

# Bezpečnost v počítačových sítích

Petr Grygárek

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

1

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

2

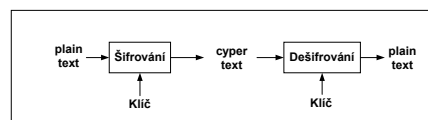
## Základní pojmy

- Utajení (confidentiality) – 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

3

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

4

## Symetrický systém

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

5

## Vlastnosti symetrického systému

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

6

## Autentizace v symetrickém systému

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

7

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

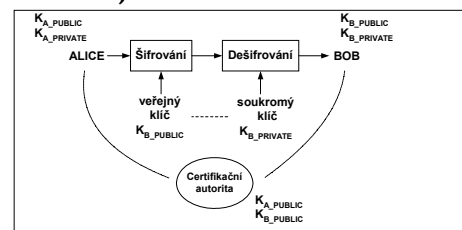
8

## Asymetrický systém

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

9

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

10

## Použití asymetrického systému

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

11

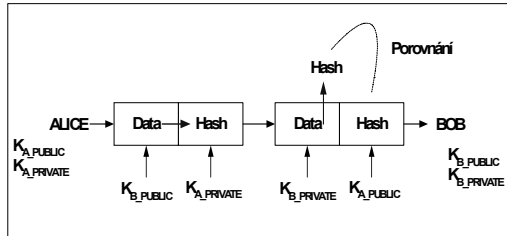
## Certifikační autorita

- 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 vlastníkově po ověření jeho identity
- Veřejný klíč certifikační autority musí být důvěryhodným způsobem zaveden do každého systému
  - „na disketě“, součást distribuce OS nebo prohlížeče WWW

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

12

## Autentizace v asymetrickém systému



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

13

## Možnosti zabezpečení přenášených dat

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

14

## Zabezpečení na jednotlivých vrstvách OSI-RM

- L2
  - hop-by-hop, neefektivní
  - Layer 2 tunneling protocol (L2TP), point to point tunnelling 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

15

## Filtrace provozu

- Bezstavová (paketové filtry)
  - Výsledkem propuštění nebo zahazení 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

16

## Paketové filtry

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

17

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

18

## 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 nezkontrolují
- Na konci ACL implicitní zákaz veškerého provozu
  - co není explicitně dovoleno, je zakázáno

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

19

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

20

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

21

## Příklad: Použití ACL na Cisco IOS

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

22

## 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”

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

23

## 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)
```

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

24

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

25

## 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)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

26

## 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 :-)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

27

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

28

## 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 předjet situaci, kdy je paket nejprve směrován a pak zahozen výstupním ACL
- Definice obsahu jednotlivých ACL
  - Nezapomínat na povolení zpětného směru provozu !

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

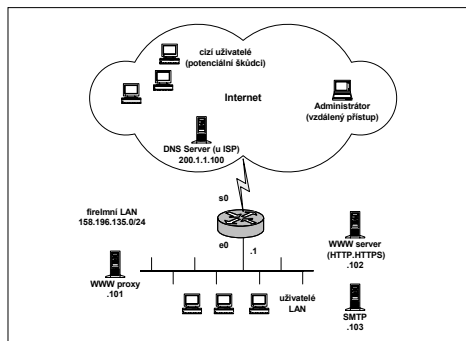
29

## Příklad použití ACL

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

30

## Situace



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

31

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

32

## 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.

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

33

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

34

## 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	*	*	*	*

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

35

## 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	zakázat	IP	*	*	*	*

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

36

## 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
```

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

37

## 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
```

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

38

## Stavová inspekce provozu

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

39

## Firewally

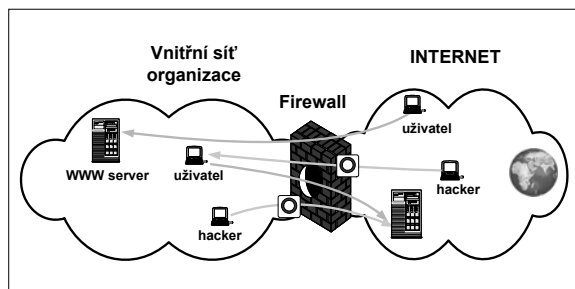
Oddělují důvěryhodnou a nedůvěryhodnou část sítě

- 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 sítí
- Transparentní (chování jako router/bridge)
- Proxy servery

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

40

## Funkce firewallu



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

41

## 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
  - ...

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

42

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

- Zkoumá řídicí 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)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

43

## Bezpečnost a NAT

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

44

## 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 zvenjšku pod různými adresami

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

45

## Virtuální privátní sítě (Virtual Private Networks - VPN)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

46

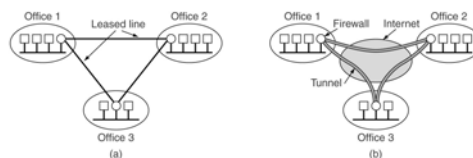
## Princip VPN

- 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

47

## Srovnání VPN s klasickou sítí



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

48

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

49

## Výhody VPN

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

50

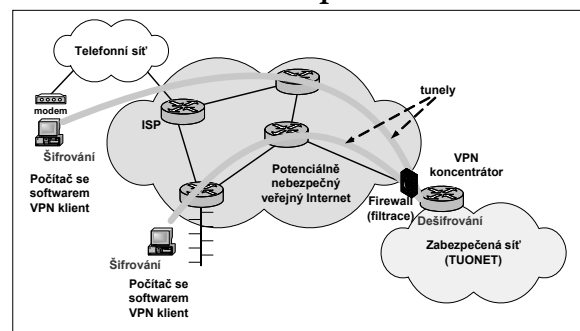
## Obvyklé varianty aplikace VPN

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

51

## Příklad: Přístup vzdálených uživatelů do intranetu přes VPN



© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

52

## 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 zřizování
    - Security Association s časově omezenou životností
- Jen pro IP (unicast) provoz
  - ale jiný provoz možno před předání IPSec zabalit do IP

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

53

## Bezpečnost vybraných technologií sítí LAN a WAN

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

54

## Bezpečnost ARP

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

55

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

56

## Bezpečnost přepínaných sítí

- možnost připojení pouze vyjmenovaných stanic (MAC adres) na port
- možnost omezení počtu MAC adres na portu
  - proti source-spoof DoS
    - přepřítování 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 ;-)

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

57

## 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 položena otázka
  - většina OS přepíše v cache

Návrh řešení: DNSSEC

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

58

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

59

## 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 zařízením

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

60

## Útoky na počítačové sítě

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

61

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

62

## Příklady DoS útoků

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

63

## Intrusion Detection System (IDS)

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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

64

## Autentizace, autorizace a účtování aktivit uživatelů

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

65

## 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

© 2005 Petr Grygárek, FEI VŠB TUOstrava, Počítačové sítě (Bc.)

66