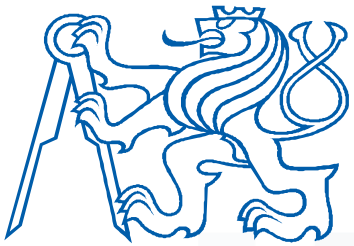
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE 10. přednáška

VPN - IPsec

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



Osnova

VPN

- rozdělení
- L2 – L2F, L2TP, PPTP
- L3 – IPsec
  - AH
  - ESP
  - IKE
- L4 - SSL/TLS … příští přednáška
- L7 - SSH … příští přednáška

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.

Z čeho se VPN skládá

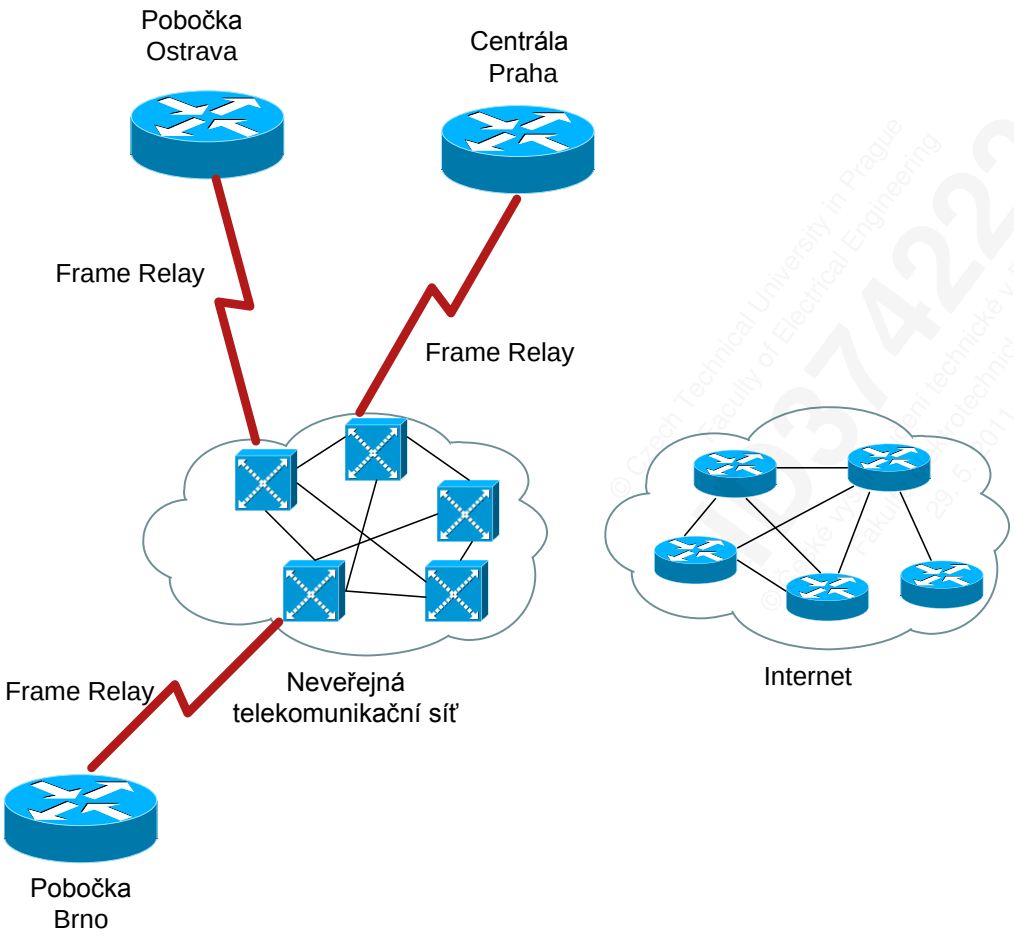
- **VPN brána** – zařízení pro připojení celé sítě k VPN
- **VPN klient** – software na koncovém zařízení umožňující připojení k VPN
- **autentizační server** – např. Radius, Kerberos, …
  – není nutný

IP VPN a MTU

Možnost fragmentace tunelovaných paketů, z důvodu překročení MTU při zapouzdřování paketů do tunelu. Informace o překročení MTU - ICMP zpráva typ 3

Řešení: předejít překročení MTU menšími pakety

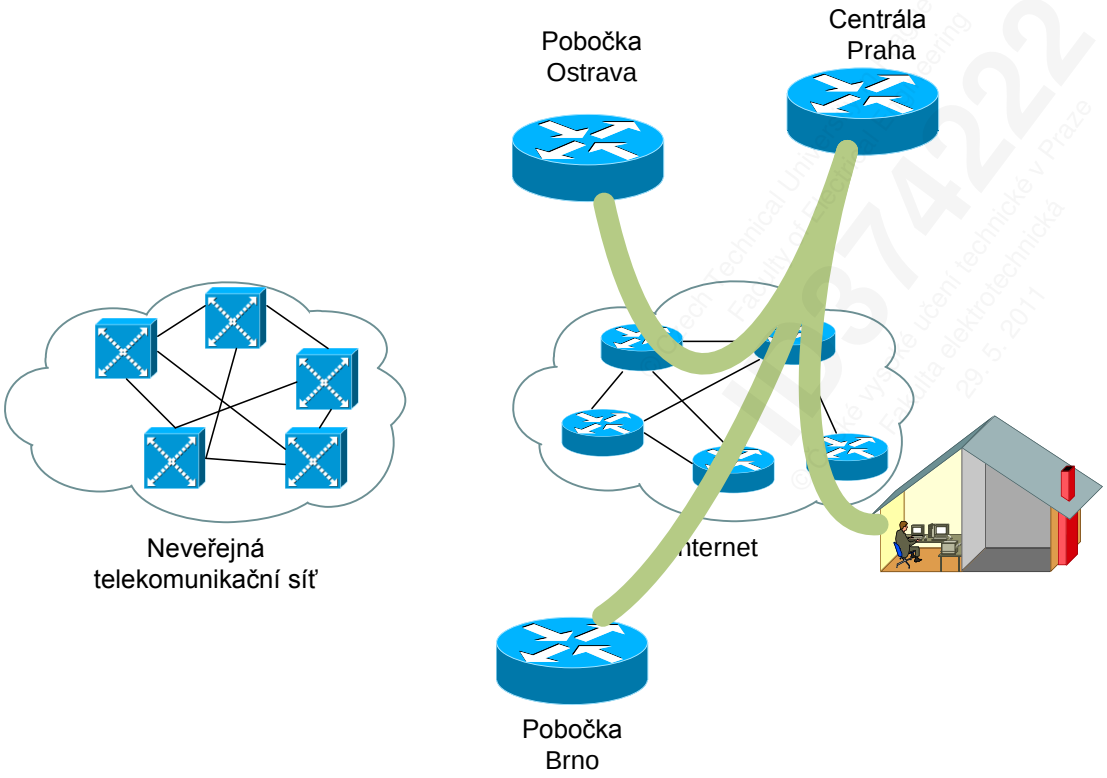
VPN - dříve



- 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…)

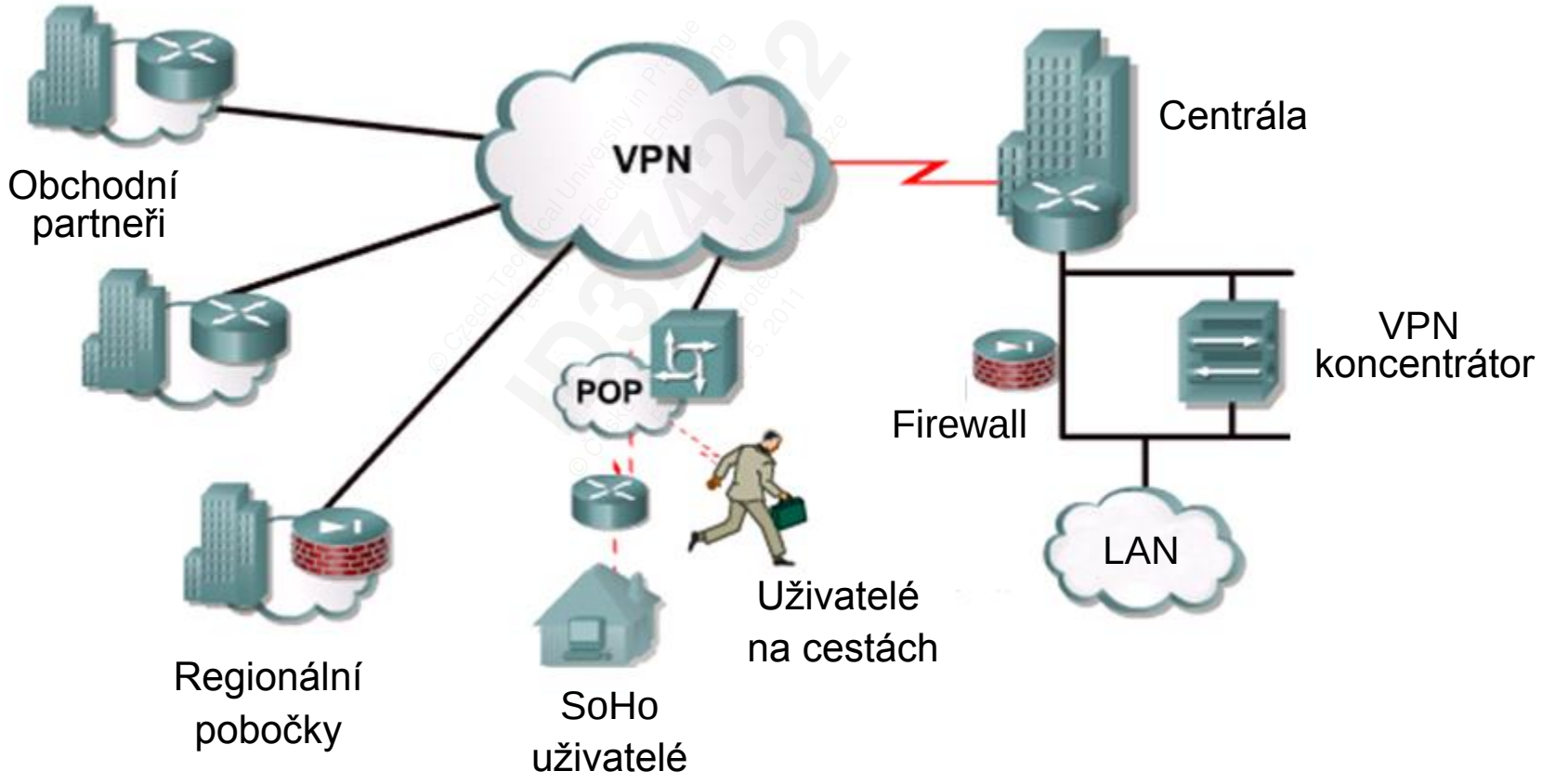
VPN – dnes (od konce 90. let)



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

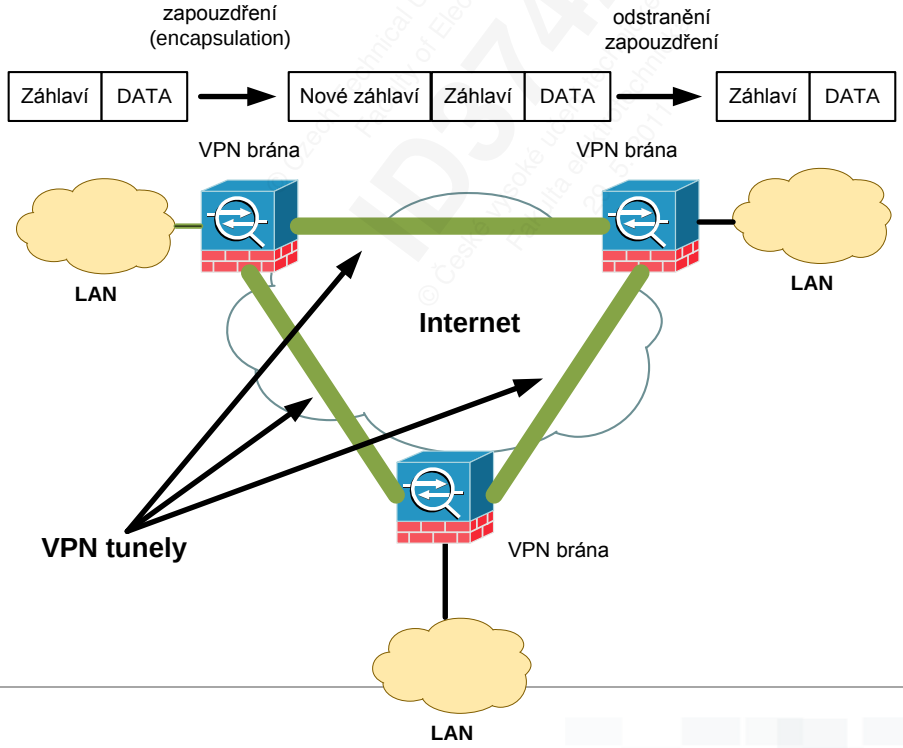
- telco operátoři dnes zajišťují pouze L1/L2/L3 konektivitu

VPN – co můžeme propojit ?



