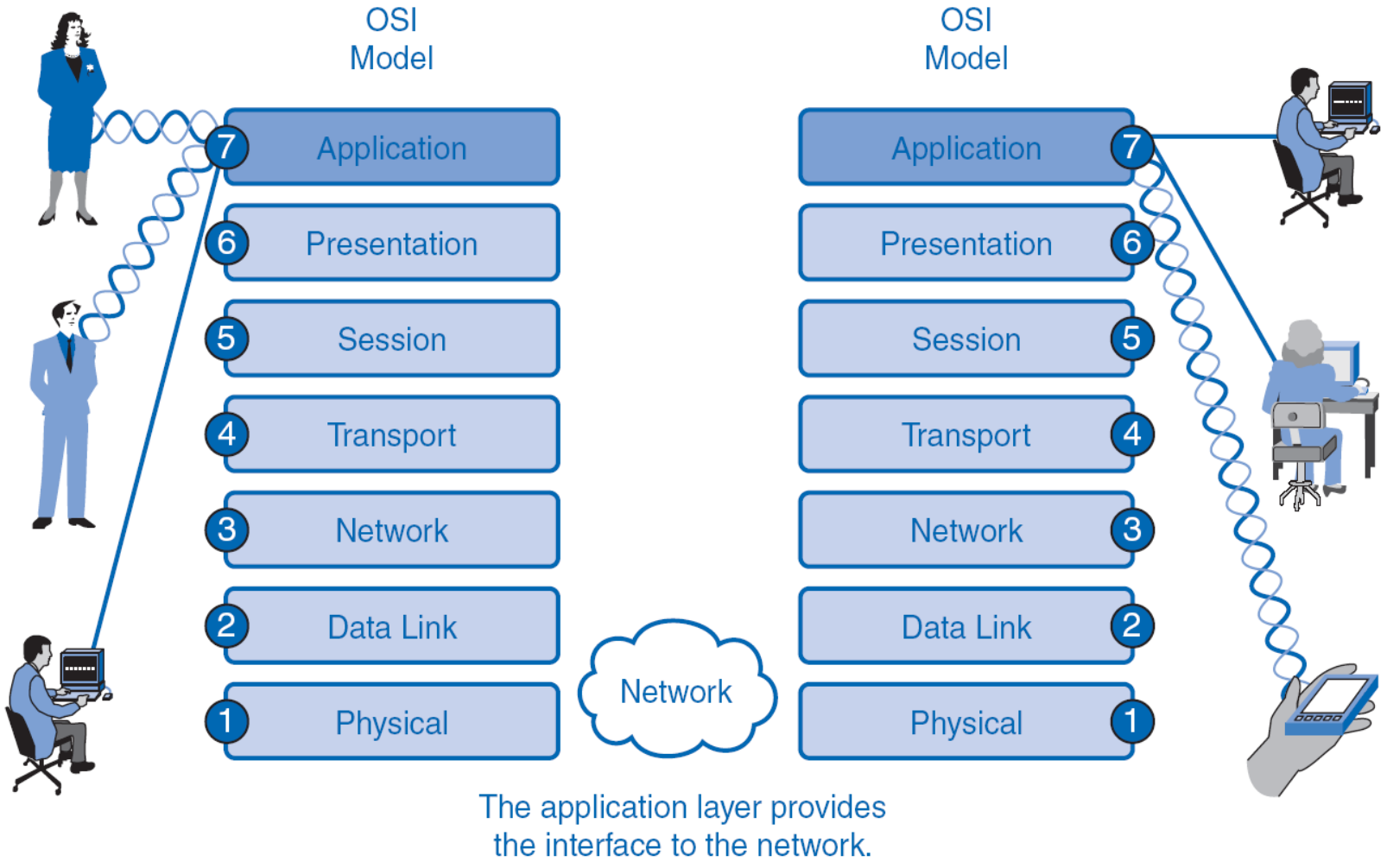
Protokoly aplikační vrstvy
Zabezpečení počítačových sítí

Jaromír Plhák
xplhak@fi.muni.cz

Aplikační vrstva (1)

- Programy a procesy, které využívají síťové komunikace pro služby uživatelů
- Telnet, (T/S)FTP, HTTP, DHCP, DNS, SMTP, IMAP, IRC, NFS, NTP, POP3, SMB, SNMP, SSH

Aplikační vrstva (2)



