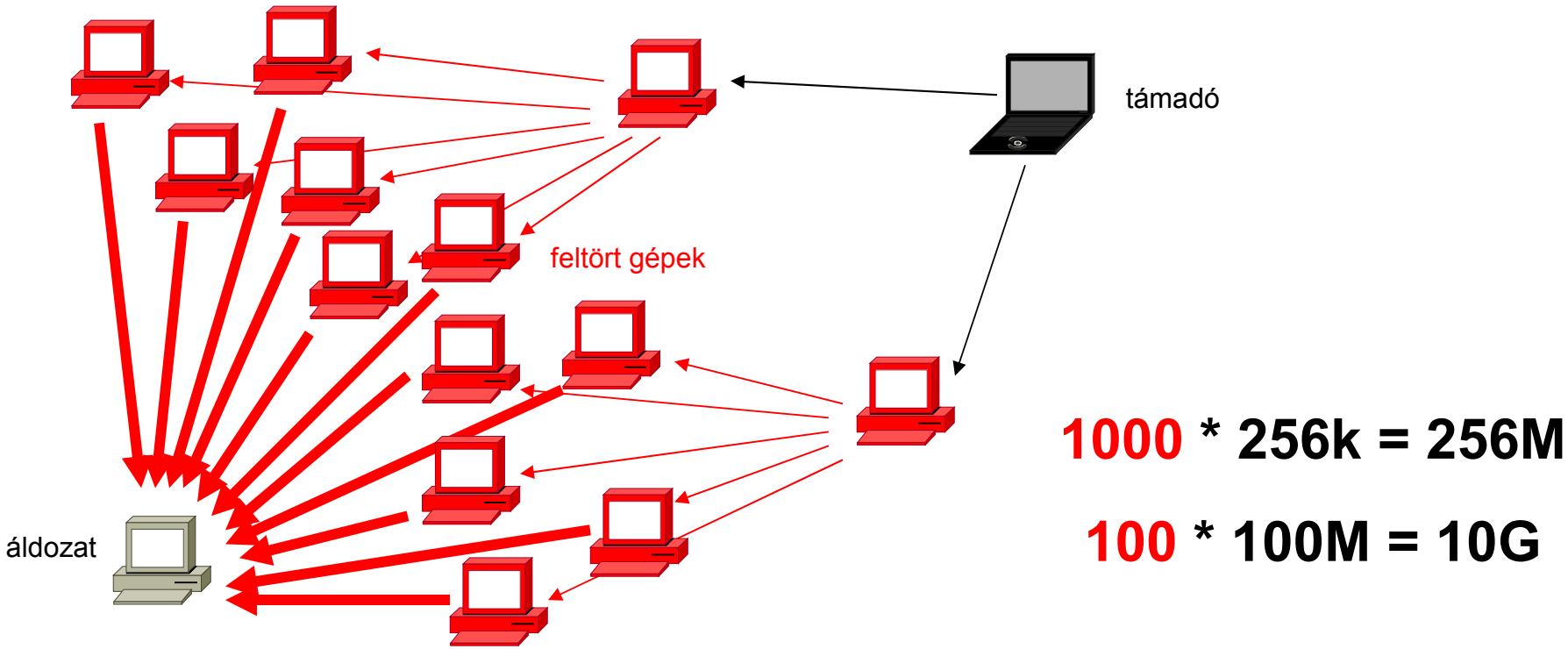
Elosztott IP forgalomszűrés

Jákó András
jako.andras@eik.bme.hu
BME TIO

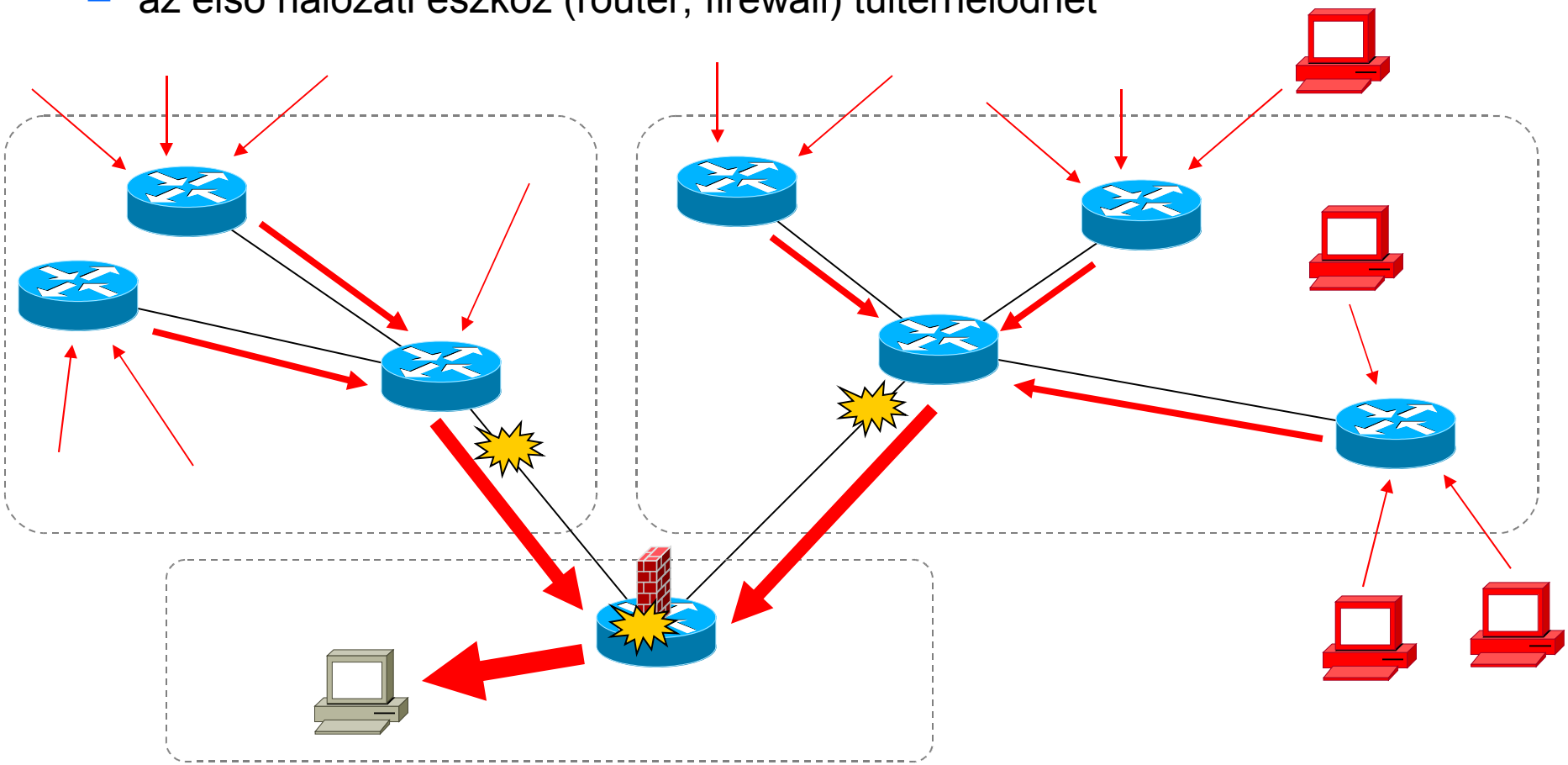
A probléma

- túlterheléses, szolgáltatást bénító elosztott támadás (DDoS)
  - egyszerre sok helyről küldenek kéréseket, csomagokat, stb. az áldozatnak
  - az áldozat hálózati kapcsolata megbénul
    - jelentős torlódás alakul ki
    - köztes eszköz (firewall, load balancer) túlterhelődik
  - a megtámadott host vagy szolgáltatás környezete is szenved



