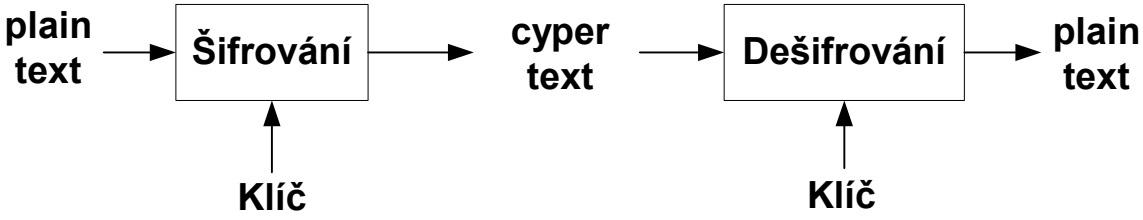
Bezpečnost-základní pojmy

- 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

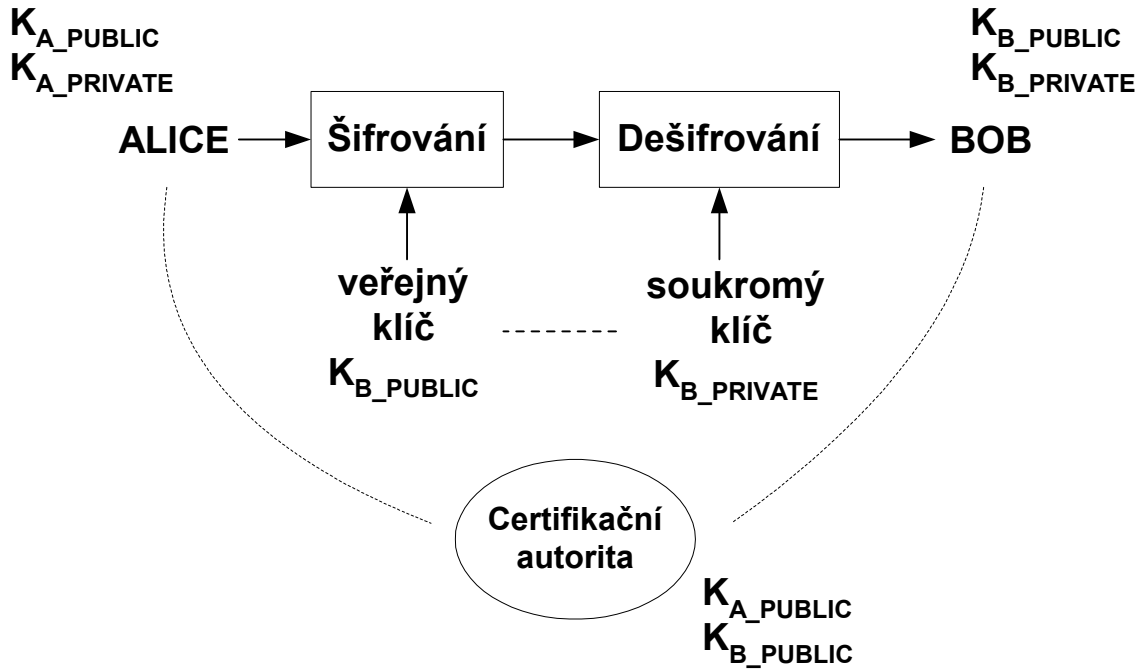
Symetrický systém

- 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 Hash hodnoty ke jménu a kontrolní výpočet s porovnáním na přijímači)

Asymetrický systém



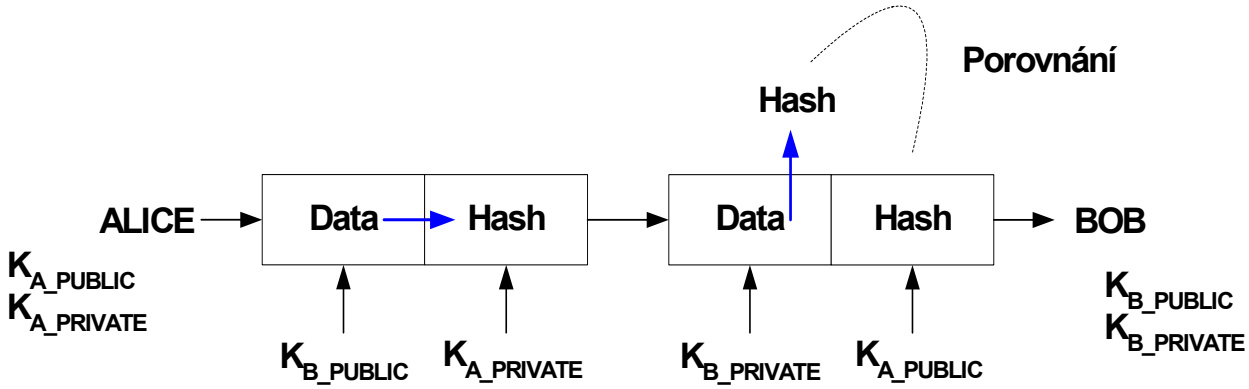
- Klíče se generují jako doplňující se pár – veřejný (public) a soukromý (private) klíč
- Jeden klíč použit pro šifrování, druhý pro dešifrování (je jedno, který z nich k čemu)
- Mnohem náročnější na výpočty, pomalejší

