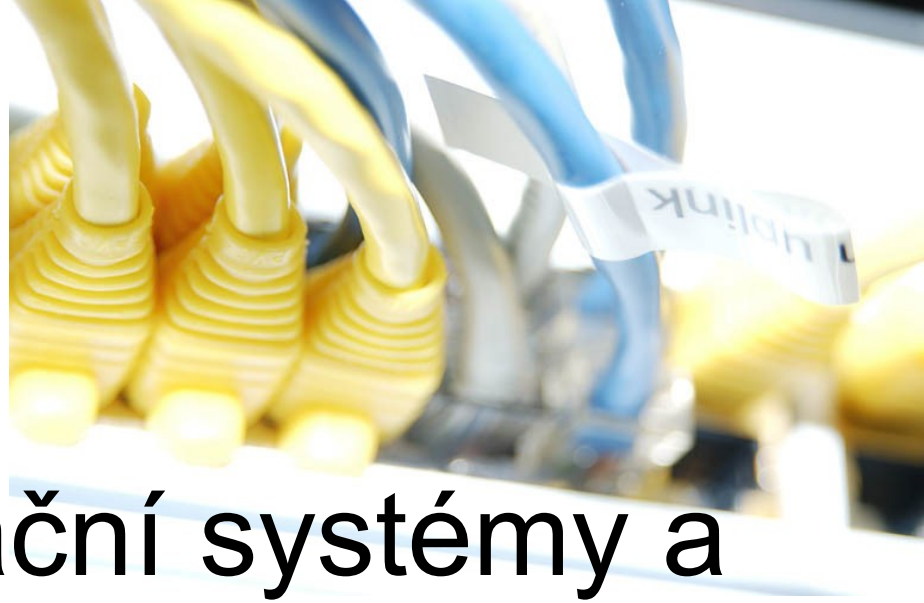


PB169 – Operační systémy a sítě

Zabezpečení počítačových sítí

Marek Kumpošt, Zdeněk Říha

Zabezpečení sítě – úvod

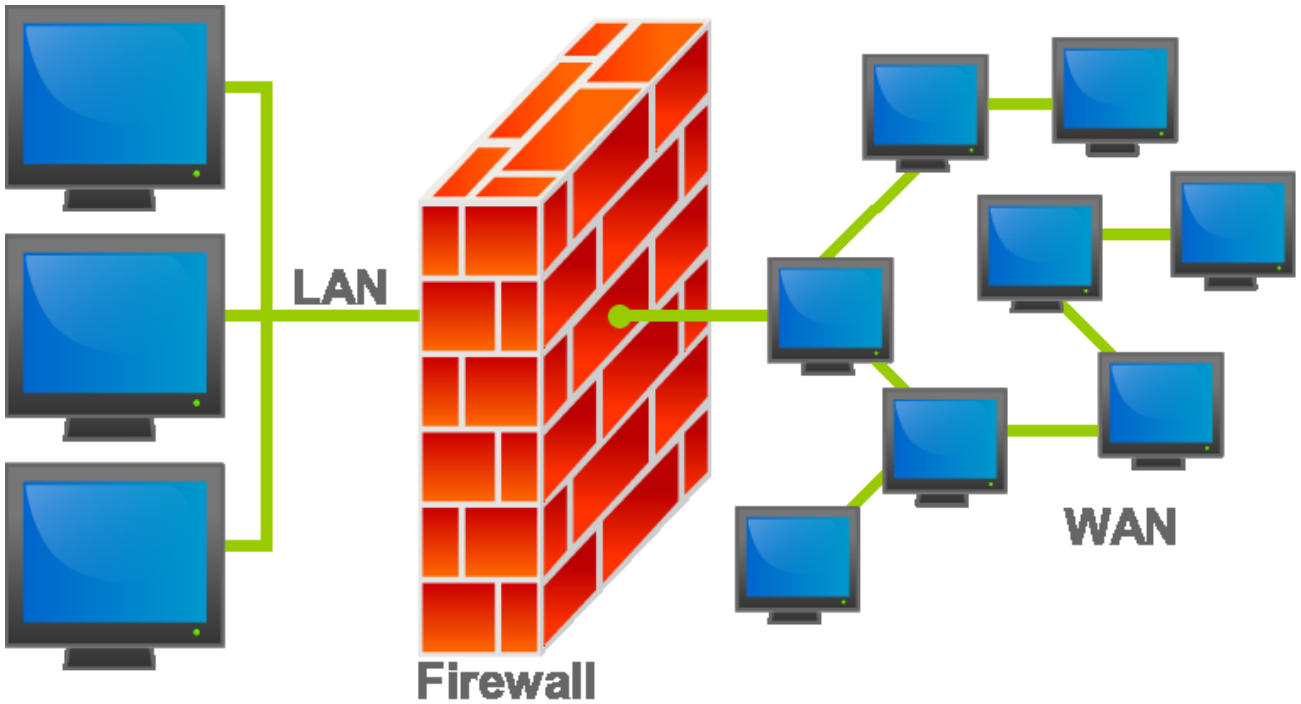
- Důvody pro zabezpečení (interní) sítě?
- Nebezpečí ze strany veřejného Internetu
  - Spyware
  - Malware
  - BOTy
  - Rootkity
  - Viry
  - Exploity
  - Skenování vnitřní sítě a hledání zranitelných míst
  - Spam
  - …
- Ohrožení (vnitřní) sítě, pokud je např. možné připojovat soukromé stanice (typicky notebooky)