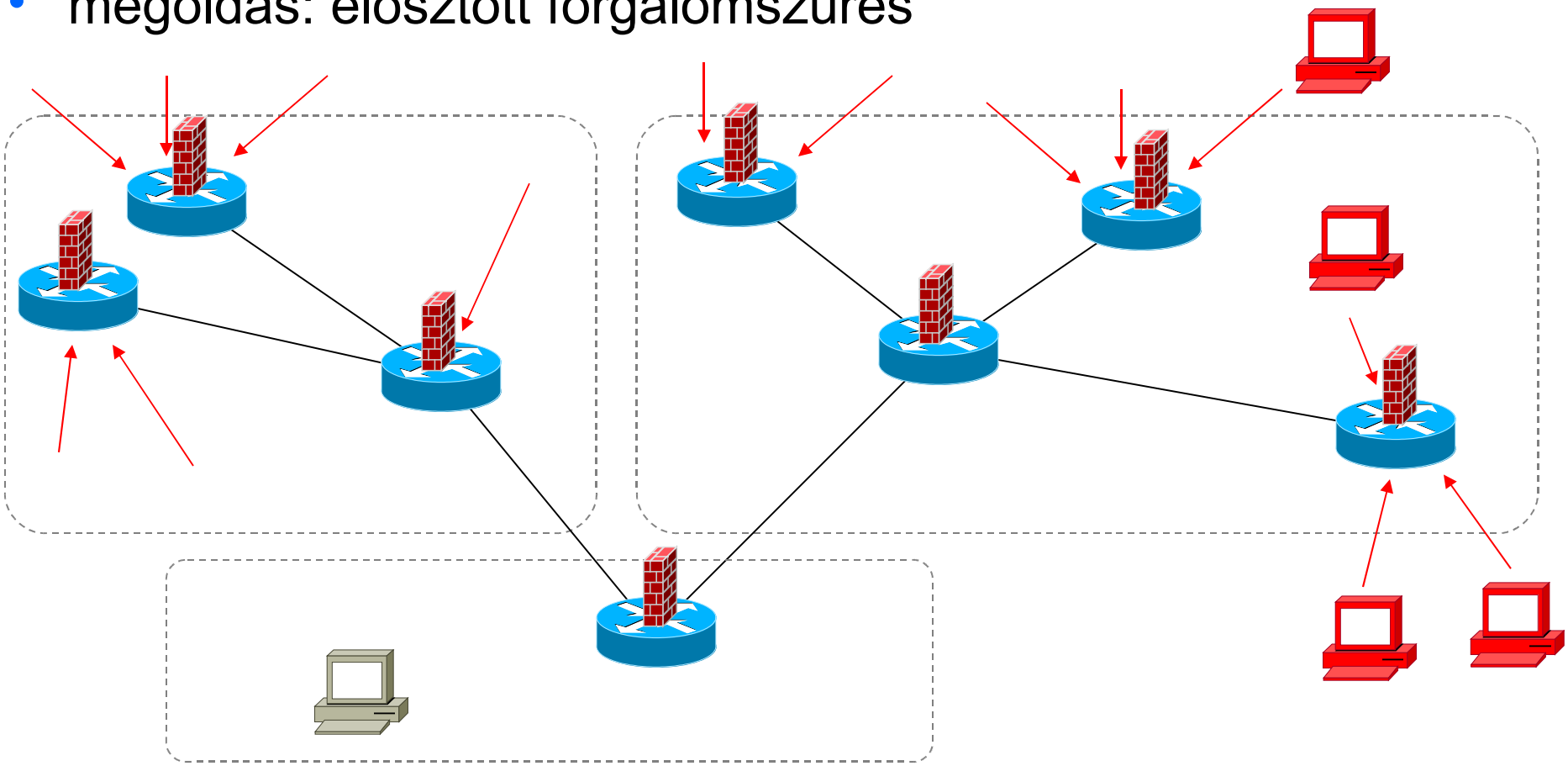
Védekezési kísérlet

- az áldozat megpróbálhatja kiszűrni a túlterhelő forgalmat saját hálózata határán – rossz esélyekkel indul
  - a torlódás már az áldozat első hálózati eszköze előtt kialakulhat
  - az első hálózati eszköz (router, firewall) túlterhelődhet