Asymetrický systém se běžně využívá pro předávání (dynamicky generovaných) klíčů pro symetrický systém.

Certifikační autorita

- Entita, které je důvěřováno
- Registruje (podepsané) veřejné klíče
- První kontakt s certifikační autoritou musí proběhnout osobně (získání dvojice podepsaný veřejný-privátní klíč)
- Veřejný klíč certifikační autority musí být důvěryhodným způsobem zaveden do každého systému

Autentizace v asymetrickém systému



Zajištění integrity

Hashing algoritmus = jednosměrná funkce

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

Zabezpečení na jednotlivých vrstvách OSI-RM

L7 – S/MIME
L4 – SSL (jen TCP)
L3 – IPSec – nezávislé na médiu i aplikaci
L2 – hop-by-hop, neefektivní

Bezestavová inspekce paketů

Implementačně nejjednodušší metodou zabezpečení je inspekce jednotlivých procházejících paketů samostatně, tedy bez ohledu na ostatní předchozí a následné pakety, s nimiž společně tvoří jeden datový tok. Výsledkem inspekce je buďto propuštění nebo zahození (vyfiltrování) paketu. Proto také někdy hovoříme o paketových filterech.

Výhodou je, že není třeba procházející pakety rozřazovat do datových toků a udržovat informaci o každém z nich, nevýhodou zase skutečnost, že můžeme kontrolovat pouze korektnost dat zcela obsažených v jednom paketu, nikoli tedy nebezpečná data rozložená do více samostatných paketů.

Nebezpečí pro úspěšné použití bezestavové inspekce plyne i z fragmentace.V hlavičce fragmentů s výjimkou prvního totiž není záhlaví 4. vrstvy, takže podle něj nelze filtrovat. Lze to řešit např. timeoutem na propouštění fragmentů podle IP Identification spuštěným prvním fragmentem, ale to již nese potřebu ukládat stavovou informaci. Častá implementace kontroluje 4. vrstvu jen je-li v IP hlavičce Fragment Offset=0 (tedy u prvního fragmentu), ostatní fragmenty propouští. To přináší nebezpečí, pokud první fragment úmyslně nepřenáší celou hlavičku 4. vrstvy.

Paketové filtry se nejčastěji aplikují na rozhraních směrovačů.

Access Control Lists (ACL)

Nejčastější forma implementace bezestavové inspekce paketů jsou tzv. Access Control Lists (ACL). ACL je v podstatě filtr umístěný na některé rozhraní aktivního prvku. Zpravidla se jedná o směrovač nebo L3 switch, i když i některé přepínače dovolují vložit na port nebo VLAN ACL filtrující podle zdrojové nebo cílové MAC adresy, popřípadě typu protokolu 3. vrstvy. Dále se budeme zabývat jen ACL na směrovačích, které budou kontrolovat informace ze 3., popřípadě 4. vrstvy OSI RM.

ACL je obvykle tvořen sekvencí položek zakazující nebo povolující průchod paketů vyhovující kritériím definovaným danou položkou. Při průchodu paketu rozhraním, na němž je ACL aplikován, se postupně odshora procházejí jednotlivé položky ACL, až se narazí na první položku, jejímž kritériím zkoumaný paket vyhovuje. Podle toho, zda je položka definována jako příkaz k propuštění paketu nebo k jeho zahození se pak paket propustní nebo zlikviduje. Další položky ACL se pak už dále nezkoumají. Na konci ACL typicky bývá implicitní položka přikazující „zahodit vše“, vlivem čehož ACL respektují filosofii „co není explicitně povoleno, je zakázáno“.

