Bezpečnost v počítačových sítích

Petr Grygárek

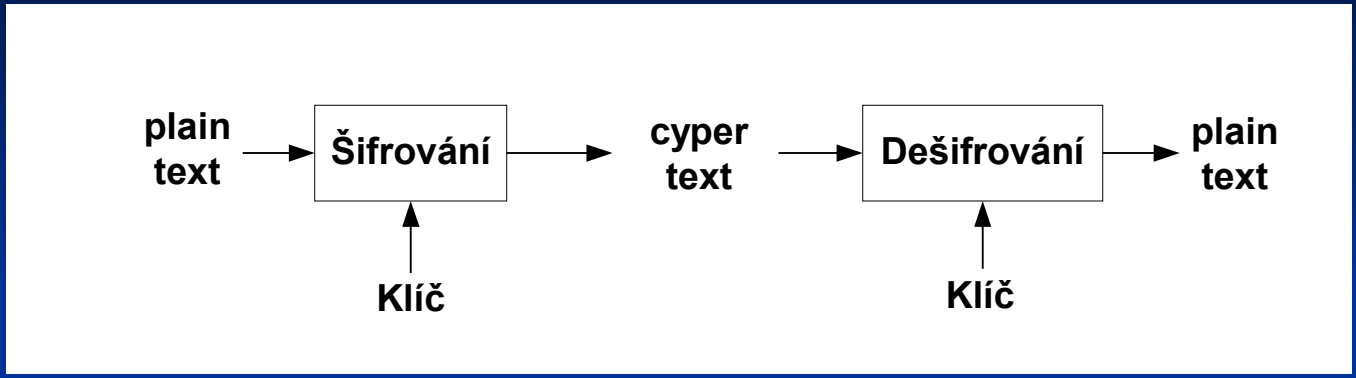
Rozsah problematiky bezpečnosti

- Bezpečnost je proces, ne technické opatření
  - Zahrnuje i firemní politiky k použití sítě (vč. sankcí za porušení)
  - Vždy je pro uživatele omezující
    - je třeba najít kompromis mezi pohodlím uživatelů a bezpečností
- Zahrnuje síťovou infrastrukturu i OS koncových stanic
  - Včetně problematiky virů
  - Infikované stanice mohou útočit na síťovou infrastrukturu

Základní pojmy

- Utajení (confidentality) – posluchač na kanále datům nerozumí
- Autentizace (authentication) – jistota, že odesílatel je tím, za koho se vydává
- Integrita (integrity) – jistota, že data nebyla na cestě zmodifikována
- Nepopiratelnost (non-repudiation) – zdroj dat nemůže popřít jejich odeslání

Kryptografický systém



Možnosti implementace:

- Utajit algoritmus
  - když se prozradí, je implementace k ničemu
- Zavést klíče parametrizující algoritmus
  - je-li dost možných klíčů, může být algoritmus známý

Symetrický systém

Vlastnosti symetrického systému

- Sdílený klíč
- Implementace algoritmů efektivní (rychlost), lze realizovat hardwarově
- Algoritmy DES, 3DES, AES, …
- Problém s distribucí klíčů

Autentizace v symetrickém systému

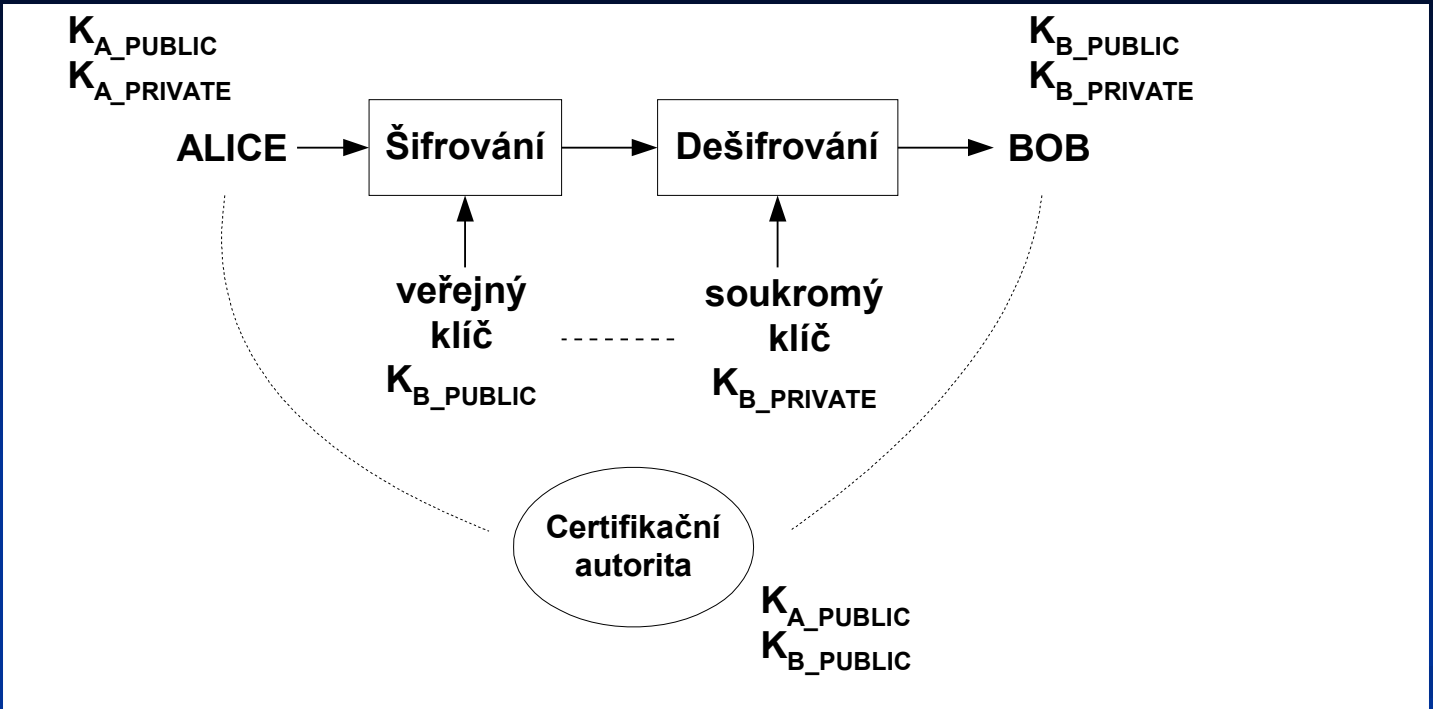
- Zakódování username klíčem u odesílatele, stejným klíčem dekódování u příjemce + test smysluplnosti jména
  - např. připojení otisku (hash) ke jménu na vysílači a kontrolní výpočet s porovnáním hashe na přijímači