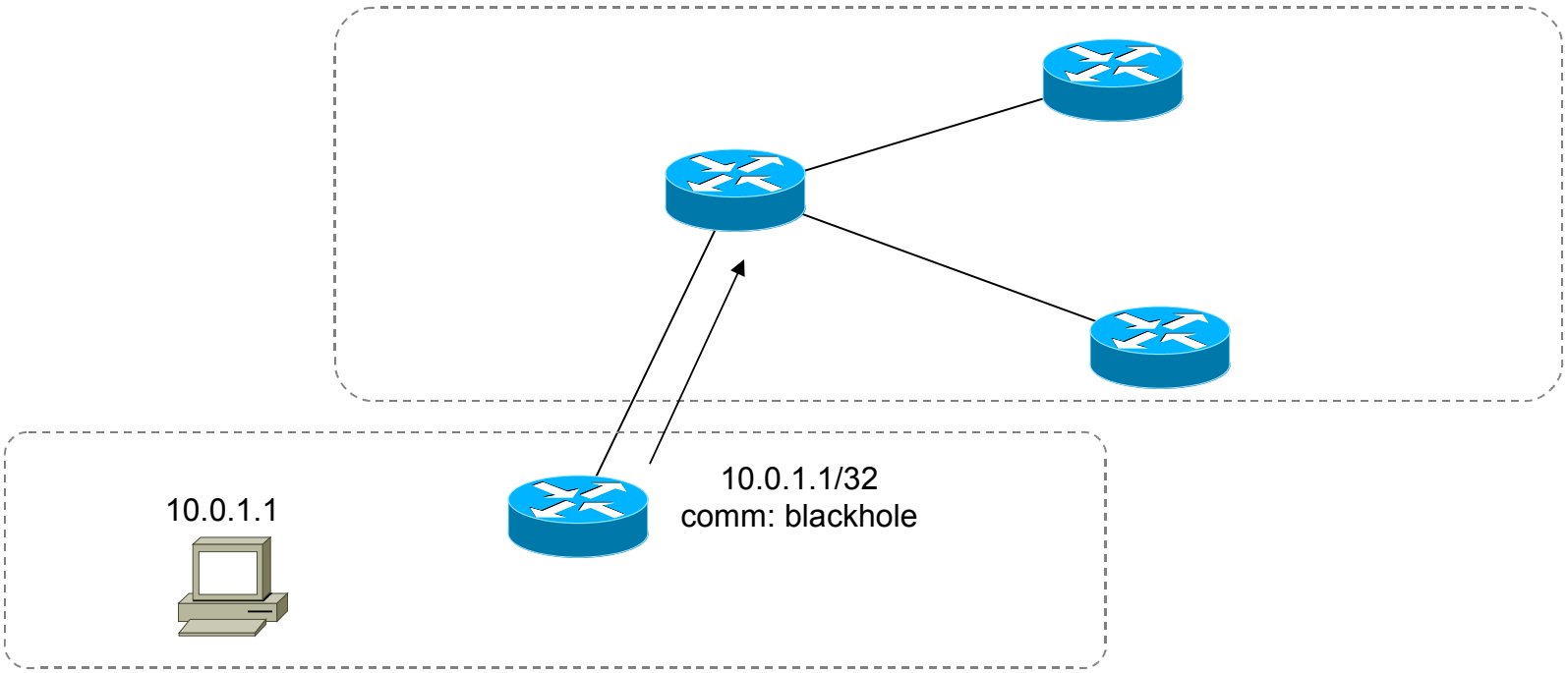
Elosztott forgalomszűrés

- jobbak az áldozat esélyei, ha
  - korábban, a támadóhoz közelebb tud szűrni
  - több helyen, de mindenütt kisebb forgalmat kell szűrnie
- megoldás: elosztott forgalomszűrés