VPN - rozdělení

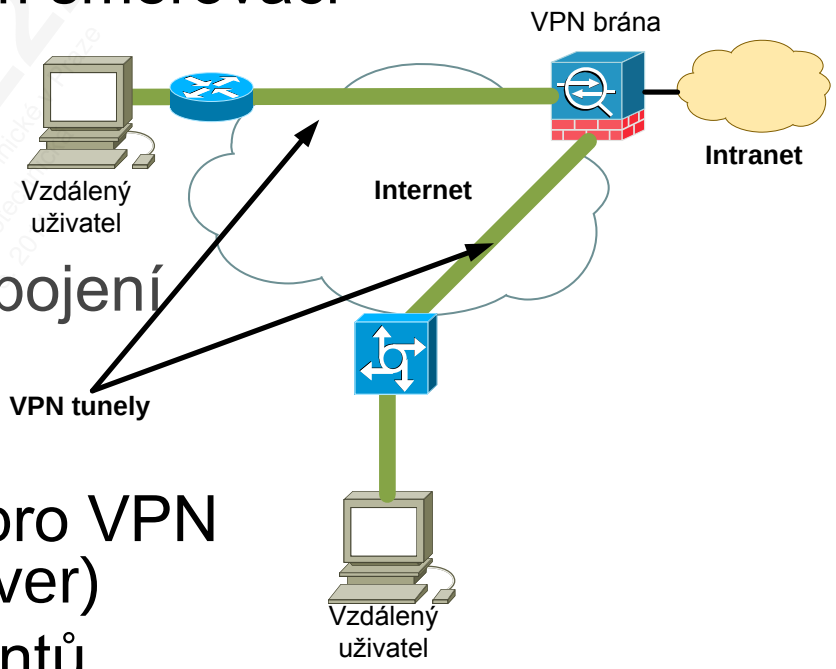
- Site-to-site nebo LAN-to-LAN
- propojení celých sítí
- tunely jsou obvykle permanentní
- VPN tunely terminovány na hraničním směrovači



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

Rozdělení VPN podle vrstev OSI modelu

Tunelování na L2:
- tunelování rámců spojové vrstvy (např. PPP) skrz Internet
- PPTP, L2TP, GRE, L2F, EoIP
- tunelovací protokoly využívají PPP k autentizaci uživatele, kompresi, šifrování,dynamické adresaci
- tunel je nutné udržovat

Tunelování na L3
- tunelování paketů síťové vrstvy (IP) skrz Internet
- IPsec, IP-over-IP
- není nutná udržovací fáze

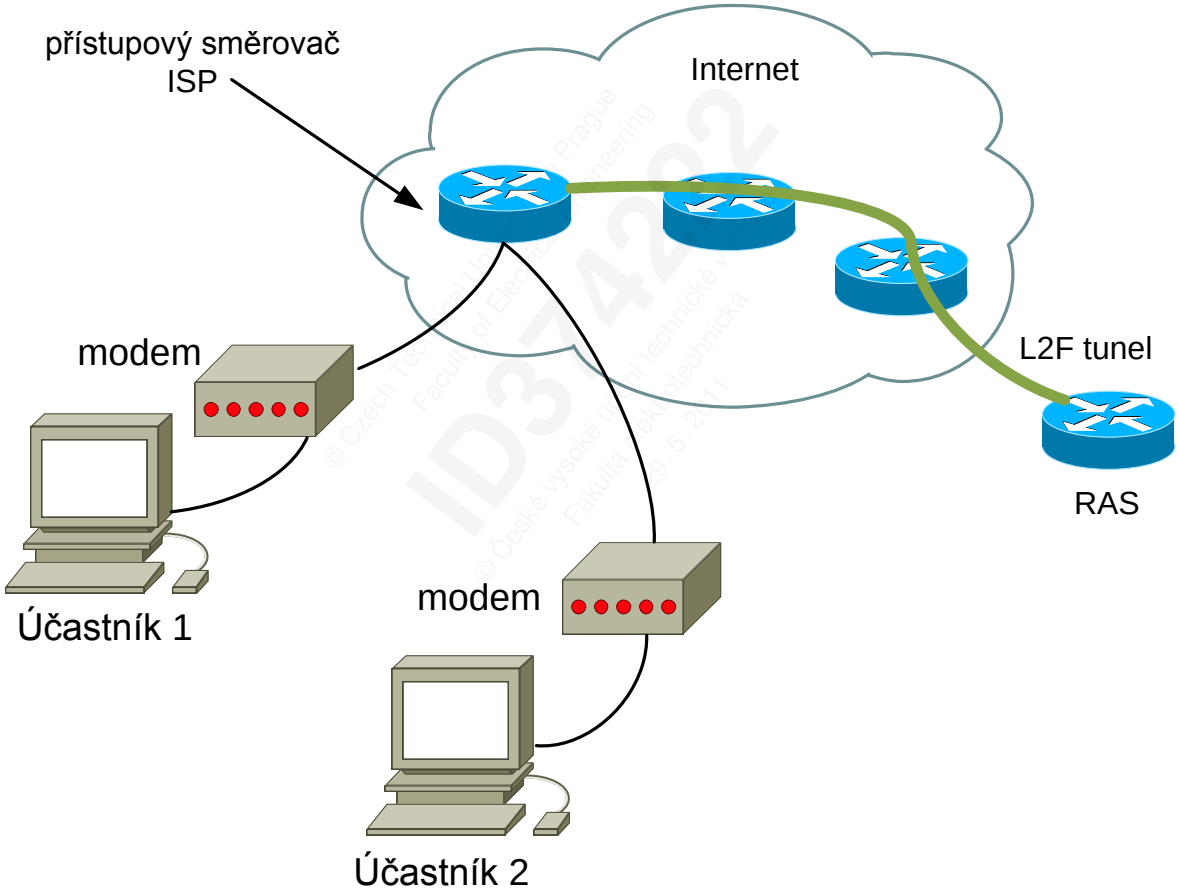
Tunelování 7. vrstvě - SSH, SSL VPN

L2 VPN – protokol L2F

- L2F - Layer 2 Forwarding
- RFC 2341
- nejstarší z L2 tunelovacích protokolů ~ 1998
- vyvinutý firmou Cisco
- nepodporuje šifrování
- zastaralý
- umožňuje tunelování PPP nebo SLIP skrz IP síť
- v jednom tunelu může být více spojení
- záhlaví 12B
- **závislý na prostředcích ISP**
- **vyžaduje spolupráci ISP**

L2F Header	Payload (PPP/SLIP)	L2F Checksum

L2 VPN – protokol L2F - topologie



L2 VPN – protokol GRE

- RFC 2784
- vyvinut firmou CISCO
- umožňuje přenášet různé síťové protokoly ve virtuálních point-to-point spojích přes jiné sítě
  - např. IPv6 tunely přes IPv4 síťě, nebo
  - multicast / broadcast zapouzdřovaný do IPsec
- podpora různých síťových protokolů (IP, IPX, Appletalk,…)
- zcela bezestavový
- nezajišťuje šifrování / autentizaci
- **dokáže přenášet síťový provoz typu multicast a broadcast**
- záhlaví 8B

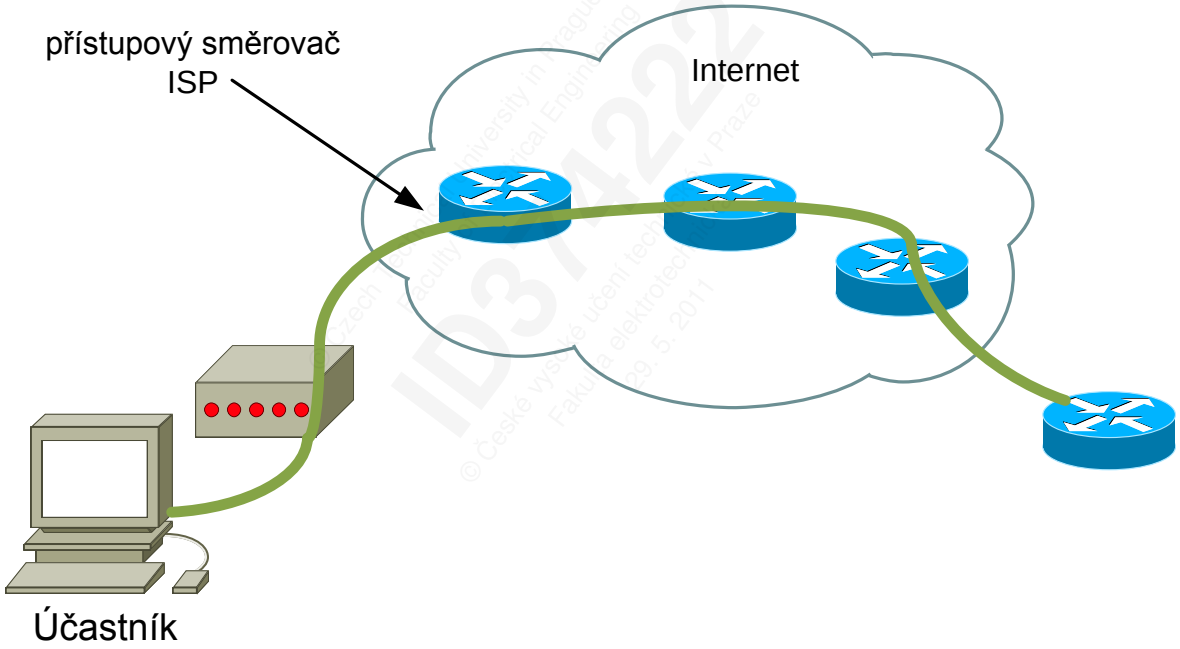
L2 VPN – protokol PPTP

- RFC 2637
- vyvinutý firmami Microsoft, Alcatel-Lucent, 3Com
- nativní podpora ve Windows
- využívá pozměněné GRE záhlaví
- umožňuje tunelování PPP protokolu skrz IP síť
- vytváří, spravuje a ukončuje tunelové připojení a zapouzdřuje rámce PPP
- potřebuje dvě síťové relace
  - řídící spojení – tcp/1723
  - druhá relace – GRE tunel pro data

L2 VPN – protokol PPTP

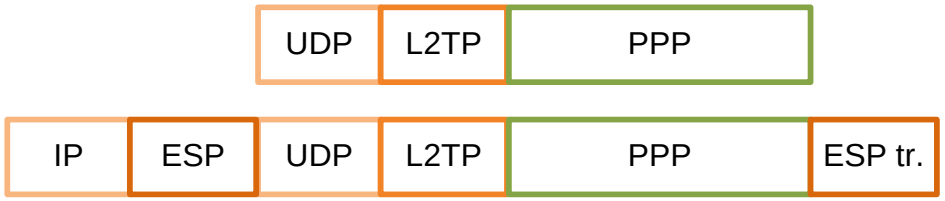
- nezajišťuje šifrování ani kontrolu integrity
- šifrování rámců PPP v PPTP protokolu lze v MS Windows volitelně zajistit pomocí MPPE
  - MPPE - Microsoft Point-to-Point Encryption
  - není bezpečné - klíče jsou odvozeny přímo z uživatelova hesla
  - klíč 40 bitů (LM hash) nebo 128 bitů (NTLMv2 hash)
  - www.schneier.com/paper-pptp.pdf
- autentizace pomocí MS-CHAPv2
- klient-server architektura
- spojení iniciuje vždy klient - „dobrovolné tunelování“
  - srovnejte s L2TP

L2 VPN – protokol PPTP



L2 VPN – protokol L2TP

- Layer 2 Tuneling Protocol
- RFC 2661
- vychází z L2F a PPTP
- poskytuje stejné funkce jako protokol PPTP
- výhodou proti PPTP je podpora více protokolů než jen IP
- L2TP paket se zapouzdřuje do UDP
- obvykle přenáší PPP relace
- neřeší šifrování a autentizaci (sám o sobě)
  - kombinace s IPsec



IP over IP

- RFC 2003
- tunelují se celé IP pakety
  - IPv4-in-IPv6
  - IPv6-in-IPv4
  - IP-in-IP
- malá režie
- není zabezpečené
- příliš se nepoužívá
- potencionální využití v Mobile-IP
  - umožňuje připojení mobilních účastníků
  - ICMP relaying – přeposílání zpráv z brány, která paket sestavila skutečnému odesílateli

SSTP

- alternativa k L2TP over IPsec
- Secure Socket Tunneling Protocol
- MS Vista SP1, Windows 7, Server 2008, RouterOS
- podporuje PPP a L2TP relace zapouzdřené do SSL 3.0
- pouze pro vzdálený přístup (remote access)
- nepodporuje site-to-site VPN
- SSTP server se povinně autentizuje během navazování SSL fáze
- SSTP klient se volitelně autentizuje během SSL fáze
- SSTP klient se povinně autentizuje během navazování PPP relace (např. EAP-TLS, MS-CHAPv2)

IPsec

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

- režimy činnosti
  - transportní
  - tunelovací

IPsec

Transportní režim

- určen pro spojení host-to-host
- efektivnější než tunelovací
- zůstává původní hlavička
  - pasivní útočník může sledovat kdo spolu komunikuje

Tunelovací režim

- určen pro spojení site-to-site
- kompletně nová IP hlavička
- útočník nemůže zjistit, kdo s kým komunikuje

IPsec

IPsec se skládá z:

- bezpečnostních protokolů: AH – Authentication Header
  ESP – Encapsulating Security Payload
- protokolů pro výměnu klíčů: ISAKMP
  IKE – Internet Key Exchange
- databází: SPD - Security Policy Database
  SAD - Security Association Database

Nejdůležitější RFC popisující se IPsec :

- RFC 2401: přehled architektury
- RFC 2402: popis protokolu AH
- RFC 2406: popis protokolu ES
- RFC 2408: IKE - správa klíčů

IPsec – přehled RFC

- 1321 The MD5 Digest Algorithm (and 1810 Report on MD5 Performance)
- 1750 Randomness Recommendations for Security (revision in draft)
- 1828 IP Authentication using Keyed MD5
- 2094 Group Key Management Protocol (GKMP) (Experimental)
- 2104 HMAC: Keyed Hashing for Message Authentication (and RFC 2202, Test Cases)
- 2284 PPP Extensible Authentication Protocol (EAP)
- 2394 IP Payload Compression Protocol (IPComp)
- 2451 The ESP CBC-Mode Cipher Algorithms
- 2460 Internet Protocol, Version 6 (IPv6) Specification (and related RFCs)
- 3168 The Addition of Explicit Congestion Notification (ECN) to IP
- 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- 3456 Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
- 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- 3526 More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)
- 3554 On the Use of Stream Control Transmission Protocol (SCTP) with IPsec
- 3566 The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- 3602 The AES-CBC Cipher Algorithm and Its Use With IPsec
- 3664 The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- 3686 Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
- 3715 IPsec-Network Address Translation (NAT) Compatibility Requirements
- 2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson.
- 2402 IP Authentication Header. S. Kent, R. Atkinson.
- 2403 The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn.
- 2404 The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn.
- 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy.
- 2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson.
- 2407 The Internet IP Security Domain of Interpretation for ISAKMP. D. Piper.
- 2408 Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, M. Schertler, M. Schneider, J. Turner.
- 2409 The Internet Key Exchange (IKE). D. Harkins, D. Carrel.
- 2410 The NULL Encryption Algorithm and Its Use With IPsec. R. Glenn, S. Kent.
- 2411 IP Security Document Roadmap. R. Thayer, N. Doraswamy, R. Glenn.
- 2412 The OAKLEY Key Determination Protocol. H. Orman. (Informational)