Zajištění integrity zpráv

- [zpráva+sdílený tajný klíč]->hash
  - Hashing algoritmus = jednosměrná funkce
- Pošle se zpráva+hash
- Na přijímači se za zprávu připojí sdílený tajný klíč, vypočte se hash, porovná s přijatým

Asymetrický systém

Veřejné a soukromé klíče



- Klíče se generují jako doplňující se pár
  - – veřejný (public) a soukromý (private) klíč
- Jeden klíč použit pro šifrování, druhý pro dešifrování
  - (je jedno, který z nich k čemu)
- Mnohem náročnější na výpočty, pomalejší

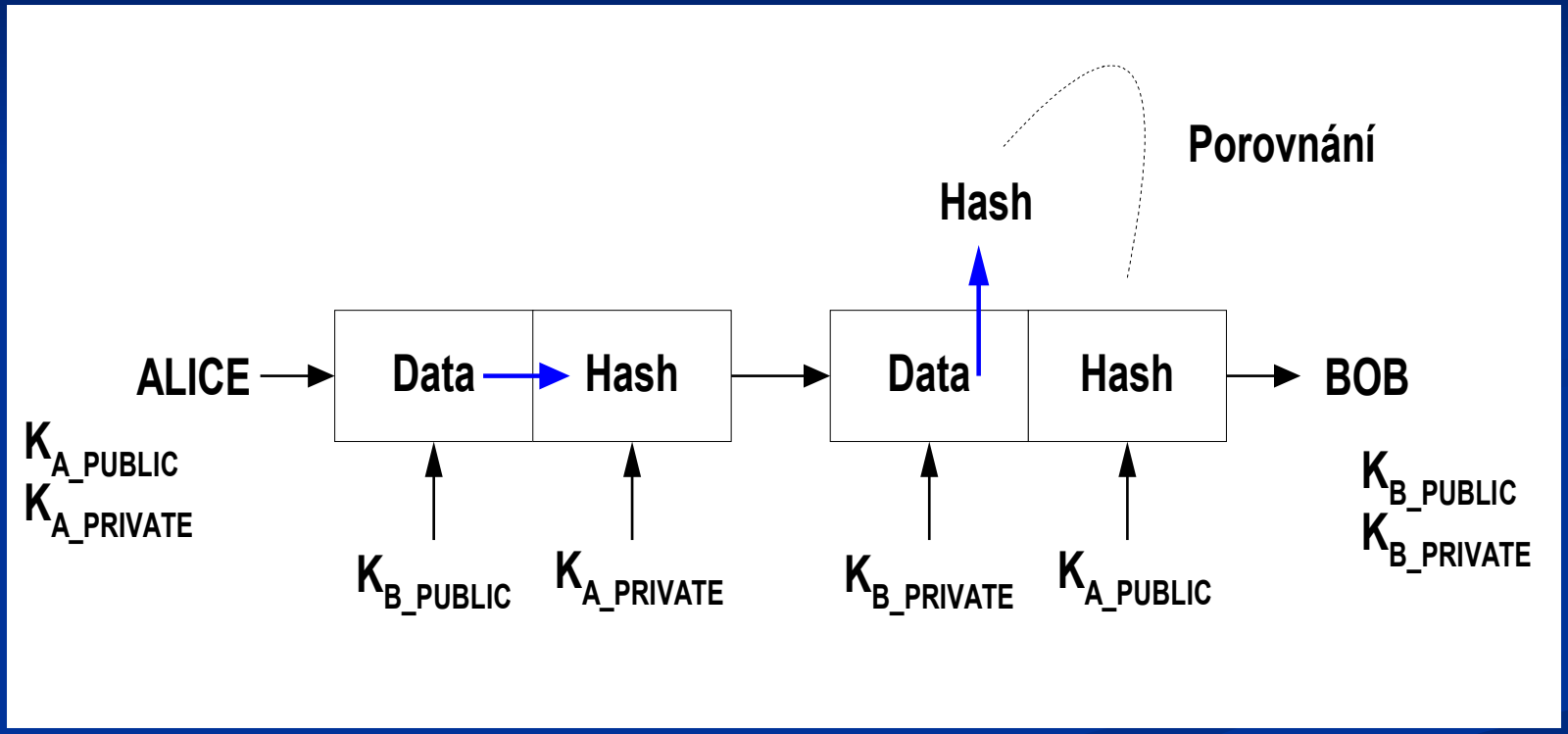
Použití asymetrického systému

- Digitální podpisy
  - Odpadá problém s distribucí klíčů
- Asymetrický systém se běžně využívá pro předávání (dynamicky generovaných) klíčů pro symetrický systém.