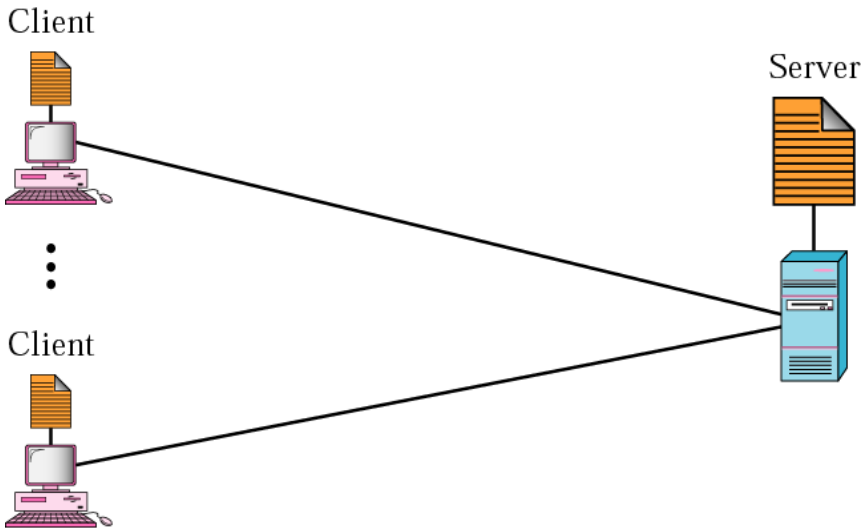
Klient-server

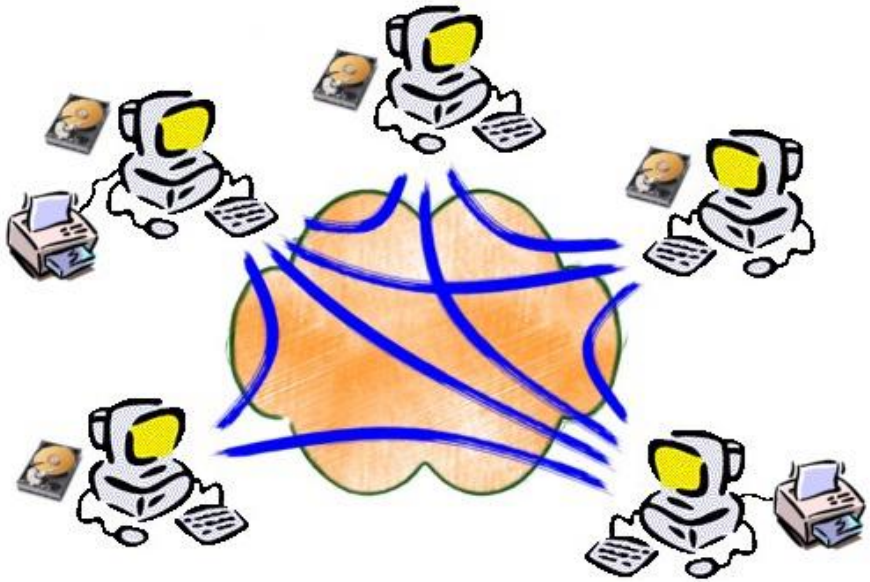
- Komunikace iniciována klientem (klient = aplikační program ovládaný uživatelem)
- Po ustavení komunikačního kanálu klient zasílá požadavky na server, ten mu odpovídá (mechanismus request-response)
- Po ukončení komunikace je komunikační kanál uzavřen (centralizace zdrojů)
- Valná většina aplikací v Internetu (WWW, FTP, DNS, SSH, . . .)

Peer-to-peer

- Jednotliví klienti spolu komunikují přímo (uzly jsou si rovnocenné)
- Každý uzel poskytuje své zdroje (výpočetní síla, úložná kapacita, atp.) ostatním uzlům
- Každý uzel využívá zdrojů poskytovaných ostatními uzly (decentralizace zdrojů)
- Např. sdílení souborů (Gnutella, G2, FastTrack), Skype, VoIP, atp.

Komunikační modely





Tenký klient

- Aplikace, u nichž se na straně klienta vykonává minimum aplikační logiky (většina se vykonává na straně serveru)
  - Větší hardwarové nároky na server a na komunikaci
- Jednodušší, menší nároky na HW (může tak být levnější)
- Menší škálovatelnost (příliš mnoho práce dělá server)
  - Většinou vyšší objemy přenášených dat
  - Existence Single point of failure (server)
- Příklad – vzdálené terminály

Tlustý klient

- Přesný opak tenkého klienta
  - Většina aplikační logiky se vykonává na straně klienta
  - Větší hardwarové i softwarové nároky na klienta
- Menší nároky na server => dobrá škálovatelnost
- Většinou nižší objem přenesených dat
  - Možnost práce offline
- Komplexní provedení i instalace, značná spotřeba lokálních zdrojů (CPU, paměť, disk)
- Příklad – Firefox

Telnet

- Protokol pro přihlášení ke vzdálenému systému (síťový virtuální terminál)
- Spojení typu klient-server protokolem TCP
- Umožňuje vzdálenou správu/řízení pomocí příkazů
- Standardně TCP/23
- Duplexně
- Nešifrované spojení
- Prostřednictvím telnetu se lze připojovat i na jiné (textově orientované) služby aplikační vrstvy

TFTP (1)

- Trivial File Transfer Protocol (1980)
- Jednoduchý protokol pro přenos dat/souborů
- Není zdaleka tak obsáhlý jako FTP
- Používá se v případech, kdy se celý protokol musí vejít do omezené paměti
  - Bootování bezdiskových stanic ze sítě
  - Flashování firmware do síťových zařízení

TFTP (2)

