Spoofing issue

40% of attacks!

Really hard to find source!

IX spoofing issue

- IX do not filter spoofing
- Impossible to implement on L2 devices (we need millions of ACL rules)

Internal spoofing

- BCP 38 do not cover this case
- In «safe subnet» somebody could use neighbour's IP address for attacking Internet or local resources.

Any solutions?

- sFLOW / NetFlow / SPAN traffic monitoring against spoofing
- TTL check could be useful for mitigation
- Amplificators monitoring
- FastNetMon