Certifikační autorita

- Entita, které je důvěřováno
- Vytváří dvojice soukromý klíč-veřejný klíč
  - veřejný klíč označí údaji identifikujícími vlastníka, „podepíše“soukromým klíčem certifikační autority a zveřejní
  - soukromý klíč předá osobně vlastníkovi po ověření jeho identity
- Veřejný klíč certifikační autority musí být důvěryhodným způsobem zaveden do každého systému
  - „na disketě“, součást distribuce OS nebo prohlížeče WWW

Autentizace v asymetrickém systému



Možnosti zabezpečení přenášených dat

Zabezpečení na jednotlivých vrstvách OSI-RM

- L2
  - hop-by-hop, neefektivní
  - Layer 2 tunneling protocol (L2TP), point to point tunelling protocol (PPTP)
- **L3**
  - **nezávislé na médiu/síťové technologii i aplikaci**
  - IPSec
- L4
  - Secure Sockets Layer (SSL)
  - jen TCP
- L7
  - řeší jednotlivé aplikace
  - např. S/MIME

Filtrace provozu

- Bezestavová (paketové filtry)
  - Výsledkem propuštění nebo zahození paketu
  - Pouze na základě dat obsažených v paketu
  - Problém s inspekcí 4. a vyšší vrstvy při použití fragmentace
- Stavová (transparentní nebo proxy server)
  - Rekonstrukce datových toků
  - Potřeba udržovat stav pro každý tok
    - omezená škálovatelnost

Paketové filtry

Access Control Lists – ACL

- Aplikovány nejčastěji na rozhraních směrovačů
  - lze filtrovat i podle záhlaví 2. vrstvy na přepínačích
- Filtrují provoz vstupující do rozhraní nebo vystupující z rozhraní
- Filtrace podle informací ze síťové a vyšších vrstev
  - příp. i podle 2. vrstvy

Definice ACL

- ACL tvořen sekvencí položek zakazující nebo povolující průchod paketů vyhovující kritériím definovaným danou položkou
- ACL procházen postupně odshora dolů, až se narazí na první položku, jejímž kritériím zkoumaný paket vyhovuje
  - Podle typu položky se paket propustí nebo zahodí
  - Další položky se nezkoumají
- Na konci ACL implicitní zákaz veškerého provozu
  - co není explicitně dovoleno, je zakázáno

Návrh filtrace provozu pomocí ACL

Je třeba stanovit

- na kterém rozhraní kterého směrovače bude ACL aplikován
  - Často i více ACL na více rozhraních
- zda bude ACL filtrovat provoz vstupující do rozhraní nebo z rozhraní vystupující
  - Na rozhraní max. jeden ACL ve směru dovnitř a jeden ve směru ven
- jaká kritéria (položky) způsobující propuštění nebo zahození procházejících paketů bude ACL obsahovat

ACL – obvyklá chyba

Při návrhu ACL je třeba mít neustále na zřeteli, že nestačí povolit datový tok povoleného aplikačního protokolu pouze ve směru z vnitřní sítě ven, ale i „odpovědi“ ve směru dovnitř.

- Čísla zdrojového a cílového portu budou pro zpětný směr přehozená

Příklad:
Použití ACL na Cisco IOS

Definice položek ACL - Syntaxe

access-list <acl_number> {permit | deny} <PROTOCOL> <source-IP-addr> <source-addr-wildcard> [<source-port>] <destination-IP-addr> <destination-addr-wildcard> [<destination-port>] [protocol-dependent-options]

- Wildcard maska říká, které bity se mají srovnávat a které ne
  - 0=srovnávat, 1=nesrovnávat
  - "Obrácená subnet maska"

Příklad definice ACL (ACL č. 101)

```
access-list 101 permit udp 200.1.1.100 0.0.0.0
  eq 53 158.196.135.0 0.0.0.255
```

- Povolit UDP z portu 53 stroje 200.1.1.100 do sítě 158.196.135.0/24

```
access-list 101 permit icmp 0.0.0.0
  255.255.255.255 158.196.135.0 0.0.0.255 echo-
  reply
```

- Povolit ICMP zprávy Echo Reply odkudkoli do sítě 158.196.135.0/24

```
access-list 101 deny ip 100.1.1.0 0.0.0.255
  158.196.135.0 0.0.0.255
```

- Zakázat IP (a tím i všechny protokoly v něm nesené) ze sítě 100.1.1.0/24 do sítě 158.196.135.0/24

```
access-list 101 permit tcp 0.0.0.0
  255.255.255.255 eq 80 158.196.135.101 0.0.0.0
  established
```

- Povolit TCP odkudkoli z portu 80 na stroj 158.196.135.101, ale jen již zřízená spojení (nedovolí průchod TCP segmentu se SYN=1, ACK=0)

Syntaktické zkratky

- **any**
  - = libovolná IP adresa
    + wildcard mask 255.255.255.255
- **host X.X.X.X**
  - = IP adresa X.X.X.X + wildcard mask 0.0.0.0

Příklad:

permit tcp host 158.196.100.100 any eq 80

Přiřazení ACL na rozhraní

```
interface s0
 ip access-group 101 in
```

- Na určité rozhraní se přiřadí ACL identifikovaný číslem
  - in = filtruje provoz směrem do rozhraní (vstupující do směrovače)
  - out = filtruje provoz směrem z rozhraní (vystupující ze směrovače)