Zabezpečení sítě – úvod

- Zabezpečení se typicky realizuje na úrovni
  - Firewallů
  - Systémů pro detekci narušení (IDS)
  - Antivirových systémů
  - Antispamových ochran
  - Aktivního monitoringu sítě

Firewall

- Aktivní síťový prvek na rozhraní LAN / WAN
- Cílem je (aktivní) ochrana vnitřní sítě (LAN)
  - Definice pravidel pro komunikaci



Firewall

- Firewall je typicky v každé větší lokální síti
  - Koncový uživatel nemůže zasahovat do nastavení
- Uživatelé mohou provozovat firewall i lokálně na svém stroji
  - Využitelné zejména v případě přístupu do nedůvěryhodné sítě (free Wi-Fi apod.)
  - Uživatelé si sami definují bezpečnostní politiky
  - Různé (i free) produkty, integrace přímo v OS
- Běžná „home“ síťová zařízení (Wi-Fi AP) poskytují funkcionalitu firewallu (je vhodné provést alespoň základní nastavení)

Firewall

- Firewally dělíme do několika kategorií
  - Paketový filtr
  - Stavový paketový filtr
  - Aplikační brána nebo proxy firewall
  - Pokročilé stavové filtry

Paketový filtr

- Pravidla a rozhodování se děje na úrovni IP adres a čísla portu
  - 3. a 4. vrstva ISO/OSI modelu
- Např.:
  - příchozí provoz (TCP) na adresu 147.251.48.1 na portu 80 povolit
  - příchozí provoz (TCP) na adresu 147.251.48.1 na jiném portu zahodit
  - příchozí provoz (TCP) na adresu 147.251.48.1 na portu 21 zalogovat

Paketový filtr

- Výhodou je rychlé zpracování provozu
  - Využití zejména ve vysokorychlostním prostředí
- Neumožňuje důkladnou analýzu procházejících dat (např. přenos FTP – obsah přenášených dat)
- Konfigurace v Linuxu primárně pomocí iptables
  - Existují i „klikatelné“ moduly pro „snažší“ nastavení
  - Dělení provozu do řetězců INPUT, OUTPUT a FORWARD a dále do tabulek