IPsec

Výhody IPSec

- transparetnost
  - není potřeba nijak modifikovat protokoly vyšších vrstev
- IPSec může zabezpečit libovolný protokol využívající IP
- zabezpečuje staré protokoly, které jsou nezabezpečené (telnet,ftp,SMB,…)

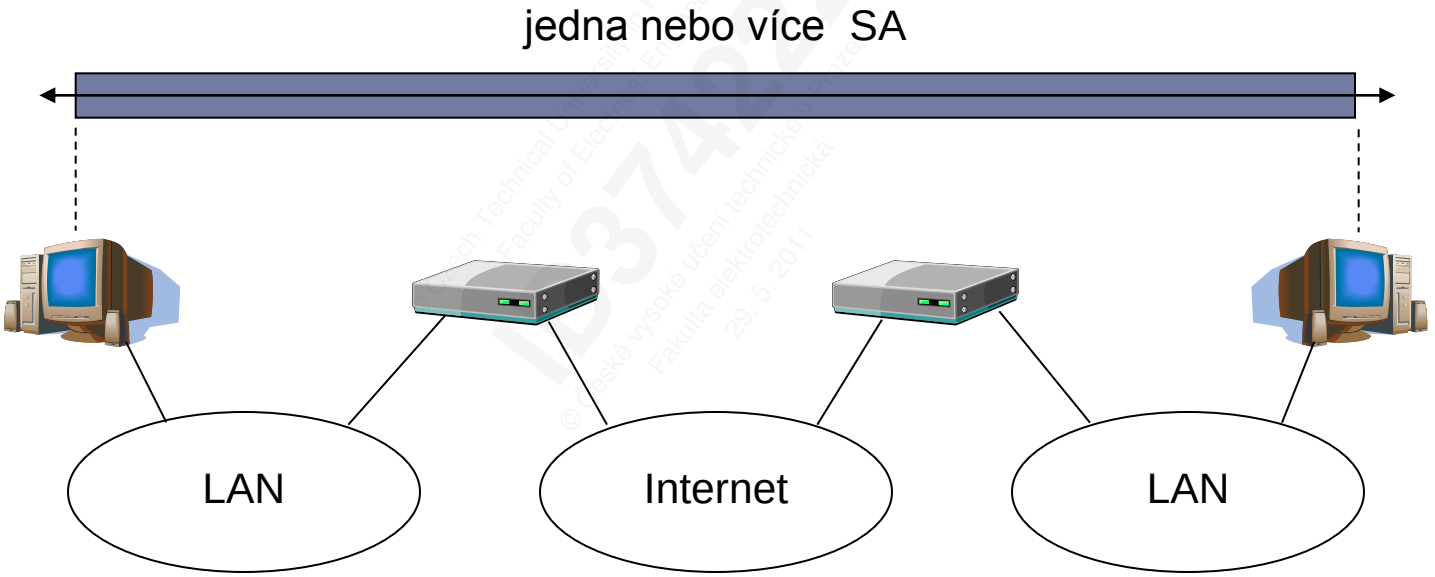
Široká podpora mezi výrobci HW i SW - Cisco, Microsoft, Network Associates, CheckPoint Software, Juniper, Nortel,…

IPsec – kryptografické prostředky

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

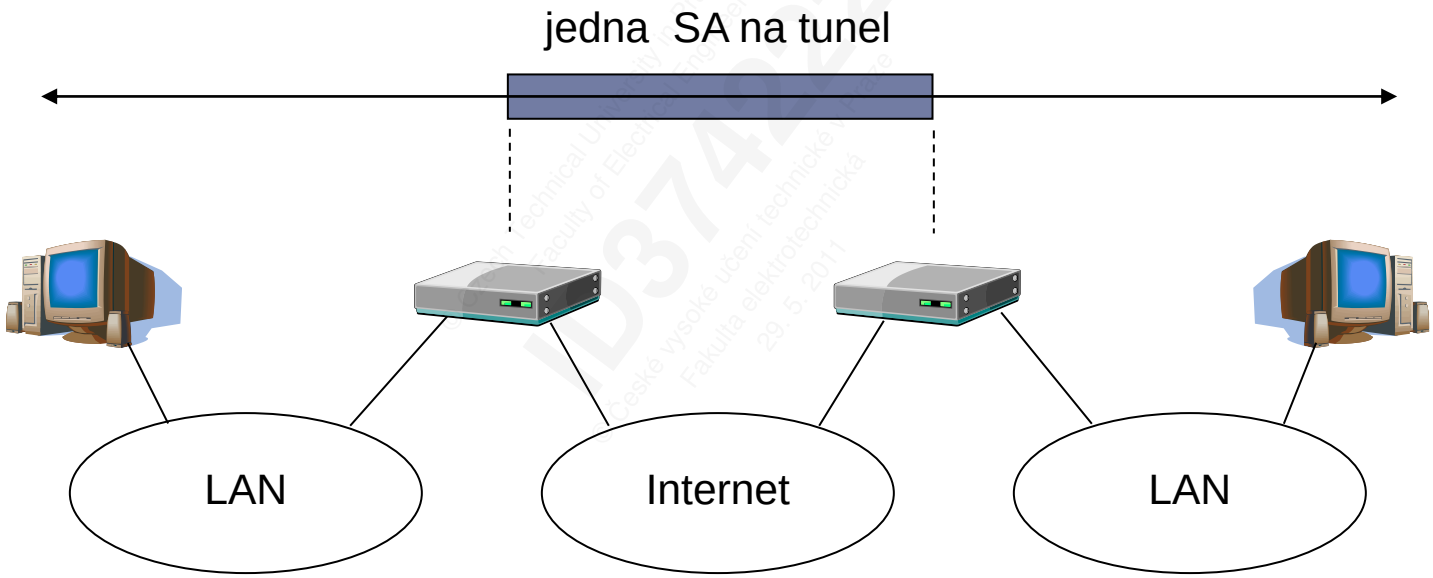
IPsec - režimy činnosti

Případ 1: spojení host-to-host



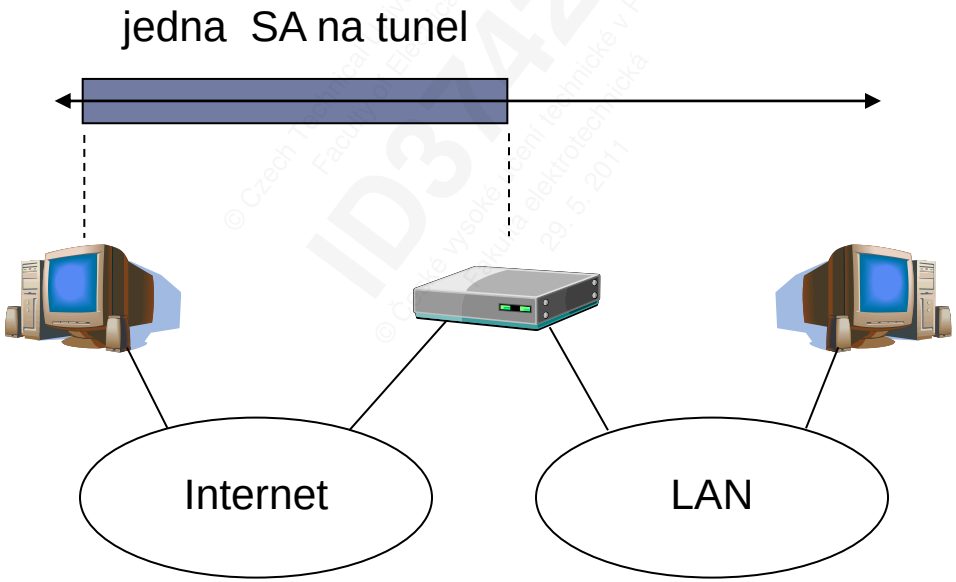
IPsec - režimy činnosti

Případ 2: bezpečné spojení LAN-to-LAN



IPsec - režimy činnosti

Případ 3: spojení host-to-gateway



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

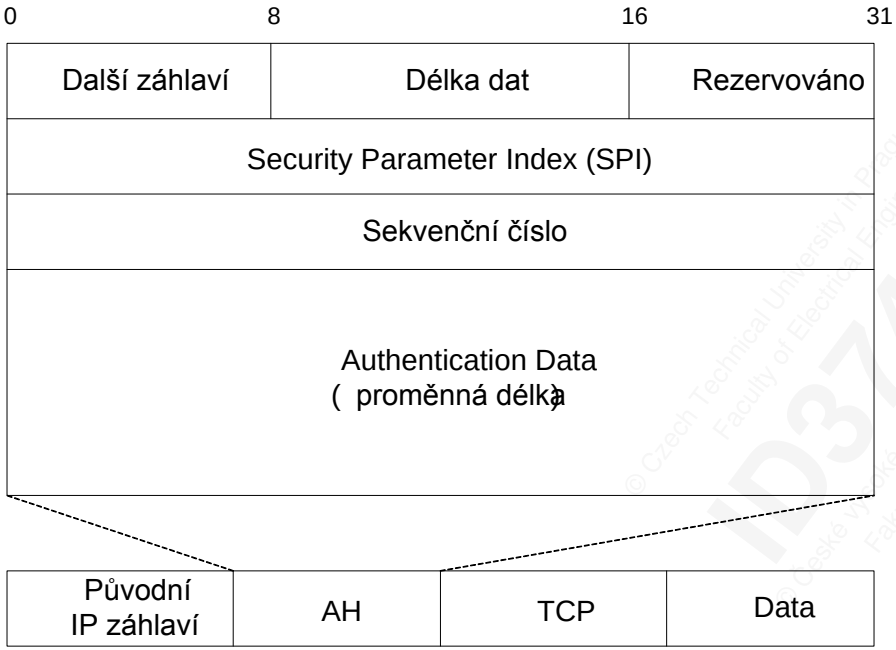
AH - Authentication Header

- 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)

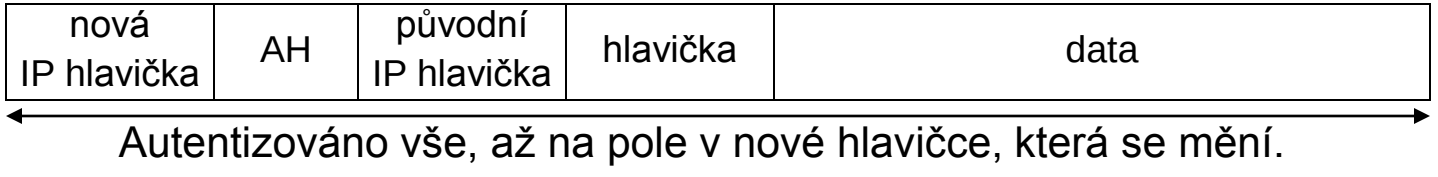
Authentication Data – kontrolní součet přenášených dat

