České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

VPN - IPsec

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz

VPN – co to je

Formální definice:

VPN je komunikační prostředí, ve kterém je řízen přístup ke komunikaci mezi jednotlivými entitami. Komunikační prostředí je vytvořeno nějakou formou rozdělení společného komunikačního média, a kde tato nižší vrstva komunikačního média poskytuje síťové služby na ne-exkluzivní bázi.

Méně formální definice:

VPN je neveřejná (počítačová) síť, vybudovaná v rámci veřejné síťové infrastruktury, jakou je např. Internet. Tato síť typicky zajišťuje zabezpečené připojení vzdálených poboček nebo účastníků k mateřské síti.

VPN – co to je

- logická síť v rámci sdílené veřejné infrastruktury
- poskytuje stejný výkon a pravidla jako soukromá LAN
- základní problémy při použití VPN
  - zajištění bezpečnosti
  - zajištění poskytování požadované kvality služeb (QoS) podle požadavků provozu …v KBE toto neřešíme
- tyto požadavky TCP/IP neřeší
- požadavky na bezpečnost se řeší pomocí
  - tunelování
  - šifrování
  - autentizace
  - řízení přístupu

VPN – základní pojmy

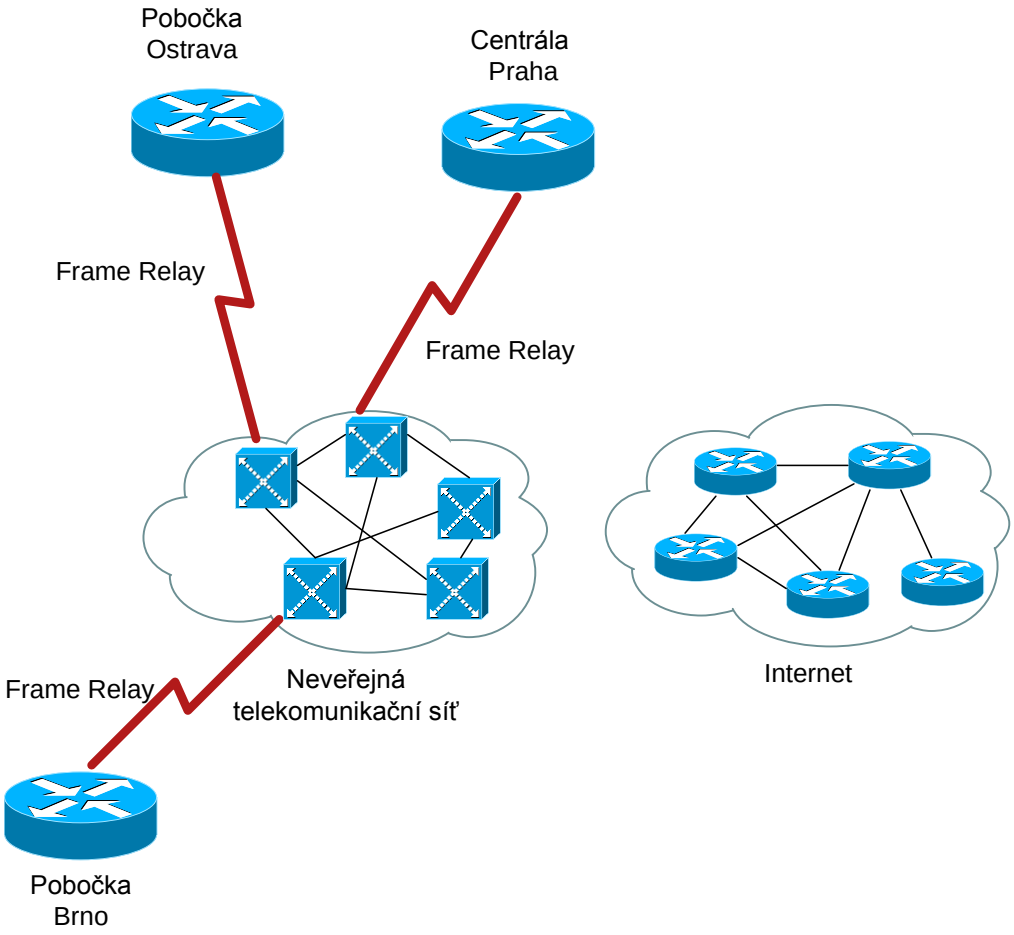
Tunelování – proces zapouzdření původního paketu do jiného. Původní paket je všechna mezilehlá zařízení nečitelný po celou dobu přenosu.

Důvody tunelování

- zajištění bezpečnosti
- transportní mechanismus

Rozdělené tunelování (split tunneling) – klient může současně komunikovat jak s VPN, tak i s Internetem.

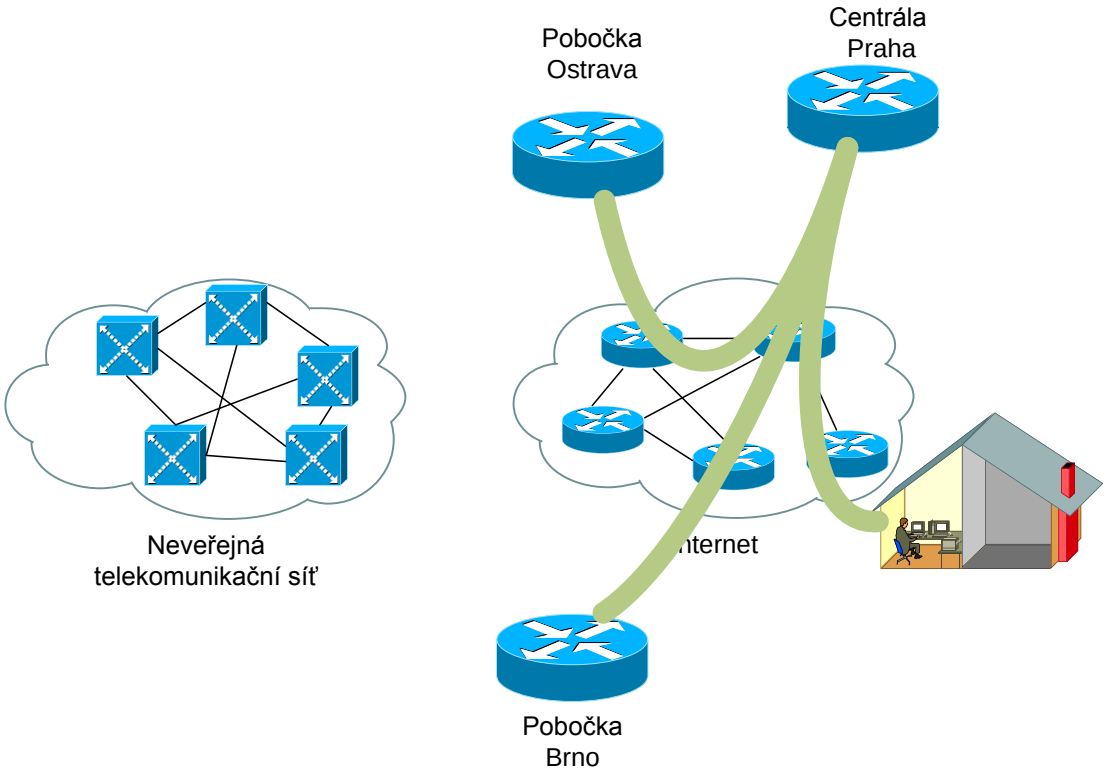
VPN - dříve



- vysoká cena
- nízká flexibilita
- omezená dostupnost
- složitá konfigurace
- site-to-site

- garance kvalitativních parametrů spojení
- málo firem mělo vlastní telco sítě mezi státy/kontinenty (AT&T, BT, IBM…)

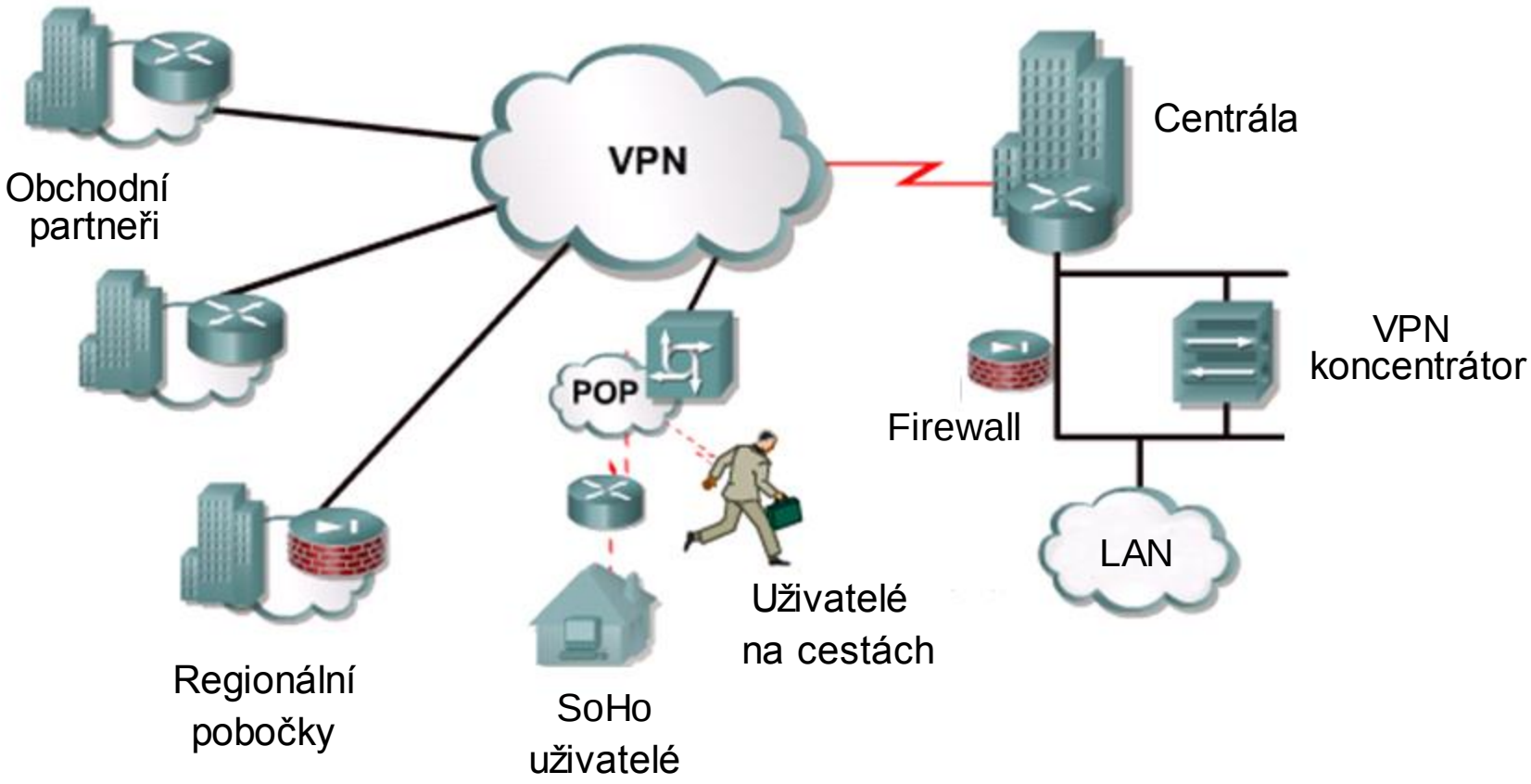
VPN – dnes (od konce 90. let)