- Založeno na protokolu UDP
- Nutnost vlastního řízení spojení
  - Jedno spojení – jeden soubor
  - Při komunikaci je v síti vždy jen jeden paket
  - Čeká se na potvrzení a pak se pošle další
  - Pomalé spojení
- Maximální velikost souboru je 32 MB
- Nezabezpečený přenos dat

FTP (1)

- File Transfer Protocol
- Platformně nezávislý protokol pro přenos souborů protokolem TCP/21 a TCP/20
- Součástí prohlížečů nebo správců souborů
- Podpora textového nebo binárního přenosu
- Interaktivní protokol

FTP (2)

- Podpora přihlášení pomocí login/password
- Přihlašovací údaje i přenášená data jsou nešifrovaná
  - Existuje několik rozšíření, které podporuje kryptografii, např. FTPS (nezaměňovat s SFTP)
- Snížení rychlosti při přenosu velkého množství malých souborů

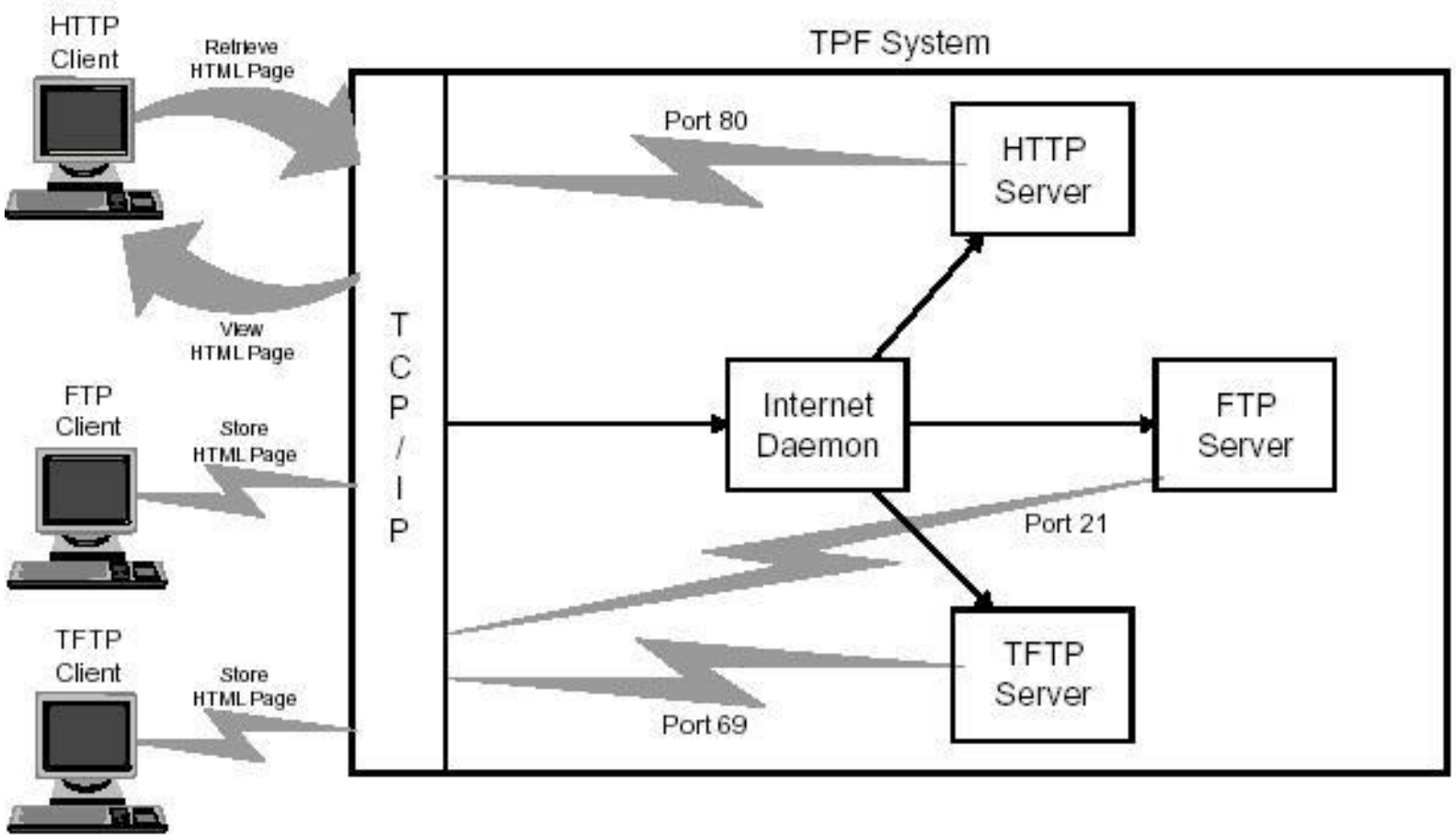
FTP (3)

- Pasivní režim
  - Navázání připojení pro přenos dat provádí klient
  - Na základě znalosti IP a portu serveru
- Aktivní režim
  - Navázání připojení pro přenos dat provádí server
  - Klient pouze naslouchá
  - Problém při použití NAT