Časově závislé ACL

- Jednotlivé položky ACL (permit/deny) mohou platit jen v zadané časovém rozsahu
- Např. propouštění provozu z učeben na WWW servery Internetu pouze v době mimo výukové hodiny :-)

Reflexivní ACL

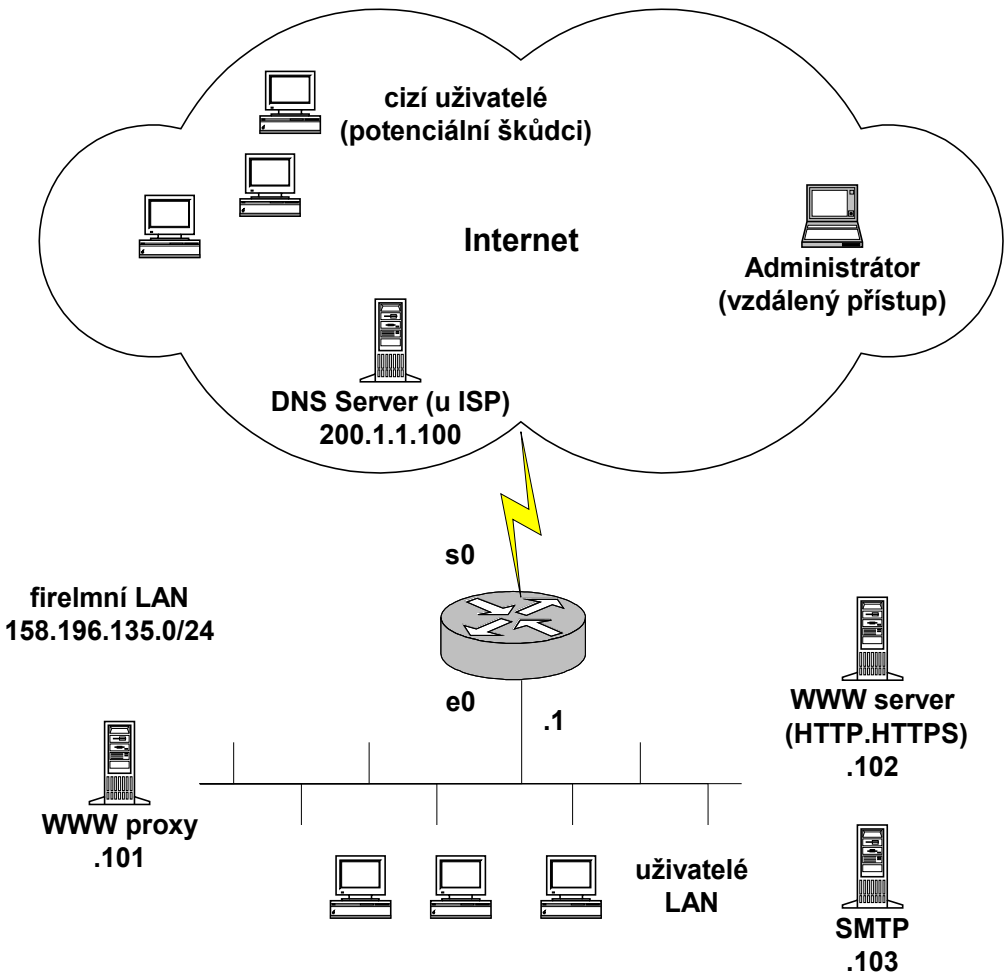
- Automaticky propouští vstupní provoz, který odpovídá povolenému provozu výstupnímu
  - Povolený výstupní provoz definován manuálně – výstupní ACL
  - Vstupní ACL implicitně zakazuje vše
  - Při průchodu určitého typu povoleného provozu ven automaticky vzniká „permit“ položka ve vstupním ACL s přehozenou zdrojovou a cílovou adresou a portem
- Otevření ACL trvá po dobu trvání odpovídajícího výstupního datového toku
  - do detekce FIN (RST) v TCP spojení nebo vypršení timeoutu neaktivity u UDP relace

Použití ACL - postup

- Analýza aplikací
  - Jaké aplikace v síti podporujeme ?
  - Jaký protokol a jaké porty každá aplikace používá ?
    - Jsou použity dynamické porty ?
- Na která rozhraní aplikujeme ACL ?
  - V typickém případě jeden ACL pro filtraci provozu dovnitř a jiný pro filtraci provozu ven
    - Je vhodné předejít situaci, kdy je paket nejprve směrován a pak zahozen výstupním ACL
- Definice obsahu jednotlivých ACL
  - Nezapomínat na povolení zpětného směru provozu !

Příklad použití ACL

Situace


cizí uživatelé
(potenciální škůdci)
Internet
Administrátor
(vzdálený přístup)
DNS Server (u ISP)
200.1.1.100
s0
firelmní LAN
158.196.135.0/24
e0
.1
WWW server
(HTTP.HTTPS)
.102
WWW proxy
.101
uživatelé
LAN
SMTP
.103

Požadavky na podporované služby

- Firma provozuje svůj vlastní poštovní server (SMTP) přístupný zvenčí na adrese 158.196.135.103.
- Firma provozuje svůj vlastní WWW server (HTTP, HTTPS) přístupný zvenčí na adrese 158.196.135.102.
- Přístup lokálních klientů ke službě WWW (HTTP i HTTPS) jde výhradně přes proxy server s adresou 158.196.135.101.
- Ze stanic LAN lze do Internetu otevírat pouze spojení SSH.
- DNS server provádějící rekurzivní vyhledávání jmen pro všechny klienty na LAN je u poskytovatele Internetu (ISP) na adrese 200.1.1.100.
- Je povolen ping z LAN do Internetu, v opačném směru však z bezpečnostních důvodů nikoli.
- Vzdálený administrátor je schopen připojit se odkudkoli z Internetu na počítač s WWW serverem pomocí služby SSH.