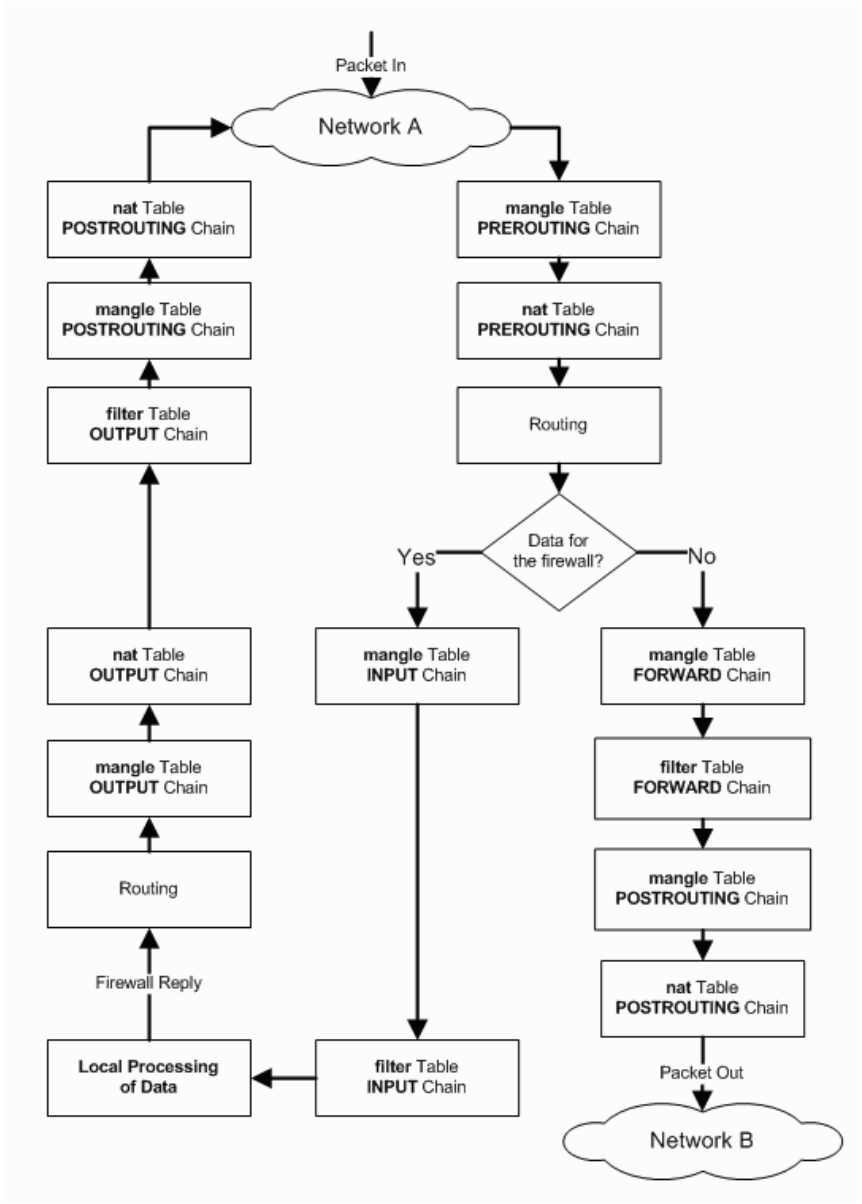
Paketový filtr

- Pakety lze nejen filtrovat, ale i modifikovat!
  - tzn. přepisovat IP adresy a čísla portů v IP hlavičkách jednotlivých paketů
- Pomocí packet filteru lze řešit dostupnost služeb za NATem
  - např. web server na adrese 192.168.0.1:80
  - iptables -A PREROUTING -t nat -i eth1 -p tcp --dport 8080 -j DNAT --to 192.168.0.200:80
  - iptables -A INPUT -p tcp -m state --state NEW --dport 8080 -i eth1 -j ACCEPT
  - bude dostupný na IP adrese serveru na portu 8080

Paketový filtr

- Nastavení paketového filtru:
  - Ve velkých sítích složité
  - I v malých sítích „relativně“ složité ☺
- Je potřeba nastavit i příjem odpovědních paketů a případně otevřít další potřebné porty (typicky FTP a port 20)
- Z důvodu složitosti nastavení může vzniknout chyba – hrozba vniknutí do vnitřní sítě za firewallem