Při návrhu filtrace provozu pomocí ACL je vždy třeba stanovit

- na kterém rozhraní kterého směrovače bude ACL aplikován
- zda bude filtrovat provoz vstupující do tohoto rozhraní nebo z tohoto rozhraní vystupující

- jaká kritéria způsobující propuštění nebo zahození procházejících paketů bude ACL obsahovat

Zabezpečení sítě není zpravidla možné zajistit pouze jedním ACL, ale kombinuje se funkčnost několika různých ACL umístěných na vhodná rozhraní. Na každé rozhraní lze umístit vždy jeden ACL filtrující provoz vstupující do rozhraní a jeden ACL filtrující provoz vystupující.

Poznámka:
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. Při tom si je třeba vždy ujasnit, že čísla zdrojového a cílového portu budou pro zpětný směr přehozená. Nerespektování tohoto faktu je nejčastější chybou při konfiguraci ACL.

Použití ACL na Cisco IOS

Na směrovačích (a směrovaných portech L3 přepínačů) s Cisco IOS spočívá aplikace ACL ve dvou krocích:

1. Definice ACL
2. Aplikace ACL na příslušné rozhraní a určení směru provozu, pro který bude ACL filtrovat (dovnitř nebo ven z rozhraní)

U protokolové rodiny TCP/IP mohou ACL filtrovat podle zdrojové a cílové IP adresy, protokolu, zdrojového a cílového portu, precedence (ToS) a některých dalších položek hlaviček 3. a 4. vrstvy. Jednotlivé ACL se jednoznačně identifikují číslem, v tomto případě v rozsahu 100-199. Základní syntaxe definice jednotlivých položek ACL je následující:

access-list <N> {permit | deny} <PROTOCOL> <source-IP-addr> <source-addr-wildcard> <destination-IP-addr> <destination-addr-wildcard>

- N je číslo ACL, do kterého má být položka přidána (vždy na konec). Pokud ACL s tímto číslem ještě neexistuje, zařazením první položky se automaticky vytvoří

- **permit | deny** určuje, zda paket vyhovující kritériím dané položky bude propuštěn (permit) nebo zahozen (deny)

- **PROTOCOL** určuje typ protokolu (3./4.vrstva), na který se položka ACL vztahuje. Lze zvolit **ip**, **tcp**, **udp**, **icmp** nebo **igmp**. Volba **ip** ostatní z možných protokolů zahrnuje.

- **source-IP-addr** a **destination-IP-addr** jsou zdrojová, resp.cílová IP adresa uváděná jako čtyři dekadické číslice oddělené tečkami

- **source-addr-wildcard** a **destination-addr-wildcard** jsou tzv. wildcard masky určující, které bity zdrojové a cílové adresy testovaného paketu mají být porovnávány s adresami specifikovanými v položce a které mají být při tomto porovnávání ignorovány. Maska se zadává jako čtveřice dekadických číslic, avšak můžeme ji

chápat jako 32-místnou sekvenci jedniček a nul odpovídající jednotlivým bitům IP adresy. Binární nula v masce znamená, že bit IP adresy na příslušné pozici bude při porovnávání brán v úvahu. Naopak jednička vyjadřuje, že daný bit IP adresy bude při porovnávání ignorován.

Poznámka:
Všimněte si, že konvence zápisu wildcard masky je opačná, než při vyjadřování masek podsítě. V masce podsítě binární jednička znamená, že odpovídající bit adresy patří do adresy sítě a bude při vyhledávání ve směrovací tabulce vzat v úvahu. Při porovnávání adres v testovaném paketu s adresami zadanými v položce ACL naopak budou brány v úvahu jen ty bity, u nichž je na odpovídající pozici wildcard masky uvedena nula.

Poznámka:
Pokud chceme, aby se zdrojová nebo cílová adresa nekontrolovala vůbec, můžeme uvést libovolnou adresu a masku 255.255.255.255. Jedničkami na všech pozicích wildcard masky říkáme, že žádný z bitů nebude při porovnávání s adresou v paketu brán v úvahu. Pro zkrácení a zpřehlednění zápisu můžeme namísto kombinace libovolné IP adresy s wildcard maskou 255.255.255.255 psát také klíčové slovo **any**. Například

… permit ip 192.168.1.0 0.0.0.255 any

povolí všechny IP pakety ze zdrojových adres začánajících prefixem 192.168.1 na libovolnou cílovou adresu.