Explicitně nejmenovaný provoz je zakázán

Analýza aplikací

Služba (aplikační protokol)	Protokol	Port
HTTP	TCP	80
HTTPS	TCP	443
SMTP	TCP	25
DNS	UDP	53
ping	ICMP	Zprávy Echo request a Echo reply

Žádná z použitých služeb nevyužívá dynamicky přidělované porty.

Určení rozhraní pro aplikaci ACL

Označení ACL	Rozhraní	Směr
101	s0	in
102	e0	in

- Provoz přicházející z vnější sítě a vstupující do rozhraní s0 před dalším směrováním profiltrujeme ACL 101
- Provoz přicházející z vnitřní sítě a vstupující do rozhraní e0 před dalším směrováním profiltrujeme ACL 102

Návrh ACL 101 (s0, in)

Pořadí položky	Povolení / zákaz	Protokol	Zdrojová IP adresa	Zdrojový port	Cílová IP adresa	Cílový port
1	zakázat	IP	158.196.135.0/24		*	
2	povolit	TCP	*	*	158.196.135.103	25
3	povolit	TCP	*	*	158.196.135.102	80
4	povolit	TCP	*	*	158.196.135.102	443
5	povolit	TCP	*	*	158.196.135.102	22
6	povolit	UDP	200.1.1.100	53	158.196.135.0/24	*
7	povolit	ICMP	*		158.196.135.0/24	Echo reply+
8	povolit	TCP	*	80	158.196.135.101	*
9	povolit	TCP	*	443	158.196.135.101	*
10	povolit	TCP	*	22	158.196.135.0/24	*
11	zakázat	IP	*		*	

+ Poznámka:
Echo Reply je bližší specifikace typu zprávy ICMP, nikoli číslo portu (uvedeno ve sloupci portu jen pro úsporu místa)

Návrh ACL 102 (e0, in)

Pořadí položky	Povolení / zákaz	Protokol	Zdrojová IP adresa	Zdrojový port	Cílová IP adresa	Cílový port
1	povolit	TCP	158.196.135.101	*	*	80
2	povolit	TCP	158.196.135.101	*	*	443
3	povolit	TCP	158.196.135.0/24	*	*	22
4	povolit	UDP	158.196.135.0/24	*	200.1.1.100	53
5	Povolit	ICMP	158.196.135.0/24		*	Echo request+
6	povolit	TCP	158.196.135.103	25	*	*
7	povolit	TCP	158.196.135.102	80	*	*
8	povolit	TCP	158.196.135.102	443	*	*
9	povolit	TCP	158.196.135.102	22	*	*
10	zákaz	IP	*		*	

+ Poznámka:
Echo Reply je bližší specifikace typu zprávy ICMP, nikoli číslo portu (uvedeno ve sloupci portu jen pro úsporu místa)

Cisco IOS: konfigurace ACL 101
(+přiřazení na rozhraní)

```
access-list 101 deny ip 158.196.135.0 0.0.0.255 any
access-list 101 permit tcp any  host 158.196.135.103 eq 25
access-list 101 permit tcp any  host 158.196.135.102 eq 80
access-list 101 permit tcp any  host 158.196.135.102 eq 443
access-list 101 permit tcp any  host 158.196.135.102 eq 22
access-list 101 permit udp host 200.1.1.100 eq 53 158.196.135.0 0.0.0.255
access-list 101 permit icmp any 158.196.135.0 0.0.0.255 echo-reply
access-list 101 permit tcp any eq 80 host 158.196.135.101 established
access-list 101 permit tcp any eq 443 host 158.196.135.101 established
access-list 101 permit tcp any eq 22 158.196.135.101 0.0.0.255 established

interface s0
 ip access-group 101 in
```

Cisco IOS: konfigurace ACL 102

(+přiřazení na rozhraní)

```
access-list 102 permit tcp host 158.196.135.101 any eq 80
access-list 102 permit tcp host 158.196.135.101 any eq 443
access-list 102 permit tcp 158.196.135.0 0.0.0.255 any eq 22
access-list 102 permit udp 158.196.135.0 0.0.0.255 host 200.1.1.100 eq 53
access-list 102 permit icmp 158.196.135.0 0.0.0.255 any echo
access-list 102 permit tcp host 158.196.135.103 eq 25 any established
access-list 102 permit tcp host 158.196.135.102 eq 80 any established
access-list 102 permit tcp host 158.196.135.102 eq 443 any established
access-list 102 permit tcp host 158.196.135.102 eq 22 any established

interface e0
 ip access-group 102 in
```