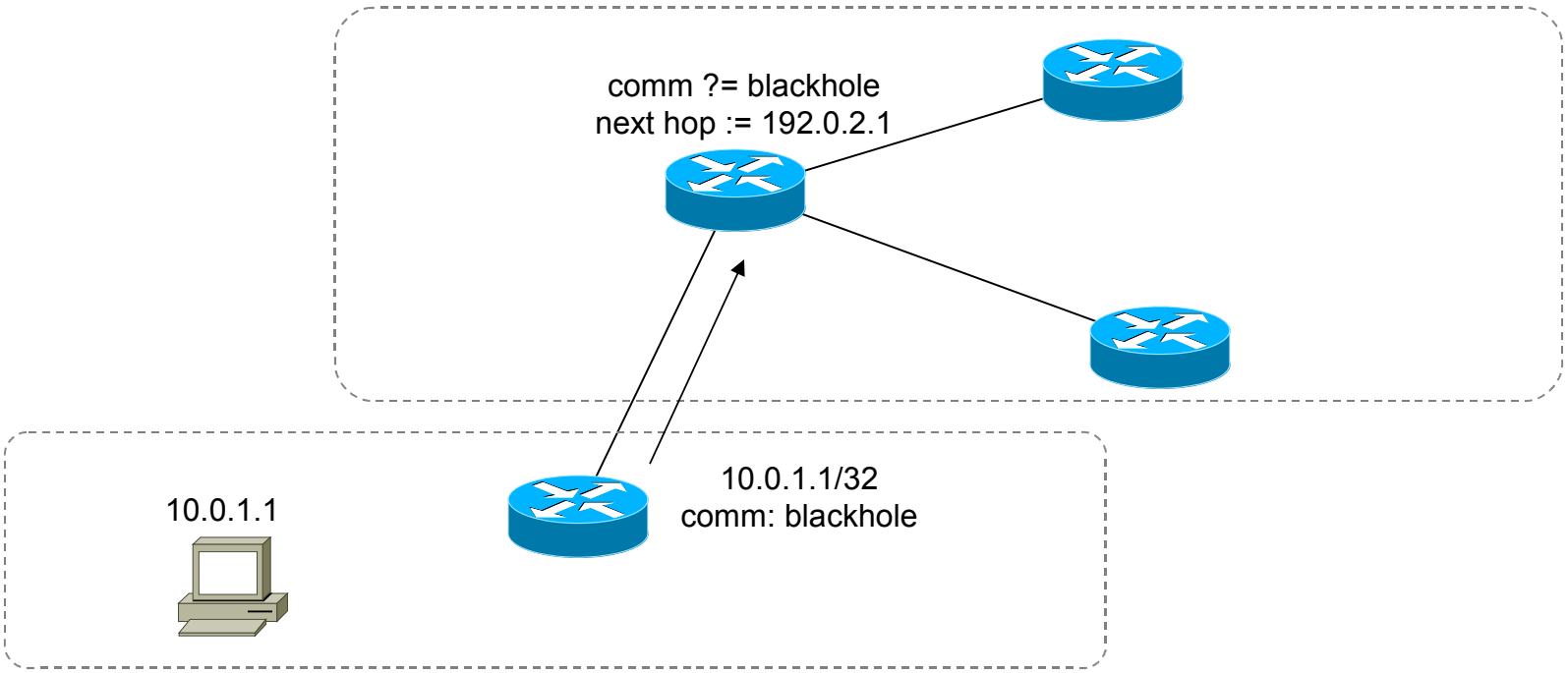
Blackhole routing

- az áldozat IP címére küldött csomagok eldobása
  - az áldozat BGP-vel hirdeti a megtámadott IP címeket, megjelölve (community)