SFTP

- Tunelování FTP skrz spojení navázané protokolem SSH (o SSH více později)
- Data jsou následně při přenosu šifrována
  - A tedy není možné zjistit, co se přenáší
- Klient pro bezpečný přenos souborů
  - WinSCP

FTP vs. TFTP


HTTP
Client
Retrieve
HTML Page
View
HTML Page
FTP
Client
Store
HTML Page
TFTP
Client
Store
HTML Page
TPF System
T
C
P
/
I
P
Port 80
HTTP
Server
Internet
Daemon
FTP
Server
Port 21
TFTP
Server
Port 69

DHCP

- Dynamic Host Configuration Protocol
- Automatické přidělování IP adres připojeným počítačům
- Zjednodušení a centralizování správy
- Nastavuje se
  - IP adresa
  - Maska
  - Brána (gateway)
  - DNS servery a případně další (např. NTP)
- Zprávy DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK

Možnosti přidělení IP adresy

- Ruční nastavení
  - Nevyužívá DHCP serveru
  - Konfigurace se zapisuje jednotlivě přímo do stanice
- Statická alokace
  - DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres
  - Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu
- Dynamická alokace
  - Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány
  - Časové omezení
  - Nepoužívané adresy přiděleny jiným stanicím

IRC

- Internet Relay Chat
- Otevřený protokol na textovou komunikaci
- Architektura klient – server
- Jedna z prvních možností on-line komunikace v reálném čase
- Komunikace probíhá(la) v kanálech („místnostech“)
- Dnes se sice ještě používá, ale už není na vzestupu

