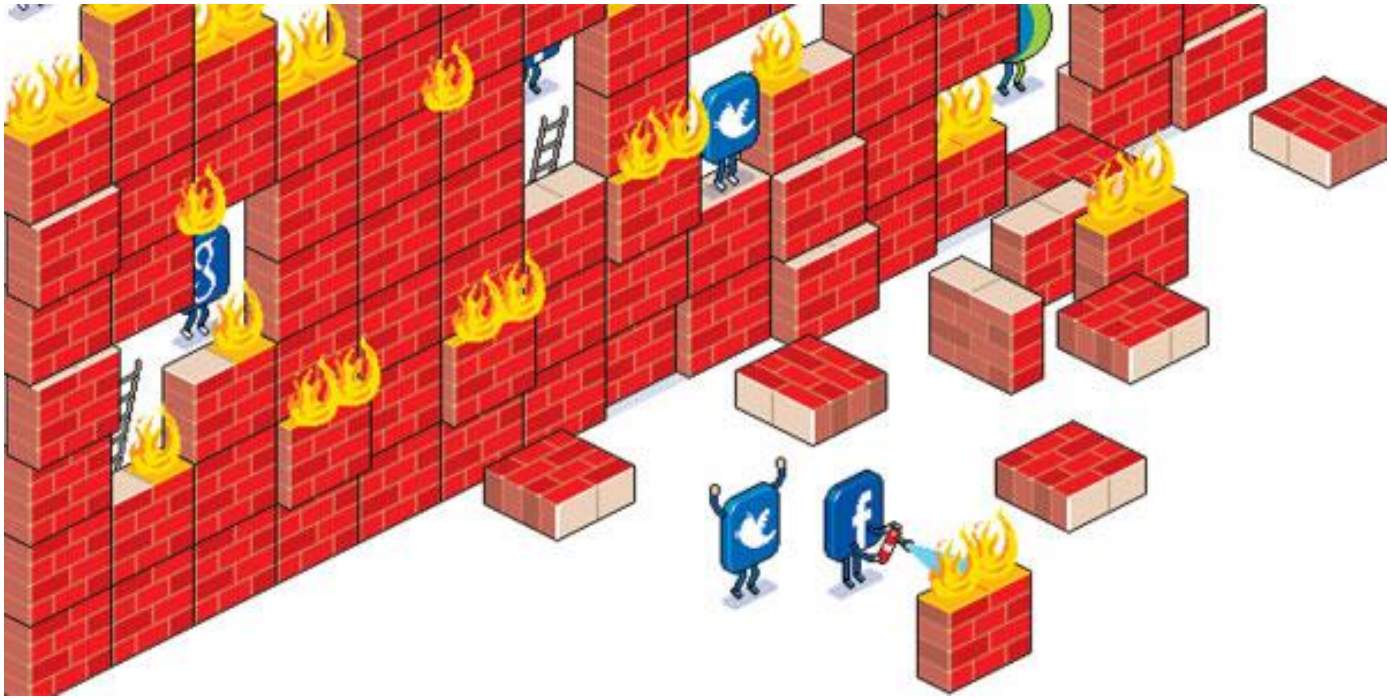
Cvičení 12 – PGP a Firewall



Funkce certifikátu veřejného klíče

- Digitální certifikát je v AK digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita
  - Na základě principu přenosu důvěry je možné důvěřovat neznámým certifikátům, které jsou podepsány důvěryhodnou certifikační autoritou
- Certifikační autorita (zkratka CA) je v AK subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče)

Certifikační autorita

- Usnadňuje využívání PKI (Public Key Infrastructure)
- Certifikační autorita vydává digitální certifikáty, což jsou elektronicky podepsané veřejné šifrovací klíče, které obsahují identifikační údaje svého majitele, za jejichž správnost se certifikační autorita zaručila
- Svou autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny

PGP

- Vytvořte si soukromý klíč pomocí PGP
  - Například Open PGP Encryption Tool
- Zakódujte a dekódujte soubor / zprávu
- Vyhledat uložiště kořenových certifikátů pro uživatele a místní počítač v systému Windows 10
- Vyhledat uložiště certifikátů v Ubuntu pro uživatele

Firewall

- Nastavení filtrovacích pravidel
  - Zdrojová/cílová IP adresa
  - Zdrojový/cílový port
  - Protokol
  - Status
  - Akce

Firewall - Windows 10

- Zakažte pomocí Firewallu odchozí provoz jednoho z prohlížečů (např. Explorer)
  - Poté pravidlo zakažte a povolte tak provoz
- Zablokujte rozmezí adres 185.17.119.0 - 185.17.199.255
  - Ověřit = zkusit ping na adresu z rozsahu a zkusit idnes.cz v prohlížeči
  - Zakažte pravidlo a ověřte (ne)funkčnost

Firewall Ubuntu

- Zahazovat všechny pakety z adres 185.17.119.0 - 185.17.199.255
  - iptables
  - Ověřit = zkusit ping na adresu z rozsahu a zkusit idnes.cz v prohlížeči
- Zablokujte doménu facebook.com
  - A zároveň logujte všechny zahozené pakety
  - Pokuste se připojit a prohlédněte si logy
- Vypsat všechna pravidla z iptables
- Vyčistit všechna pravidla
- Podívat se na logy
  - /var/log/kern.log
- Odmítnout všechny pakety s ICMP zprávou
  - Ověřit = zkusit ping na nějakou adresu