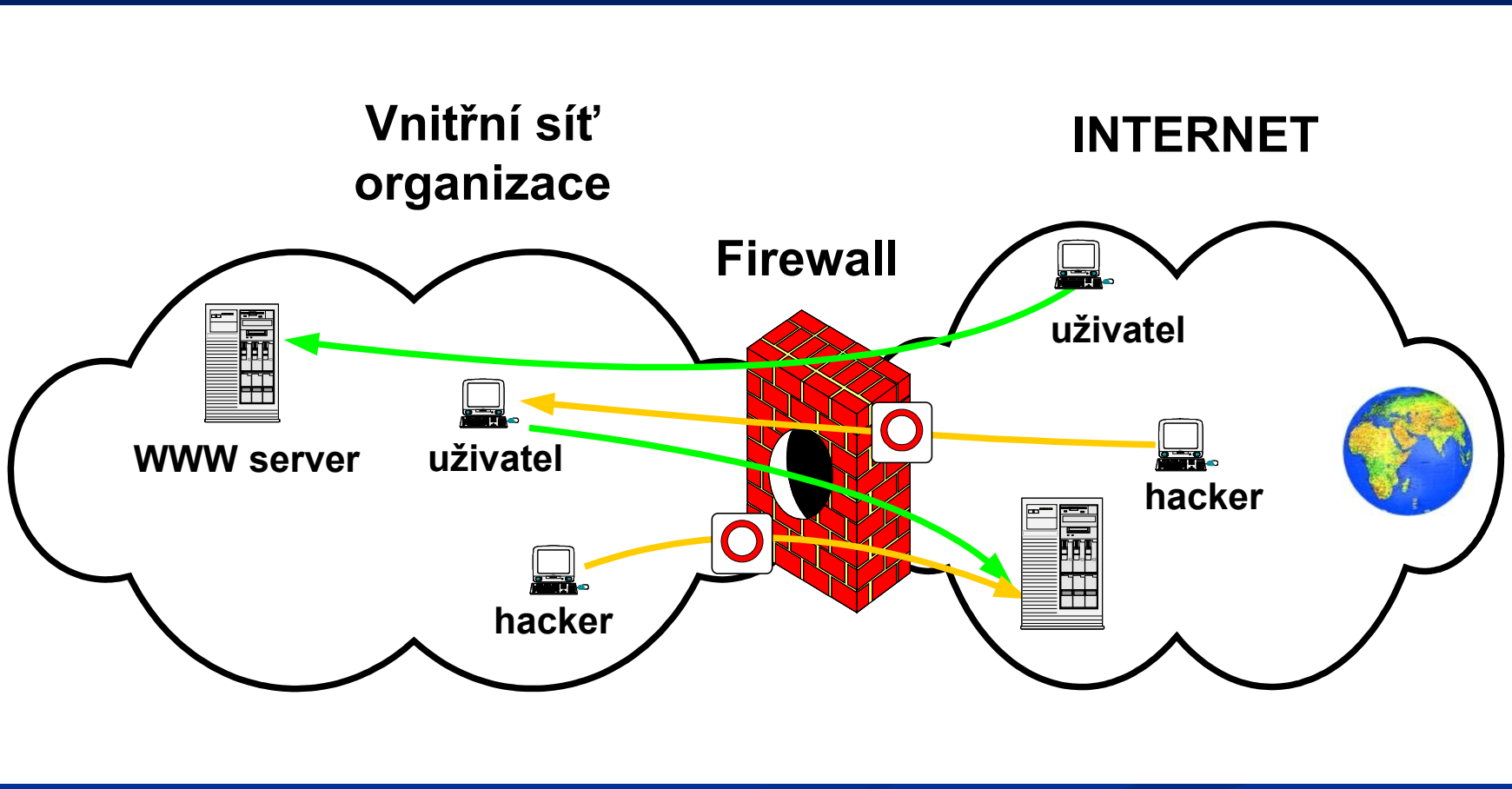
Stavová inspekce provozu

Firewally

Oddělují důvěryhodnou a nedůvěryhodnou část sítě

- Často uspořádání s demilitarizovanou zónou
  - Vnitřní síť, vnější síť, demilitarizovaná zóna (DMZ)
  - V DMZ „bastillon hosts“ (servery s řádně zabezpečeným OS)
  - Zákaz přímého provozu mezi vnější a vnitřní síti
- Transparentní (chování jako router/bridge)
- Proxy servery

Funkce firewallu



Implementace stavových firewallů

- Hardwarové
  - např. Cisco PIX, …
  - není známa vnitřní implementace OS – bezpečnost
- Softwarové
  - Linux – iptables (umí i stavovou filtraci)
  - NetBSD – velmi pružný, snadno čitelné konfigurační soubory
  - …

Cisco IOS with Firewall Feature Set: Context-Based Access Control

- Zkoumá řídící kanál vybraných aplikačních protokolů, podle aktivit na něm otevírá dynamické porty pro data (FTP, protokoly IP telefonie, …)
  - Otevírá vstupní ACL pro návratový provoz patřící k relaci některého z vybraných aplikačních protokolů iniciované z vnitřní sítě
  - Pro neznámé aplikační protokoly pracuje na úrovni TCP/UDP podobně jako reflexivní ACL
- Umí detekovat i některé známé útoky (SYN flood, podezřelá sekvenční čísla mimo aktuální okno, umí rušit half-open spojení)

