Firewall management in Tatra banka, a.s.

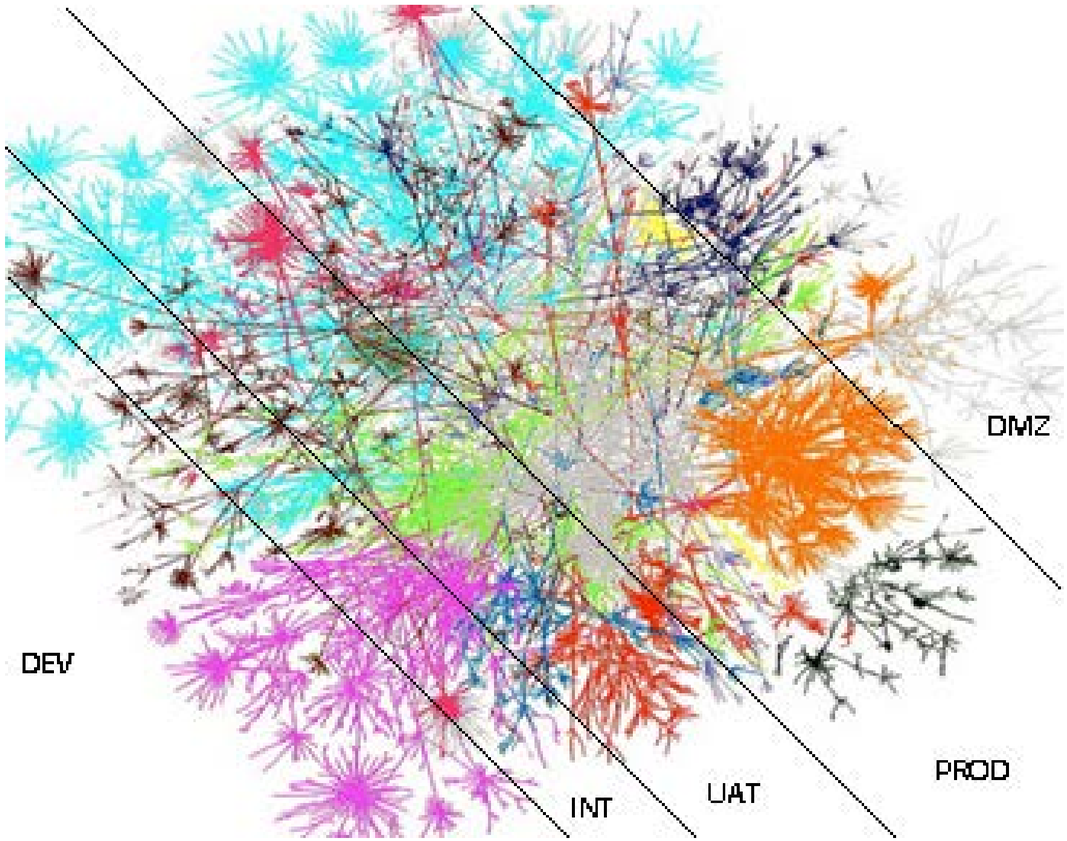
efocus.sk

Why?

Essential purposes

Network system complexity (more than 18 000 devices in network).
Number of rules between firewalls (in hundred thousands).
Lot of changes (tenths per months).
Missing security threads monitoring on existing FW settings.
Security standard requirements (PCI DSS and GNSP).
IN TB, We have 10 important FW + 1 between RPC a TB.
Aproximatelly half a milion important rules.
Everything is managed only in excel files.
Regular vulnerability scan producing a lot of information

Sample for communication between selected applications and segments in TB:



Zdroj:

What we are looked for?

- Network model
- Firewall analysis
- Rule Lifecycle
- Vulnerability analysis
- Analysis of attack surface
- Prioritize response
- Tracking remmediation

- Monitor compliance

Zdroj:

efocus.sk

What We have?

