Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Siete, Internet a telekomunikácie
Virtuálne privátne siete VPN

Ladislav Hudec

2013

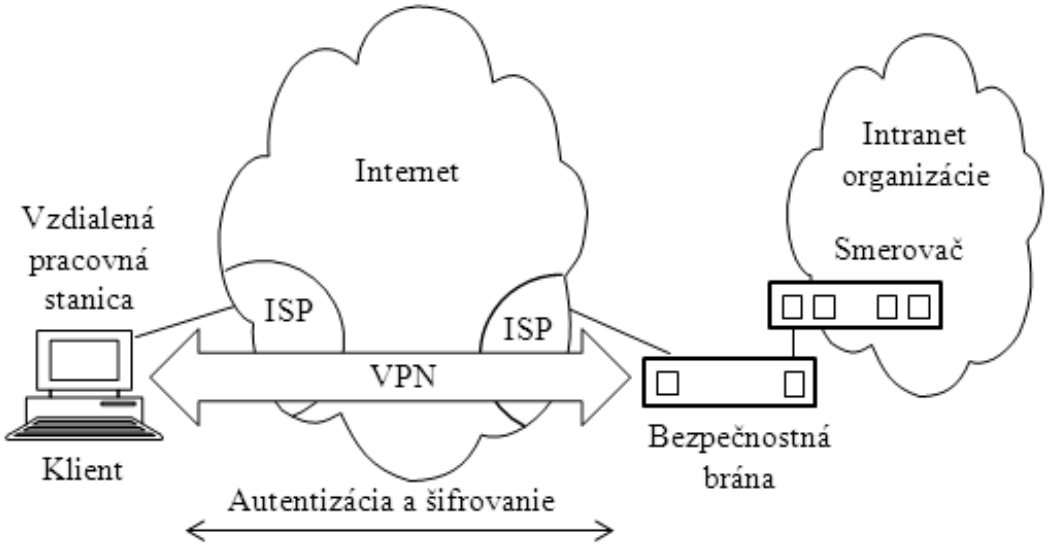
KPMG
cutting through complexity™

Úvod

- **Virtuálna privátna sieť** (Virtual Private Network) je rozšírenie privátnej siete organizácie (intranetu) cez verejné siete, ako je napríklad Internet alebo sieť poskytovateľa internetových služieb ISP (Internet Service Provider), vytvorením bezpečného privátneho spojenia.
- Charakteristika VPN:
  - Je **virtuálna sieť.** To znamená, že fyzická infraštruktúra sieti musí byť transparentná pre každé spojenie VPN. Vo väčšine prípadov to tiež znamená, že fyzická sieť nie je vlastnená používateľom VPN, ale je to verejná sieť spoločne používaná s mnohými ďalšími používateľmi. Na podporu potrebnej transparentnosti pre vyššie vrstvy sa používajú techniky **tunelovacích protokolov**.
  - Je **privátna sieť**, čo v tomto kontexte znamená zaistenie privátnosti premávky prenášanej cez VPN. VPN premávka sa často vykonáva cez verejné siete a preto musia byť realizované opatrenia na zaistenie potrebnej bezpečnosti, ktorá je požadovaná pre každý jednotlivý profil premávky cez spojenie VPN.
  - Je **sieť** a musí byť prakticky tak chápaná a musí byť s ňou narábané ako s rozšírením sieťovej infraštruktúry organizácie. To sa týka zariadení a aplikácií, ktoré ju vytvárajú, vrátane smerovania a adresovania.
- V praxi je možné rozpoznať tri charakteristické scenáre používania VPN a to je:
  - pripojenie vzdialeného používateľa do počítačovej sieti organizácie
  - pripojenie obchodného partnera do počítačovej sieti organizácie
  - prepojenie počítačovej sieti pobočky organizácie a počítačovej sieti v hlavnom sídle organizácie.