- nižší cena
- dostupnost
- flexibilní
- site-to-site i remote-access
- tunelování

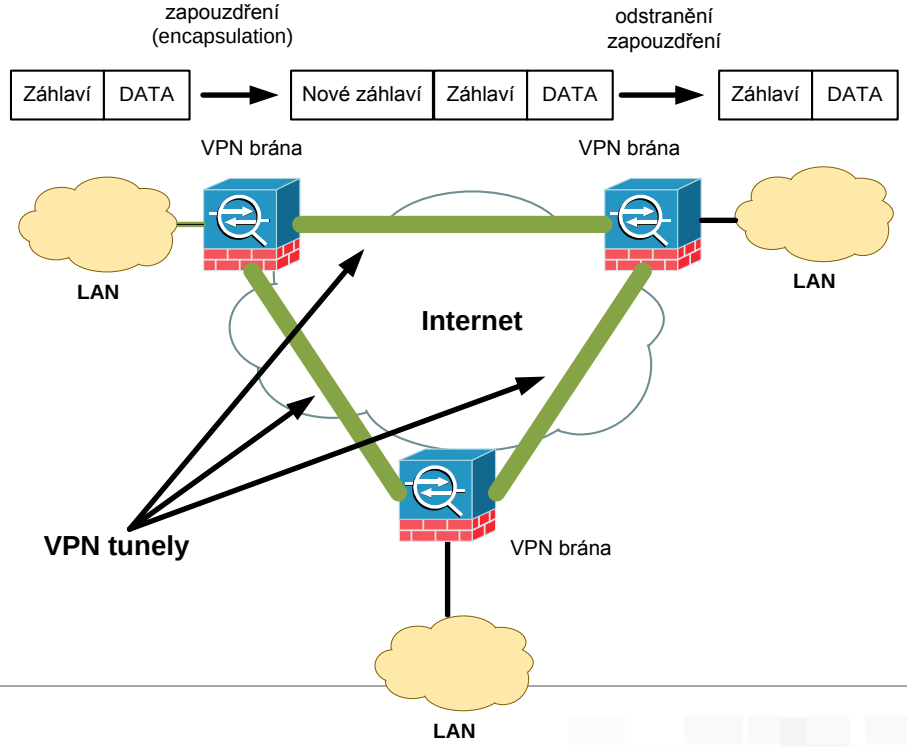
- telco operátoři dnes zajišťují pouze L1/L2/L3 konektivitu

VPN – co můžeme propojit ?



VPN - rozdělení

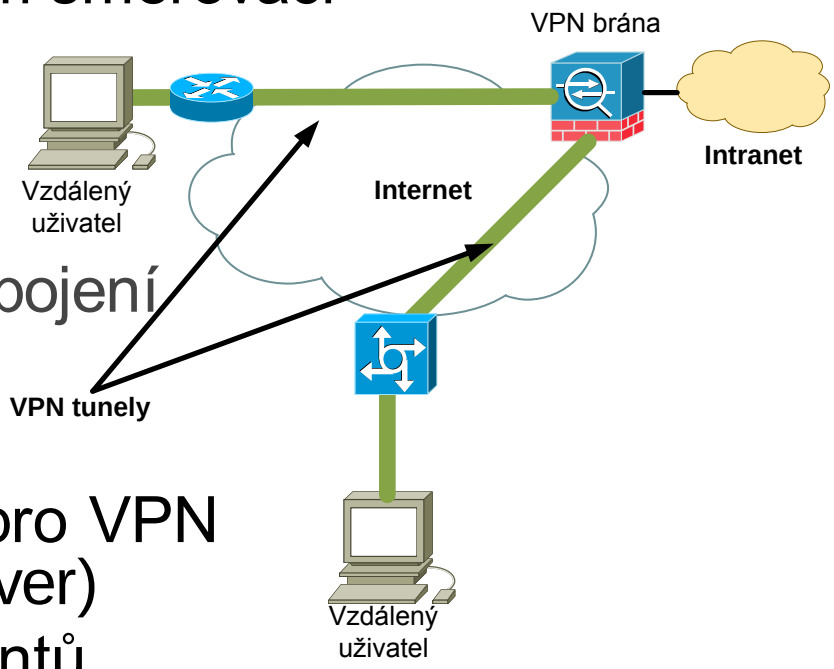
- Site-to-site nebo LAN-to-LAN
- propojení celých sítí
- tunely jsou obvykle permanentní
- VPN tunely terminovány na hraničním směrovači



VPN - rozdělení

- remote-access
- bezpečné připojení jednotlivých vzdálených účastníků
- provoz terminován na hraničním směrovači
  - menší počet uživatelů

  nebo na
- VPN koncentrátoru
  - stovky / tisíce současných spojení



- VPN brána plní i další funkce pro VPN klienty (DHCP server, DNS server)
- vyšší nároky na autentizaci klientů
  - připojují se kdykoliv a odkudkoliv

IPsec

- **I**nternet **P**rotocol **Sec**urity
- komplexní soubor protokolů řešící:
  - šifrování
  - autentizaci
  - integritu
  - tunelování
- zabezpečení síťové vrstvě RM OSI
- doporučená ~~povinná~~ součást IPv6
- volitelné rozšíření IPv4

IPsec – základní komponenty

- bezpečnostní protokoly:
  - AH – Authentication Header
  - ESP – Encapsulating Security Payload
- protokoly pro výměnu klíčů:
  - ISAKMP
  - IKE – Internet Key Exchange
- pomocné databáze
  - SPD - Security Policy Database
  - SAD - Security Association Database
- Domain Of Interpretation (DOI)
  - DOI obsahuje různé hodnoty jako identifikátory, ukazatele pro SA

IPsec – dokumenty RFC

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- **RFC 4301: Security Architecture for the Internet Protocol**
- **RFC 4302: IP Authentication Header**
- **RFC 4303: IP Encapsulating Security Payload**
- RFC 4304: Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)

IPsec - dokumenty RFC

- **RFC 4307: Cryptographic Algorithms for Use in the IKEv2**
- **RFC 4308: Cryptographic Suites for IPsec**
- **RFC 4309: Using AES CCM Mode with IPsec ESP**
- RFC 4543: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE)
- RFC 4806: Online Certificate Status Protocol (OCSP) Extensions to IKEv2
- RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4945: The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- **RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)**

Experimental RFC

- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2) Protocol

IPsec - dokumenty RFC

Informational RFC

- RFC 2367: PF_KEY Interface
- RFC 2412: The OAKLEY Key Determination Protocol
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3715: IPsec-Network Address Translation (NAT) Compatibility Requirements
- RFC 4621: Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
- RFC 4809: Requirements for an IPsec Certificate Management Profile
- **RFC 6071: IPsec and IKE Document Roadmap**

Obsolete RFC

- RFC 2401: Security Architecture for the Internet Protocol (IPsec overview)
- RFC 2409: The Internet Key Exchange
- RFC 4306: Internet Key Exchange (IKEv2) Protocol
- RFC 4718: IKEv2 Clarifications and Implementation Guidelines

IPsec – pracovní režimy

Transportní režim

- určen pro spojení host-to-host
- efektivnější než tunelovací
- zůstává původní hlavička

Tunelovací režim

- určen pro spojení site-to-site
- kompletně nová IP hlavička

- IPsec neobsahuje v záhlaví žádné v pole k určení režimu
- režim se určí podle hodnoty pole „next-header“
  - IP … tunelovací režim
  - TCP, UDP, ICMP, cokoliv jiného – transportní režim

IPsec – výhody a nevýhody

- **Výhody**
  - transparetnost
    - není potřeba nijak modifikovat protokoly vyšších vrstev
    - IPsec může zabezpečit libovolný protokol využívající IP
  - zabezpečuje staré protokoly, které jsou nezabezpečené
  - velká podpora mezi výrobci HW i SW
- **Nevýhody**
  - overhead
  - NAT
  - multicast/broadcast

IPsec – kryptografické prostředky

- Šifrování
  - Symetrické – DES, 3DES, AES
  - Asymetrické – RSA, DH
- Integrita
  - HMAC – HMAC-MD5, HMAC-SHA1
  - digitální podpisy
- Autentizace
  - PSK
  - certifikáty X.509

IPsec srovnání

	AH	ESP (pouze šifrování)	ESP (šifrování a autentizace)
integrita	x		x
autentizace původu dat	x		x
detekce replay útoků	x	x	x
utajení		x	x
omezená možnost utajení toku dat		x	x
řízení přístupu	x	x	x

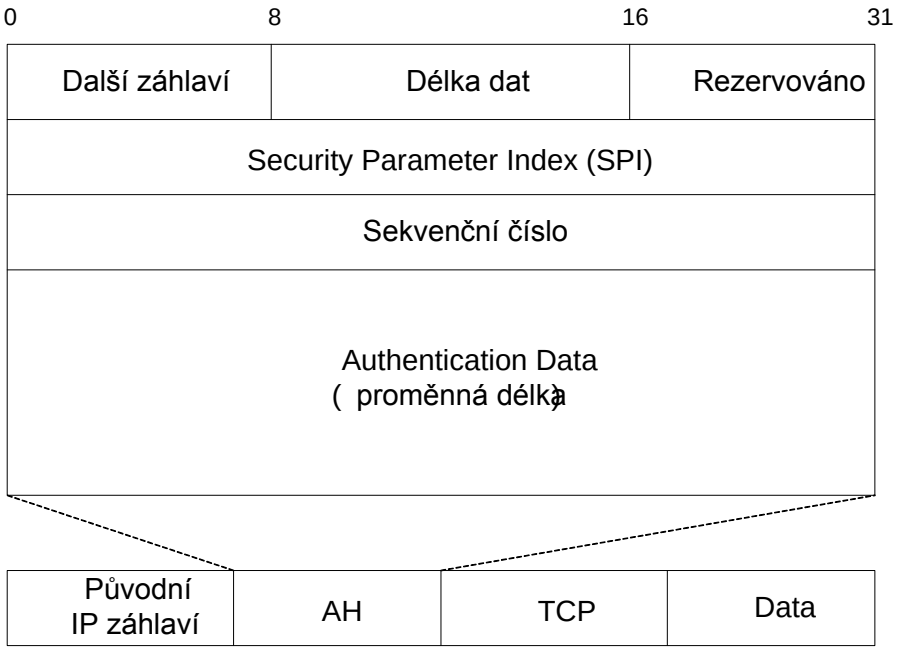
AH - Authentication Header

- nešifruje data
- protokol č. 51 (v IP hlavičce)
- autentizace záhlaví IP paketu
  - pouze neměnná pole
  - nelze chránit všechna pole – proč ?
- přidává se za původní IP záhlaví
- integritu zajišťují algoritmy MD5, SHA-1, Tiger, SHA-2
- vhodné pro aplikace, kde není nutné utajovat přenášená data, ale stačí je chránit před změnami

AH zajišťuje:

- integritu přenášených IP datagramů
- autentizaci odesílatele IP datagramů
- ochrana proti *replay* útokům