Firewall management

- Skybox on all main firewalls
- Firewall change management
  - It is only one possible way, how to change Firewall settings in TB
- Ability to immediately analyze possible network access
- Firewall configuration optimization
  - automatic identification of shadowed, redundant rules, unsupported changes
- Risk based process for documented firewall changes
- Automatic detection of devices accessible from internet (custom)
- Automatic detection of new services on devices accessible from internet (custom)

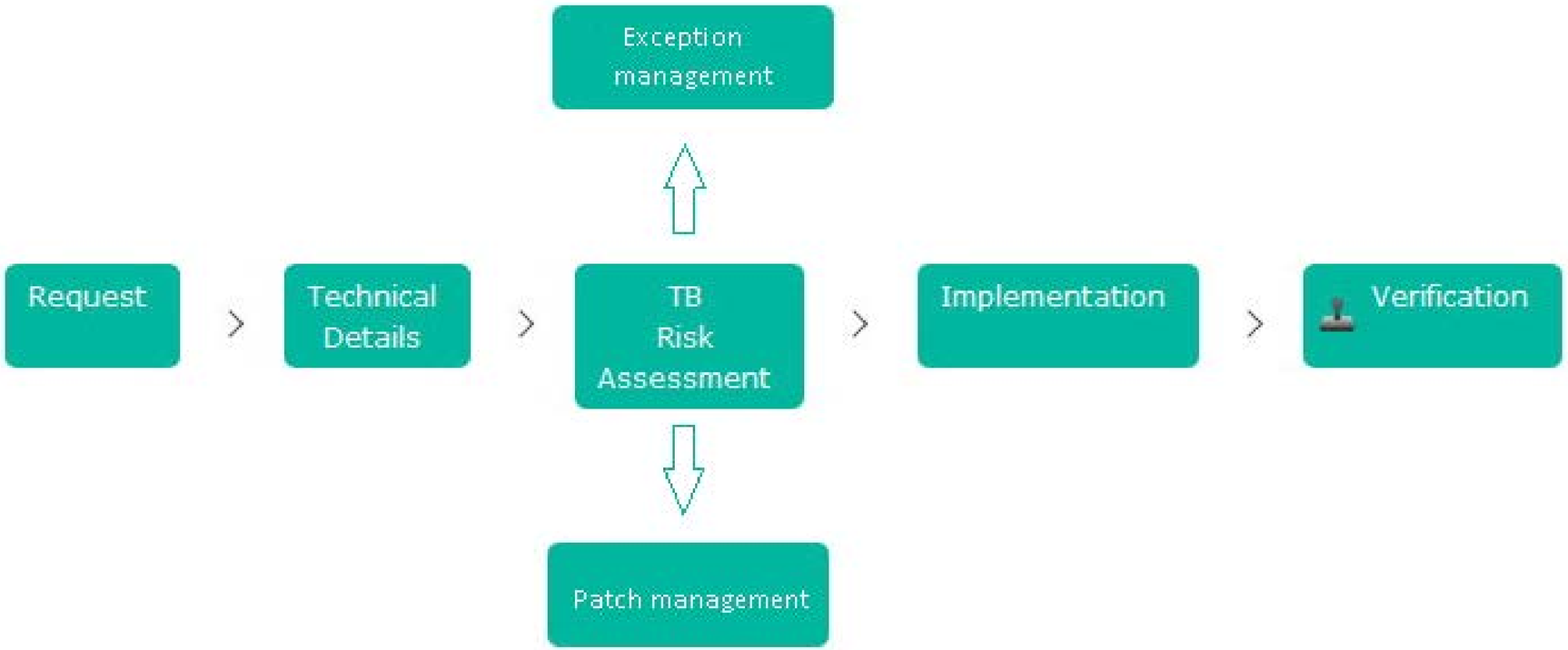
Vulnerability management

- All vulnerability data in one view
- Identification of vulnerabilities
- Prioritization of vulnerabilities
- Notification of new exposed vulnerability to attacker/internet

