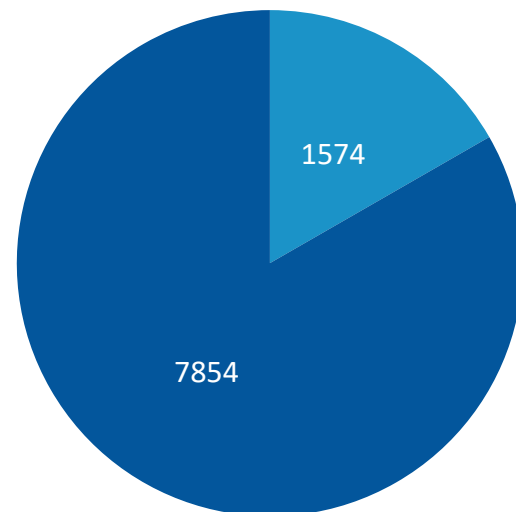


Case study 3: szabályrendszer konszolidáció

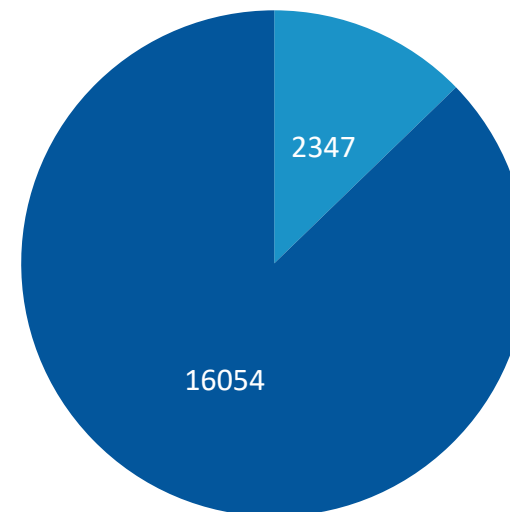
Case study 3: szabályrendszer konszolidáció

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

Zero-hitcount – “C” ügyfél



Zero-hitcount – “D” ügyfél



Összefoglalás

Összefoglalás

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

Bármí megoldható, ami nem, arra ott a DevNet.

Fejlesztési lehetőségek



Köszönöm a figyelmet!



Papp Ádám

Rendszermérnök

papp.adam@getcon.hu

+36-20-495-9289