Paketový filtr – zpracování dat



Stavový filtr

- Funguje podobně jako paketový, ale:
  - udržuje si informace o povoleném spojení a toto využije při rozhodování, zda propustit pakety (patří k povolenému spojení? ano/ne)
  - např. povolení FTP (pouze port 21, ale je potřeba i 20 – ten otevře stavový filtr automaticky)
- Výhody stavového filtru
  - vysoká rychlost zpracování paketů
  - jednodušší konfigurace než paketový filtr
  - slušná úroveň zabezpečení

Aplikační brána

- Kompletní oddělení sítí, mezi kterými jsou umístěny
- Požadavky klientů zpracuje brána a klientovi předá pouze výsledek
- Musí umět zpracovat řadu protokolů
- Automaticky provádí NAT
- Vysoká náročnost na použitý HW

Aplikační firewally

- Umí rozpoznat síťové aplikace
  - Velmi detailní nastavení politik
- Umí rozpoznat uživatele v síti
  - Nepracujeme s IP adresami
  - Nutnost integrace s autentizačním serverem
- Umí kontrolovat i šifrovaný provoz
  - Řízený MITM útok
- Náročné na výpočetní výkon HW

Pokročilé stavové filtry

- Fungují principielně stejně jako stavové filtry
- Navíc umožňují detailní analýzu přenášených dat a následné rozhodování
  - např. špatné hlavičky emailu
  - pokus o tunelování jiného typu provozu na portu, který je určený standardně např. pro WWW
  - heuristické analýzy s cílem identifikovat nebezpečný kód (funkcionalita podobná antiviru)
- Poskytují vysokou úroveň zabezpečení, ale jsou již velmi komplexní (PaloAlto, Kernun, Fortinet)

