Kiberfenyegetések észlelése a hálózati forgalom elemzésével

Detecting cyberthreats with network traffic analysis

Somogyi Zsolt Zoltán

Konzulens: Dr. Göcs László, adjunktus

Előadás tartalma

1. Bevezetés
2. Környezet bemutatása, hipotézisek
3. Konklúzió

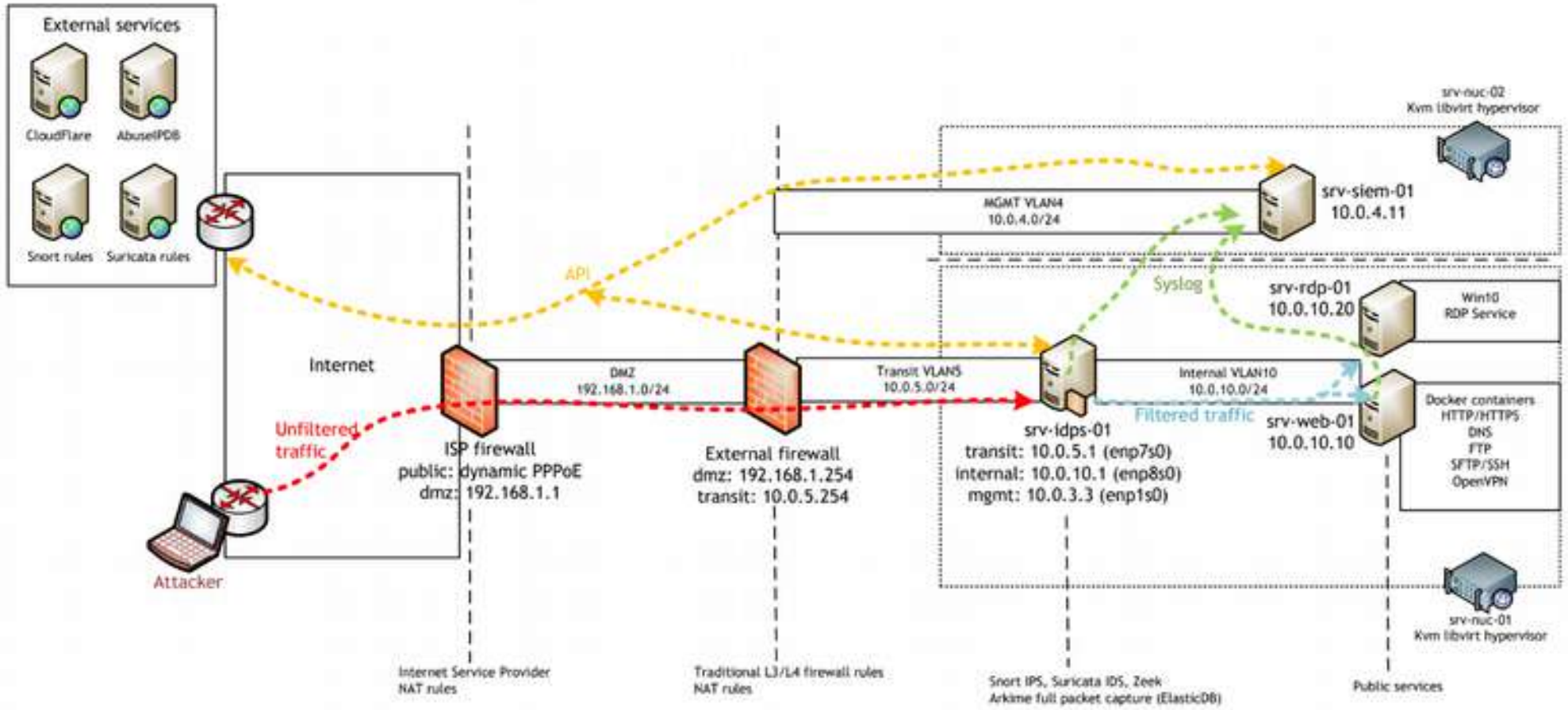
Bevezetés

- Motiváció
  - Hálózati forgalom vizsgálata
  - Kiberbiztonsági vonatkozással
- Kiberbiztonság aktualitása
  - Kiberfenyegetések növekedése
  - Információ elleni védekezés
  - Jogi és szabályozási környezet
- Célkitűzések
  - Publikus szolgáltatások védelme
  - IDS/IPS rendszer kialakítása
  - Teljes hálózati forgalom rögzítése
  - Központi naplózás
  - Hipotézisek vizsgálata

