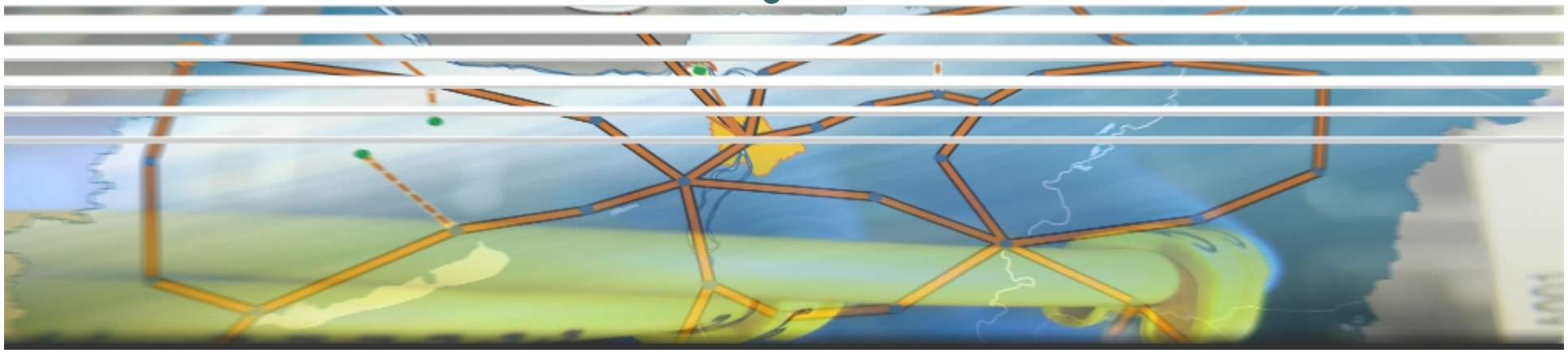
Változások a Sulinet szűrési szabályokban



02/06/15

Timár Zsolt

Jelenlegi szűrés

- Az internet felől alapértelmezetten csak bizonyos portok vannak nyitva, minden más zárva van
- A belső hálózatokon alapértelmezetten csak bizonyos portok vannak tiltva, minden más engedélyezve van

- Két módszer van:
  - CBAC (Context-based Access Control)
  - ZBF (Zone-based Firewall)

CBAC felépítése

- Hátrányai
  - Cisco már nem támogatja
  - Nem minden protokollt/parancsot támogat (pl. STARTTLS)
- Előnyei
  - Könnyen átlátható, kezelhető
  - Régebbi verziójú IOS-en is implementálható (pl. Cisco 1711)

CBAC felépítése (folytatás)

- Szükségesek hozzá:
  - Szűrést végző ACL-ek
  - `ip inspect name #NÉV# #protokoll#` globális parancs
  - `ip inspect name #NÉV# in | out` parancs az interfészen
  - `ip access-group #ACL-NÉV# in | out` parancs az interfészen

CBAC működése

- Az ip inspect parancs miatt a router session táblát tart karban
- A session tábla miatt, ha egy olyan csomagot kap a router, ami egy belső, privát tartománybeli kérésre válasz, akkor a router automatikusan beengedi ezt a válaszcsomagot annak ellenére, ha a bejövő interfészen lévő ACL mindent tiltana

CBAC működése (folytatás)

- Az interfészeken lévő szűrőlistákkal (ACL) lehet szabályozni azt, hogy mit kezdjen a router az egyes csomagokkal:
  - Mivel a belső hálózatnál alapértelmezetten csak bizonyos portok vannak zárva, minden más pedig nyitva van, így itt annak van értelme, ha további tiltásokat veszünk fel
  - Az internet felőli interfészen alapértelmezetten minden port zárva van és csak a 25, 80, 443-as portok vannak nyitva, így itt további portok megnyitására van lehetőség (Dashboardon pl.)