AH - Authentication Header



Další záhlaví – jaký protokol je zapouzdřen v AH

Rezerva – nepoužívá se

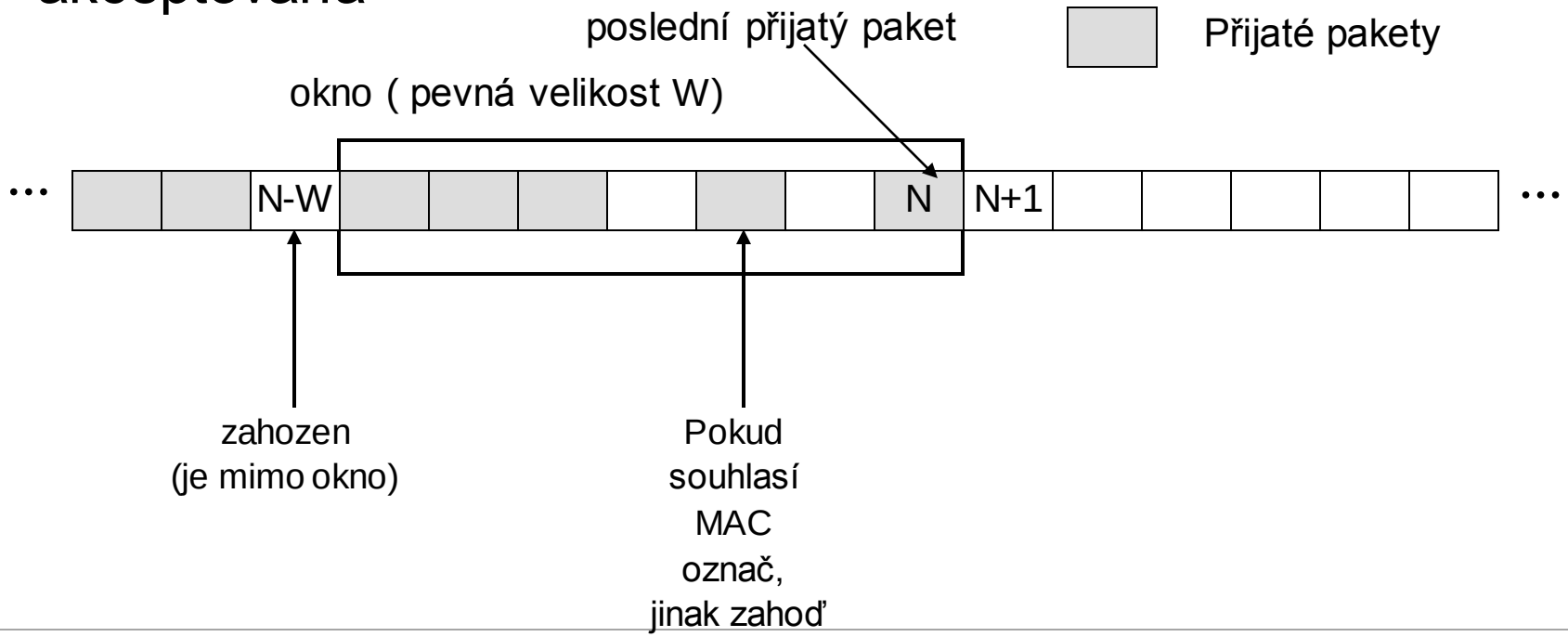
SPI - 32-bitové pseudo-náhodné číslo identifikující bezpečnostní asociaci datagramu (SA). Pokud není SA sestavena má hodnotu 0x00000000.

Sekvenční číslo – pořadové číslo paketu protokolu AH (proti replay útoku)

Authentication Data – kontrolní součet přenášených dat

AH - detekce replay útoků

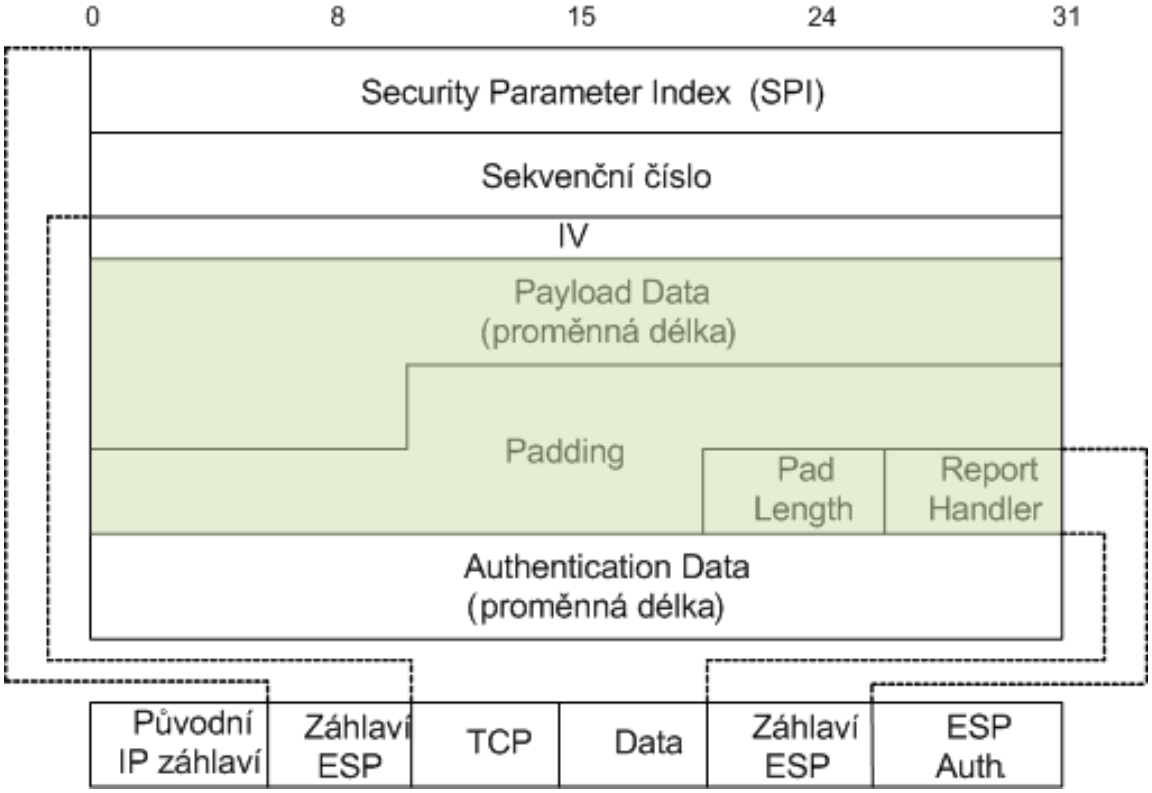
- **replay útok**: útočník získá autentizovaný paket packet a později ho znovu pošle k zamýšlenému cíli
- výchozí velikost anti-replay okna příjemce W = 64
- okno určuje max. rozptyl sekvenčních čísel, která budou akceptována



ESP - Encapsulating Security Payload

- RFC 2406
- protokol č. 50 (v IP hlavičce)
- zajišťuje přenášená data šifrováním
  - záhlaví IP není v transportním režimu chráněno – proč ?
- integrita - volitelná
- algoritmy DES,3DES, IDEA, CAST, RC-5, AES
  …vše v režimu CBC
- blokové šifry → zárovnání paketů !
- při volbě algoritmu NULL se chová jako AH

ESP – struktura záhlaví



SPI - 32-bitové pseudo-náhodné číslo identifikující bezpečnostní asociaci datagramu (SA). Pokud není SA sestavena má hodnotu 0x00000000.

Sequence Number Field – pořadové číslo paketu

Initialization Vector – pro šifrování v režimu CBC

Payload Data - vlastní šifrovaná data

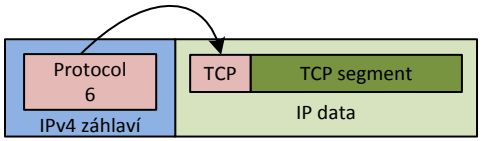
Padding – výplň

Payload Length – délka výplně

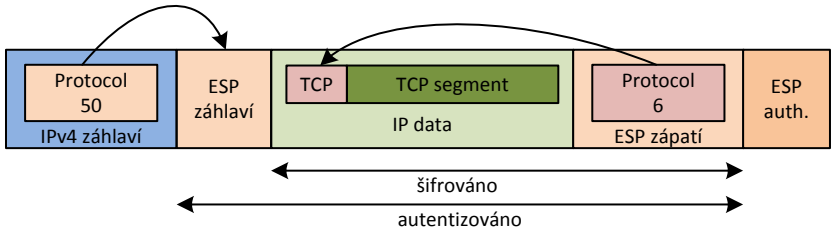
Next Header – číslo zapouzdřeného protokolu