AH - zapouzdření

Původní paket IPv4

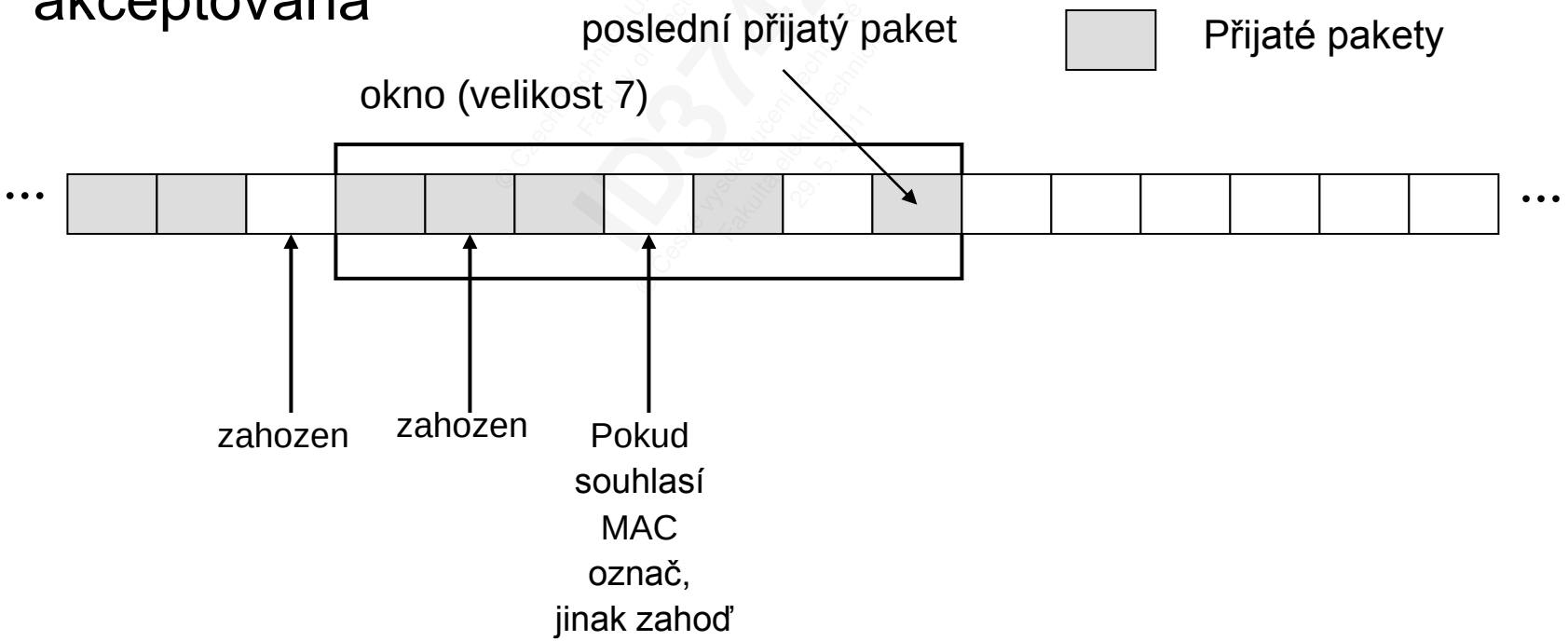
AH v transportním režimu

AH v tunelovacím režimu



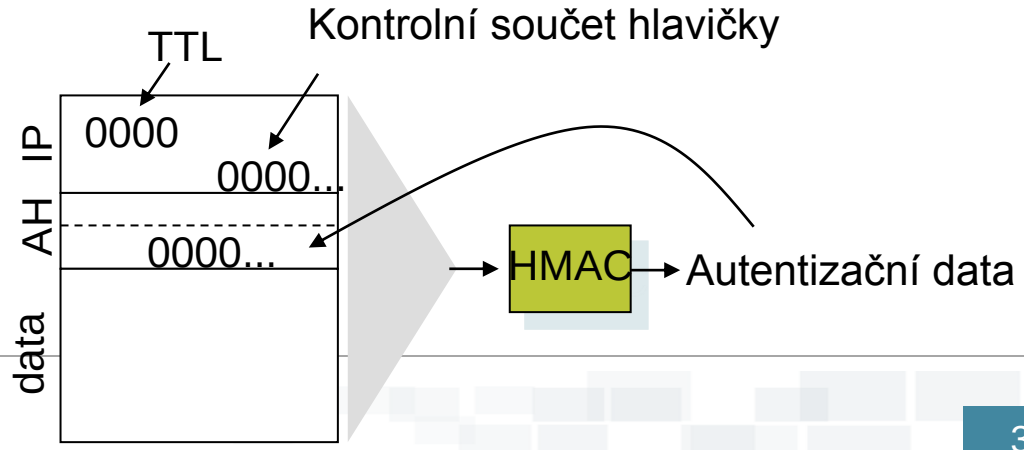
AH - detekce replay útoků

- **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



AH – zajištění integrity

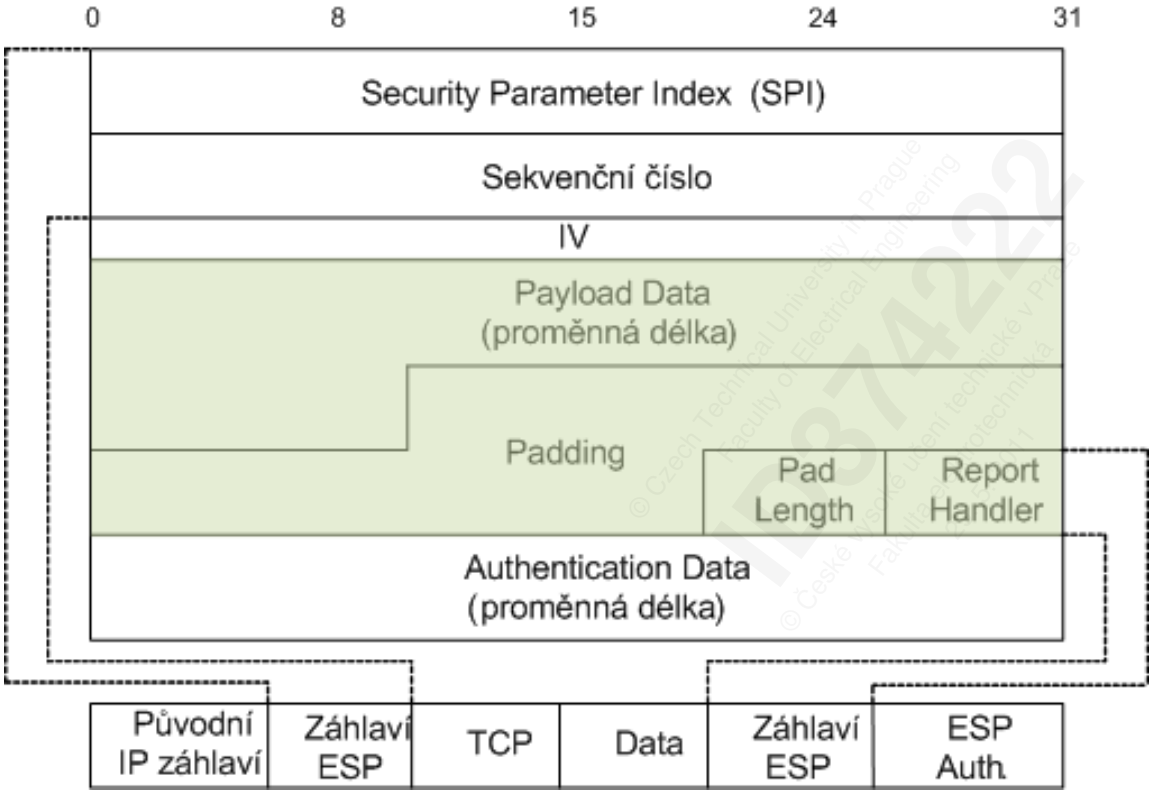
- Povinná implementace algoritmů:
  - HMAC-MD5-96
  - HMAC-SHA1-96
- HMAC is spočítán z
  - polí IP záhlaví, která se v průběhu přenosu nemění
  - ze polí záhlaví AH kromě pole „Authentication data“
  - všech užitečných dat
- pole, která se nejsou chráněna pomocí HMAC mají ve výpočtech hodnotu 0



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

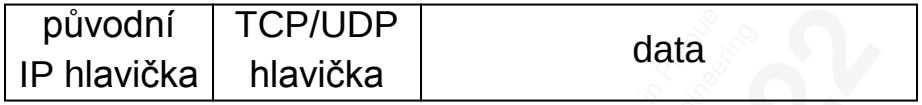
Payload Length – délka výplně

Next Header – číslo zapouzdřeného protokolu

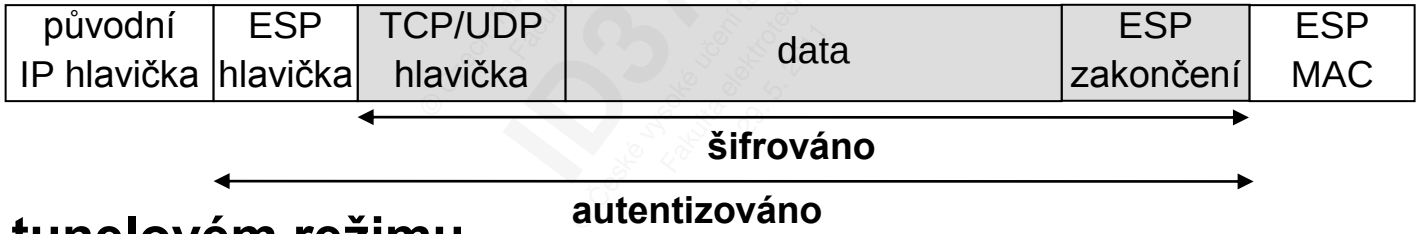
Authentication Data – kontrolní součet přenášených dat

ESP - zapouzdření

Původní paket IPv4

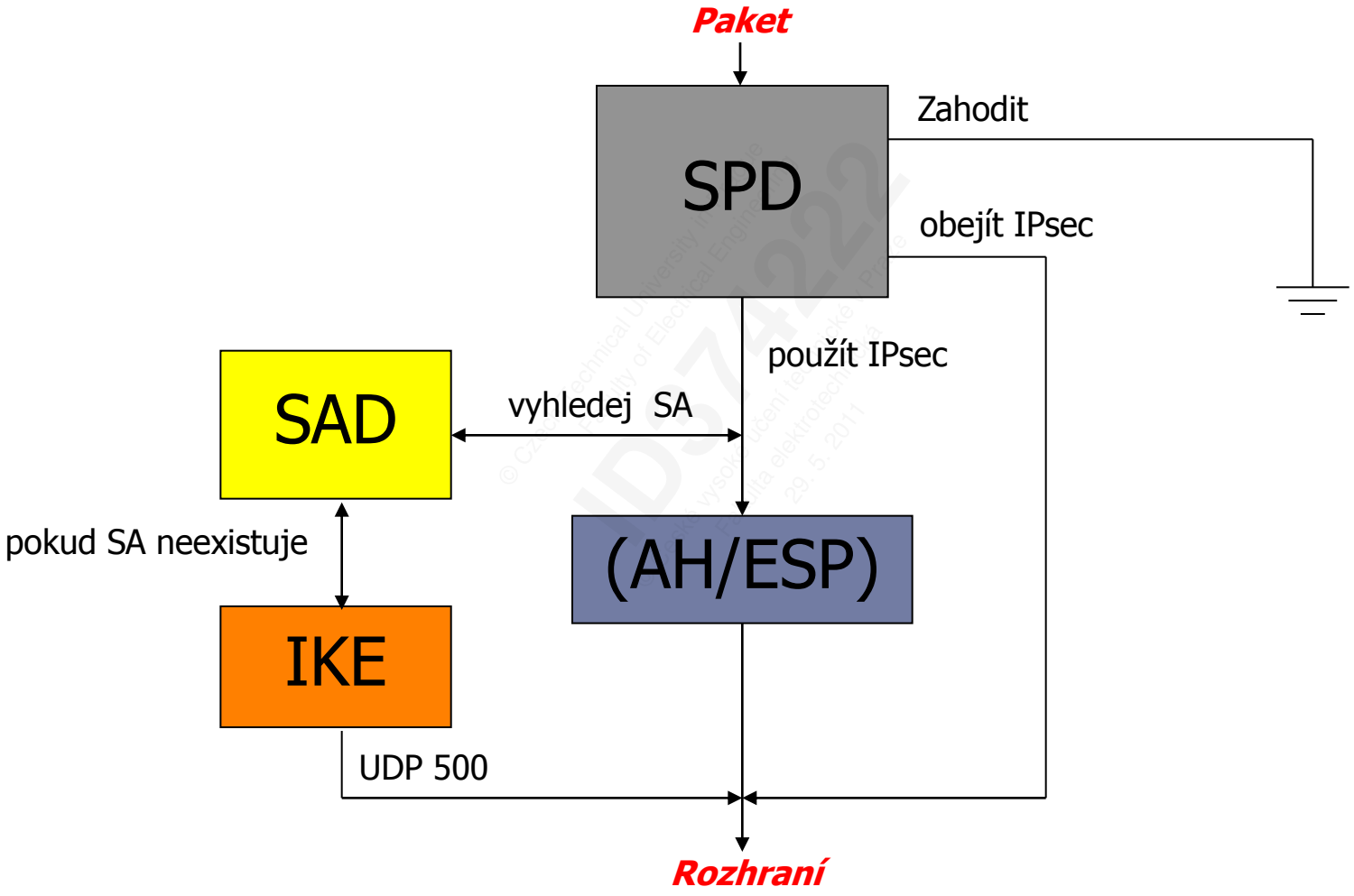


ESP v transportním režimu



ESP v tunelovém režimu

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 a cílové IP adresy a protokolu se určuje, zda se má :
  1) použít IPsec
  2) paket doručit bez použití IPsec
  3) paket zahodit

Pro každé rozhraní existují dvě SPD - (příchozí a odchozí směr)

! 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
- jaká šifra a jaký klíč 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.

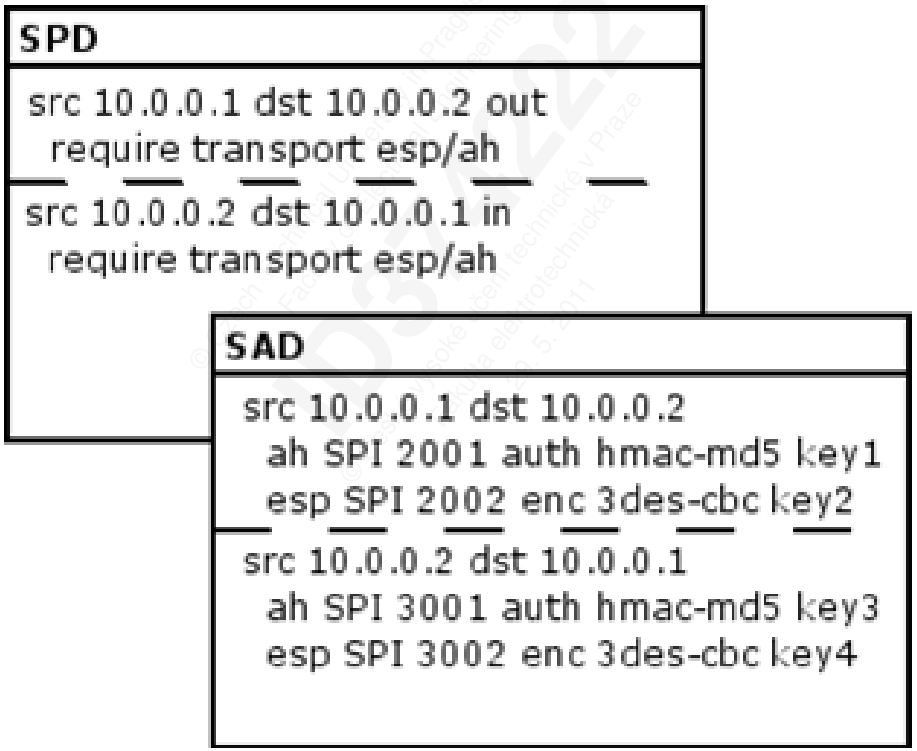
SPI – Security Parameter Index

- 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
- pro každý směr existuje jiná SA
- pro jedno IPsec spojení potřebuji minimálně dvě SA