Naopak namísto uvádění wildcard masky 0.0.0.0, podle níž se musí shodovat všechny bity adresy, můžeme použít klíčové slovo **host**. Například

… deny tcp host 10.0.1.100 192.168.1.0 0.0.0.255

zakáže TCP spojení ze stanice 10.0.1.100 na síť 192.168.1.0/24.

Položky jednoho ACL (tj. označované společným číslem N) se řadí za sebe v pořadí, jak jsou vkládány. Přidávat položky lze tedy vždy jen na konec ACL. Pokud je třeba přidat položku mezi již existující položky, je třeba ACL nejprve jako celek odstranit (**no access-list <N>**) a poté vložit všechny položky v požadovaném pořadí znovu.

Příklad

Ukažme si příklad vytvoření ACL s číslem 100:

access-list 100 deny tcp 120.12.0.0 0.0.0.127 host 130.11.12.100
access-list 100 permit tcp 120.12.0.0 0.0.0.127 130.11.12.0 0.0.0.255
access-list 100 permit udp any 10.0.0.1 0.0.0.0

Prvním řádkem zakazujeme ze sítě 120.12.0.0/25 TCP spojení na stroj 130.11.12.100. Druhým řádkem ze sítě 120.12.0.0/25 TCP spojení na zbývající stanice sítě 130.11.12.0/24 naopak povolujeme. Třetím řádkem povolujeme průchod UDP datagramů z libovolné zdrojové adresy na stanici 10.0.0.1 (zde bychom také opět mohli využít klíčového slova host). Všimněte si na příkladu prvních dvou řádků, že pořadí položek v ACL je důležité.

Již jsme zmínili, že ACL zakazuje vše, co nebylo explicitně povoleno. Na konci každého ACL si tak můžeme představit implicitní položku zakazující vše:

access-list *N* deny ip any any

ACL protokolů transportní vrstvy

U protokolů transportní vrstvy (UDP,TCP) můžeme filtrační kritéria rozšířit i o čísla zdrojových a cílových portů a také o některé příznaky z hlavičky TCP segmentu. Kontrolu na shodu portu zajistíme připojení výrazu **eq číslo_portu** za specifikaci zdrojové, resp. cílové adresy. Klíčovými slovy **lt**, **gt** je také možné vybrat všechna čísla portů menší nebo větší než zadaná hodnota a nebo za klíčovým slovem **range** uvést minimální a maximální hodnotu portu, které musí při srovnávání vyhovovat. Například

permit udp host 10.0.0.1 eq 520 any

propustí UDP pakety ze stanice 10.0.0.1 se zdrojovým portem 520 kamkoli,

deny tcp 172.16.0.0 0.0.255.255 gt 5000 host 120.1.1.100 eq 23

zakáže ze sítě 172.16.0.0/16 a z portů vyšších než 5000 TCP spojení na port 23 (Telnet server) stanice 120.1.1.100. Konečně

permit udp any range 16000 17000 host 172.16.1.100 gt 4096

propustí UDP datagramy z kterékoli adresy z rozsahu zdrojových portů 16000 až 17000 na adresu 172.16.1.100 na cílové porty větší než 4096.

V souvislosti s protokolem TCP je také užitečné klíčové slovo **established**. To umožní, aby v jednom směru byla navazována TCP spojení a ve druhém směru nikoli, avšak data spojení navázaného z povoleného směru byla v protějším směru ACL propouštěna. To např. můžeme dovolit otevírání TCP spojení z vnitřní sítě do Internetu, avšak zakázat (potenciálně nebezpečné) navazování spojení ze stanic na Internetu na stanice vnitřní sítě. Data TCP spojení předtím navázaného z vnitřní sítě budou však i ve směru z Internetu do vnitřní sítě propouštěna. Klíčové slovo **establised** lze přidat na konec položky ACL povolující TCP spojení a jejím uvedením zajistíme, že ACL propustí pouze TCP segmenty s nastaveným flagem ACK=1 nebo RST=1. ACK=0 je totiž pouze v prvním segmentu TCP spojení (trojfázového handshake), tedy ve výzvě k navázání spojení. V každém dalším TCP segmentu (vč. 2. a 3. fáze 3-fázového handshake) je již flag ACK nastaven, takže se všechny ostatní segmenty mimo prvotní žádosti o navázání spojení propustí (**establised** má smysl pouze ve spojitosti s položkou typu **permit**). Mimo to se propustí také i případné segmenty s příkazem k násilnému ukončení spojení (RST).