- Bevezetés
  - Motiváció
  - Saját tapasztalat
  - Hipotézisek felállítása
- Irodalmi áttekintés
  - Aktuális trendek
  - Jogi környezet
  - Hálózatalapú IDS áttekintés
- Módszertan
  - Környezet kialakítása
  - Védett szolgáltatások
  - Felhasznált biztonsági eszközök
  - Adatgyűjtési terv
- Eredmények
  - Adatok ismertetése
  - Statisztikai/vizuális elemzése
  - Hipotézisek értékelése
  - Lehetőségek
- Összefoglalás

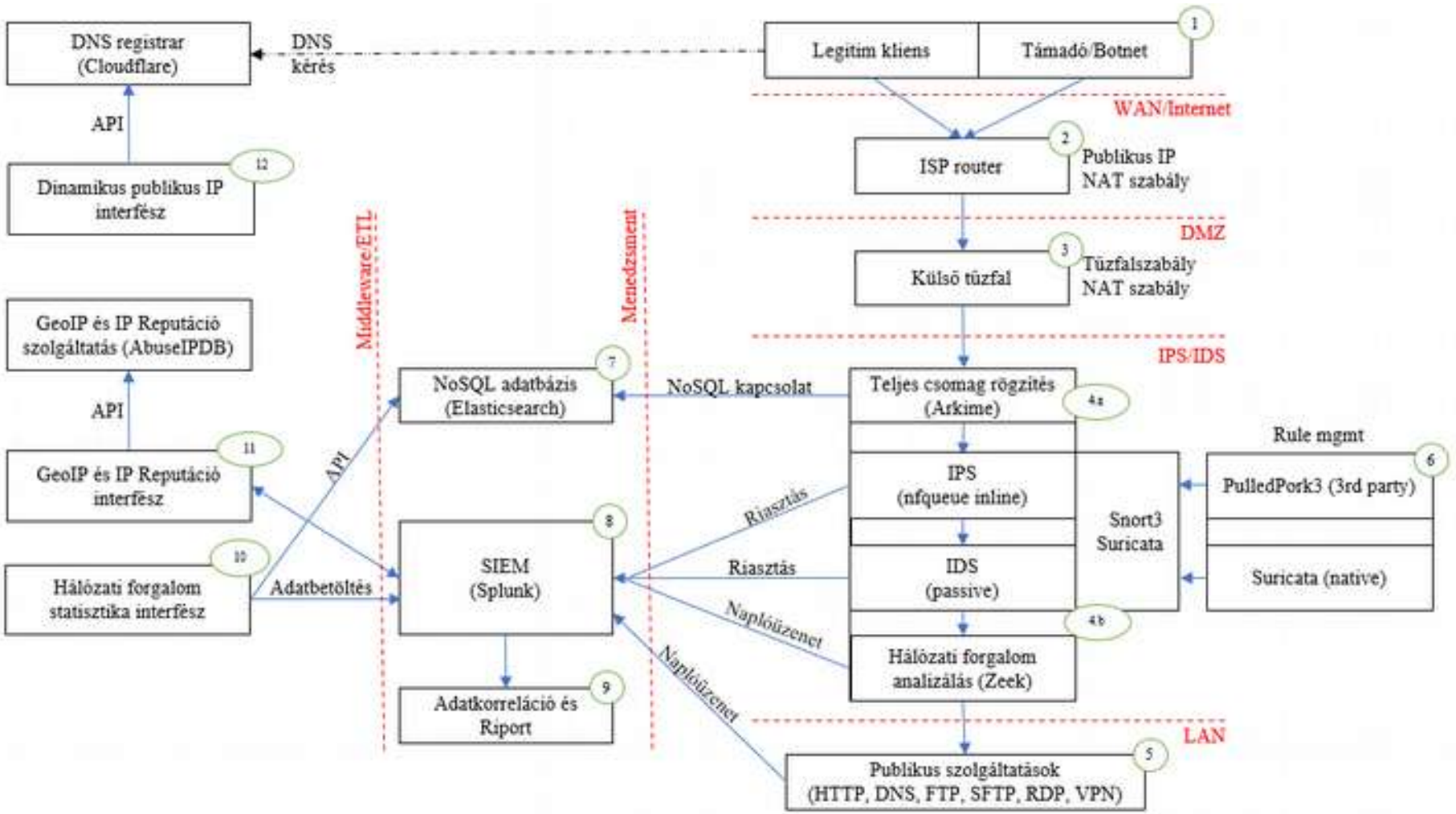
Környezet bemutatása

Logikai topológia



Környezet bemutatása

Folyamatábra



Hipotézisek

No.	Hipotézis	Indoklás	Konklúzió
H1	A nyílt forráskódú IDS rendszerek hatékonyan képesek észlelni a nyilvános szolgáltatásokat érő kiberfenyegetéseket, és releváns riasztásokat generálnak a hálózati forgalom automatikus elemzésével.	A modern IDS rendszerek fejlett észlelési képességekkel rendelkeznek, melyek lehetővé teszik a különböző támadási minták és anomáliák azonosítását. [8]	Igazolt
H2	Az IDS rendszerek kombinált alkalmazása növeli a kiberfenyegetések észlelésének hatékonyságát és csökkenti a hamis negatív riasztások arányát.	A különböző rendszerek erősségeinek kombinálása szélesebb körű és mélyebb észlelést tesz lehetővé, lefedve mind az aláírás alapú, mind az anomália alapú észlelési módszereket. [9]	Igazolt
H3	A hálózati forgalom elemzésével azonosított kiberfenyegetések megfelelnek az aktuális fenyegetési trendeknek, melyeket a legfrissebb kiberbiztonsági jelentések és tanulmányok alátámasztanak.	A gyűjtött adatok elemzése során várható, hogy a gyakori támadási minták és trendek megjelennek a riasztásokban, összhangban a Verizon [5] és az ENISA [3] jelentéseivel.	Részben igazolt