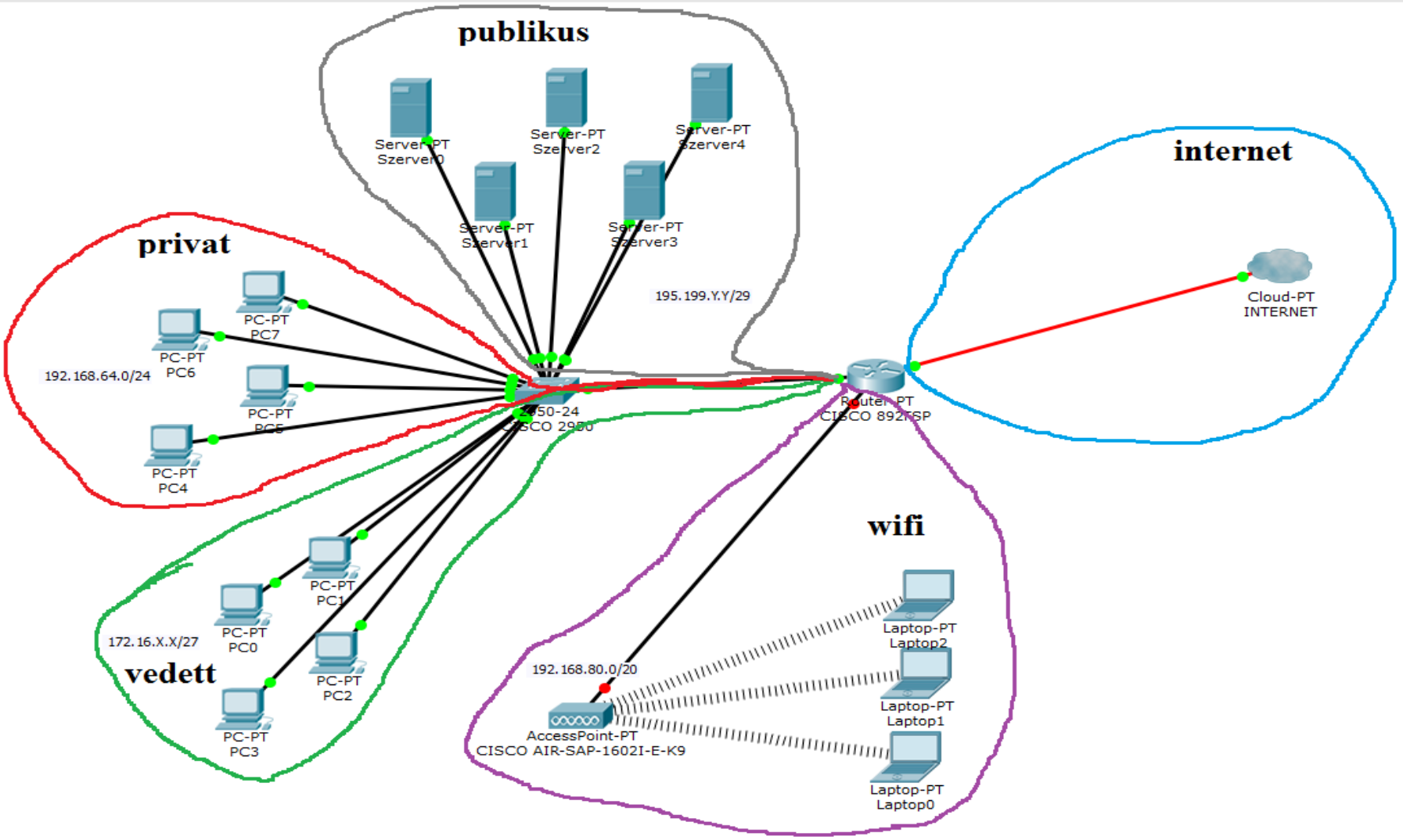
ZBF felépítése

- Hátrányai
  - Nehezebb átlátni, mint a CBAC-et
  - Bonyolultabb a különböző zóna-párok miatt
  - 15-ös verziójú IOS-től elérhető (pl. 892FSP)
- Előnyei
  - A Cisco által ajánlott és támogatott
  - Több protokollt/parancsot képes kezelni, mint a CBAC
  - Alkalmazás-szinten (Layer 7) is tud szűrni

ZBF felépítése (folytatás)

- Szükségesek hozzá
  - Zónák
  - Zóna-párok
  - Class-map-ek
  - Policy-map-ek
  - Service-policy-k
  - Opcionálisan ACL-ek

Példa-topológia



ZBF zónák, zóna-párok

- A zónáknak nevet kell adni; ez alapján a név alapján lehet majd később rájuk hivatkozni (egy interfész csak egyetlen zónába tartozhat)
- A zóna-párok azért szükségesek, hogy bizonyos forrás zónából induló- és bizonyos célzónába érkező csomagokra különböző szabályokat lehessen meghatározni
- Azonos zónák között, illetve zónák nélküli interfészek között alapértelmezetten engedélyezett a kommunikáció

ZBF zónák, zóna-párok (folytatás)

- Különböző zónák között alapértelmezetten nem engedélyezett a kommunikáció, amennyiben nincs policy konfigurálva az adott zóna-párhoz (ha van, akkor az adott policy lép életbe)