ACL řídících protokolů¨

U protokolů ICMP a IGMP je základní syntaxe zápisu ACL také rozšířená, aby bylo možné filtrovat selektivně jednotlivé typy zpráv. Typy zpráv se pojmenovávají symbolicky, jejich

přehled lze zjistit z kontextové nápovědy IOS stiskem otazníku při vkládání položky ACL. ACL propouštějící, resp. zakazující některé ICMP zprávy pak mohou vypadat např:

… permit icmp 172.16.1.0 0.0.0.255 any echo-request
… deny icmp 172.16.2.0 0.0.0.255 host 172.16.3.1 redirect

První položka dovoluje průchod ICMP zpráv echo-request (ping-dotaz) ze sítě 172.16.1.0/24 kamkoli, druhá zakazuje průchod zpráv ICMP redirect ze sítě 172.16.2.0/24 zasílaných na adresu 172.16.3.1

Přiřazení ACL na rozhraní

Aby nadefinovaný ACL začal filtrovat, je třeba jej neprve přiřadit na příslušné rozhraní a zvolit směr provozu, který má filtrovat. To lze provést v sekci odpovídající požadovanému rozhraní příkazem **ip access-group** s uvedením čísla ACL a směru provozu. Směr do rozhraní se označuje klíčovým slovem **in**, směr z rozhraní ven klíčovým slovem **out**. Například

interface FastEthernet 0/0
ip access-group 101 in
ip access-group 102 out

Jak jsme si již řekli, může být na každé rozhraní přiřazen nejvýše jeden ACL ve směru **in** a nejvýše jeden ve směru **out**. Pokud je to užitečné, může být jeden ACL přiřazen i na více rozhraní a to jak ve směru in tak out.

Time-based ACL

Jednotlivé položky ACL (permit/deny) mohou platit jen v čase definovaném pomocí zadaného časového rozsahu:

… permit | deny … time-range MY_TR

Časový rozsah lze zadat buďto jako periodicky se opakující nebo jednorázový (absolutní):

time-range MY_PERIODIC_TR periodic
periodic <week_days> hh:mm to [<week_days>] hh:mm

time-range MY_ABSOLUTE_TR absolute
<čas a datum začátku platnosti>
<čas a datum konce platnosti>

Reflexivní ACL

Reflexivní ACL automaticky rozeznávají vstupní provoz, který odpovídá povolenému provozu výstupnímu a otevírají pro něj vstupní ACL. Otevření ACL trvá po dobu trvání odpovídajícího výstupního datového toku (tj. do detekce FIN nebo RST v TCP spojení nebo vypršení timeoutu neaktivity u UDP relace). Pokud výstupní ACL propustí tok z adresy SA

portu SP na adresu DA port DP, zajistí reflexivní ACL vytvoření dočasné položky ve vstupním ACL, který povoluje stejný protokol (UDP,TCP,ICMP) z adresy DA portu DP na adresu SA port SP. V případě protokolu ICMP se otevření vstupního ACL omezí na typ zprávy párující s odchozí ICMP zprávou (typicky Echo Reply k Echo Request).

Poznámka:
V současných verzích IOS jsou reflexivní ACL podporovány pouze pro extended named ACL.

```
ip access-list extended  MY_ACL_OUT
 permit TCP any 158.196.135.0 0.0.0.255 reflect MY_ACL_DYNAMIC

ip access-list extended  MY_ACL_IN
 evaluate MY_ACL_DYNAMIC
 …

inteface s0
 ip access-grout MY_ACL_OUT out
 ip access-grout MY_ACL_IN in
```

Strategie implementace ACL

- Vnitřní síť, vnější síť, demilitarizovaná zóna (DMZ)
- V DMZ „bastillon hosts“ (servery)
- Zákaz přímého provozu mezi vnější a vnitřní síti

Technologie Lock and Key (Cisco)

Položky ACL vkládané do jiných ACL na základě spouštěcí akce (autentizovaný telnet na router + spouštěcí příkaz)

Context-Based Access Control - CBAC – (Cisco)

- Základní implementace (stavového) firewallu, v Cisco IOS Firewall Feature Set
- Zkoumá data vybraných aplikačních protokolů (řídící kanál), podle aktivit těchto protokolů otevírá dynamické porty
- 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)

Konfigurace:

1. Aplikační protokoly, které se mají zkoumat („inspection“)
2. Rozhraní a směr (in,out), kde se mají zkoumat (pro směr in je provoz nejprve filtrován vstupním ACL, je-li na rozhraní aplikován)
3. ACL zakazující vše v opačném směru než je zkoumán provoz (na tomtéž nebo i jiném rozhraní). Do něj bude CBAC vytvářet „díry“.

ip inspect name JMENO <protocol_1> [timeout <secs>]
ip inspect name JMENO <protocol_2> [timeout <secs>]
…
interface s0
description Rozhrani do Internetu
ip inspect JMENO in|out
interface e0
description Rozhrani do LAN
ip access-group 101 out

access-list 101 deny ip any any

Volitelná kontrola fragmentace:
ip inspect name JMENO fragment <max_fragments>

Nastavení UDP timeout:
ip inspect udp idle-time <t>

Nastavení povolených/zakázaných WWW serverů pro Applety (inspekce HTTP):
ip inspect name JMENO http java-list <ACL#>

Bezpečnost a NAT

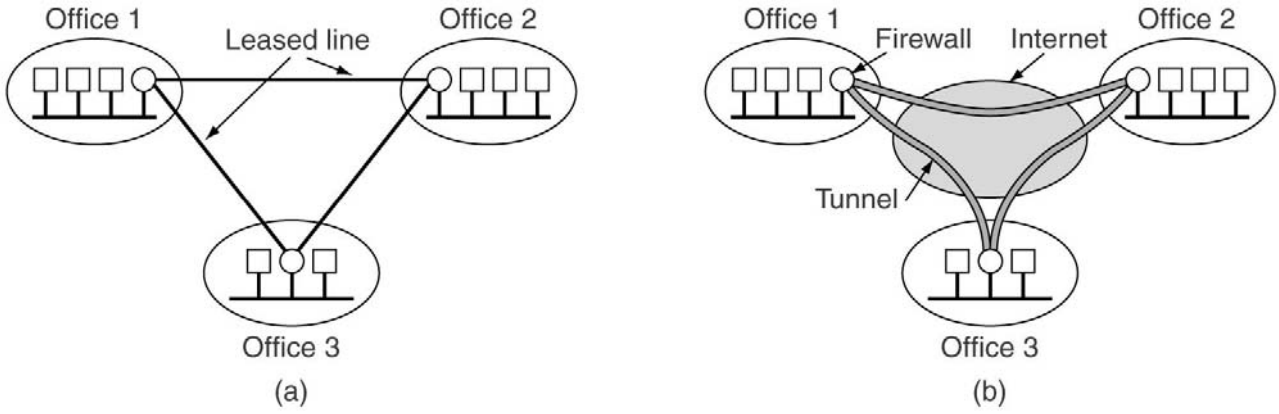
- Skrytí vnitřní struktury sítě
- Dynamický NAT – směr dovnitř dovolen pouze dočasně, po dobu trvání komunikace směrem ven

Virtual Private Networks (VPN)

VPN realizuje přenos privátních dat přes veřejnou síť s použitím kryptovacích metod a tunelů
Poskytuje autentizaci, integritu dat a utajení

Výhodou cena, flexibilita topologie, odpadá management WAN linek

Tunel – virtuální dvoubodové spojení přes veřejnou síť, nese data jednoho protokolu ve druhém protokolu.



a) klasická virtuální síť b) virtuální privátní síť s použitím tunelů (VPN)

Možnosti aplikace

- Router-router/firewall (nebo i proti více routerům)
- Vzdálený uživatel – VPN koncentrátor
- Přístup k Network Access Serveru poskytovatele (nejčastěji dialup), z něj tunel do firemní sítě

IPSec

(RFC 2401)
Sada bezpečnostních protokolů a algoritmů pro zabezpečení dat na síťové vrstvě

- Poskytuje autentizaci, integritu dat a šifrování
- obecný framework, nezávislý na konkrétních algoritmech
- jen pro IP (unicast) provoz
- obdoba zabudována do IP v.6

Terminologie IPSec

Internet Security Association and Key Management Protocol (ISAKMP)