Příklad SPD a SAD

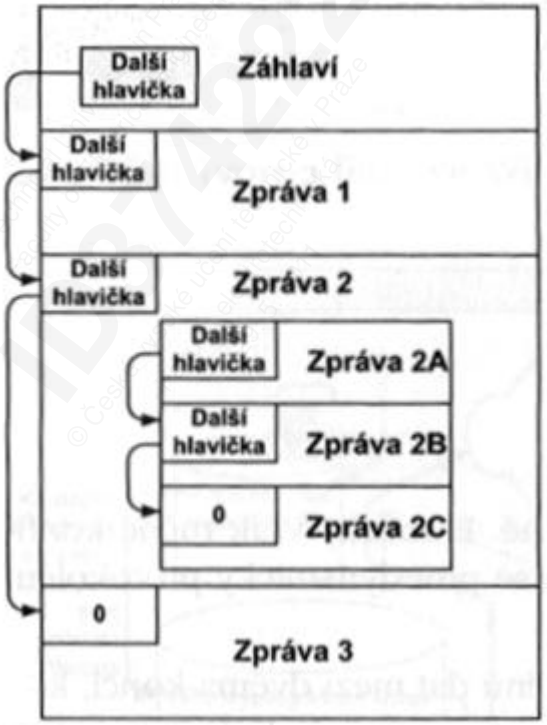


ISAKMP

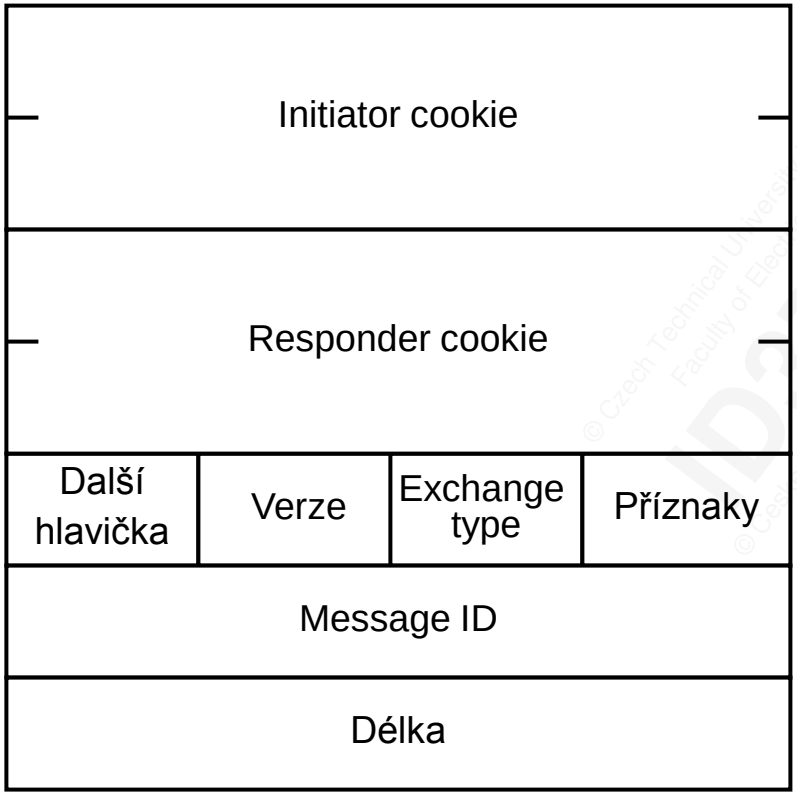
- Internet Security Association and Key Management Protocol
- RFC 2408
- používá UDP (port 500)
- nejde o C-S komunikaci, ale výzva/odpověď
- strana, která chce vytvořit nové SA iniciuje komunikaci protokolem ISAKMP
- ISAKMP definuje vlastní SA
- ISAMP slouží k:
  - autentizaci komunikujících stran
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

ISAKMP – struktura záhlaví

- zpráva ISAKMP může obsahovat vnořené zprávy



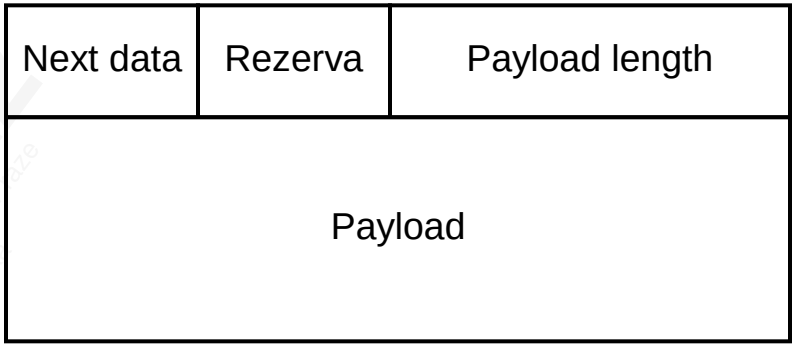
ISAKMP - záhlaví



- Initiator Cookie , Responder Cookie – čísla pro identifikaci komunikace
- Další hlavička - existuje 14 typů dalších vnořených hlaviček: NONE, SA, Proposal, Key Exchange, Nonce, Hash…
- Verze – 1.0
- Message ID – jedinečný identifikátor zprávy
- Délka – délka záhlaví a všech payloadů

ISAKMP - obecný formát zprávy

- Next data
  - typ dalších zapouzdřených dat (např.: zpráva transform, key exchange, certificate, …)
  - 0 pokud je žádná zpráva už není zapouzdřena
- Exchange type
  - počet vnořených payloadů a jejich typ
  - 5 základních typů
    - Base Exchange
    - Identity Protection Exchange
    - Authentication Only Exchange
    - Agressive Exchange
    - Informational Exchange



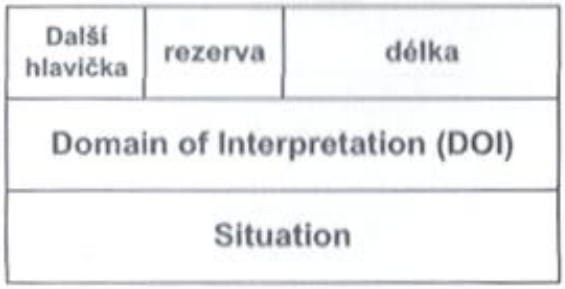
ISAKMP – typy datových částí

- **Security Association**
  - používá se na začátku ustanovení nové SA
  - nese v sobě různé atributy (zprávy)
- **Proposal Payload**
  - používá se během sestavení SA
  - určuje použitý protokol (AH nebo ESP) a počet použitých transformací (=algoritmů)
- **Transform Payload**
  - používá se během sestavení SA
  - označuje použité transformace (např. DES, 3DES) a její atributy
- **Key Exchange Payload**
  - obsahuje data pro výměnu klíčů (např. pomocí IKE nebo Oakley)
- **Certificate Payload**
  - obsahuje certifikát s veřejným klíčem (např. PGP, X.509,…)

ISAKMP – typy datových částí

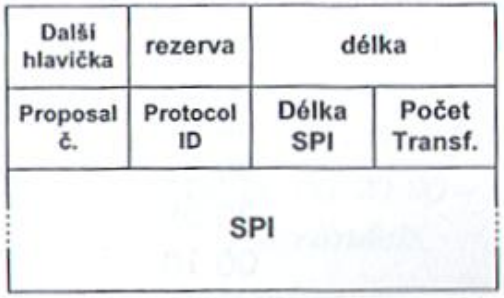
- Notification Payload
  - obsahuje chybová a stavová hlášení
- Delete Payload
  - označuje SA (jednu nebo více), které odesílatel smazal ze své databáze (a tím pádem už neplatí)
- Identification Payload
  - obsahuje data používaná k výměně identifikačních informací (např. IP adresu)
- Certificate Request Payload
- Hash Payload
- Signature Payload
- Nonce Payload
- Venndor ID Payload

ISAKMP - příklady zpráv

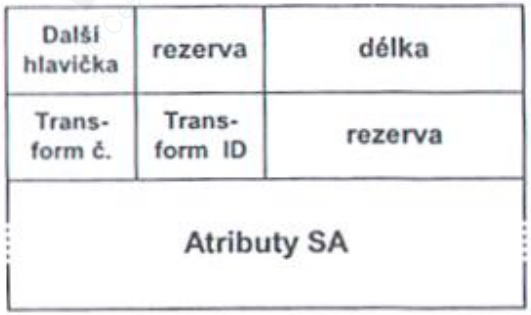


Zpráva Security Association

- vyjednání metod a algoritmů pro bezpečnou komunikaci



Zpráva Proposal – vnořena do SA, odesílatel nabízí podporovaná pravidla a algortimy



Zpráva Transform – vnořena do Proposal – popisuje konkrétní pravidla a kryptografické algoritmy pomocí tzv. atributů