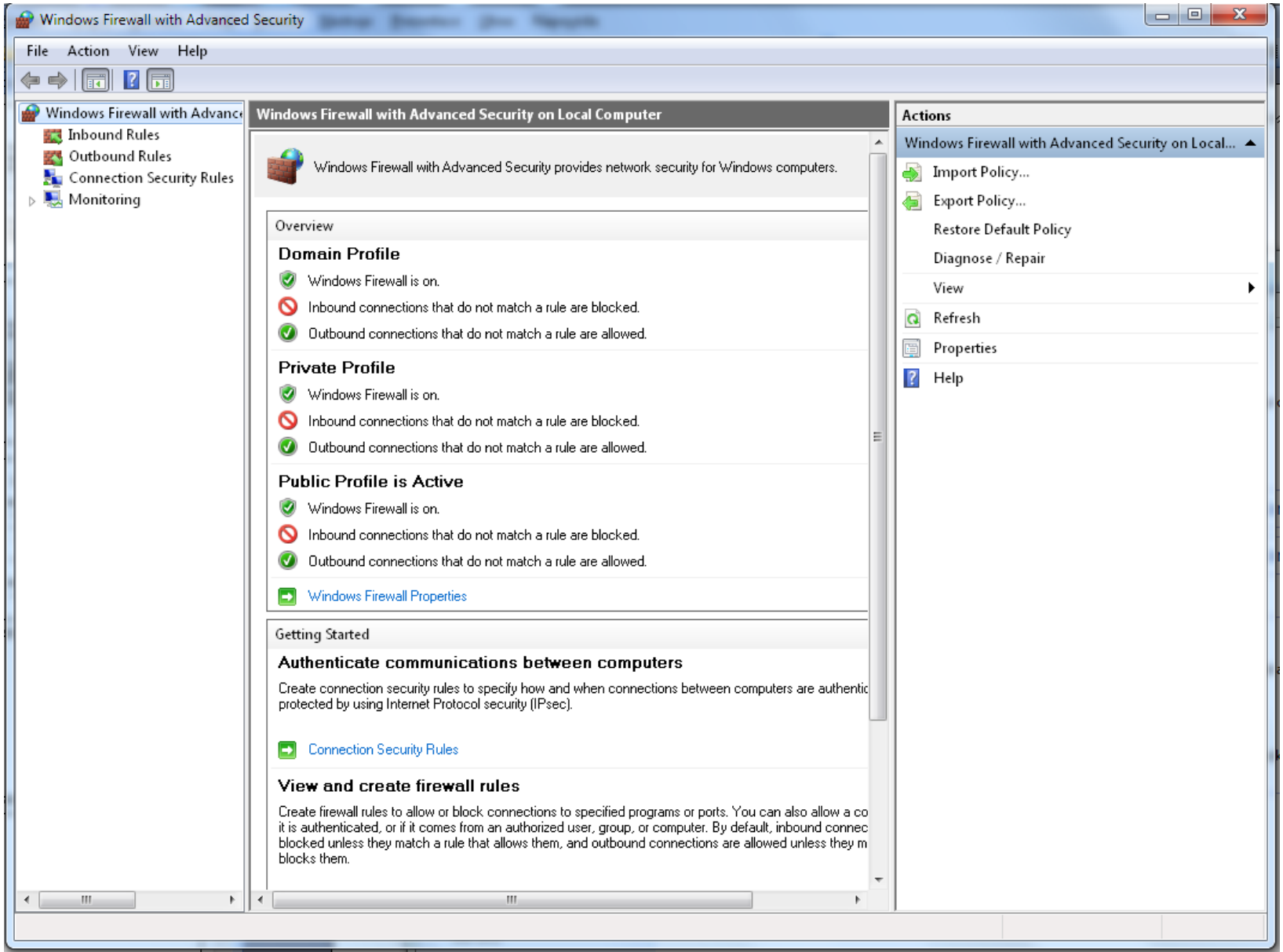
Lokální firewall

- Firewall nainstalovaný přímo v počítači uživatele nebo integrovaný v OS
  - Windows 2000 a vyšší
  - iptables v Linuxu
- Vhodné v situacích, kdy se s počítačem budeme připojovat do „nedůvěryhodné“ sítě (zákaz všech příchozích spojení)
- Existuje řada produktů třetích stran (placené i free)
  - Comodo, Zone Alarm, …