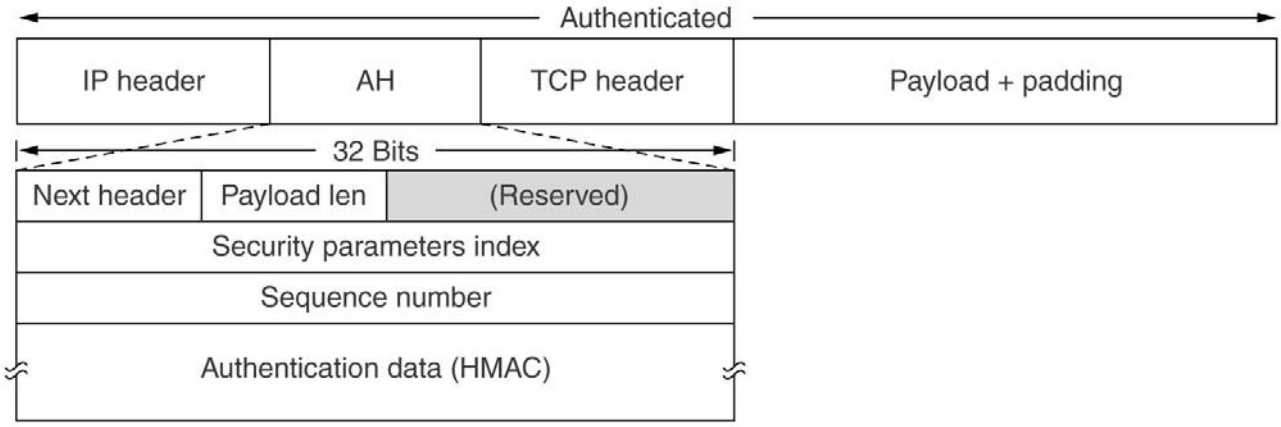
- Obecná architektura (technická platforma-framework) pro implementaci výměny klíčů a dohody SA
- Definuje formáty zpráv, ne interpretaci vyměňovaného kryptografického materiálu

Internet Key Exchange (IKE)

- Konkrétní definice způsobu použití ISAKMP

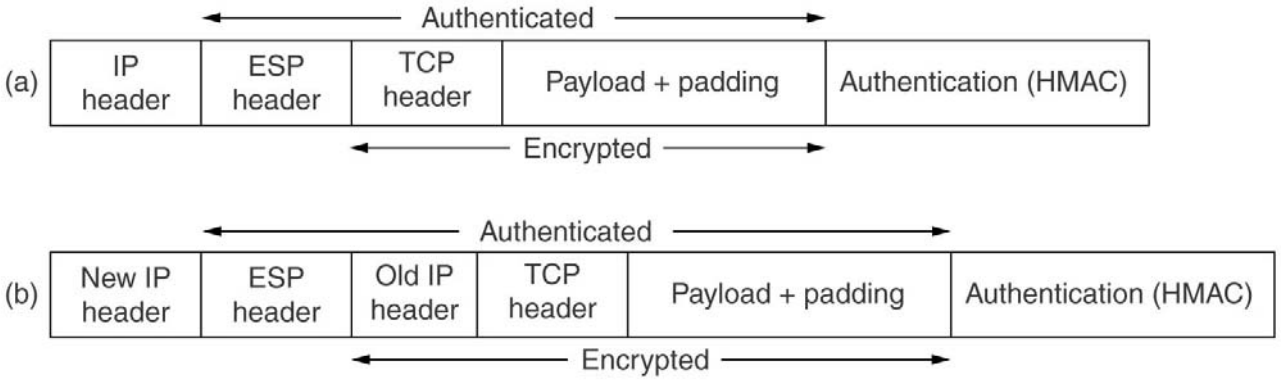
Authentication Header (AH)

- Chrání integritu IP hlavičky (neměnná pole) + IP dat
- Nekompatibilní s NAT (zdrojová adresa chráněna testem integrity)
- Obsahuje Security Parameters Index (SPI) – index do tabulky SA a autentizační data (Hashed Message Authentication Code-HMAC, RSA neaplikován přímo na celou zprávu, ale na hash)
- Podpora pro anti-replay (příjemce musí kontrolovat vzrůstající řadu sekvenčních čísel, po vyčerpání řady dohoda nového SA)
- Všechny funkce AH mohou být plněny ESP – AH zatím udržován z historických důvodů
- Autentizační hlavička (v transportním módu):



Encapsulating Security Payload (ESP)

- Šifrování přenášených dat, volitelná kontrola integrity (jen data) a autentizace včetně anti-replay
- Obsahuje SPI, sekvenční číslo a inicializační vektor
- Data pro autentizaci/test integrity na konci (ESP trailer) – možnost HW implementace výpočtu HMAC
- ESP header v a) transportním a b) tunelovém módu:



Security Association (SA)