Bezpečnost a NAT

Výhody NAT pro zabezpečení sítě

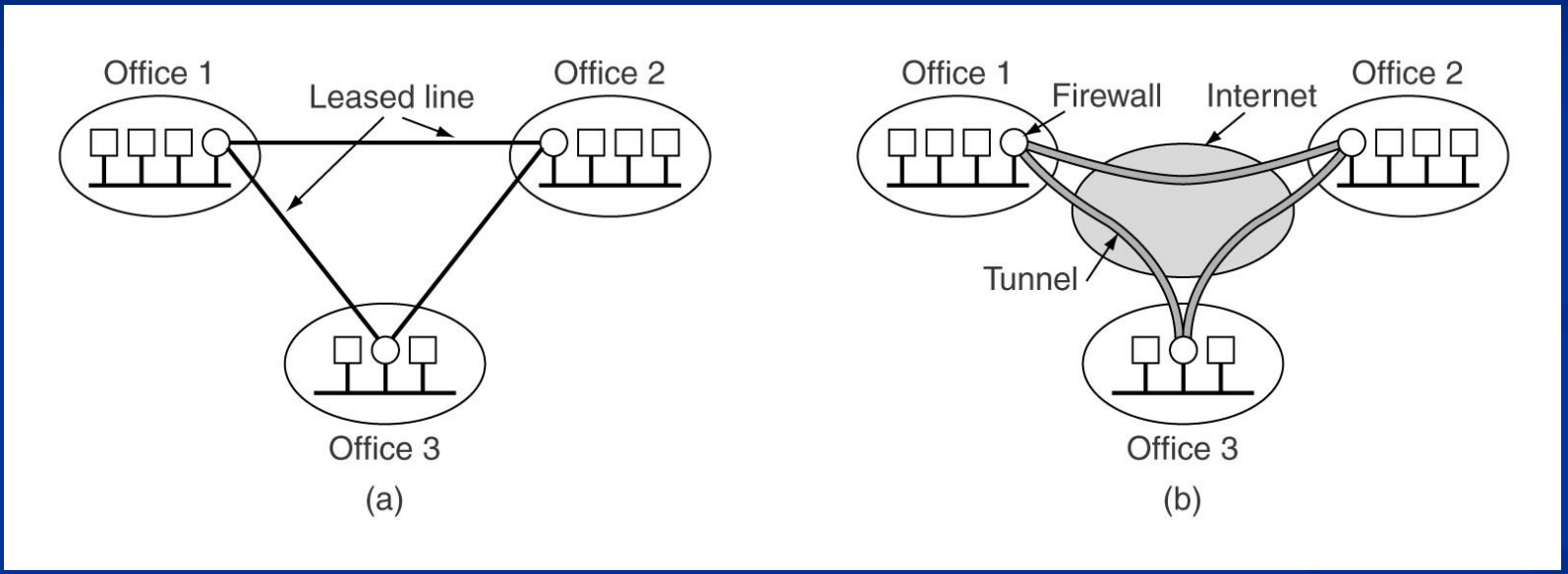
- Skrytí vnitřní struktury sítě
- Dynamický NAT
  - směr dovnitř dovolen pouze dočasně, po dobu trvání komunikace směrem ven
  - stanice střídavě viditelná zvnějšku pod různými adresami

Virtuální privátní sítě (Virtual Private Networks - VPN)

Princip VPN

- VPN poskytují možnost budovat privátní sítě s použitím sdílené infrastruktury sítě se stejnou úrovní konfigurovatelnosti a bezpečnosti jako při použití vlastní infrastruktury
- Použití tunelování a šifrovacích metod
  - včetně autentizace

Srovnání VPN s klasickou sítí



Tunel

- virtuální dvoubodové spojení přes sdílenou infrastrukturu
  - Často autentizované a šifrované
- nese pakety jednoho protokolu zabalené v jiném protokolu
  - Často i ve stejném protokolu – IP over IP
- Lze tunelovat i L2 rámce
  - Přenos jiných protokolů přes IP síť