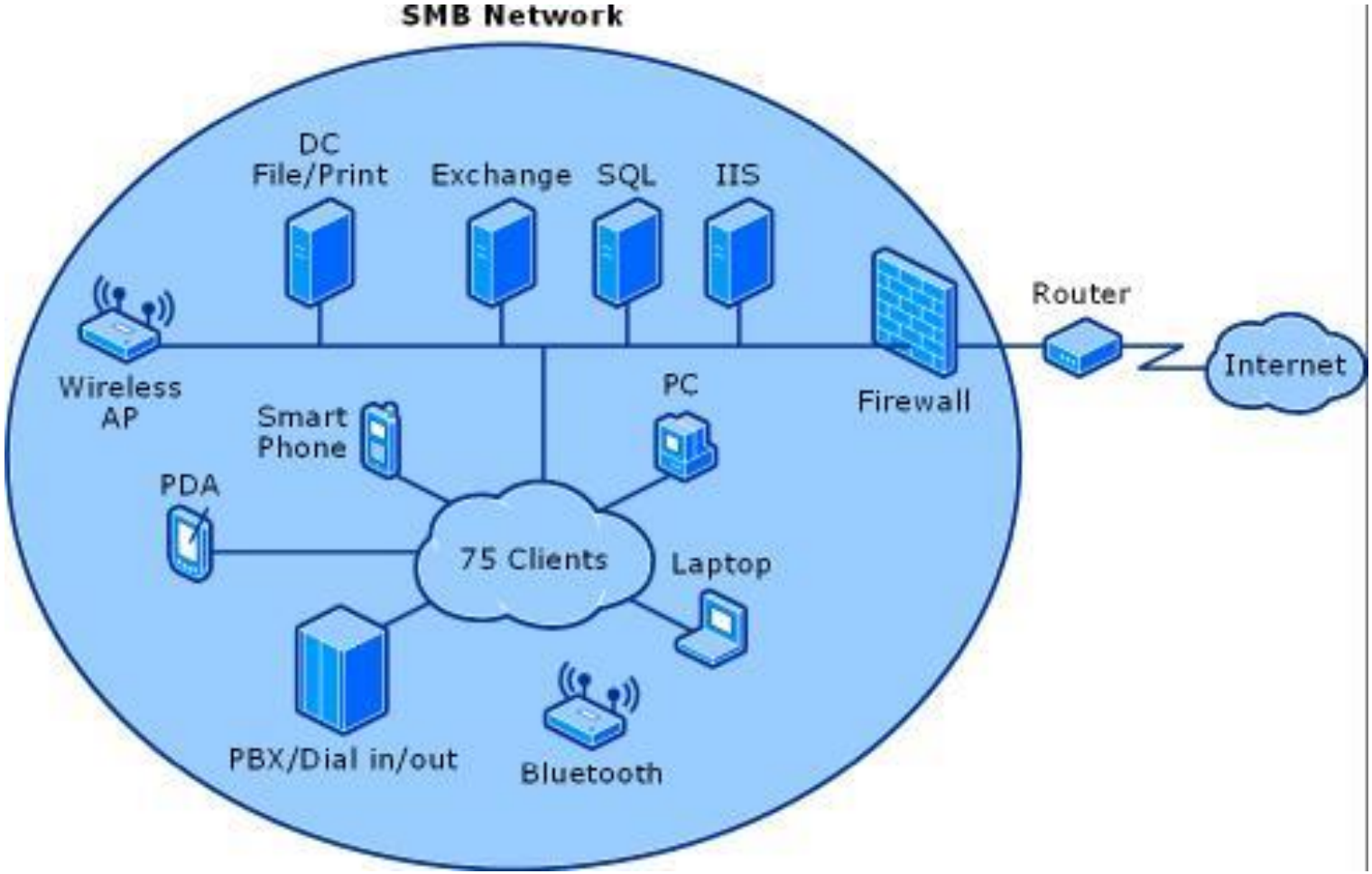
NFS

- Network File System
- Protokol pro vzdálený přístup k souborům
- Využívá protokolu UDP a později i TCP
- Typické použití
  - Připojení vzdáleného disku, který se pak jeví jako lokální úložiště
  - Nejčastěji v prostředí Linuxu
  - mount -t nfs server:/home /home

SMB

- Server Message Block
- Protokol sloužící ke sdílení tiskáren, souborů, skenerů apod. zejména v prostředí Windows
- Podporuje autentizaci klienta/uživatele
- Pracuje na principu klient-server
  - Server poskytuje přístup ke sdíleným prostředkům

SMB síť


SMB Network
DC
File/Print
Exchange
SQL
IIS
Router
Internet
Wireless
AP
Smart
Phone
PC
Firewall
PDA
75 Clients
Laptop
PBX/Dial in/out
Bluetooth

SNMP

- Simple Network Management Protocol
- Protokol pro správu sítě
  - Sběr různých dat (např. průtok dat na routeru)
  - Vyhodnocování (tabulky, grafy, přehledy)
  - Hledání potenciálních problematických míst v síti
  - Automatické reakce na zadané podmínky
    - Router při přetížení vzbudí administrátora SMSkou

NTP

- Network Time Protocol
- Protokol pro nastavení přesného času
- Nastavení času na základě odpovědí z několika NTP serverů
  - Přesnost v řádu milisekund
- Navržený protokol dokáže odolat zpoždění při doručování paketů
- V Linuxu příkaz ntpdate

SSH

- Secure Shell (TCP/22)
- Zabezpečený komunikační protokol pro vzdálené přihlášení
  - Náhrada za nezabezpečený telnet
- Podpora autentizace
- Transparentní šifrování přenášených dat
- V současnosti verze SSH-2
  - Silná kryptografie a kontrola integrity dat
  - Veřejný klíč vzdáleného stroje
- Putty

POP3

- Post Office Protocol version 3 (TCP/110)
- Protokol pro získávání emailových zpráv ze vzdáleného serveru
  - Ze vzdáleného serveru se stáhnou všechny zprávy na lokálního klienta
- Původně nešifrovaný přenos dat a autentizace
- V současnosti lze komunikaci šifrovat

IMAP

- Internet Message Access Protocol
- Protokol pro vzdálený přístup k emailové schránce vyžadující trvalé připojení
  - Nabízí pokročilou správu
  - Se schránkou je možné pracovat odkudkoliv
- IMAP podporuje zabezpečenou/šifrovanou variantu komunikace

HTTP

- Hypertext Transfer Protocol (TCP/80)
- Protokol pro výměnu zpráv/dokumentů ve formátu HTML
  - MIME (Multipurpose Internet Mail Extensions) umožní přenášet i multimediální a jiný obsah
- URL (Uniform Resource Locator) pro jednoznačnou identifikaci zdroje v Internetu
- Protokol pracuje na principu dotaz-odpověď
  - Tzn. je bezstavový (kontinuální komunikaci je potřeba řešit jinak)
- Zabezpečená varianta protokolu – HTTPS

Zabezpečení sítě – úvod (1)

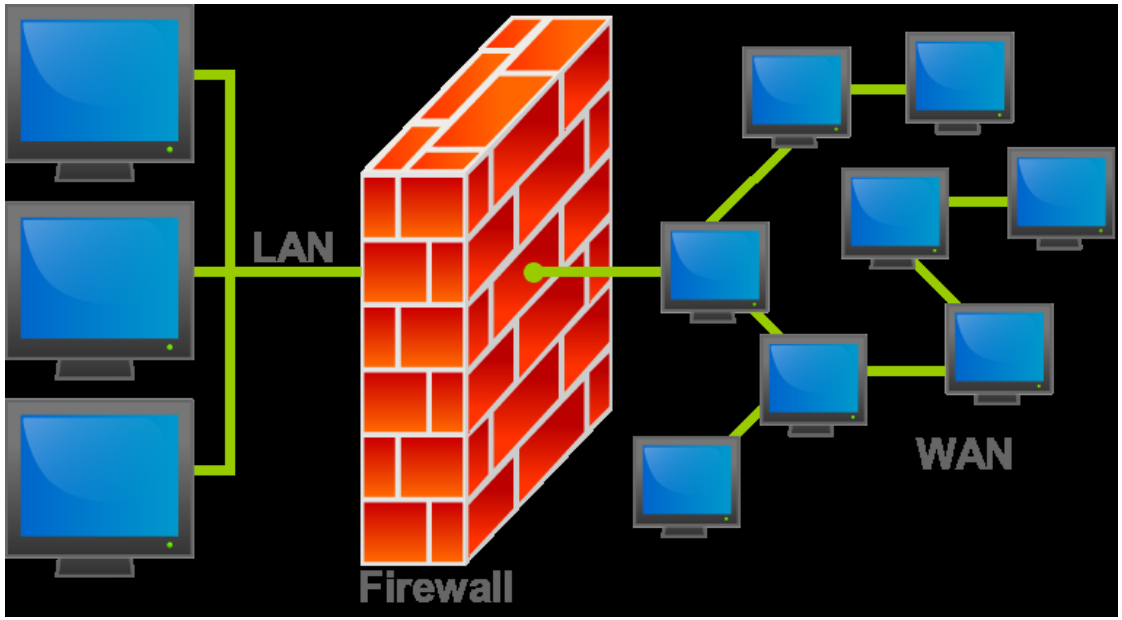
- Důvody pro zabezpečení (interní) sítě?
- Nebezpečí ze strany veřejného Internetu
  - Spyware
  - Malware
  - BOTy
  - Rootkity
  - Viry
  - Exploity
  - Skenování vnitřní sítě a hledání zranitelných míst
  - Spam
  - …
- Ohrožení (vnitřní) sítě, pokud je např. možné připojovat soukromé stanice (typicky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