Authentication Data – kontrolní součet přenášených dat

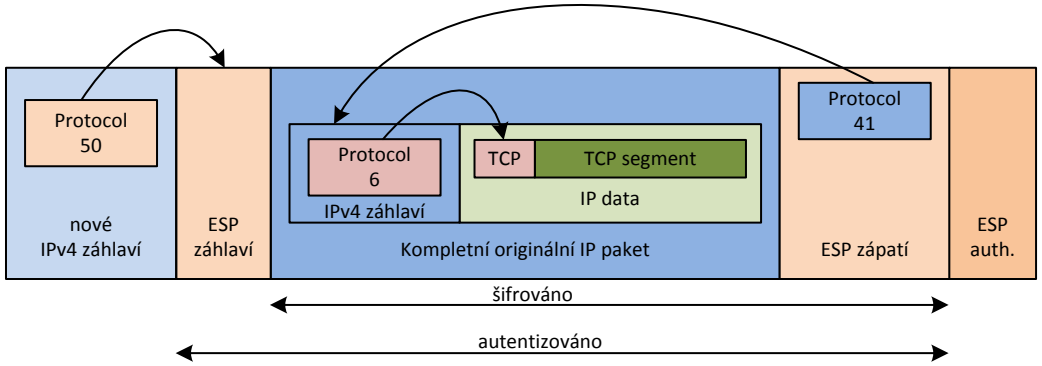
ESP – zapouzdření v IPv4



IPv4 paket

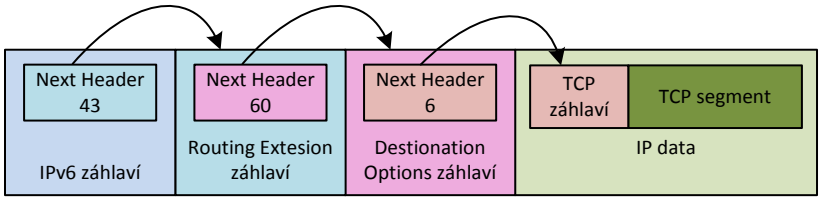


IPv4, ESP - transportní režim

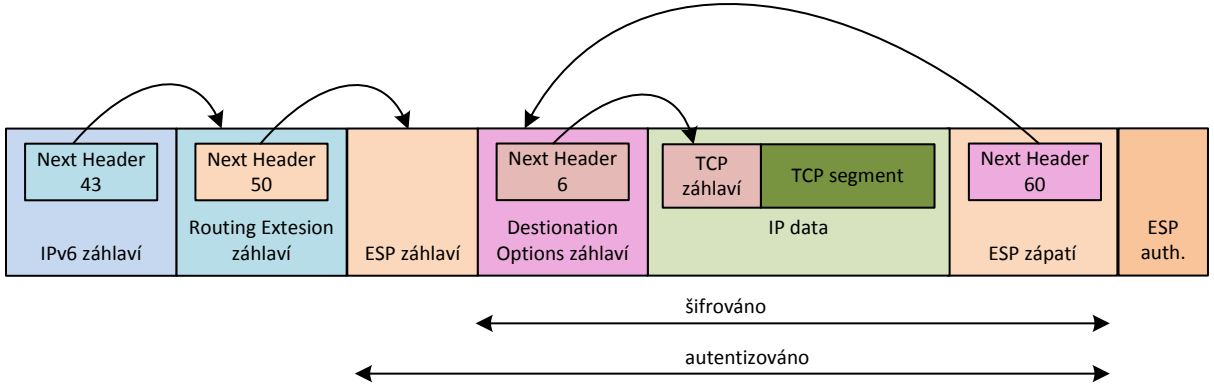


IPv4, ESP - tunelovací režim

ESP – zapouzdření v IPv6

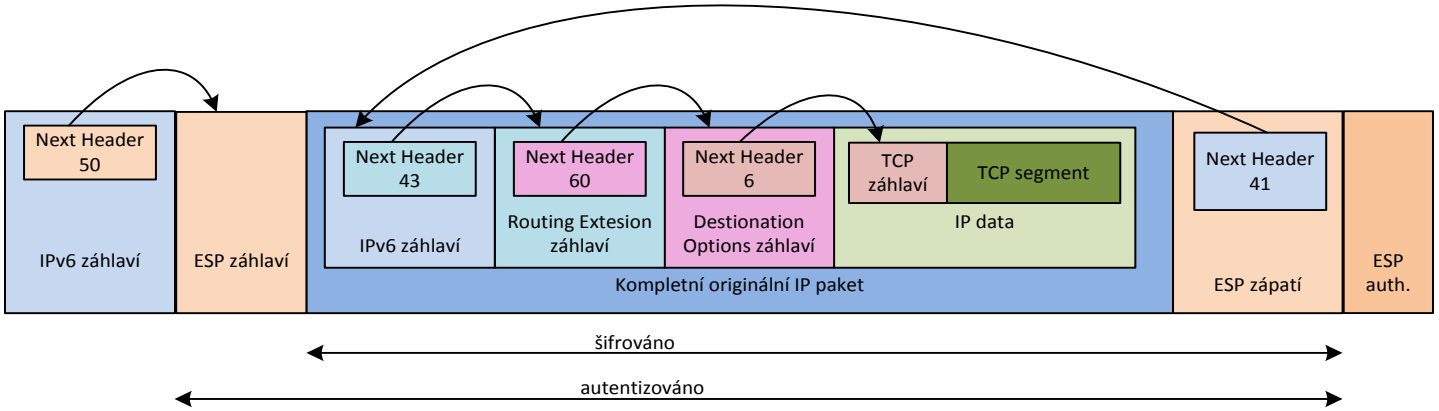


IPv6 paket



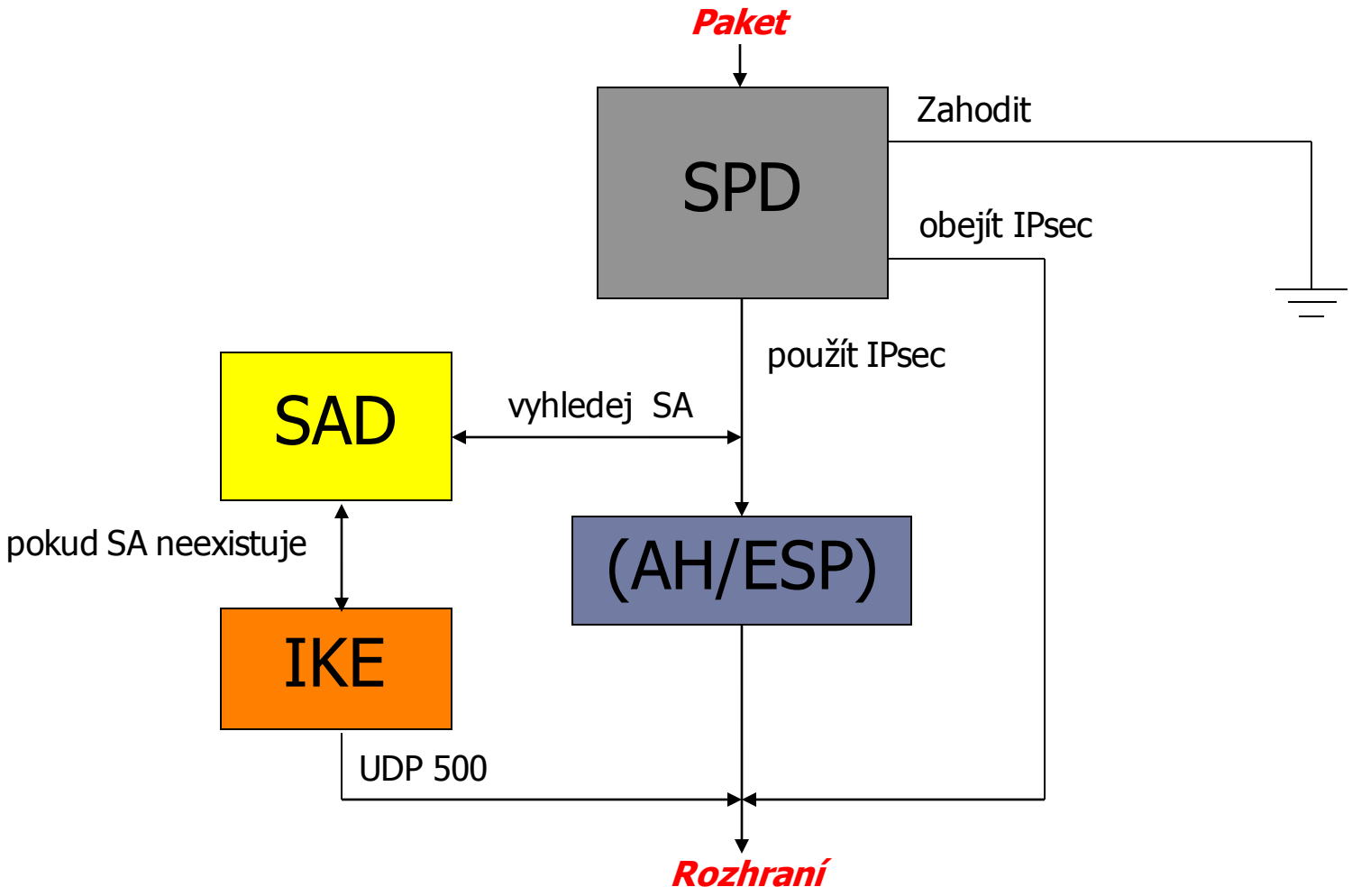
IPv6, ESP - transportní režim

ESP – zapouzdření v IPv6



IPv6, ESP - tunelovací režim

IPsec – jak to vlastně funguje



SPD, SAD

- Je nutné udržovat informace o tom, které IP toky se mají šifrovat a jak.
- K tomu slouží databáze **SPD** a **SAD**.

SPD (Security Policy Database)

- eviduje IP spojení, které se chránit pomocí IPsec
- podobné routovací tabulce
- pro každý paket se podle zdrojové/cílové IP adresy, protokolu a směru (in/out) určuje, jestli se má :

1) použít IPsec
2) paket doručit bez použití IPsec
3) paket zahodit

! V SPD nejsou uvedeny konkrétní klíče a algoritmy !

SAD - Security Association Database

- eviduje, jak se mají daty, na která má být aplikováno rozšíření IPSec chráněna
- jaké algoritmy a klíče je nutné pro konkrétní IP tok použít
- SAD obsahuje také přiřazení konkrétního SPI , dobu expirace klíčů, dobu expirace SA, minimální velikost MTU po cestě k cíli…

SPD tedy eviduje CO chceme dělat, SAD eviduje JAK to chceme provést.

SPI – Security Parameter Index

- SPI = ukazatel do SAD, kde jsou pro konkrétní spoj uvedeny požadavky na šifrování, zajištění integrity
- SPI – součást záhlaví každého paketu (AH, ESP)
- na základě detekce SPI se na příchozí paket aplikuje příslušné pravidlo
- každá strana má ke každému spojení sadu pravidel definující :
  - metodu zabezpečení (AH,ESP,obě)
  - pro každou metodu protokol pro kontrolní součet (MD-5, SHA-1)
  - pro ESP algoritmus (DES, 3DES, AES,…)

SA – Security Association

- SPI není jednoznačný
- SPI + IP adresa příjemce + protokol (AH / ESP) = SA
- SA reprezentuje sadu bezpečnostních služeb a parametrů vyjednaných pro každou zabezpečenou cestu
- SA se nastavují pomocí protokolu IKE nebo ručně
- SA je jednosměrná (pro každý směr existuje jiná)
- pro jedno IPsec spojení potřebuji minimálně dvě SA

Příklad SPD

Diagnostics: IPsec

SAD SPD

Source	Destination	Direction	Protocol	Tunnel endpoints
192.168. /24	10.0 /24	→	ESP	64.112. - 12.202
10.10 /24	10.0. /24	→	ESP	65.82 - 12.202
10.0. /24	10.0 /24	→	ESP	216.135 - 12.202
172.16 /24	10.0. /24	→	ESP	12.202. - 12.202.
10.0 /24	192.168 /24	←	ESP	12.202 - 64.112.
10.0. /24	10.10 /24	←	ESP	12.202 - 65.82
10.0 /24	10.0. /24	←	ESP	12.202 - 216.135
10.0 /24	172.16 /24	←	ESP	12.202 - 12.202

→ incoming (as seen by firewall)
← outgoing (as seen by firewall)

Příklad SAD

Diagnostics: IPsec

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.
12.202.	216.135	ESP	018c7b45	3des-cbc	hmac-md5
216.135.	12.202.	ESP	05a42292	3des-cbc	hmac-md5
12.202.	64.112	ESP	5977caa1	3des-cbc	hmac-md5
64.112.	12.202.	ESP	0c3f7f94	3des-cbc	hmac-md5

Proč řešit výměnu klíčů

Musíme zajistit:

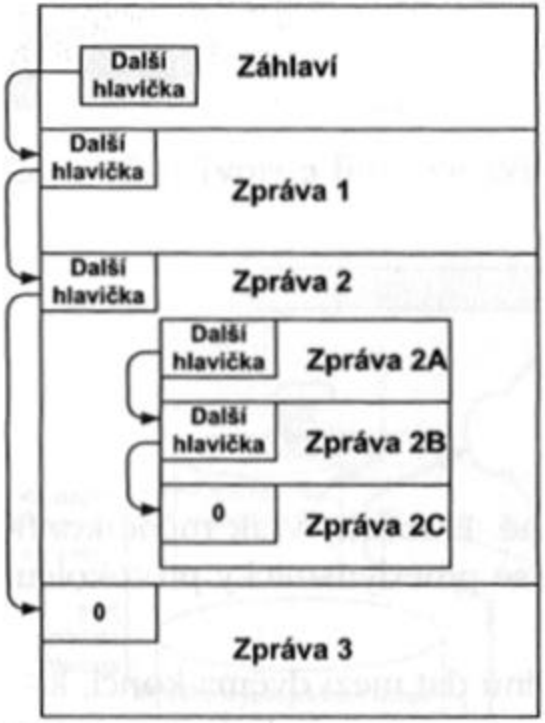
- sdílené tajemství
  - způsob jak ho vytvořit a domluvit se na něm
- autentizace
  - účastníci musí vzájemně ověřit svou identitu
- ochrana identity účastníků
  - pasivní útočník nemá být schopen odhalit identitu účastníků sledováním komunikace
- ochrana proti DoS
  - zlomyslný uživatel by neměl být schopný zneužít protokol tak, aby nutil protistranu plýtvat zdroji (CPU, pamět, BW)