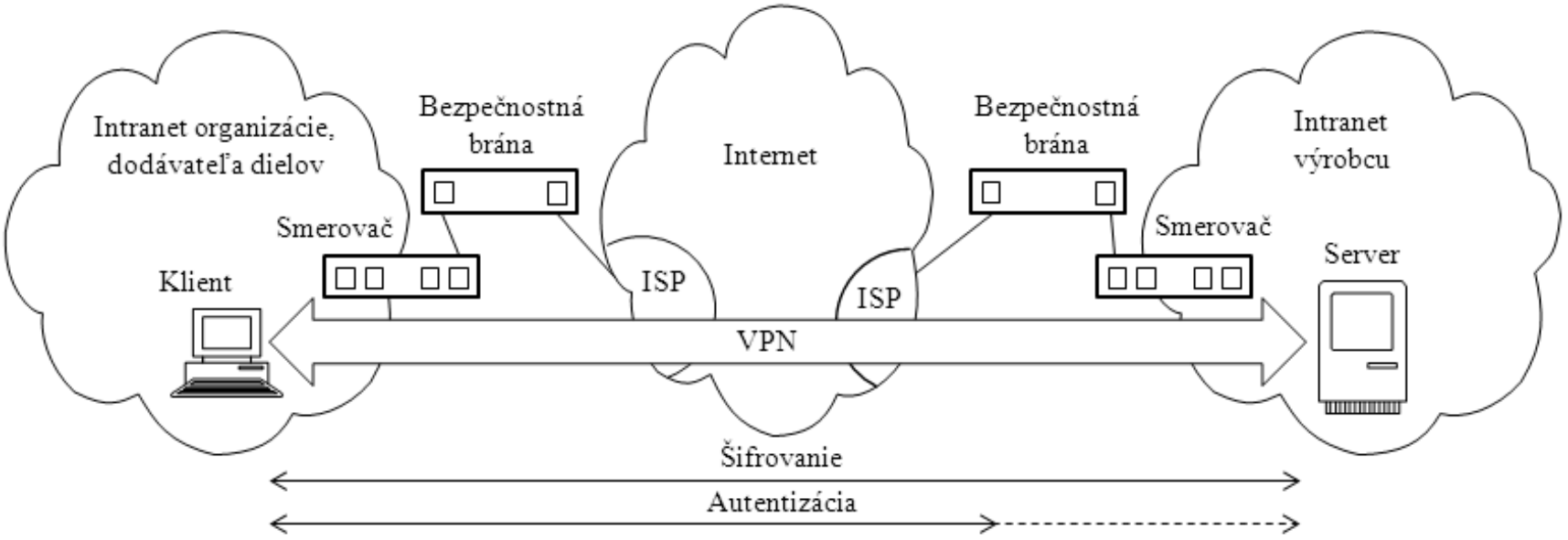
Pripojenie vzdialeného používateľa

- **Pripojenie vzdialeného používateľa do počítačovej sieti organizácie** či už z domu alebo na cestách je možné bezpečne a cenovo efektívne vykonať prostredníctvom ISP a Internetu.
  - Jeden zo spôsobov, ako realizovať tento scenár je využitie tunelovacích protokolov ako **L2TP, PPTP alebo L2F**.
  - Ďalším spôsobom je použitie protokolu **IPSec** (Internet Protocol Security), ak vzdialený klient takúto možnosť podporuje, a bezpečnostnej brány. Tento prípad je dokumentovaný na obrázku. V ideálnom prípade je možné použiť kombináciu oboch riešení, ktoré zaistí najlepšiu ochranu a cenovo najefektívnejší spôsob vzdialeného prístupu. Pomocou autentizácie protokolom IPSec medzi vzdialeným klientom a bezpečnostnou bránou je možné chrániť intranet pred nechcenými a možno škodlivými paketmi IP.
  - Ďalšou možnosťou pripojenia klienta, napríklad k serveru intenetbankingu, je vytvorenie bezpečného a autentizovaného tunela pomocou protokolu **SSL** (Secure Socket Layer).