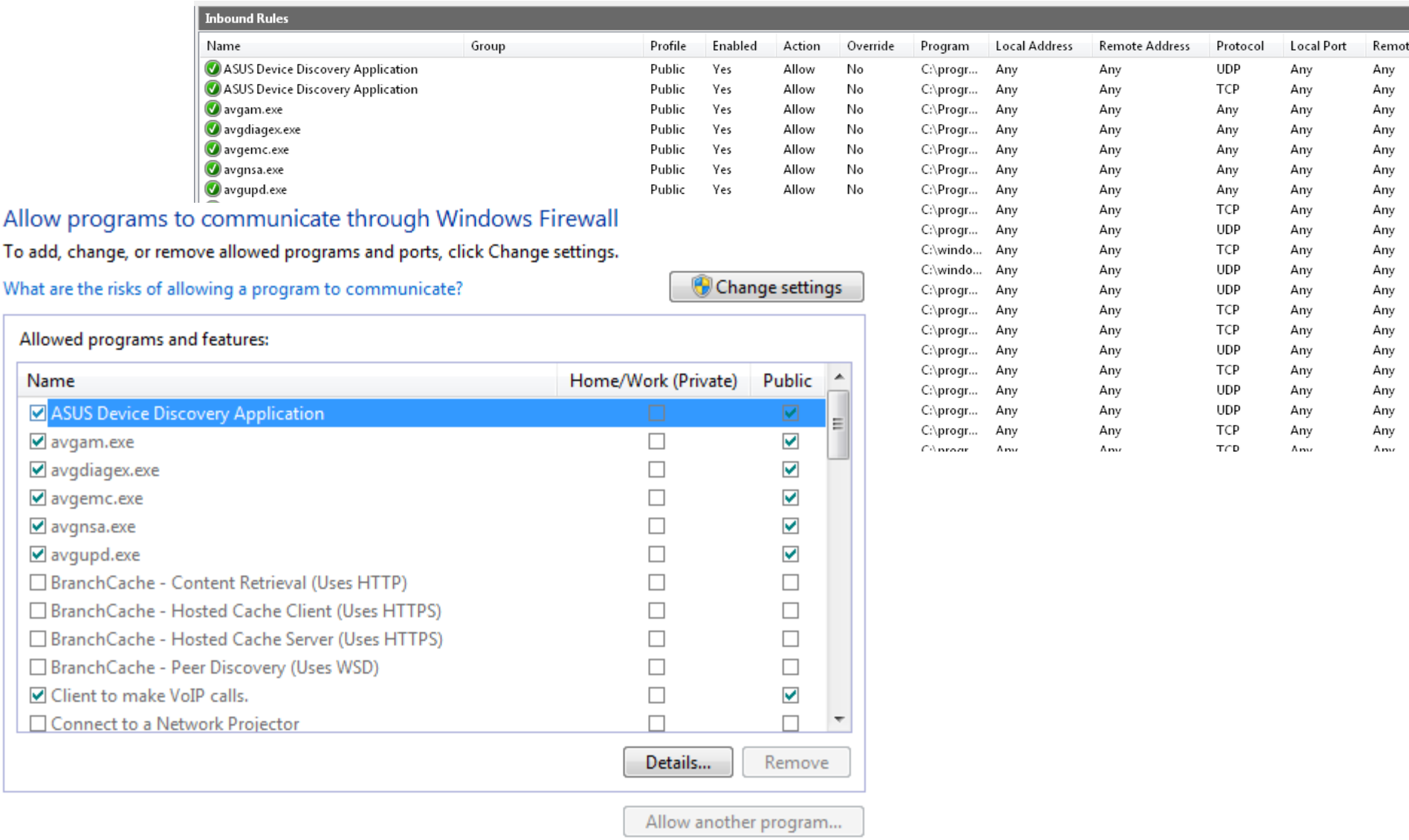
Lokální firewall ve Windows

- Windows 2000 a XP
  - Obsahují integrovaný firewall
  - Umožňuje filtrování/blokování příchozích spojení
    - i na úrovni jednotlivých aplikací/programů
  - Neumožňuje filtrování odchozích spojení!!!
    - komunikace infikovaného počítače ve vnitřní síti
- Windows 7
  - Umožňuje filtrování obou směrů