ISAKMP

- Internet Security Association and Key Management Protocol
- RFC 2408
- používá UDP (port 500)
- nejde o C-S komunikaci, ale výzva/odpověď
- strana, která chce vytvořit nové SA iniciuje komunikaci protokolem ISAKMP
- ISAKMP definuje vlastní SA
- ISAMP slouží k:
  - autentizaci komunikujících stran
  - výměně dat pro šifrovací klíče
- obecný protokol pro vytváření SA
  - ISAKMP neřeší jak konkrétně se mají autentizované klíče vyměnit (to je práce protokolu IKE)

ISAKMP – struktura záhlaví

- zpráva ISAKMP může obsahovat vnořené zprávy



IKE - Internet Key Protocol

- flexibilní vyjednávací protokol
- vyjednání konkrétní metody autentizace, šifrování, délkách klíčů a dále umožňuje bezpečnou výměnu klíčů.
- RFC 2409
- používá Diffie-Hellmanův algoritmus
- používá se k výměně relačních klíčů (session key)
  - zprávy protokolu IKE jsou zapouzdřeny do paketů protokolu ISAKMP
  - má dvě fáze

IKE - Fáze 1

- sestavení bezpečného autentizovaného kanálu mezi komunikujícími počítači
- autentizuje a ochraňuje identitu komunikujících stran
- dojedná, jaké se použijí SA
- provádí autentizovanou výměnu sdílených klíčů
- používá UDP, port 500
- sestaví bezpečný tunel pro druhou fázi
- **Dva režimy: Hlavní (Main Mode)**
  Agresivní (Agressive Mode)

IKE - Fáze 1

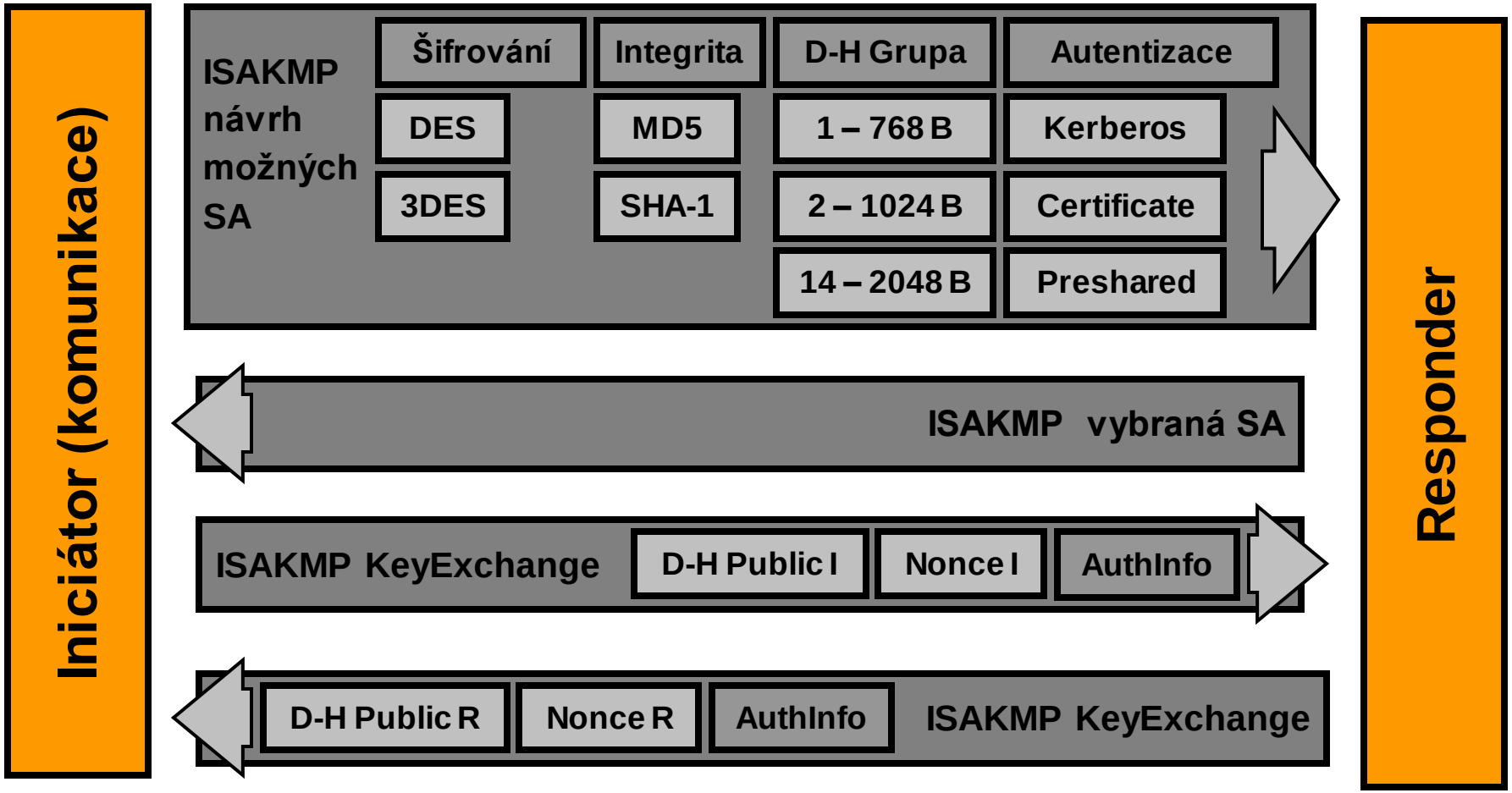
Hlavní režim IKE

- dojedná algoritmy a hashovací funkce
- vygeneruje sdílené tajemství pomocí DH algoritmu.
- ověří identitu protistrany.
- celkem 6 zpráv

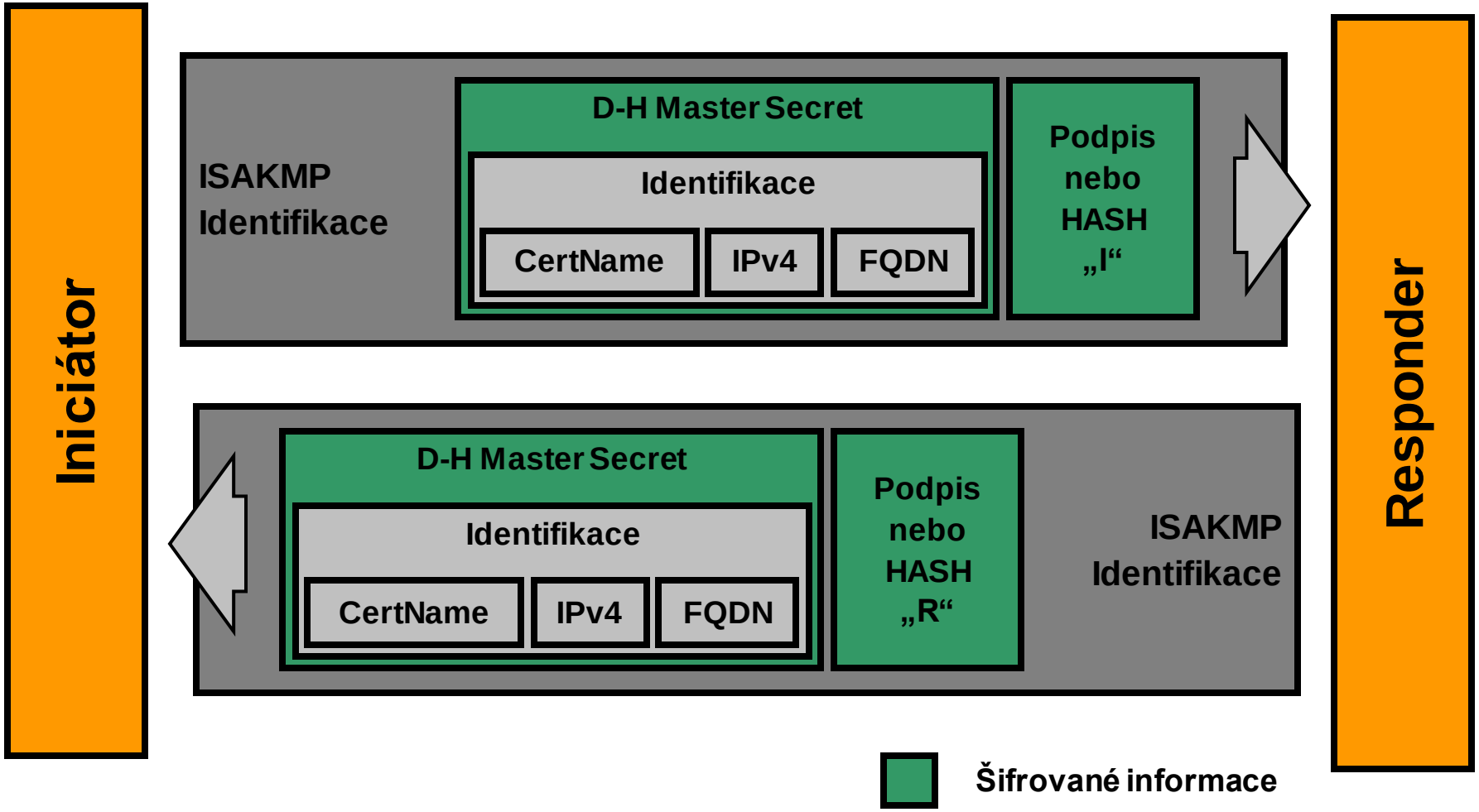
Agresivní režim IKE

- zkrátí vyjednávání do menšího množství paketů
- výhoda: šetří přenosové pásmo a čas
- nevýhoda: vyměňují se informace ještě před vytvořením šifrovaného spojení. Náchylné na odposlech (sniffing)
- celkem 3 zprávy