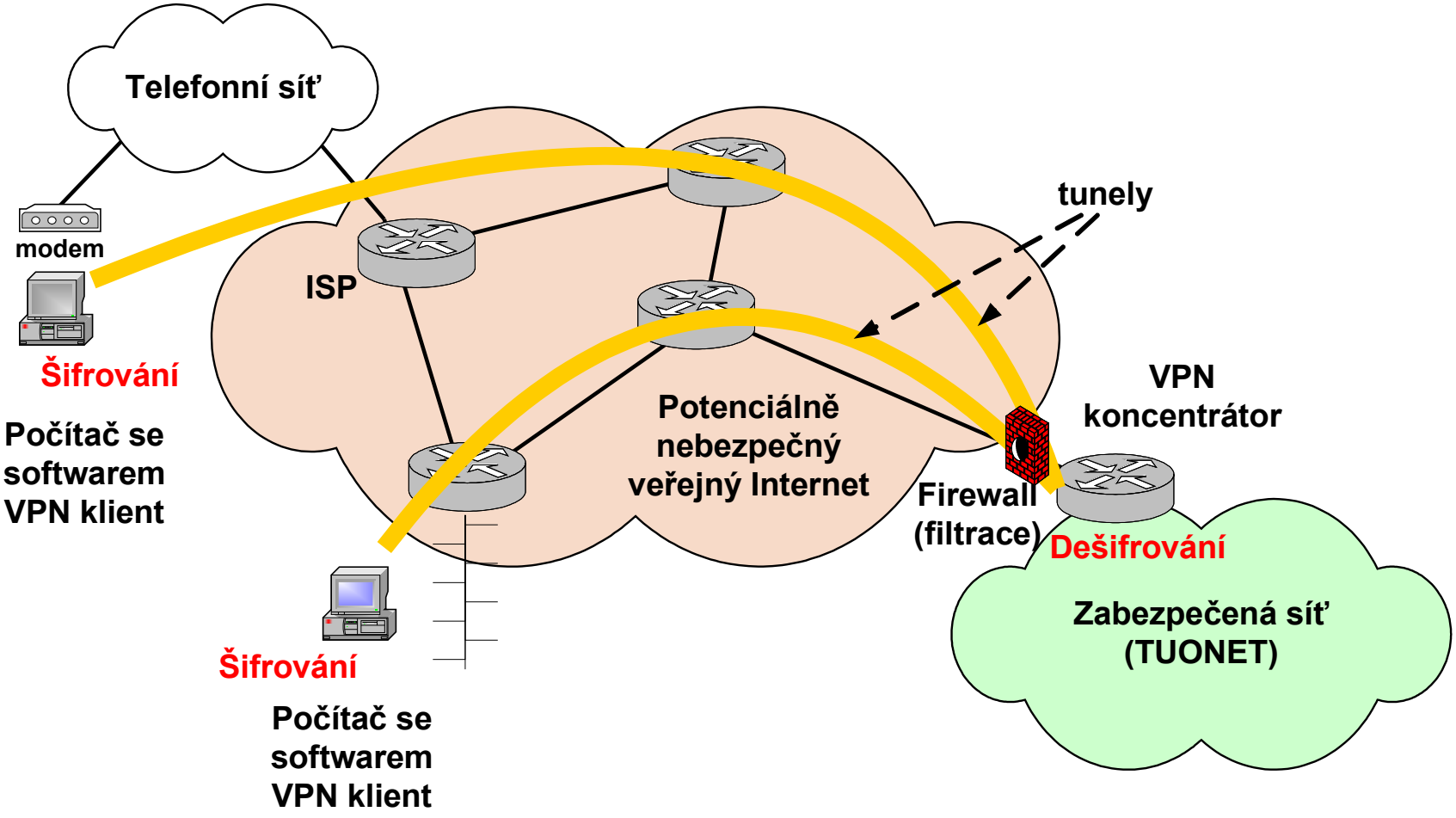
Výhody VPN

- nižší cena
- flexibilita (viruální) topologie
- odpadá management WAN linek

Obvyklé varianty aplikace VPN

- Router-router (firewall)
  - nebo i tunely z routeru k více routerům
- Vzdálený uživatel – VPN koncentrátor
  - uživatel má instalován speciální SW - VPN klient

Příklad: Přístup vzdálených uživatelů do intranetu přes VPN



Implementace VPN na 3. vrstvě: IPSec

- IPSec = architektura pro technickou realizaci (dynamicky navazovaných) tunelů
- Poskytuje autentizaci, integritu dat a šifrování
- Obecný framework, nezávislý na konkrétních algoritmech
  - konkrétní algoritmy dynamicky dohadují oba konce tunelů při jeho zřizován
    - Security Association s časově omezenou životností
- Jen pro IP (unicast) provoz
  - ale jiný provoz možno před předání IPSec zabalit do IP

Bezpečnost vybraných technologií sítí LAN a WAN

Bezpečnost ARP

- Možnost neregulérní odpovědi na ARP dotaz.
- Generování ARP dotazů s falešnou vazbou MAC-IP adresa zdroje.
- Řeší se statickými záznamy v ARP cache směrovače.

Bezpečnost směrování

Ochrana proti generování falešné směrovací informace

- Autentizace zdrojů směrovací informace (sousedů)
- Možnost aplikace ACL na adresy zdrojů směrovací informace
- Možnost filtrace propagovaných cest
- Podpora pro autentizaci ve směrovacím protokolu
  - RIPv2, OSPF, EIGRP, BGP

Bezpečnost přepínaných sítí

- možnost připojení pouze vyjmenovaných stanic (MAC adres) na port
- možnost omezení počtu MAC adres na portu
  - proti source-spoof DoS
    - přeplňování přepínací tabulky, vede k LRU odstraňování a častému floodingu
- možnost aplikace ACL na port
  - zdrojová/cílová MAC adresa, někdy i IP vrstva
- možnost aplikace ACL na VLAN jako celek
- možnost zákazu vzájemné komunikace mezi klientskými porty, přístup pouze na serverové nebo páteřní porty
  - anti-Doom ;-)

Bezpečnost DNS

Možnost podvržení informací z DNS

- falešné mapování doménových jmen na IP adresy
- falešné MX záznamy

- Modifikace odpovědi na cestě
- Generování jiné odpovědi, než byla položená otázka
  - většina OS přepíše v cache

Návrh řešení: DNSSec

Ochrana Spanning Tree

- BPDU Guard,
  - filtruje BPDU z portů, kde má být jen klientské stanice
- Root Guard
  - Nedovoluje neautorizovaným zařízením stát se kořenem Spanning Tree

Zabezpečení managementu síťových prvků

- přístupové heslo
  - Telnet, SSH, WWW, SNMP - komunity RO a RW
- idle timeout pro neaktivní administrátorské připojení
- specifikace povolené zdrojové adresy (ACL) pro management
- oddělený management VLAN

Nezapomínat na zabezpečení fyzického přístupu k zařízení

Útoky na počítačové sítě

Denial of Service (DoS) útoky

- Cílem útočníka vyčerpání systémových prostředků síťového prvku nebo serveru a jeho zhroucení nebo změna požadovaného chování
  - paměť, CPU, šířka pásma
- Zpravidla generován provoz z podvržené zdrojové adresy za účelem obejití filtrů
  - Source IP spoofing
- Nebezpečné v distribuované variantě (DDoS)
  - Charakter (zdroj) útočného provozu se mění rychleji, než stačí správce reagovat

Příklady DoS útoků

- SYN flood
- ping flood nebo pakety na neexistující síť
  - na routerech možnost omezení max. intenzity generování ICMP zpráv (hlavně unreachables)
- ping na cílovou síť s podvrženou zdrojovou adresou také z cílové sítě
- neautorizovaná změna směrování
  - ICMP redirects, falešné směrovací informace

Intrusion Detection System (IDS)

- rozpoznává podezřelé vzory komunikace
- na různých vrstvách
- klasifikuje nebezpečí, informuje správce nebo inteligentně reaguje

Autentizace, autorizace a účtování aktivit uživatelů

Uživatelé

- Autentizace před vpuštěním do sítě
- Autorizace k použití požadované služby
- Týká se i správců síťových prvků
- Vhodná centralizovaná správa oprávnění uživatelů na AAA serveru