Lokální firewall – Windows 7



Lokální firewall – Windows 7



IDS

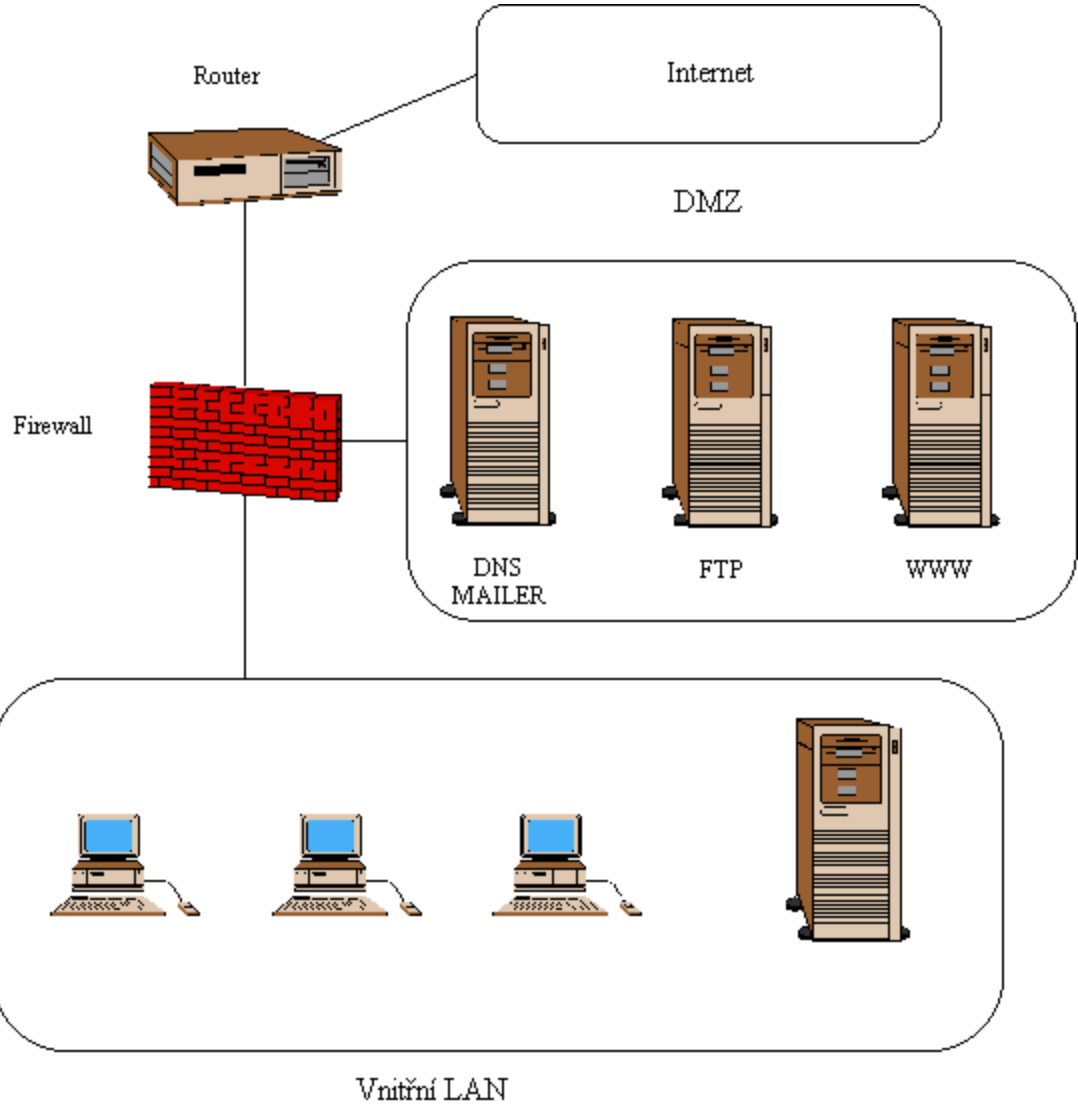
- Aktivní monitorování sítě a report podezřelé komunikace, událostí nebo porušení bezpečnostní politiky
  - Aktivní reakce na vzniklou událost (např. aktivní rekonfigurace firewallu)
  - Akce k předcházení bezpečnostních incidentů – intrusion prevention
- Typy IDS:
  - Network-based – úroveň počítačové sítě
    - Monitorování připojených síťových zařízení
  - Host-based – úrověň koncového zařízení (PC)
    - Analýza systémových volání, aplikačních logů, modifikací file-systemu, apod.
- Příklad konkrétního network-based IDS – SNORT

IDS – detekční techniky

- Detekce anomálií
  - Definice „normálního“ provozu v síti
  - Report v okamžiku, kdy dojde k odchylce od normálního provozu – např. skenování portů serveru
- Detekce na základě singatur
  - Známý útok má určitou „signaturu“ – průběh
  - Na základě detekce „průběhu“ lze odhalit počátek útoku

DMZ

- Umístění serverů, které maj
  být přístupné jak z vnitřní, ta
  vnější sítě
- Úroveň přístupu je různá (z
  vnitřní sítě typicky větší)
- Vnitřní síť nemá být přístupn
  vnější sítě



VPN, IPSec

- Ochrana vnitřní sítě tím, že přístup je povolen pouze z interních IP adres
- Jak řešit v případě, že je koncové zařízení mimo tento rozsah?
- Zabezpečený šifrovaný tunel na firemní VPN server
  - Přenášená data jsou šifrovaná až na úroveň vnitřní sítě
  - IP adresa klienta je z rozsahu vnitřní sítě – tzn. máme přístup k (jinak z venku nedostupných) vnitřní síti