IKE - Fáze 1 (Main Mode) 1/2



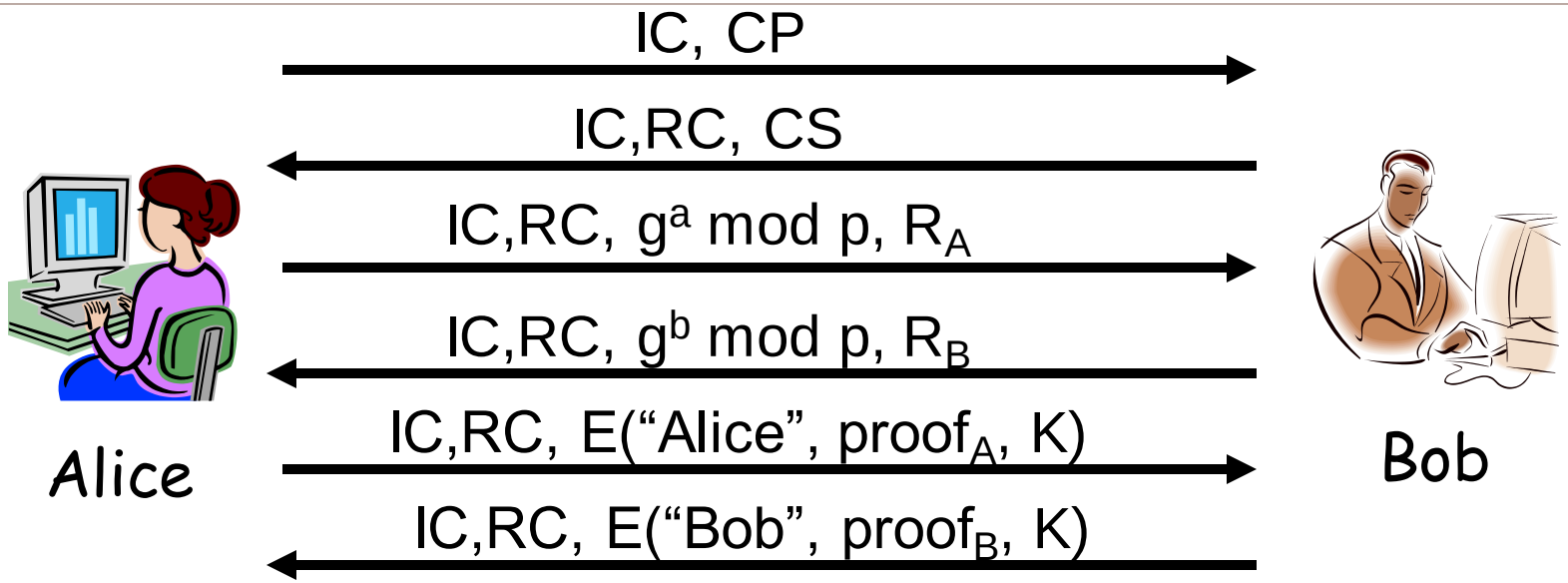
IKE - Fáze 1 (Main Mode) 2/2



IKE – Fáze 1 - varianty

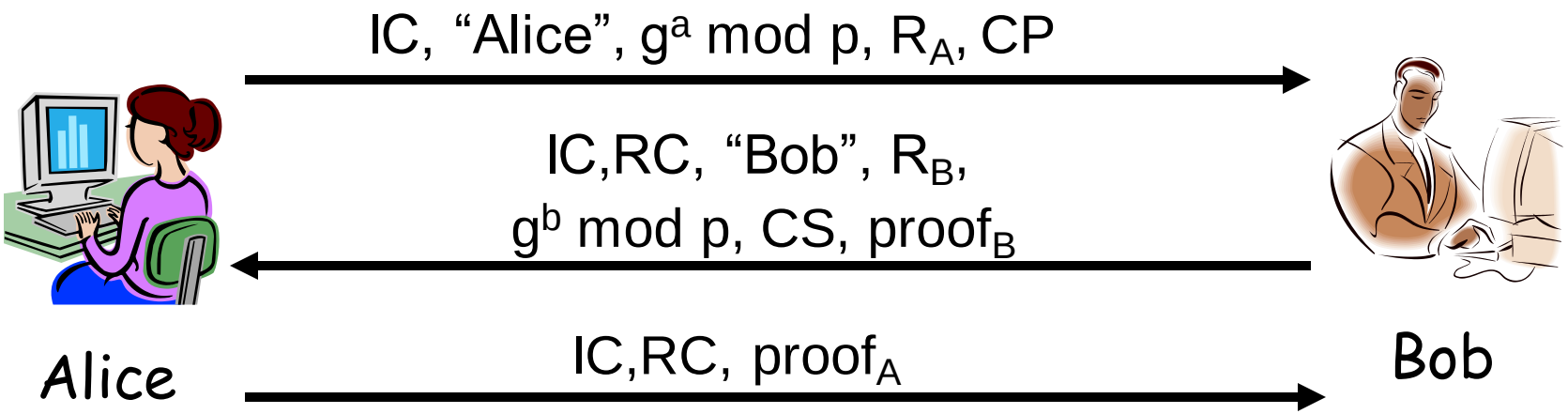
- Čtyři různé způsoby výměny klíče
  - asymetrické šifrování veřejným klíčem (původní verze)
  - asymetrické šifrování veřejným klíčem (zdokonalená verze)
  - digitální podpis
  - tajný klíč (symetrického algoritmu)
- pro každou z těchto variant existuje
  - Hlavní režim
  - Agresivní režim
- **Dohromady existuje 8 různých verzí Fáze 1 protokolu IKE!**

IKE Fáze 1: Digitální podpis (Hlavní režim)



- CP = navržené zabezpečení, CS = zvolené zabezpečení
- IC = "cookie" vyzyvatele, RC = "cookie" odpovídajícho (responder)
- R_A,R_B.. náhodná čísla (nonce)
- K = hash(IC,RC,g^{ab} mod p,R_A,R_B)
- SKEYID = hash(R_A, R_B, g^{ab} mod p)
- $proof_A$ = [hash(SKEYID,g^a,g^b,IC,RC,CP,"Alice")]$_{Alice}$
- []$_{Alice}$….podepsáno tajným klíčem Alice tzn. Kdokoliv může ověřit

IKE Fáze 1: Digitální podpis (Agresivní režim)



Zásadní rozdíly oproti hlavnímu režimu

- nesnaží se chránit identitu
- nemůže vyjednat g nebo p (tzn. už musejí být nějak předjednaná)

IKE - hlavní vs. agresivní režim

- Hlavní režim **musí** být implementován
- Agresivní režim byl **měl být** implementován

- Při autentizaci pomocí digitálního podpisu zná
  - pasivní útočník zná identitu Alice a Boba v agresivním režimu
  - aktivní útočník může určit identitu Alice i hlavním režimu (Main Mode)

IKE Fáze 1 - Cookies

- IPsec cookies – ztěžují DoS útoky na server
- žádný vztah ke cookies u HTTP
- aby se zabránilo DoS, Bob (server) se snaží udržet spojení tak dlouho jak to jen půjde bezestavové
- ale současně si Bob musí pamatovat CP ze zprávy 1 (to je nutné pro prokázání identity ve zprávě č.6)
- Vlastnosti dobré cookie
  - měla by záviset na konkrétních datech účastníka B
  - měla by osahovat nějakou tajnou informaci
  - generování a ověřování cookie by mělo být rychlé
  - strana B by si neměla cookies schovávat

Jak vytvořit cookie - hash IP adresy odesílatele/příjemce , TCP portu a nějaké tajné hodnoty

IKE – Fáze 2

Výsledkem fáze 1 protokolu IKE je

- vzájemná autentizace komunikujících stran
- výměna sdíleného symetrického klíče
- ustanovení IKE **Security Association** (SA)

Fáze 2 vytvoří SA pro IPsec relaci

Srovnání s SSL/TLS

- SSL relace odpovídá IKE Fázi 1
- SSL spojení odpovídá IKE Fázi 2

IKE – Fáze 2 – Quick Mode

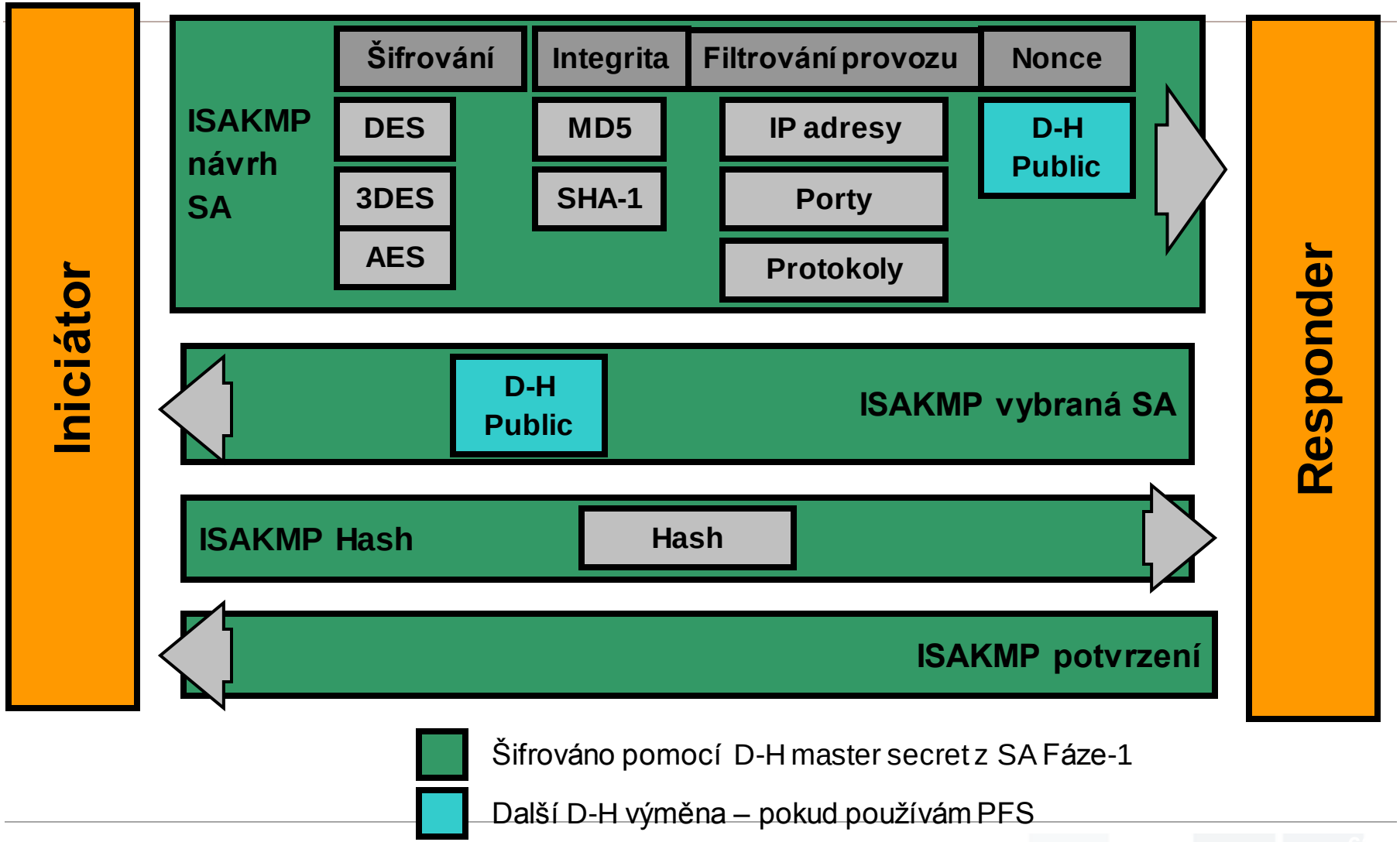
- dojednání Quick Mode SA a klíčového materiálu pro další komunikaci
- tato komunikace je od počátku chráněna pomocí algoritmů a klíčů získaných během fáze 1
- IKE Fáze 2
  - domluva na parametrech SA IPsec spojení
  - sestavení IPSec SA pro konkrétní spojení (např.: FTP, telnet, atd.)
  - periodická obnova IPSec SA
  - volitelné provedení další DH výměny
- v okamžiku, kdy byla sestavena SA pro nějaké konkrétní spojení, používá veškerý provoz na tomto spojení tuto SA