Zabezpečení sítě – úvod (2)

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

Firewall (1)

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



Firewall (2)

- 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 produkty, integrace přímo v OS
- Běžná „home“ síťová zařízení (Wi-Fi AP) poskytují funkcionalitu firewallu
  - Je vhodné provést alespoň základní nastavení

Firewall (3)

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

Paketový filtr (1)

- 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 (2)

- 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 „snazší“ nastavení
  - Dělení provozu do řetězců INPUT, OUTPUT a FORWARD a dále do tabulek

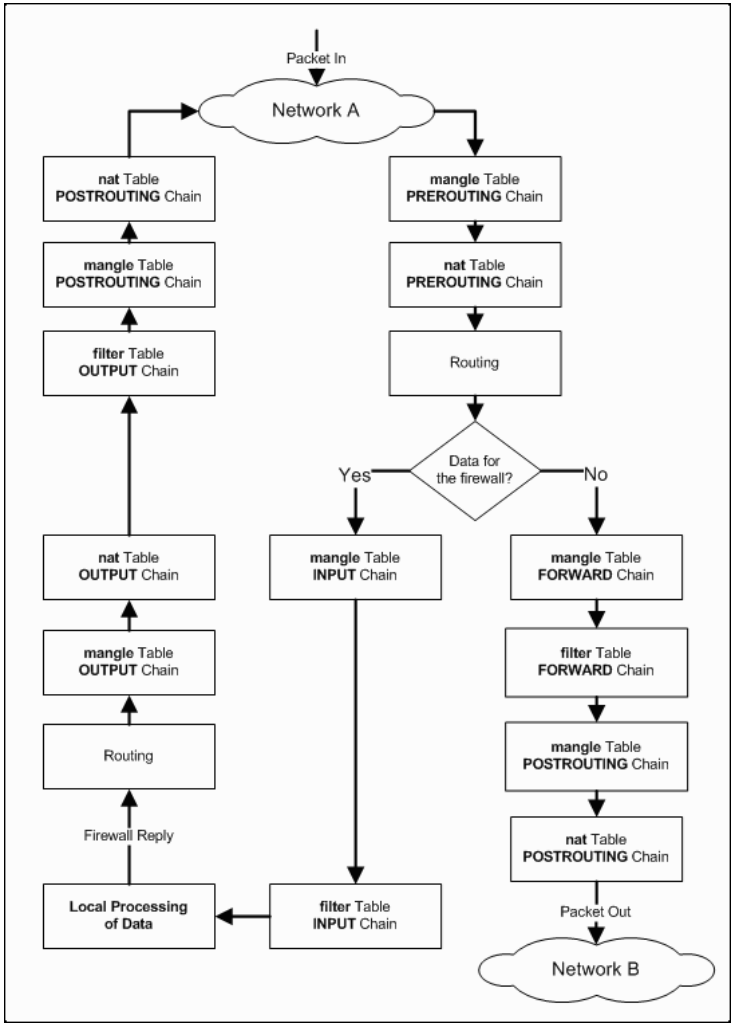
Paketový filtr (3)

- Pakety lze nejen filtrovat, ale i modifikovat!
  - Tzn. přepisovat IP adresy a čísla portů v IP hlavičkách jednotlivých paketů
- Pomocí paketového filtru 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 (4)

- 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
  - Vyšší latence
- Většinou se už tento přístup nepoužívá