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

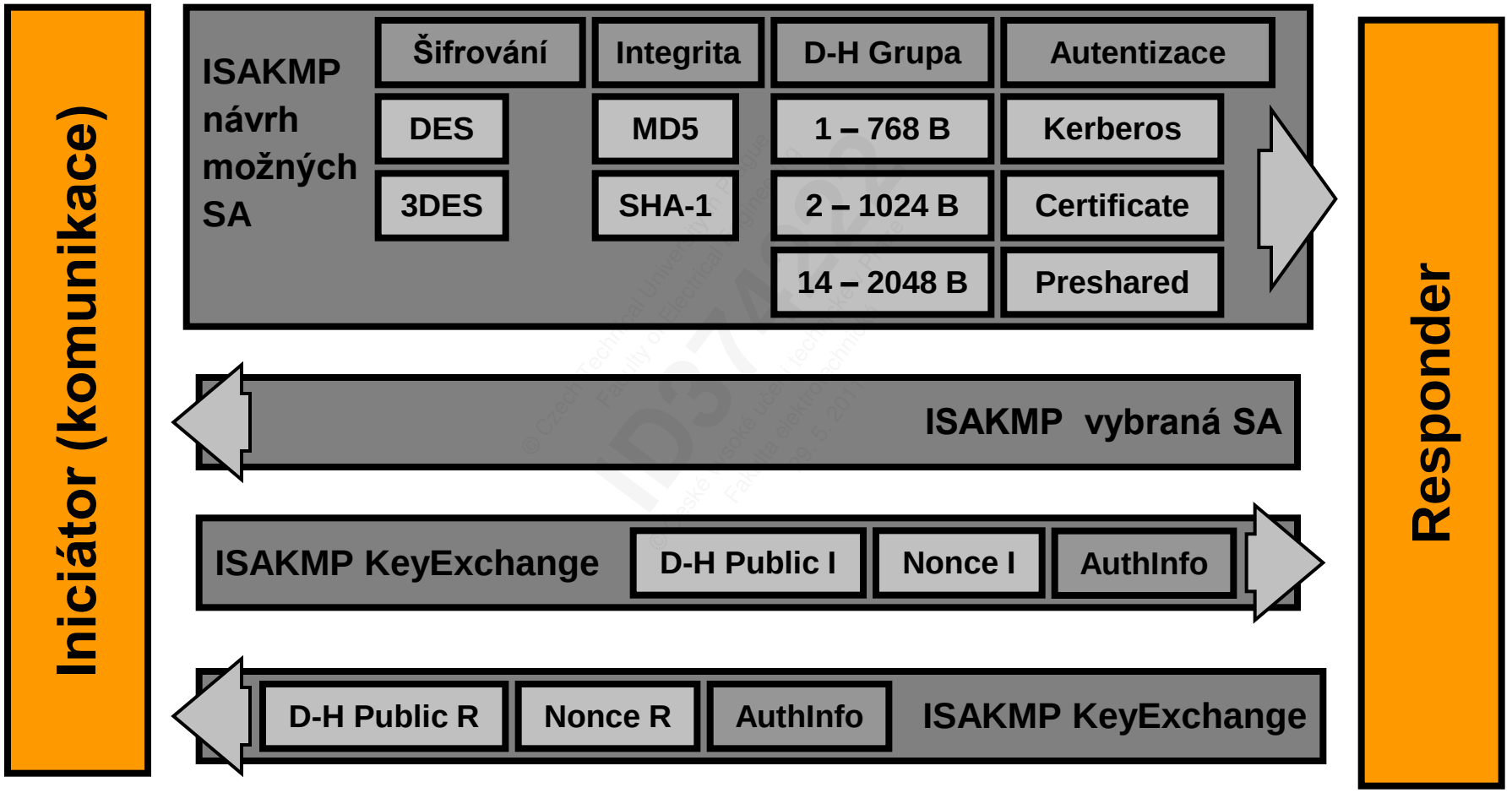
Hlavní režim IKE

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

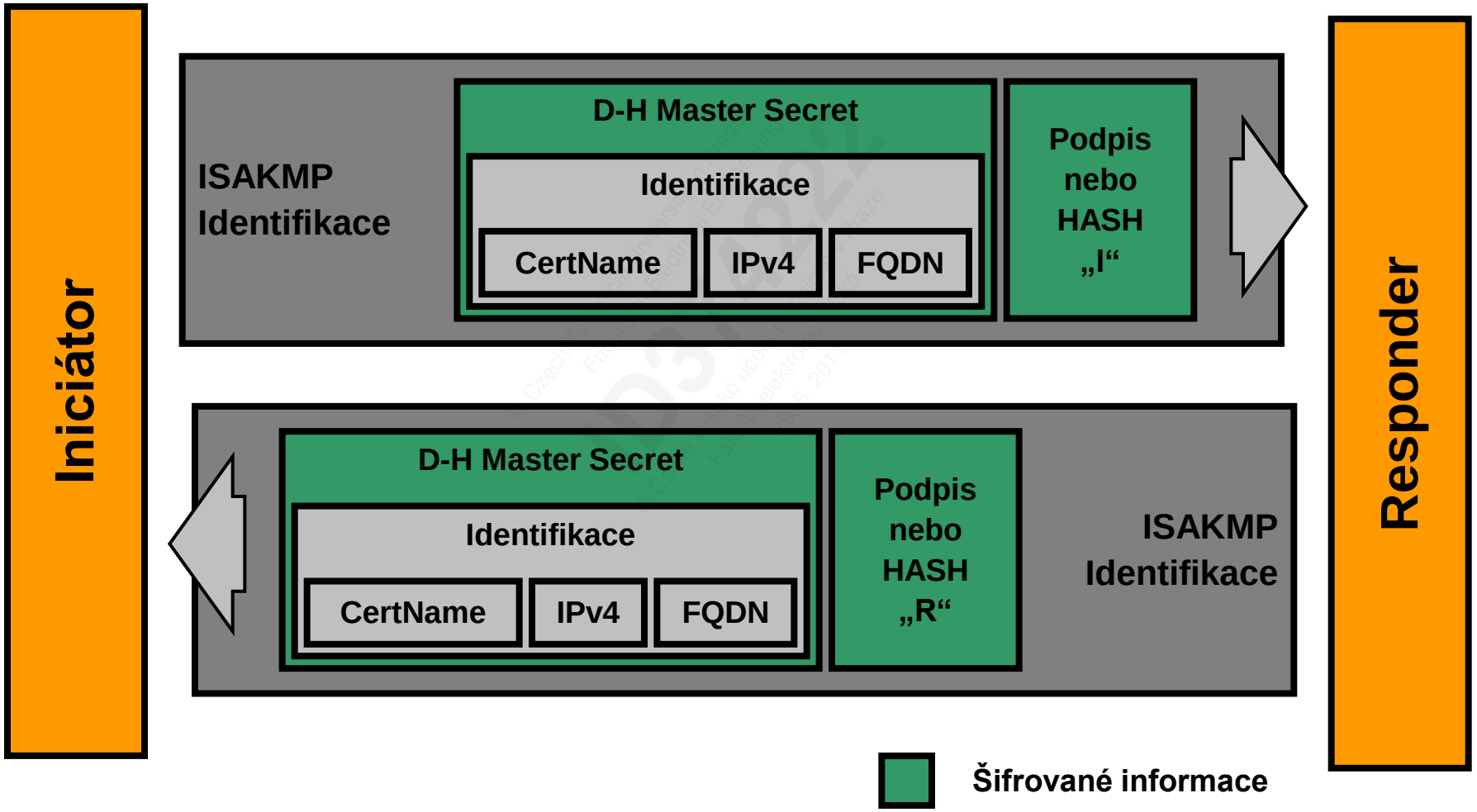
Agresivní režim IKE

- 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

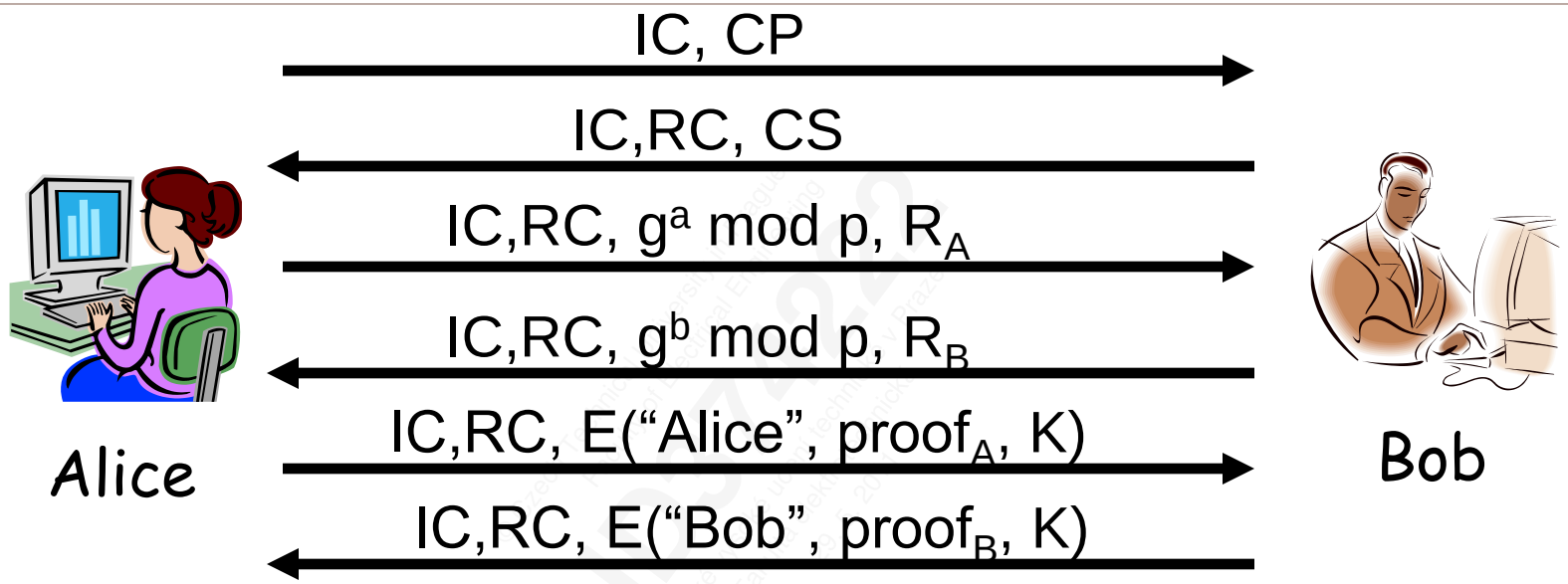
- Čtyři různé způsoby výměny klíče
  - asymetrické šifrování veřejným klíčem (původní verze)
  - asymetrické šifrování veřejným klíčem (zdokonalená verze)
  - digitální podpis
  - tajný klíč (symetrického algoritmu)
- pro každou z těchto variant existuje
  - Hlavní režim
  - Agresivní režim
- **Dohromady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

IKE – Fáze 1- varianty

- Blíže si ukážeme 6 z 8 variant fáze 1
  - digitální podpis (hlavní a agresivní režim)
  - symetrický klíč (hlavní a agresivní režim)
  - asymetrické šifrování veřejným klíčem (hlavní a agresivní režim)

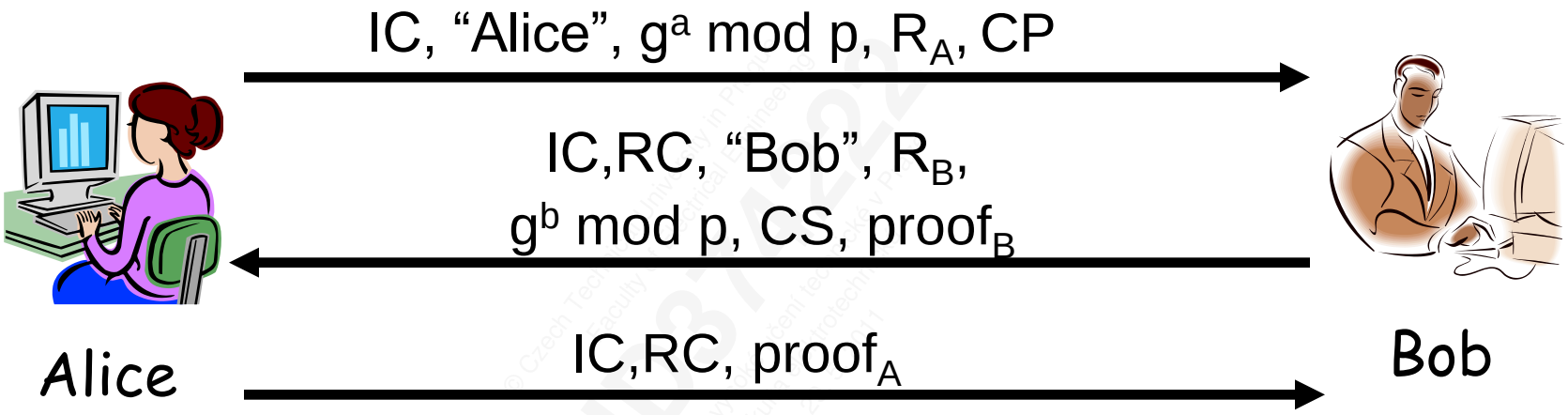
- Proč se vůbec používá varianta s digitálním podpisem ?
  - Iniciátor (komunikace) vždy zná svůj tajný klíč, ale na počátku komunikace nemusí znát veřejný klíč protistrany
  - s variantou digitálního podpisu ve fázi 1 ho ani nemusí zjišťovat
- Každá z variant Fáze 1 používá pro ustanovení klíče relace dočasnou DH výměnu. Přínosem tohoto přístupu je zajištění PFS (Perfect Forward Secrecy).

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")]$_{Alice}$

IKE Fáze 1: Digitální podpis (Agresivní režim)



Zásadní rozdíly oproti hlavnímu režimu

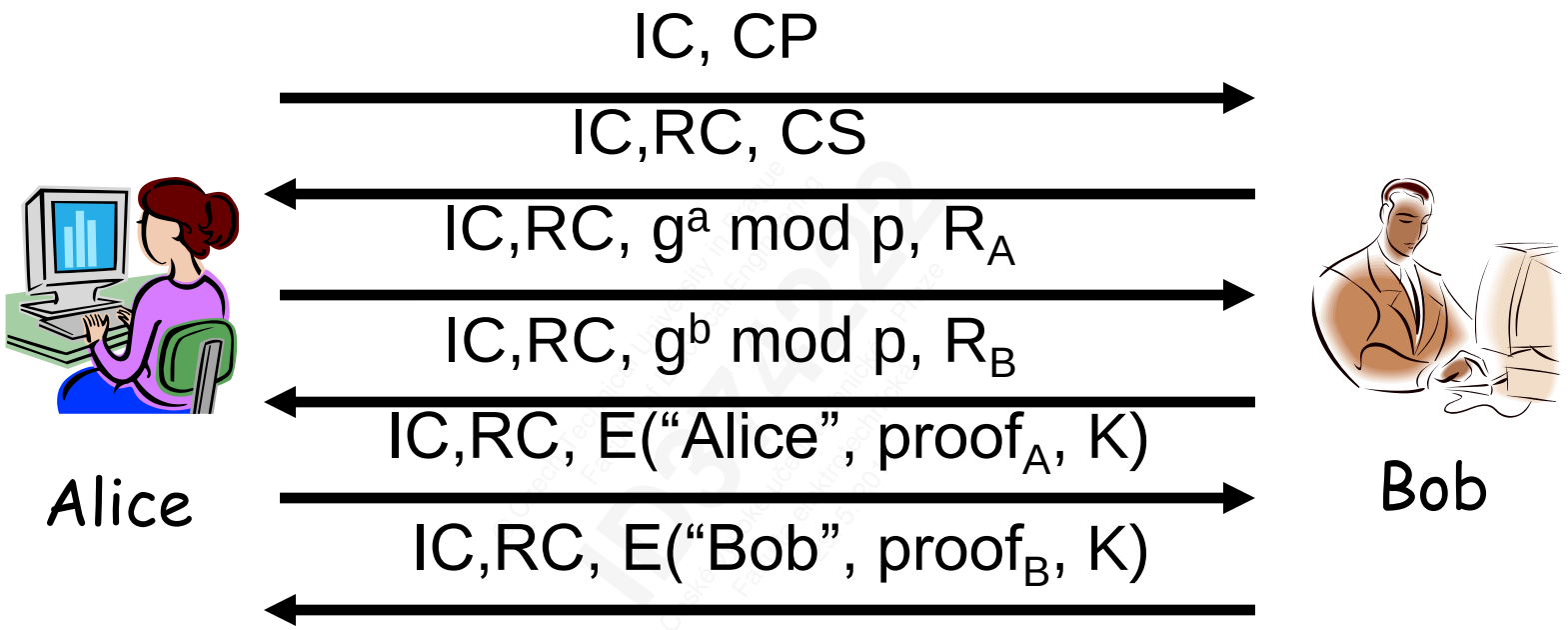
- nesnaží se chránit identitu
- nemůže vyjednat g nebo p (tzn. už musejí být nějak předjednaná)

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: symetrický klíč (hlavní režim)



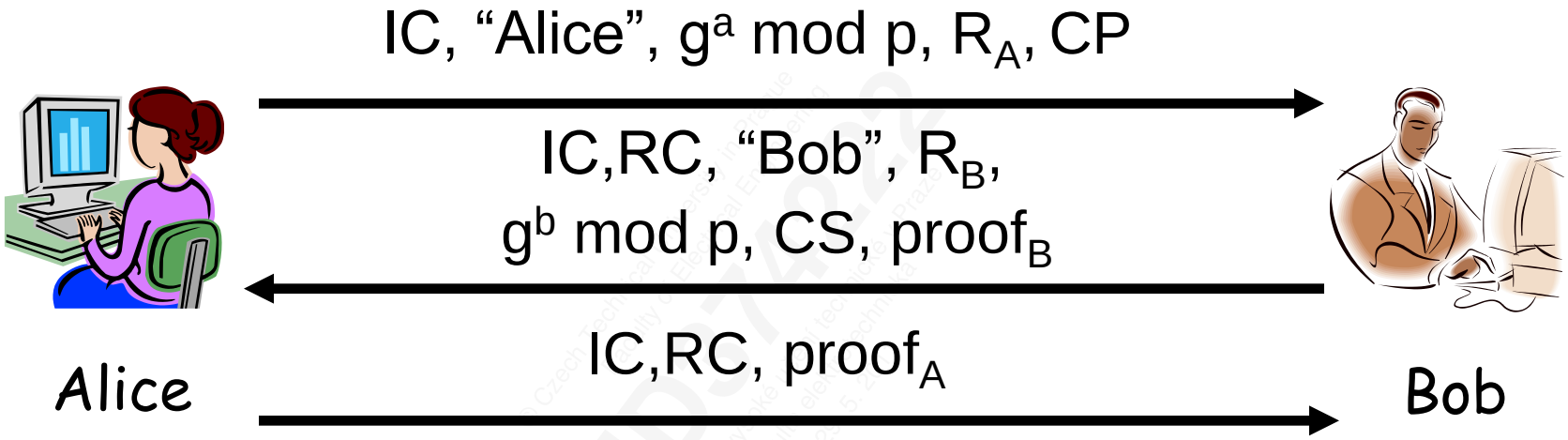
- K_{AB} = symetrický klíč získaný **nějak jinak*** dříve
- K = hash(IC,RC,g^{ab} mod p,R_A,R_B,K_{AB})
- SKEYID = hash(K, g^{ab} mod p)
- $proof_A$ = hash(SKEYID,g^a,g^b,IC,RC,CP,"Alice")