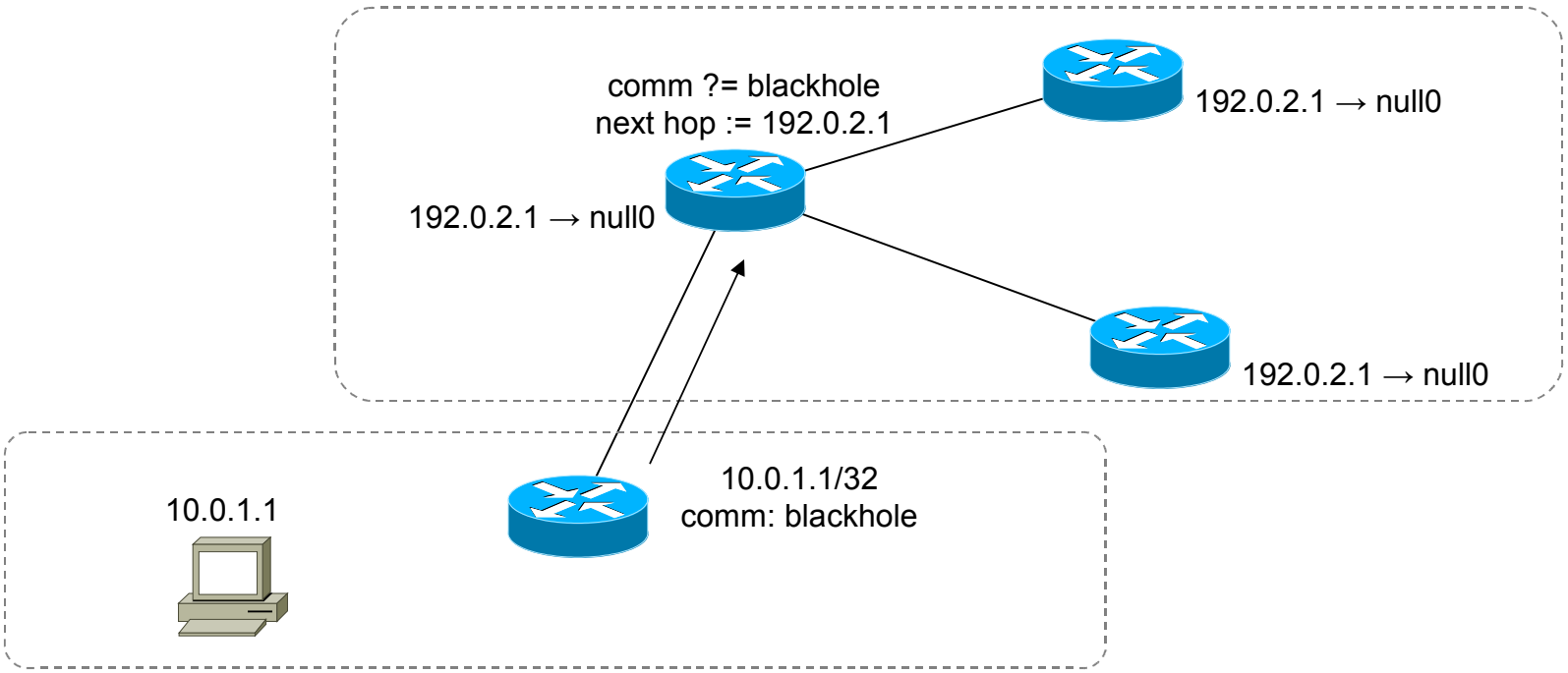
Blackhole routing

- az áldozat IP címére küldött csomagok eldobása
  - az áldozat BGP-vel hirdeti a megtámadott IP címeket, megjelölve (community)
  - a partner szolgáltató (peer, transit) a megjelölt hirdetések BGP next hopját egy speciális címre (pl. 192.0.2.1) állítja be



Blackhole routing

- az áldozat IP címére küldött csomagok eldobása
  - az áldozat BGP-vel hirdeti a megtámadott IP címeket, megjelölve (community)
  - a partner szolgáltató (peer, transit) a megjelölt hirdetések BGP next hopját egy speciális címre (pl. 192.0.2.1) állítja be
  - a speciális címet minden routerében az eldobó (null, discard) interface felé irányítja statikus útvonallal



BGP flow specification rules

- a blackhole routing nem elég jó
  - adott hostok felé menő összes forgalmat eldobja
  - cél IP prefix az egyetlen paraméter
  - ha a támadó célja az adott host elérhetetlenné tétele, akkor mi segítjük ehhez
- blackhole módszer finomítsa: BGP flow specification rules
  - forgalom pontosabb kijelölése
  - szűrés módjának meghatározása
- http://tools.ietf.org/html/draft-ietf-idr-flow-spec-00