Pokročilé stavové filtry

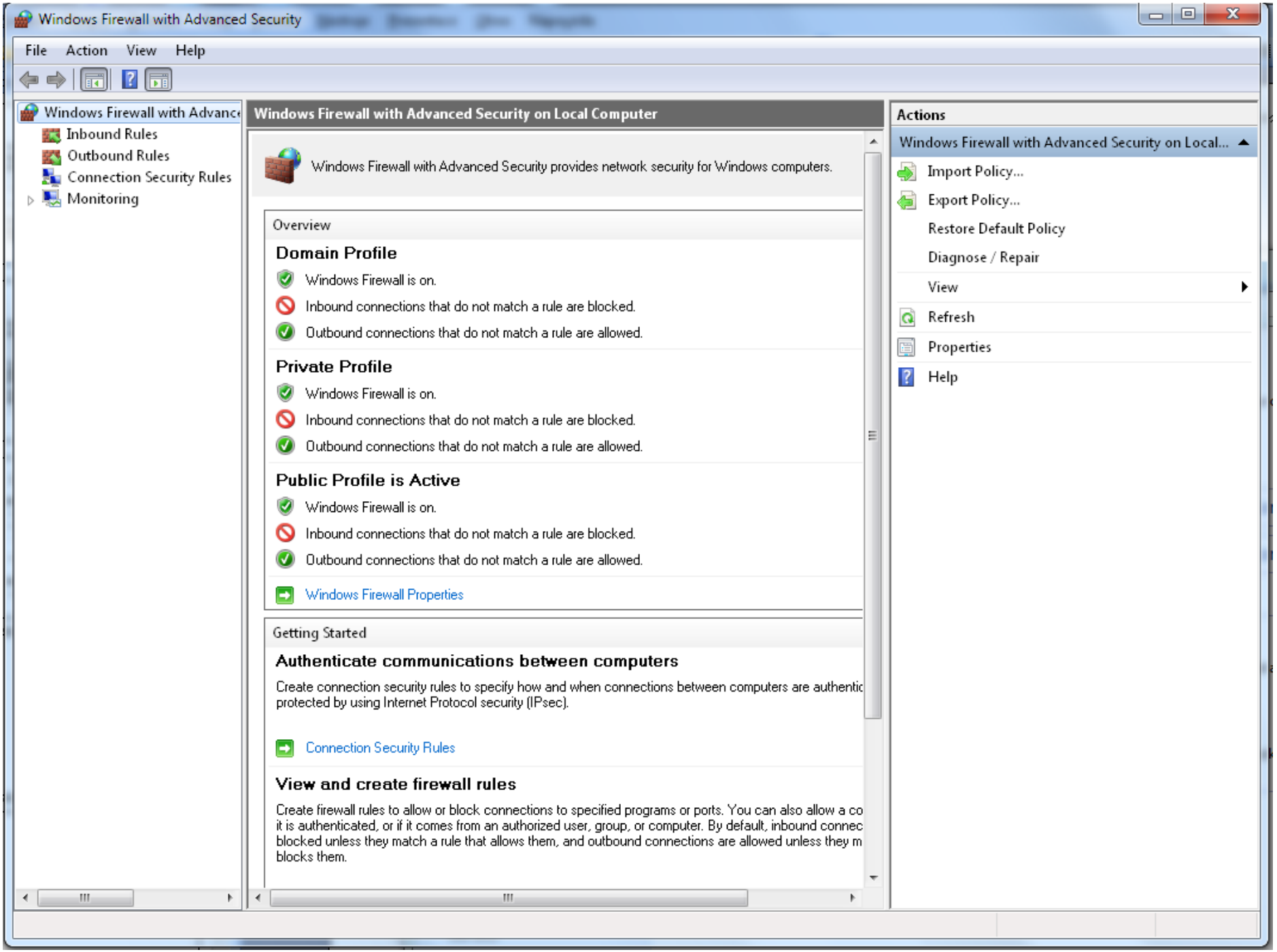
- Fungují principiálně stejně jako stavové filtry
- Navíc umožňují detailní analýzu přenášených dat a následné rozhodování
  - Např. špatné hlavičky emailu
  - Pokus o tunelování jiného typu provozu na portu, který je určený standardně např. pro WWW
- Heuristické analýzy s cílem identifikovat nebezpečný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

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
- Od Windows 7
  - Umožňuje filtrování obou směrů


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authentic
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a co
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connec
blocked unless they match a rule that allows them, and outbound connections are allowed unless they m
blocks them.
Actions
Windows Firewall with Advanced Security on Local...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remot
ASUS Device Discovery Application		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any
ASUS Device Discovery Application		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any
avgam.exe		Public	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any
avgdiagex.exe		Public	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any
avgemc.exe		Public	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any
avgnsa.exe		Public	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any
avgupd.exe		Public	Yes	Allow	No	C:\Progr...	Any	Any	Any	Any	Any
Client to make VoIP calls.		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any
Client to make VoIP calls.		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any
File Transfer Program		Public	Yes	Allow	No	C:\windo...	Any	Any	TCP	Any	Any
File Transfer Program		Public	Yes	Allow	No	C:\windo...	Any	Any	UDP	Any	Any
Miranda IM		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any
Miranda IM		Private	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any
Miranda IM		Public	Yes	Allow	No	C:\progr...	Any	Any	TCP	Any	Any
Miranda IM		Private	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any
Nokia Ovi Suite 2											Any
Nokia Ovi Suite 2											Any
Nokia Service Layer Host Process											Any
Nokia Service Layer Host Process											Any
Nokia Software Updater											Any