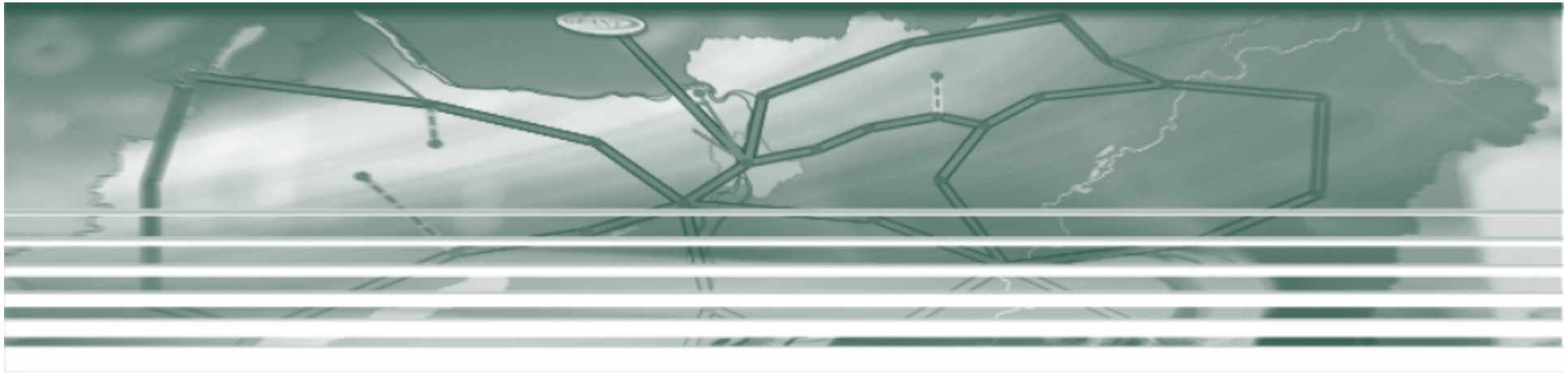
Class-map, policy-map, service-policy

- A class-map-pel lehet meghatározni, hogy mely csomagokat figyelje a router
- A policy-map meghatározható, hogy mi történjen az adott forgalommal (pass, inspect, drop, log)
- A service-policy paranccsal alkalmazható az adott policy-map zónapár-konfigurációs módban

Hogyan tovább?

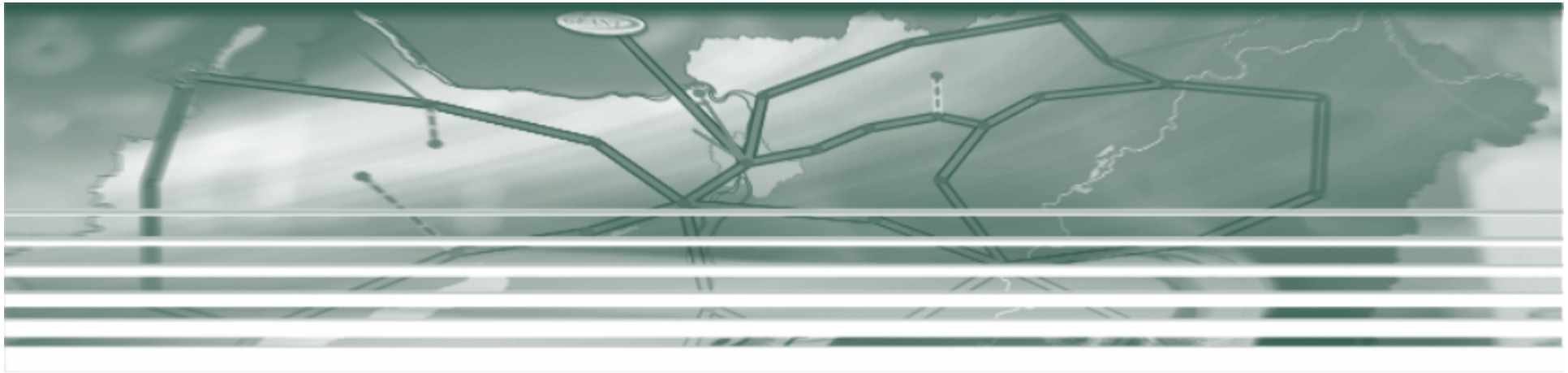
- A korábbi tűzfal-szabályok nem vesznek majd el: átkonvertálásra kerülnek úgy, hogy a ZBF értelmezni tudja majd őket
  - néhány esetben nem megoldható a konvertálás
- Lehetőség lesz majd IPv6 alapú szűrésekre is
  - emiatt a Sulinet Dashboard-on is változtatni kell

Kérdések?



Timár Zsolt

Köszönöm a figyelmet!



Timár Zsolt