Forgalom kijelölése

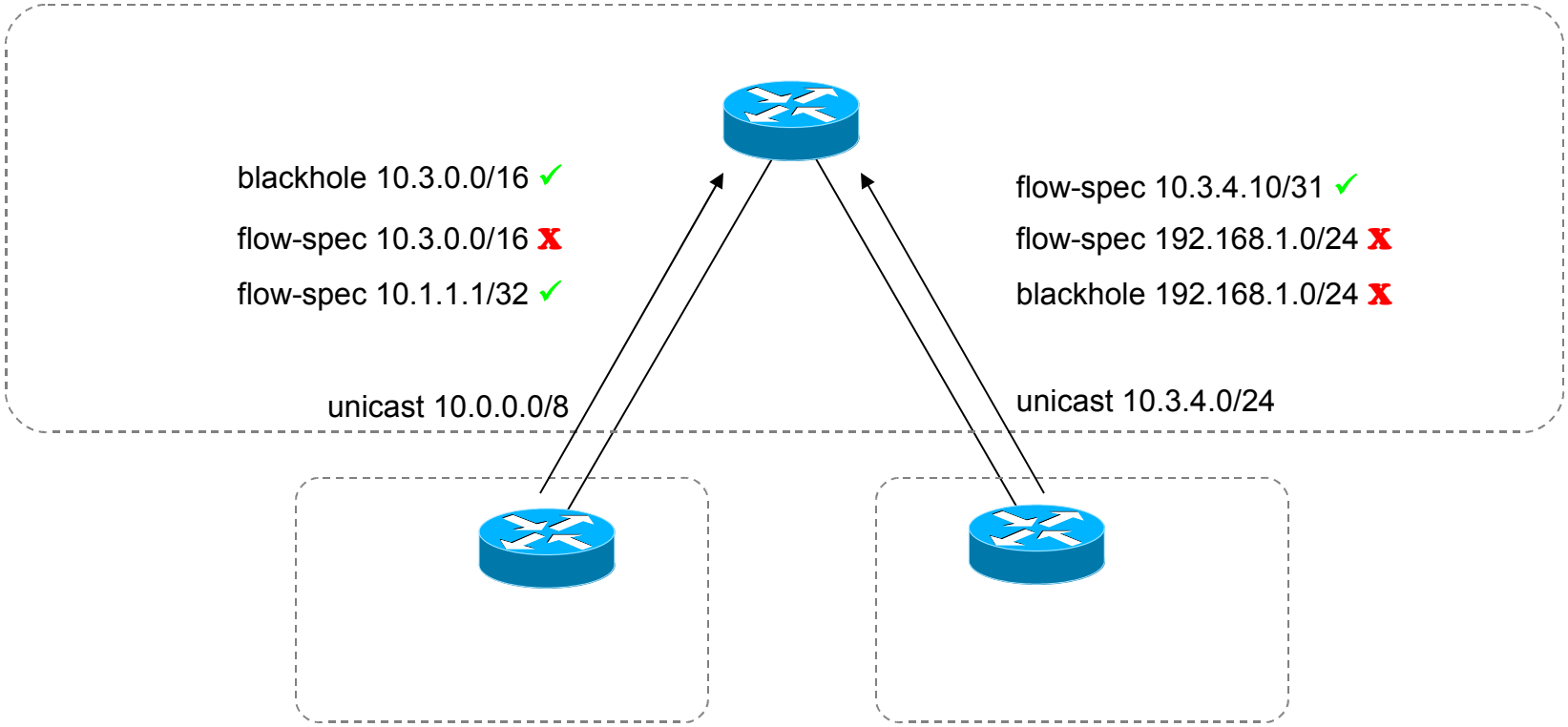
- Melyik csomagokat szűrjük?
  - több paraméter, paraméterek ÉS kapcsolatban
    - cél és forrás IP prefix
    - IP protokoll
    - TCP/UDP portok (forrás, cél, bármelyik)
    - ICMP típus, kód
    - TCP jelzőbitek
    - csomag hossza
    - DSCP
    - IP csomag töredék
  - pl.: 10.5.0.0/18-ból 172.18.2.3 felé menő TCP és UDP csomagok, ahol bármelyik port [137-139] közt van vagy pontosan 1701
- új BGP address family hordozza
  - AFI=1, SAFI=133

Szűrés módja

- Mi történjen a kijelölt forgalommal?
  - sávszélesség korlátozása (0 = teljes szűrés)
  - forgalom mintavételezése
  - forgalom átirányítása másik VRF-be
  - stb.
- BGP extended community hordozza

Ki adhat utasítást?

- a cél IP prefix tulajdonosa
  - unicast BGP szerint
- flow-spec esetén szigorúbb ellenőrzés:
  a prefix specifikusabb része sem lehet más AS irányban



Köszönöm a figyelmet!

az előadás diái:

http://splash.eik.bme.hu/