IKE – Fáze 2

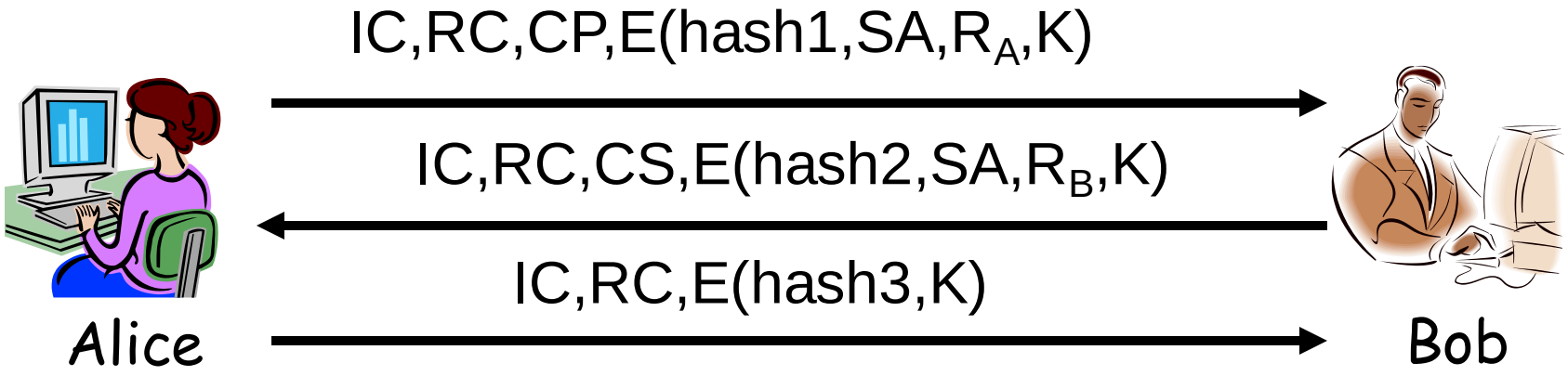
- Šifrování běžné komunikace
  - použije se Session Key odvozený z D-H Master Key získaného z Main Mode SA a z Nonce z dané Quick Mode SA

- Perfect Forward Secrecy – PFS
  - označuje stav, kdy aktuální klíče nejsou použity ke generování dalších klíčů
  - je-li náhodou konkrétní klíč rozšifrován/prozrazen, neumožní to útočníkovi snadné rozlomení dalších klíčů
  - pokud je PFS použito, v quick módu se znova pomocí DH generuje nová sdílená tajná informace
  - je to bezpečnější, ale trochu náročnější na výkon a čas při sestavování spojení
  - Session Key se získá z nového D-H Secret Key a Nonce získaných z dané Quick Mode SA
  - PFS zajišťuje, že session key není nikdy generován ze stejného materiálu

Quick Mode – SA + výměna klíčů



IKE Fáze 2



- Klíč K, IC, RC a SA jsou známé z Fáze 1
- návrh CP zahrnuje použití ESP a/nebo AH
- Hash 1,2,3 závisí na SKEYID, SA, R_A a R_B
- Klíče odvozené z KEYMAT = hash(SKEYID,R_A,R_B, junk)
- obnovení SKEYID závisí na způsobu výměny klíče ve fázi 1
- volitelné PFS (jednorázová Diffie-Hellmanova výměna)

Proč má IKE dvě fáze ?

- „drahá“ první část vygeneruje „hlavní“ SA
- „levná druhá část generuje vícenásobné vnořené SA založené na hlavní SA mezi dvěma stejnými uzly
- vnořené SA lze generovat opakovaně (ze stejné hlavní SA)
- to umožňuje
  - jiné SA pro AH a ESP
  - různý provoz může mít různé nároky na zabezpečení
  - různé SA pro různé typy služeb
    - není vždy nutné používat nejsilnější algoritmy

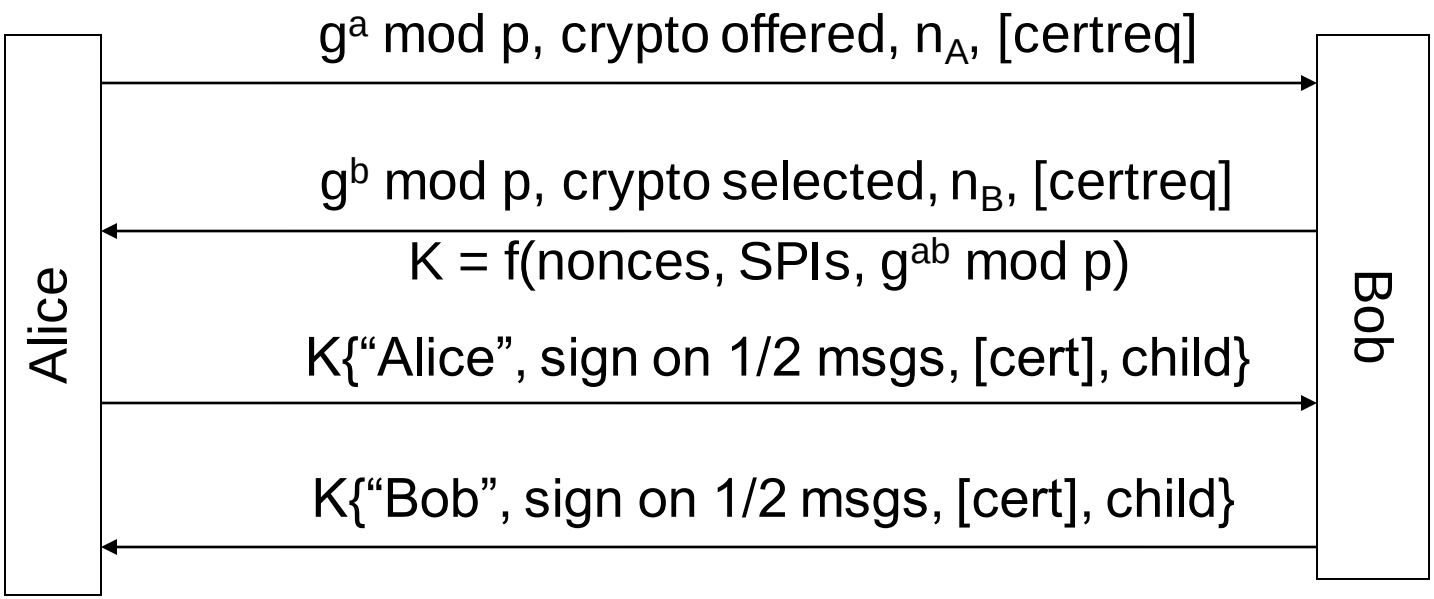
IKEv2

- 2005
- oprava chyb, zjednodušení oproti IEKv1
- snaha zůstat co nejvíc podobný IKEv1
  - „no gratuitous changes“
- jediný způsob autentizace
  - digitální podpis
- IKE SA + IPsec SA jsou vyměněny ve stejném protokolu pomocí 4 zpráv (~ Fáze 1 u IKEv1)
  - první child-SA (ESP, AH, IPcomp) vyměněny během zpráv 3 a 4 IKE SA
- vnořené/dceřiné SA (child-SA)
  - pokud je potřeba, tak se ustanoví v dalších dvou zprávách (~ Fáze 2 u IKEv1)
  - nové IPsec SA, nebo znovudojednání IKE SA

IKEv2

- zjednodušení dojednávání kryptografických parametrů
  - podpora pro „kryptografické sady“ (suites)
  - možnost oznámit „jakýkoliv z těchto šifrovacích algoritmů“, „jakákoliv z těchto hashovacích funkcí“
- vyšší spolehlivost
  - striktně challenge-response komunikace
  - odesílatel je zodpovědný za opětovné odeslání zprávy, pokud nepřijde odpověď
- dojednání parametrů pomocí „Traffic selector“
  - IKEv1: Responder může odpovídat pouze ANO/NE
  - IKEv2: přidána schopnost vyjednávat
  - více SA může mít stejný TS
- obnova klíčů:
  - může být vyvolána kdykoliv, libovolnou stranou
  - změny IKE-SA zahrnuje i všechny vnořené child-SA

Protokol pro výměnu (odpovídá Fázi 1 u IKEv1)

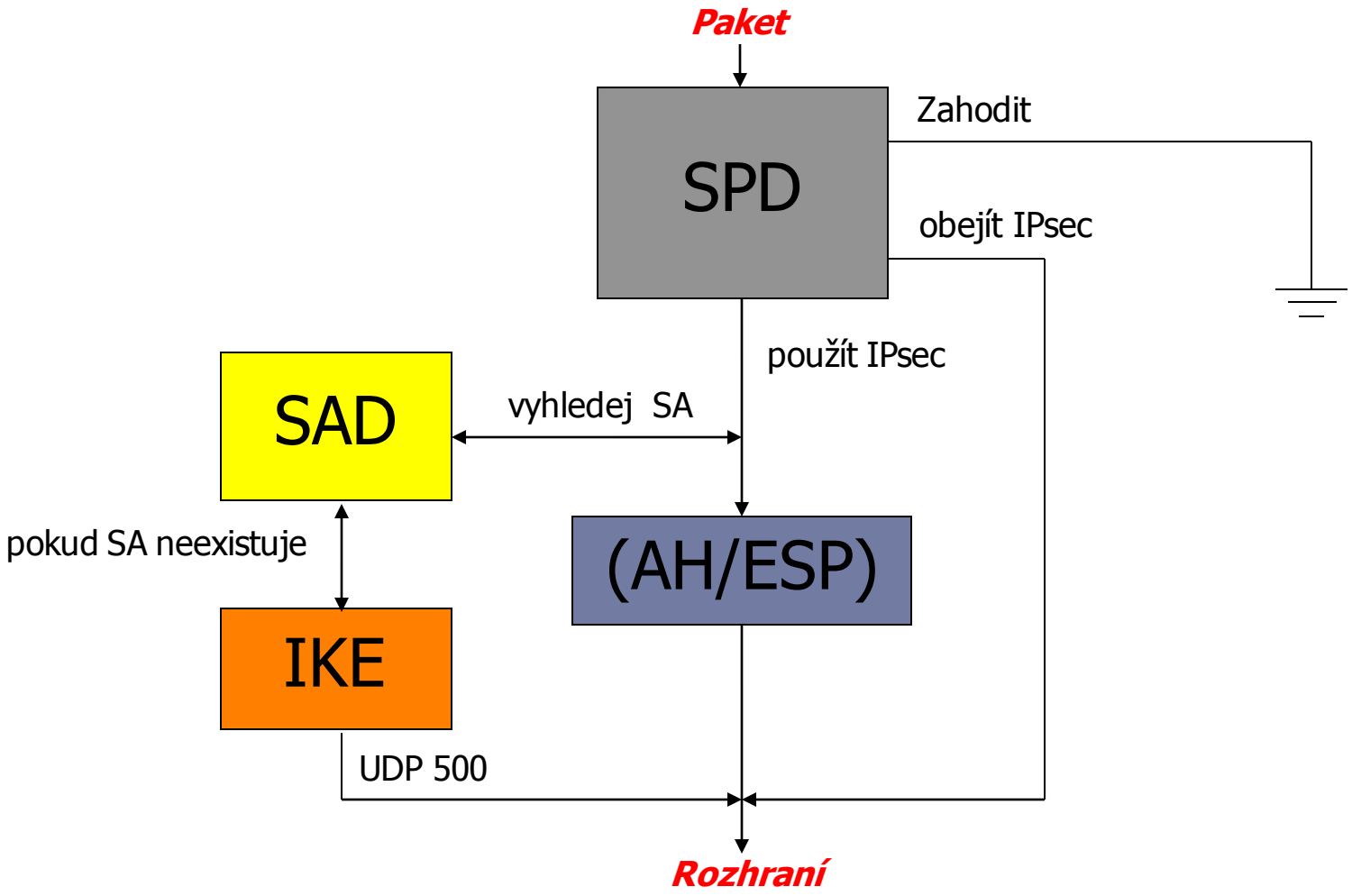


- Bob může volitelně odmítnout první zprávu a vyžadovat zaslání cookie
- vyžaduje 2 další zprávy