- Definuje šifrovací parametry pro jeden směr provozu mezi dvojicí komunikujících zařízení (algoritmus, klíče, doba platnosti klíčů, …)
- Dohaduje se v první fázi (IKE)
- Oddělené SA pro AH, ESP a IKE
- IPSec SA jsou jednosměrné, IKE SA obousměrné
- Definovaná životnost (čas/přenesený objem dat)

Fáze provozu IPSec

1. Výměna klíčů (asymetrický systém) a dohoda šifrovacích parametrů (algoritmus, hash algoritmus, životnost klíčů, …)
   - Diffie-Hellman algoritmus poskytuje způsob dohody sdíleného klíče mezi dvěma stranami za použití komunikace přes nezabezpečený kanál bez možnosti odposlechu klíče třetí stranou
   - Diffie-Hellman neřeší autentizaci, obvykle k tomu použity staticky konfigurované symetrické klíče (pre-shared keys).
     Identita zařízení v ISAKMP je buďto hostname nebo IP adresa.

   1.1 (IKE Phase 1): zřízení bezpečného kanálu pro výměnu IPSec SA (dohoda IKE SA)
   1.2 (IKE Phase 2): dohoda IPSec SA (zvlášť pro AH a ESH)
2. Přenos dat s použitím symetrického šifrování s dohodnutými klíči

Módy IPSec

- Transportní
  - zabezpečení stanice-stanice, implementace IPSec v operačních systémech
  - hlavičky AH a příp. ESP se vkládají mezi L3 a L4 hlavičku původního paketu
  - původní IP header nešifrován

  Poznámky:
  - Podle L4 záhlaví nemůže být na cestě filtrováno (je zašifrováno)
  - Není kompatibilní s NAT, zdrojová IP adresa je chráněná autentizací/integritou
- Tunelový
  - zabezpečení jen mezi routery (IPSec Gateway) oddělující koncové LAN od veřejné sítě
  - hlavičky AH a příp. ESP se vkládají na začátek obalovacího paketu, za nimi celý původní tunelovaný paket
  - šifrován celý původní paket – nelze odposlouchat ani kdo s kým komunikuje
  - nepotřebuje podporu IPSec v koncových stanicích

ESP Trailer (autentizace) vždy na konci, doplnění zprávy na velikost bloku šifry
Hlavičky AH, ESP a typ původně neseného L4 protokolu se řetězí (jako v IPv6).

Konfigurace IPSec

- definice ACL se sítěmi, na něž se bude provoz šifrovat (a odkud se má očekávat šifrovaný provoz)
- konfigurace přípustných alternativ parametrů pro dohodu IKE SA
- konfigurace přípustných alternativ parametrů pro dohodu IPSec SA
- označení interface začátku/konce IPSec tunelu
- Upravit ACL, aby byl provoz IPSec propuštěn (speciální typy protokolů (AH,ESP) v IP hlavičce (50,51), port kanálu IKE-500)

Bezpečnost technologií LAN a WAN sítí

Bezpečnost a 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: RIPv2, OSPF, EIGRP,BGP

Bezpečnost na spojové vrstvě (přepínače)

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

Akce při detekci porušení pravidel – zvýšení čítačů, port shutdown, SNMP trap

Ochrana Spanning-Tree

- BPDU Guard,
- Root Guard

Zabezpečení managementu síťových prvků

(Telnet,SSH,SNMP)

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

Nezapomínat na zabezpečení fyzického přístupu k zařízení.

Autentizace, autorizace, accounting

- Autentizační servery a protokoly TACACS+, RADIUS
- Mezi Remote Access serverem a autentizačním serverem
- Remote Access Server je i WiFi AP
- Autentizační informace se šíří ke klientovi pomocí standardu IEEE 802.1x

Bezpečnost DNS

Možnost modifikace DNS odpovědí (falešná odpověď, odpověď jiná než položená otázka – přepis v cache)

DNSSec

(RFC 2535)

- věta typu KEY
  - veřejný klíč pro doménu, podepsán privátním klíčem domény vyšší úrovně
- věta typu SIG
  - uložení elektronického podpisu (autentizace dat)

Denial of Service (DoS) útoky

Cílem útočníka vyčerpání systémových prostředků (paměť, CPU, šířka pásma) síťového prvku nebo serveru a jeho zhroucení nebo změna požadovaného chování

Source IP spoofing – podvržení zdrojové adresy za účelem obejití filtrů

Příklady DoS útoků:

- SYN flood
- ping flood, 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)