*PSK

Potíže se symetrickým klíčem (Hlavní režim)

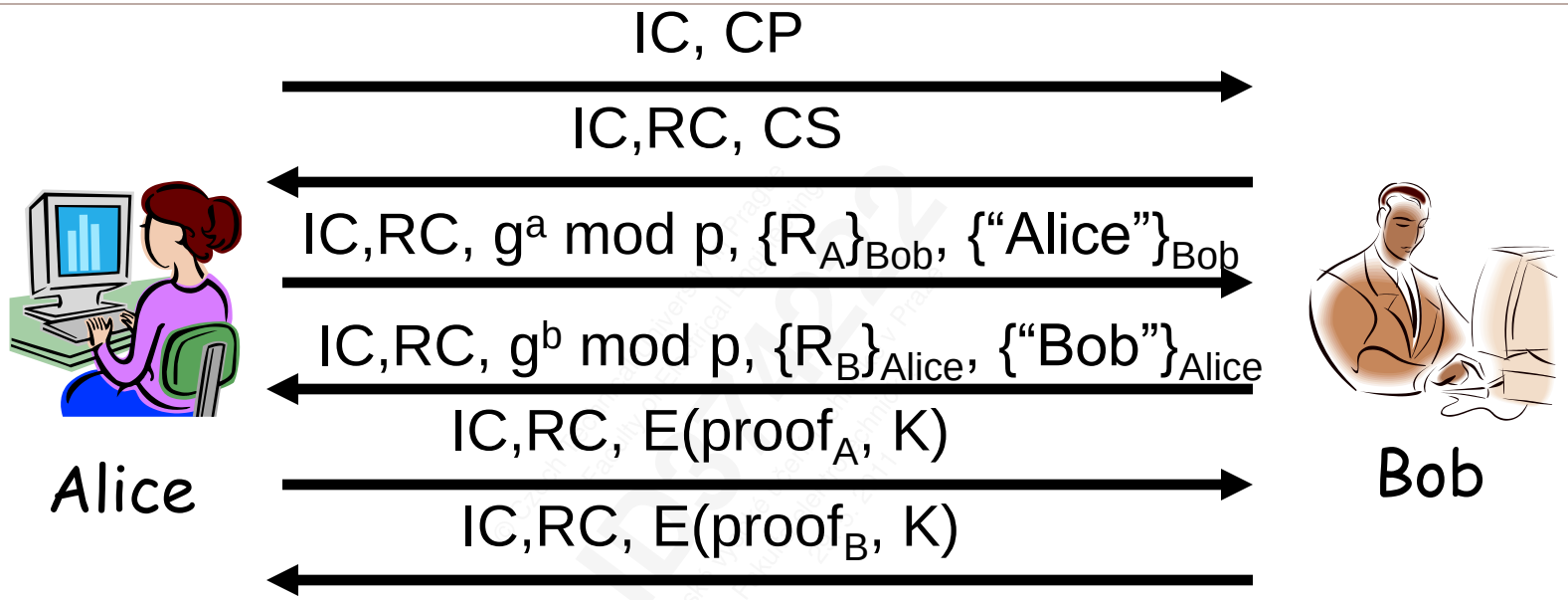
- absurdní situace alá Hlava-22
  - Alice ve zprávě 5 pošle své ID
  - ID Alice je zašifrováno pomocí klíče K
  - aby Bob zjistil K musí znát $K_{AB,}$, ale aby získal K_{AB} musí si být jistý, že mluví s Alicí!
- výsledek: **Alicino ID musí být její IP adresa,** protože Bob musí identifikovat Alici bez ohledu na protokol
- nepoužitelné pro uživatele typu “road warrior” (tam, kde se mění IP adresa)
- navíc v hlavním režimu se vyměňuje šest zpráv, kvůli utajení identity komunikujících stran, což ale nejde (protože IP adresa není tajná…)
- v tomto případě je lepší je použít agresivní režim

IKE Fáze 1: symetrický klíč (agresivní režim)



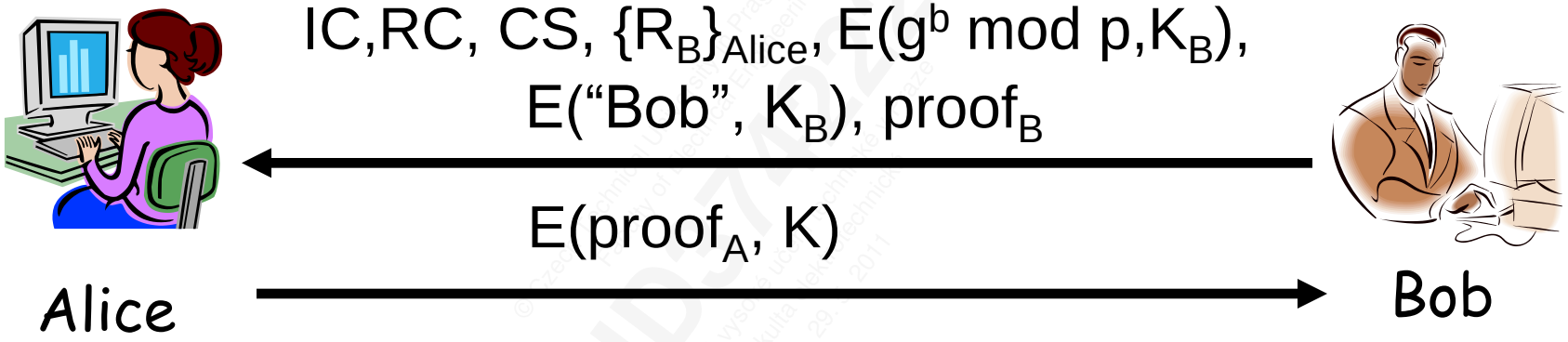
- hlavní rozdíl oproti hlavnímu režimu – neutajuje identitu komunikujících stran
- nemá problémy hlavního režimu (protože je ani neřeší)

IKE Fáze 1: šifrování veřejným klíčem (hl. režim)



- CP = navržené zabezpečení, CS = zvolené zabezpečení
- IC = "cookie" vyzyvatele, RC = "cookie" odpovídajícího (responder)
- $K = hash(IC,RC,g^{ab} \bmod p, R_A, R_B)$
- $SKEYID = hash(R_A, R_B, g^{ab} \bmod p)$
- $proof_A = hash(SKEYID, g^a, g^b, IC, RC, CP, \text{"Alice"})$
- $proof_B = hash(SKEYID, g^a, g^b, IC, RC, CP, \text{"Bob"})$

IKE Fáze 1: šifrování veřejným klíčem (ag. režim)



- $K_A = hash(R_A,IC)$
- $K_B = hash(R_B,RC)$
- $K = hash(g^{ab} \bmod p,R_A,R_B,IC,RC)$
- $SKEYID = hash(R_A, R_B, g^{ab} \bmod p)$
- $proof_A = hash(SKEYID,g^a,g^b,IC,RC,CP,\text{“Alice”})$
- $proof_B = hash(SKEYID,g^a,g^b,IC,RC,CP,\text{“Bob”})$

Zajímavá bezpečnostní riziko této metody

- tato situace může nastat jak v hlavním tak v agresivním režimu při šifrování veřejným klíčem
- nechť existuje útočník X, který
  - vygeneruje exponenty **a** a **b**
  - náhodná čísla **R_A** a **R_B**
- pak může útočník dopočítat platné klíče i „důkazy“ identity: **K_A**, **K_B**, **$g^{ab} \bmod p$**, **K**, **SKEYID**, **$proof_A$** a **$proof_B$**

Zajímavá bezpečnostní riziko této metody

IC, CP, $\{R_A\}_{Bob}$,
$E(g^a \bmod p, K_A)$, $E(\text{“Alice”}, K_A)$

IC,RC, CS, $\{R_B\}_{Alice}$, $E(g^b \bmod p, K_B)$,
$E(\text{“Bob”}, K_B)$, $proof_B$

$E(proof_A, K)$

X se tváří jako Alice

X se tváří jako Bob

- X může vytvořit relaci, která vypadá jako relace mezi Alicí a Bobem
- pro všechny pozorovatele je platná (včetně samotné Alice a Boba)

Věrohodné popření

- Útočník X může vytvořit komunikaci, která se okolním pozorovatelům jeví jako zabezpečená.

- V tomto režimu IPsecu se to nebere jako chyba, ale označuje jako kladná vlastnost:
  - **Věrohodné popření (plausible deniability):** Alice a Bob mohou popřít, že někdy v minulosti proběhla jakákoliv kombinace!
- V některých případech se ale jedná o bezpečnostní chybu:
  - Např. Alice si něco koupí od Boba, může to později popřít (pokud mu koupi předtím digitálně nepodepsala).

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

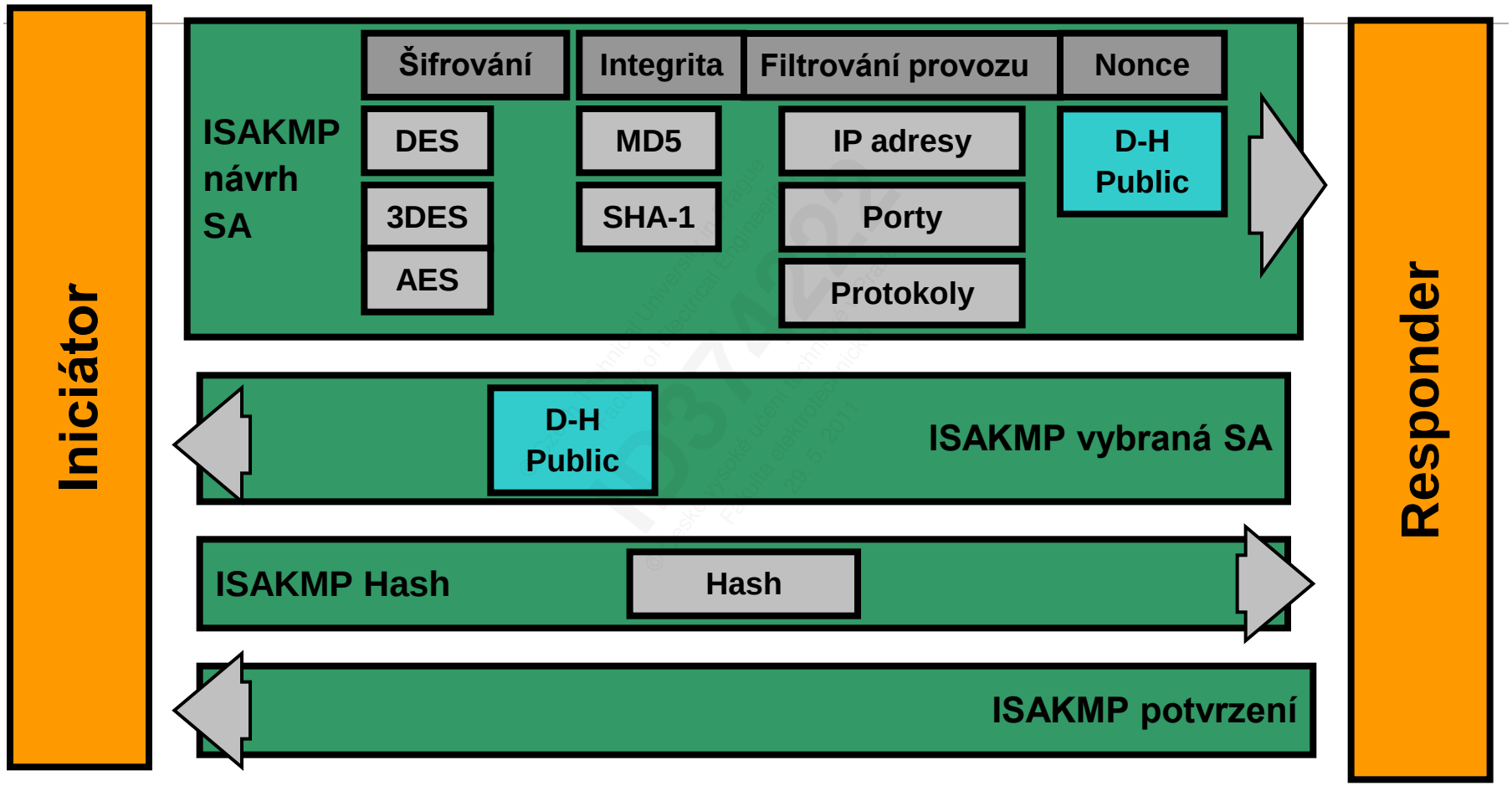
- dojednání Quick Mode SA a klíčového materiálu pro další komunikaci
- tato komunikace je od počátku chráněna pomocí algoritmů a klíčů získaných během fáze 1
- IKE Fáze 2
  - domluva na parametrech SA IPsec spojení
  - sestavení IPSec SA pro konkrétní spojení (např.: FTP, telnet, atd.)
  - periodická 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