Diffie-Hellmann algoritmus pro výměnu klíčů

- **D-H grupy**
- RFC 2409, 3526, 5114
- obvykle se používají grupy 1,2,5
- číslo grupy udává velikosti modulu (mod *p*)
  - DH-1 768 bitů
  - DH-2 1024 bitů
  - DH-5 1535 bitů
  - DH-14 2048 bitů
- např. pro DH-5 $p = 2^{1536}-2^{1472}-1+2^{64}*\{[2^{1406}\pi]+741804\}$

IPsec


Paket
SPD
Zahodit
obejít IPsec
použít IPsec
SAD
vyhledej SA
pokud SA neexistuje
(AH/ESP)
IKE
UDP 500
Rozhraní

IPsec - shrnutí

+ zabezpečuje provoz na síťové vrstvě
+ univerzální pro zabezpečení jakéhokoliv TCP/IP provozu
+ chrání i před analýzou provozu (na úrovni síťové vrstvy)
+ vhodné pro pevné připojení vzdálených uživatelů
- nepodporuje přenos multicastu a broadcastu
- problémy s překladem adres (NAT,PAT)
  - mění se adresní pole chráněná HMAC-SHA1
  - řešení: zabalit IPsec paket do UDP (NAT-T)
- u remote-access nutná instalace klienta
  - kompatibilita různých implementací

SSL VPN

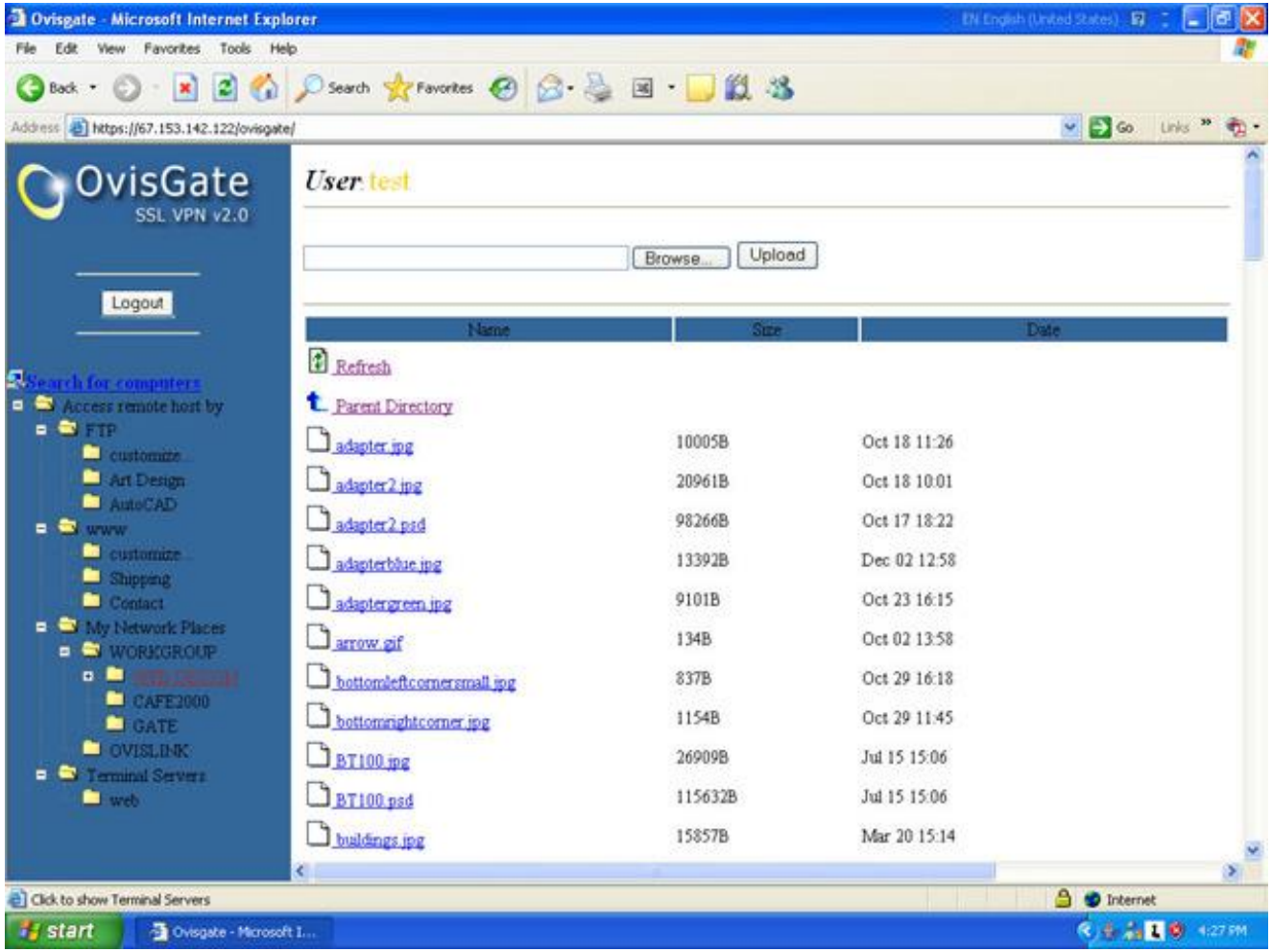
- vhodné pro VPN typu extranet
  - umožňuje jednoduše komunikaci typu B2B,B2C
- VPN brána se jeví jako běžný https server
  - dobře se vyrovnáná s NATem
  - vhodné pro mobilní uživatele
- VPN (SSL) brána ukončuje spojení a směrem do vnitřní sítě navazuje nové
- autentizace
  - heslo
  - token + heslo
  - certifikáty X.509

SSL VPN

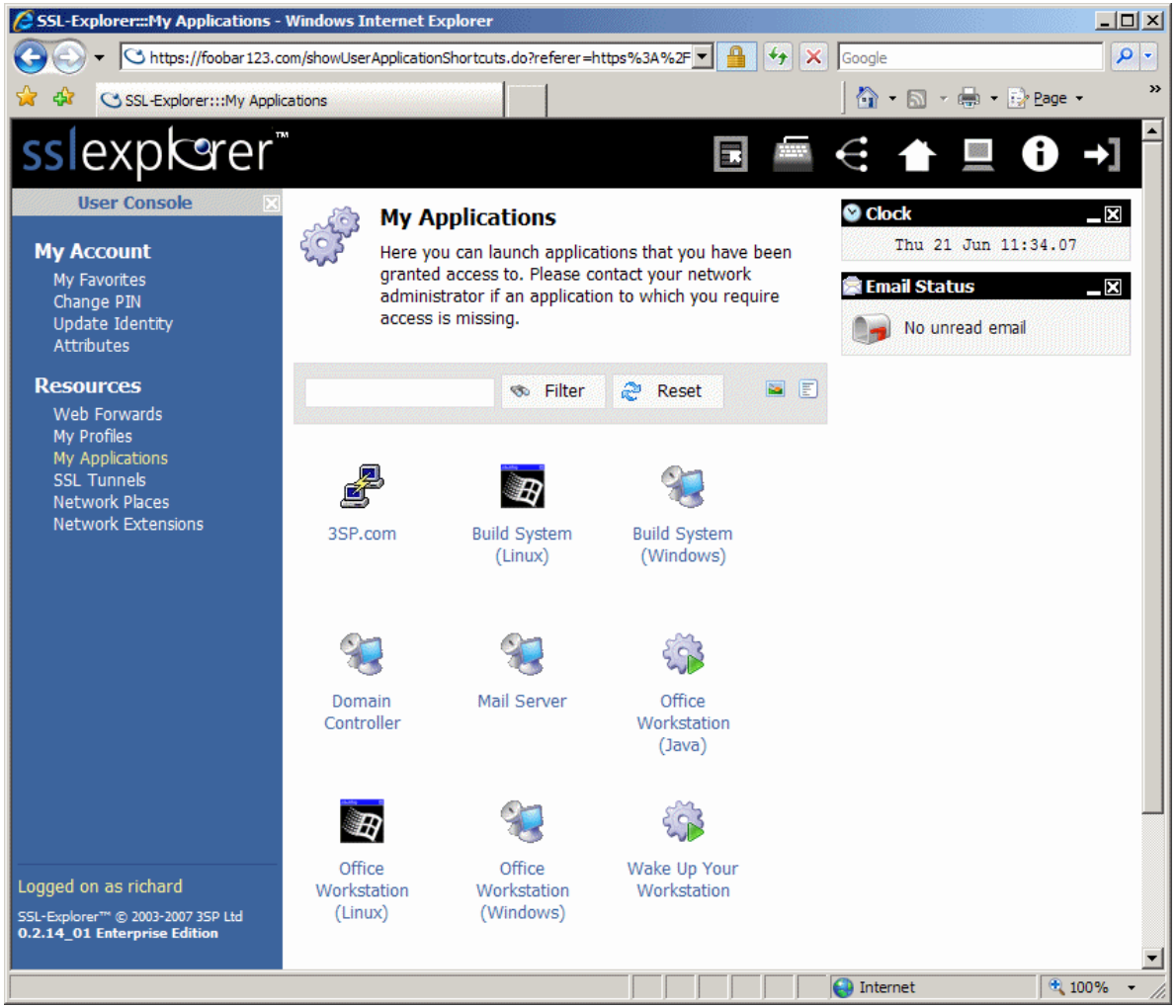
- několik variant:
  - Client-less
    - vhodné pro aplikace typu C-S (WWW, e-mail, Samba)
    - stačí prohlížeč s podporou HTTPS
  - Thin-client
    - aplikace typu Citrix, SAP
    - konektor – aplikace v Javě
    - lokální TCP proxy
  - Full-client
    - virtuální síťový adaptér

Příklad: SSL-Explorer
http://en.wikipedia.org/wiki/SSL-Explorer:_Community_Edition

Příklad SSL VPN



Příklad SSL VPN



Srovnání VPN na bázi IPsec a SSL

IPsec

+ univerzální
+ jednoduché
+ chrání celé síťové spojení
- instalace klienta
- neřeší autentizaci uživatele (sám o sobě)
- NAT
- broadcast / multicast

SSL

+ klienta má dnes každé PC
+ vhodné pro mobilní
- méně univerzální uživatele
- chrání pouze aplikační vrstvu

IPsec – univerzální v tom, kam můžu přistupovat

SSL VPN – univerzální v tom, odkud můžu přistupovat

Dotazy

Why Does AH Exist?

Skutečný důvod, proč existuje AH
(volný překlad podle Marka Stampa)

- Na jednom setkání komise IETF, která řešila tvorbu příslušných RFC o IPsec se stalo, že „..někdo z MS měl působivou řeč o zbytečnosti AH…“
- “…všichni v místnosti se navzájem podívali na sebe a řekli si „Hm. Má pravdu, AH je fakt k ničemu , taky ho nemáme rádi, ale když to vadí Microsoftu tak to tam (v návrhu doporučení) necháme, protože Microsoft nám leze na nervy více než AH.”