Zdroj:

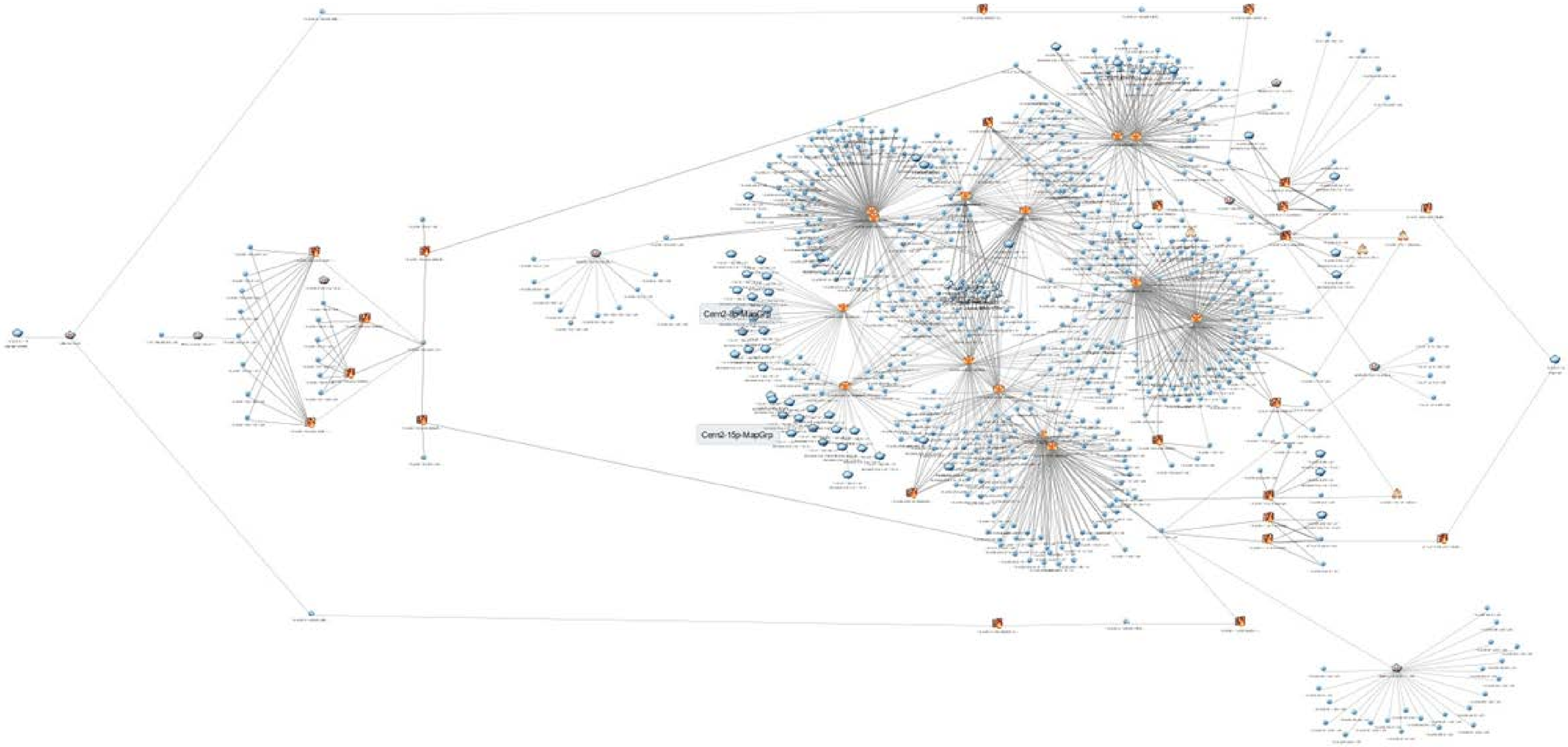
efocus.sk

Processes for FW rule change - TB



Zdroj:

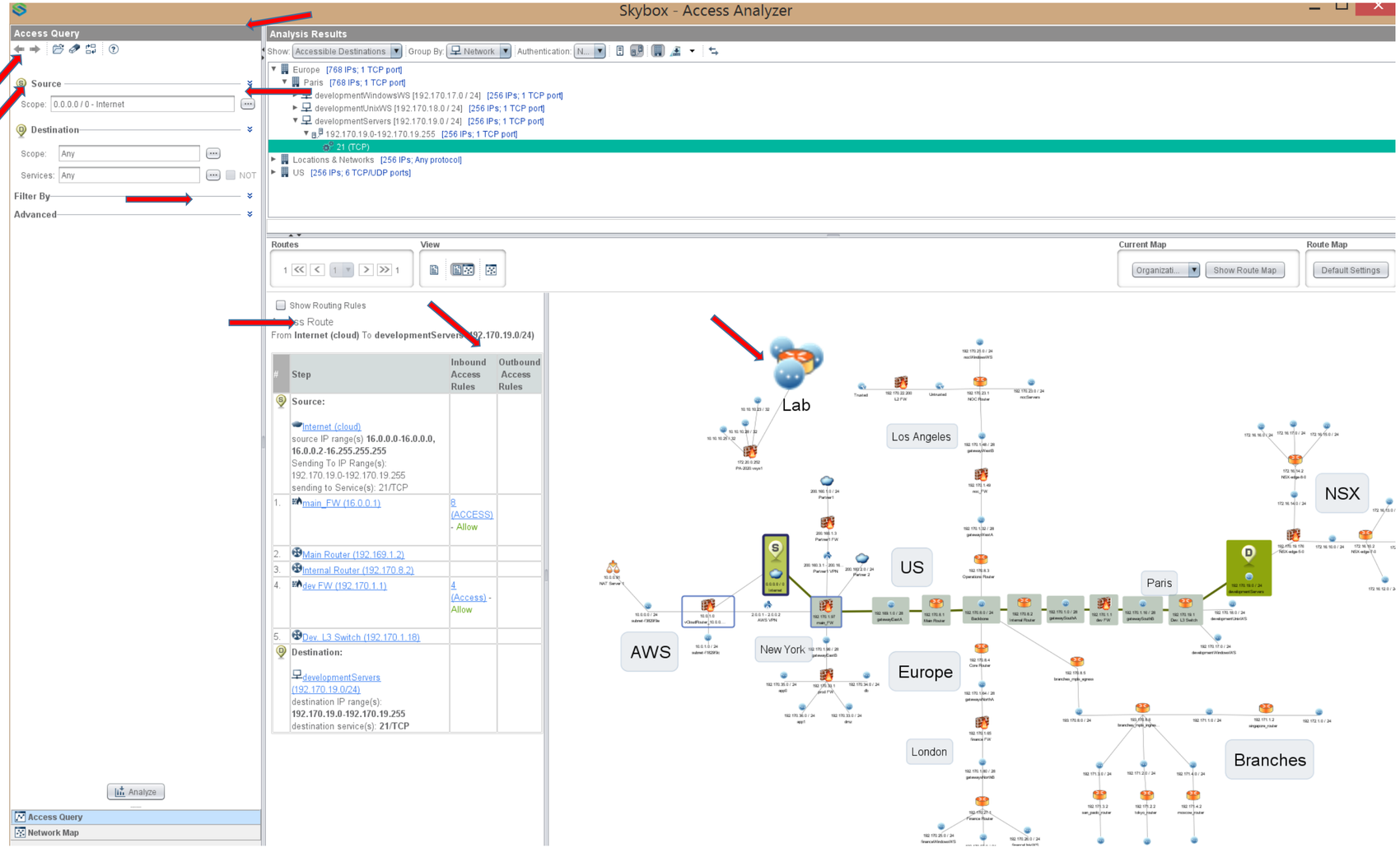
Online network topology



Zdroj:

efocus.sk

Example of access path analysis from internet



Zdroj: Example on demo data

efocus.sk

Main Advantages

- Network administrator & IT Security has possibility to **analyze real network paths**.
- IT admins, ITPM, PM requests network change by workflow with **standard approval process**.
- All **exceptions are registered** in standard manner.
- IT Security can monitor **actual setup** and implementation of new requests.
- It is possible to **find** most dangerous **vulnerabilities** and linked them with all TB environments.
- Vulnerabilities are **prioritized** in seconds.

Zdroj:

efocus.sk

Main KPI

Status of implementation

servers accessible from internet are fully covered.

Plan Q1/2018

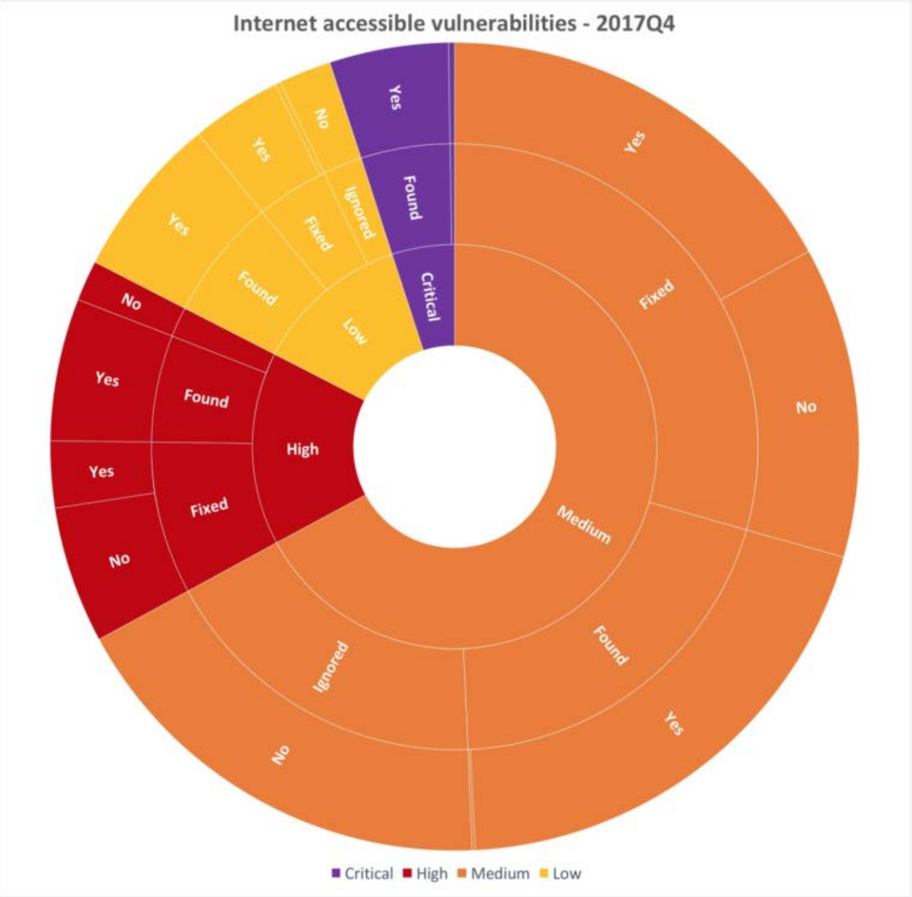
CNI (RI network)

Graph

Inner circle – severity of vulnerability

Middle circle – status of implementation

Outer circle – vulnerability handling by SD ticket



Zdroj:

efocus.sk

Zdroj:

Ďakujem za pozornosť

Ing. Ján Václavík

Tatra banka,a.s.