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Change settings

Allowed programs and features:

Name	Home/Work (Private)	Public
ASUS Device Discovery Application	☐	☑
avgam.exe	☐	☑
avgdiagex.exe	☐	☑
avgemc.exe	☐	☑
avgnsa.exe	☐	☑
avgupd.exe	☐	☑
BranchCache - Content Retrieval (Uses HTTP)	☐	☐
BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐
BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐
BranchCache - Peer Discovery (Uses WSD)	☐	☐
Client to make VoIP calls.	☐	☑
Connect to a Network Projector	☐	☐

Details... Remove

Allow another program...

IDS (1)

- Intrusion Detection System
- 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

IDS (2)

- Typy IDS
  - Network-based – úroveň počítačové sítě
- Monitorování připojených síťových zařízení
  - Host-based – úrověň koncového zařízení (PC)
- Analýza systémových volání, aplikačních logů, modifikací file systému, apod.
- Příklad konkrétního network-based IDS – SNORT

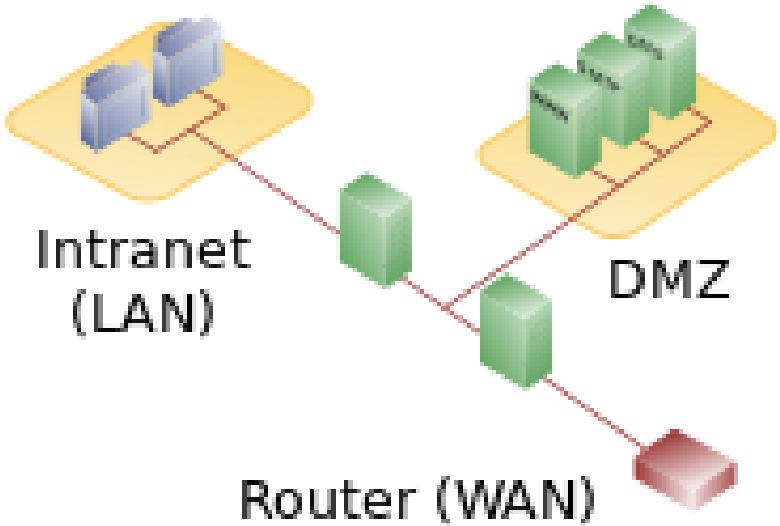
IDS – detekční techniky

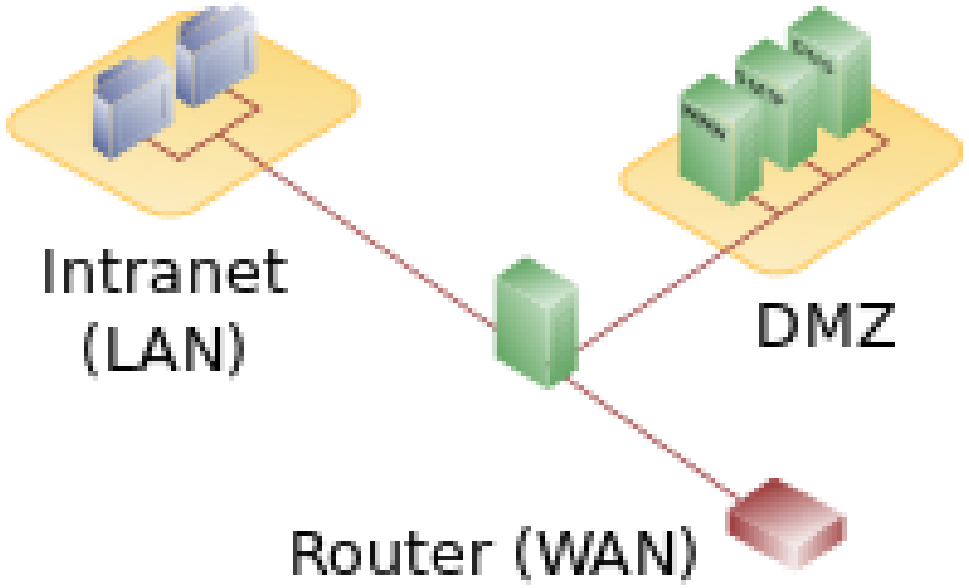
- Detekce anomálií
  - Definice „normálního“ provozu v síti
  - Report v okamžiku, kdy dojde k odchylce od normálního provozu – např. skenování portů serveru
- Detekce na základě singatur
- Známý útok má určitou „signaturu“ – průběh
- Na základě detekce „průběhu“ lze odhalit počátek útoku

DMZ (1)

- DeMilitarized Zone
- Umístění serverů, které mají být přístupné jak z vnitřní, tak z vnější sítě
- Úroveň přístupu je různá (z vnitřní sítě typicky větší)
- Vnitřní síť nemá být přístupná z vnější sítě

DMZ (2)





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