H4	A nyílt forráskódú IDS rendszerek megfelelő konfigurációja és finomhangolása mellett képesek megfelelni a NIS irányelvek által támasztott jogi és szabályozási követelményeknek.	A jogszabályi megfelelés érdekében a rendszereknek bizonyos funkciókat és jelentési képességeket kell biztosítaniuk, amelyeket megfelelő beállításokkal el lehet érni. [10]	Részben igazolt
H5	A titkosított forgalom (például HTTPS, SSH, OpenVPN) elemzése kihívást jelent az IDS rendszerek számára, és speciális megoldások vagy további eszközök alkalmazása szükséges a hatékony észleléshez.	A titkosítás megnehezíti a forgalom tartalmának elemzését, ami befolyásolja az észlelés hatékonyságát. Ezért szükség lehet SSL/TLS bontásra vagy metaadat-alapú elemzésre. [9]	Igazolt
H6	Egy korábban nem használt publikus IP-cím interneten történő engedélyezését követően gyakorlatilag azonnal megtalálják valamilyen hálózati botok, szkennelő eszközök vagy más automatizált rendszerek tevékenységei, amelyek publikus IP-címeken elérhető szolgáltatások után kutatnak.	Saját tapasztalatok alapján a publikus IP-címek folyamatos célpontjai az interneten működő nagyszámú, automatizált szkennelő rendszereknek, ezért az újonnan használatba vett IP-címek megjelenésére azonnal „reagálnak”.	Igazolt

Konklúzió

- Tradicionális periméter védelem kiegészítése
- Moduláris rendszer kialakításának szabadsága
- További lehetséges felhasználások: CTF, AI, SOAR, 10G
- Hipotézisek értékelése és kitűzött célok teljesítése

Neumann János Egyetem
Műszaki és Informatikai
Kar

Köszönöm a figyelmet!

Kiberfenyegetések észlelése a hálózati forgalom elemzésével
Detecting cyberthreats with network traffic analysis

Somogyi Zsolt Zoltán

Konzulens: Dr. Göcs László, adjunktus