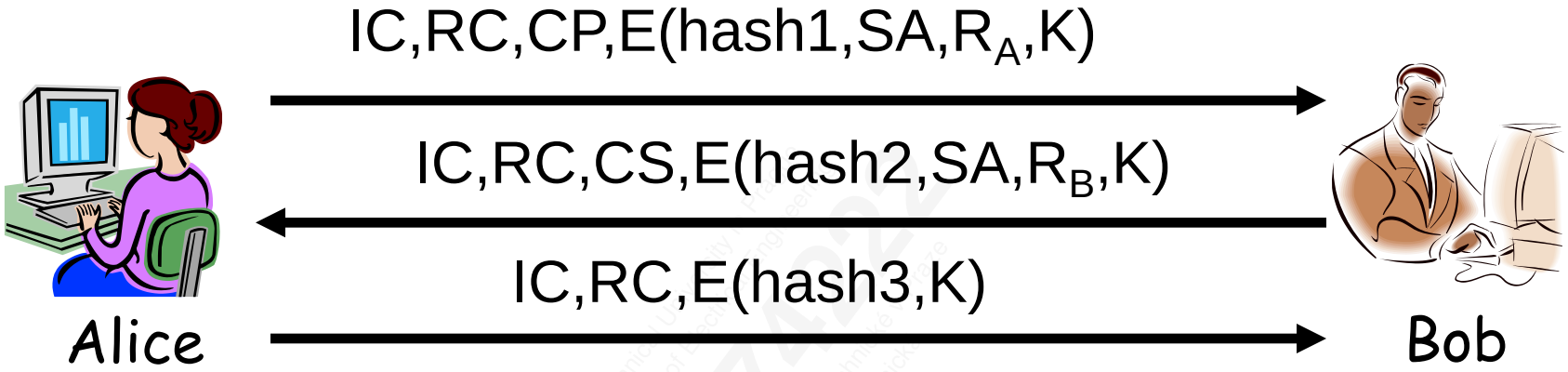
- Šifrování běžné komunikace
  - použije se Session Key odvozený z D-H Master Key získaného z Main Mode SA a z Nonce z dané Quick Mode SA

- 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)

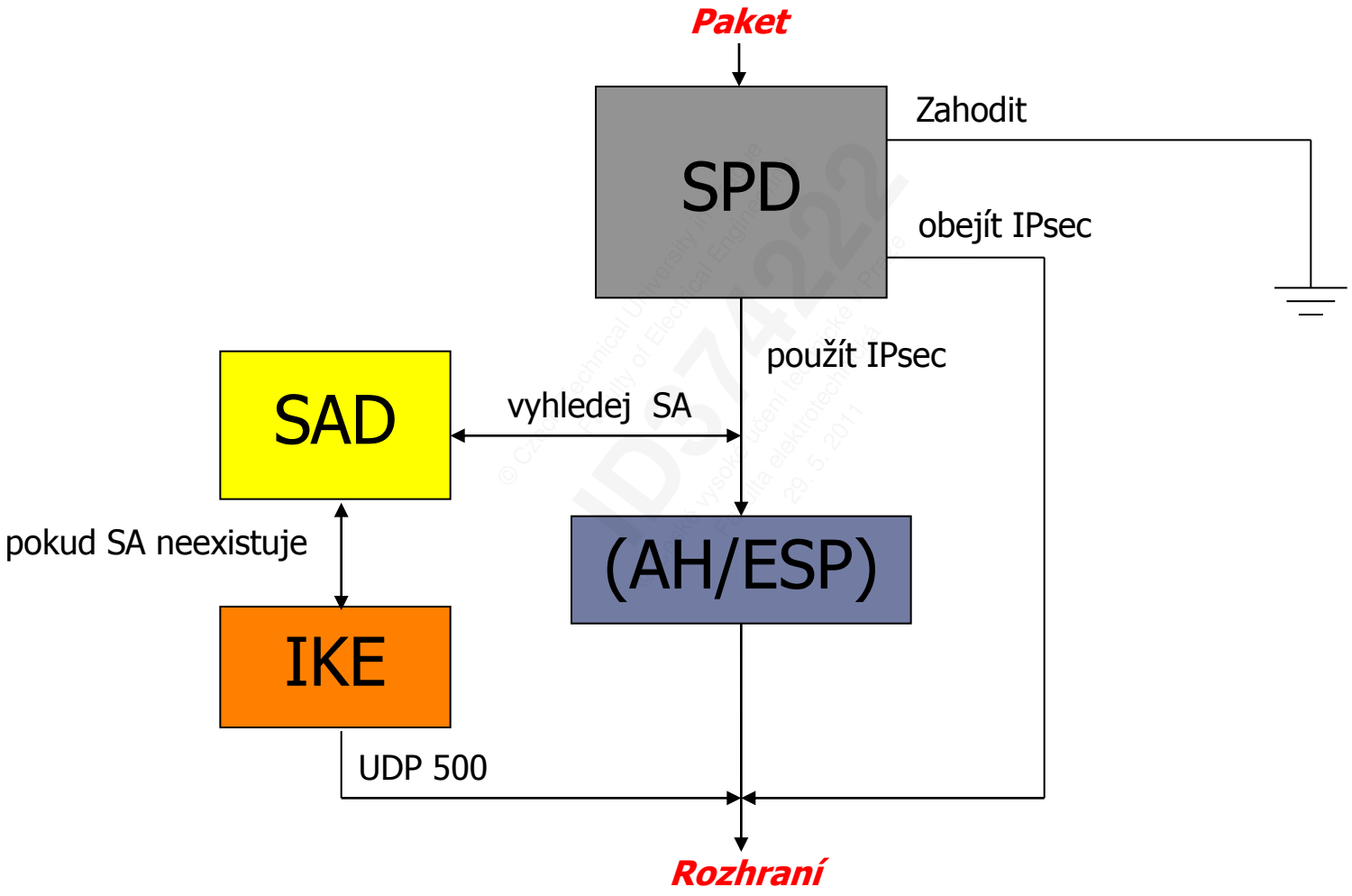
Diffie-Hellmann algoritmus pro výměnu klíčů

- **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 $p = 2^{1536} - 2^{1472} - 1 + 2^{64} * \{[2^{1406} \pi] + 741804\}$

AuthIP

- proprietární rozšíření IKE od Microsoftu
- podporováno od MS Vista SP1 a MS Server 2008
- přidává k IKE druhou autentizaci, což podle MS zvyšuje bezpečnost možnost nasazení IPsec VPN
- podporuje autentizaci uživatelů pomocí Kerberos v5 nebo SSL certifikátů
- není kompatibilní s IKEv2
- http://technet.microsoft.com/cs-cz/magazine/2007.10.cableguy%28en-us%29.aspx

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

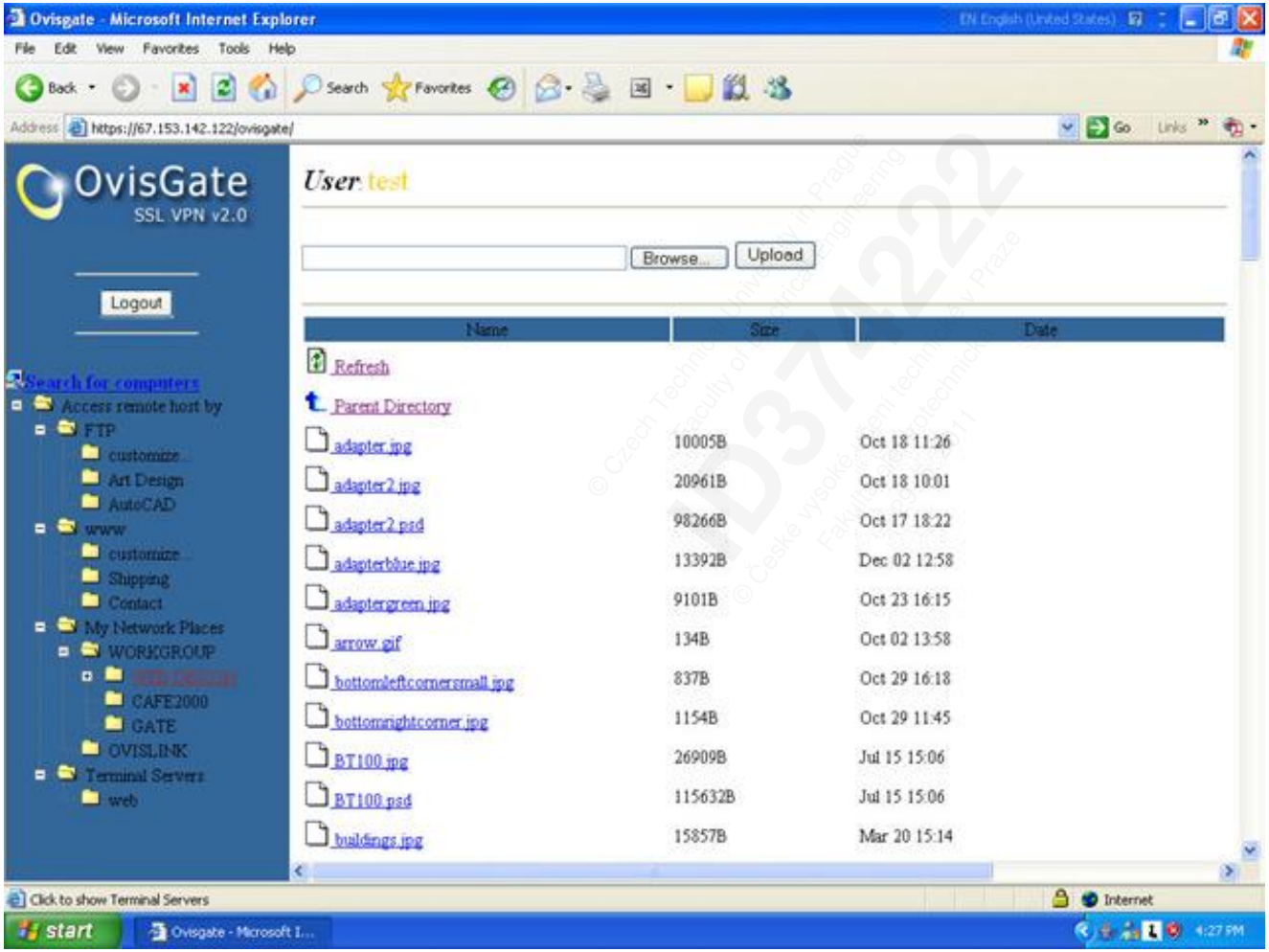
- vhodné pro VPN typu extranet
  - umožňuje jednoduše komunikaci typu B2B,B2C
- VPN brána se jeví jako běžný https server
  - dobře se vyrovnáná s NATem
  - vhodné pro mobilní uživatele
- VPN (SSL) brána ukončuje spojení a směrem do vnitřní sítě navazuje nové
- autentizace
  - heslo
  - token + heslo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

SSL VPN

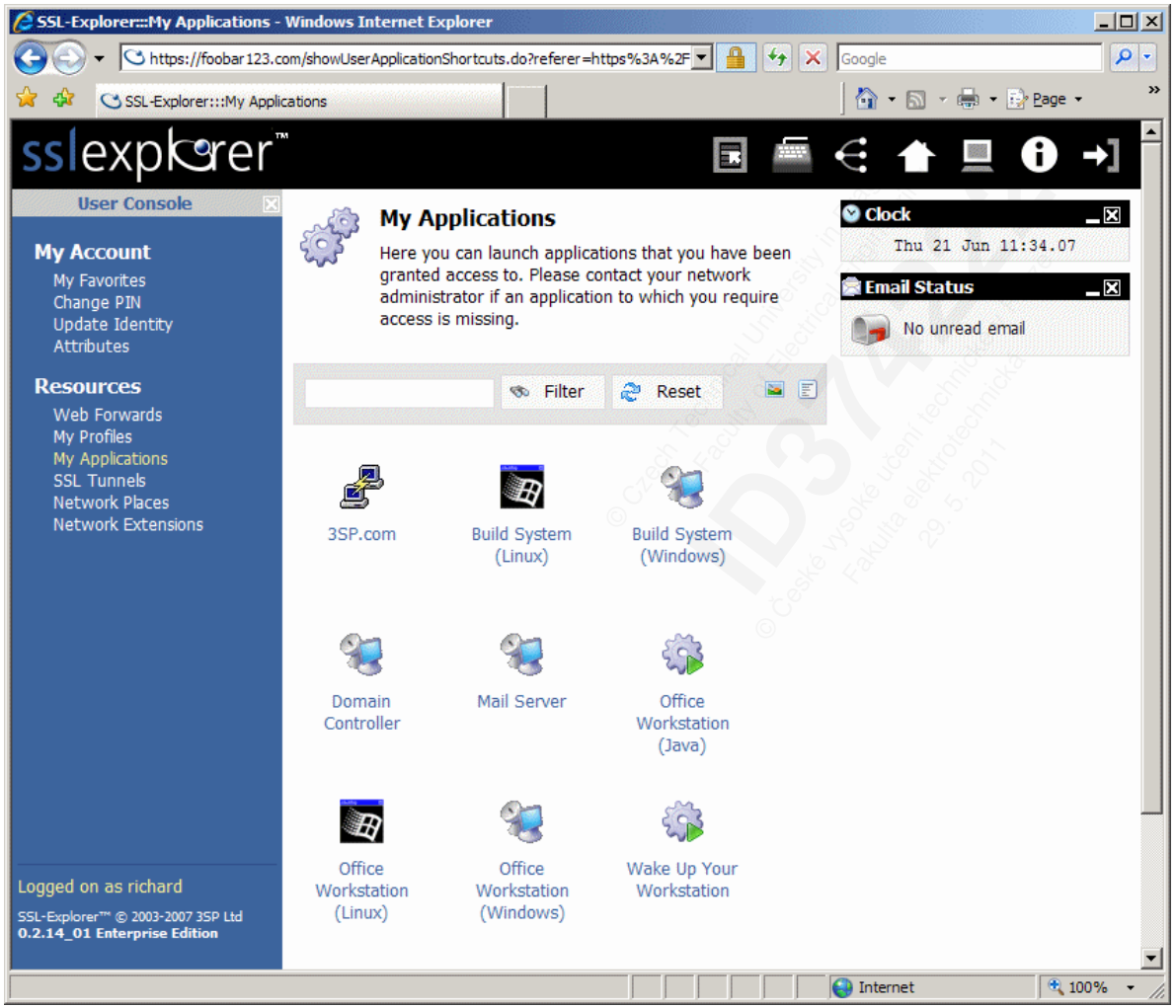
- několik variant:
  - Client-less
    - vhodné pro aplikace typu C-S (WWW, e-mail, Samba)
    - stačí prohlížeč s podporou HTTPS
  - Thin-client
    - aplikace typu Citrix, SAP
    - konektor – aplikace v Javě
    - lokální TCP proxy
  - Full-client
    - virtuální síťový adaptér

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