Pripojenie obchodného partnera

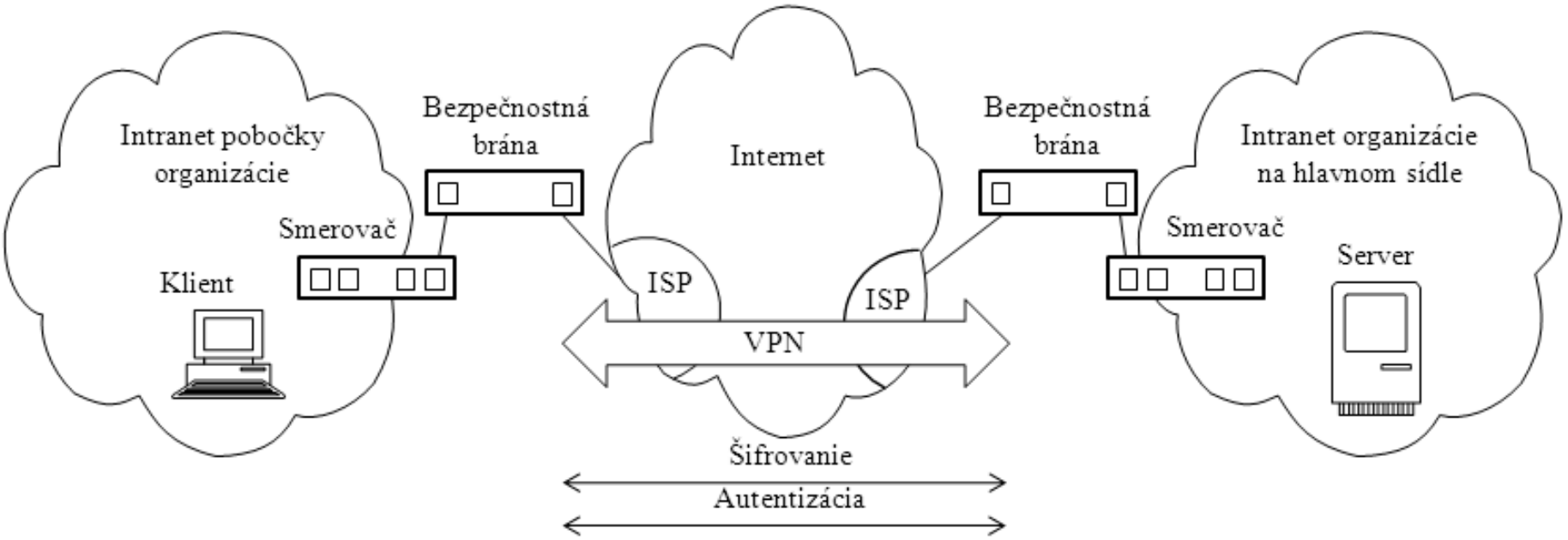
- **Pripojenie obchodného partnera do počítačovej sieti organizácie.** Niekto sa rozhodne na dosiahnutie takéhoto pripojenia implementovať protokolom Frame Relay a/alebo zakúpiť prenajaté okruhy (štátna pokladnica). Toto riešenie je často drahé a geografická pôsobnosť môže byť obmedzená.
  - Nech napríklad organizácia je hlavným dodávateľom dielov pre výrobcu. Pre hladký priebeh výroby je kritické, aby výrobca **mal na daný čas určité diely** a v určitých množstvách. Treba navrhnúť jednoduchý, rýchly a efektívny spôsob komunikácie medzi organizáciou a výrobcom.
  - Vzhľadom na dôvernosť a časovú citlivosť týchto informácií výrobcu nie je akceptovateľné zverejnenie týchto údajov na webovej stránke výrobcu alebo ich distribuovanie prostredníctvom mesačných správ. Na zaistenie bezpečnej komunikácie medzi organizáciou a výrobcom je **možné zriadiť VPN** podľa obrázku. VPN môže byť zriadená medzi klientskou pracovnou stanicou na intranete organizácie a priamo serverom (server obsahuje informácie o stave zásob dielcov a pláne potrieb) umiestneným na intranete výrobcu. Klienti sa môžu autentizovať na bezpečnostnej bráne alebo smerovači.



Prepojenie pobočky a hlavného sídla organizácie

- Scenár **prepojenia počítačovej sieti pobočky organizácie a počítačovej sieti v hlavnom sídle organizácie** zaisťuje bezpečné prepojenie dvoch dôveryhodných intranetov.
  - Bezpečnosť sa zameriava ako na **ochranu intranetu organizácie proti vonkajšiemu útočníkovi** tak na zabezpečenie údajov organizácie **pri prenose cez verejný Internet**. Prepojenie VPN (s využitím Internetu) medzi pobočkou a hlavným sídlom organizácie môže byť zriadené ľahko a môže splňovať bezpečnostné potreby organizácie. Na obrázku je dokumentované jedno riešenie prepojenia VPN medzi hlavným sídlom organizácie a jej pobočkami.
  - Organizácia si **zakúpi internetový prístup od ISP**. Na **hranici každého z intranetov** by mali byť umiestnené, z dôvodov ochrany komunikácie organizácie, **bezpečnostné brány alebo smerovače so vstavanou funkciou bezpečnostnej brány alebo v niektorých prípadoch server s funkciou IPSec**. V takomto scenári nemusia klienti a servery podporovať technológiu IPSec, pretože bezpečnostná brána (alebo smerovač) s podporou IPSec by poskytoval potrebnú autentizáciu paketov a šifrovanie údajov. Takto by všetky dôverné informácie boli skryté pred nedôveryhodnými používateľmi na Internete a navyše by bezpečnostná brána odmietala prístup všetkým potenciálnym útočníkom.
  - Zriadením pripojenia pobočiek prostredníctvom VPN bude hlavné sídlo spoločnosti schopné **komunikovať bezpečne a úsporne** so svojimi pobočkami bez ohľadu na to, kde sa pobočky **geograficky nachádzajú**. Prostredníctvom technológie VPN každá pobočka môže tiež rozšíriť rozsah svojho existujúceho intranetu, začlenením intranetov ostatných pobočiek, a tak vytvoriť rozšírenú počítačovú sieť celej organizácie. Organizácia môže potom ľahko rozšíriť takto novovytvorenú počítačovú sieť pripojením svojich obchodných partnerov, dodávateľov a vzdialených používateľov prostredníctvom napríklad technológie IPSec.

Prepojenie pobočky a hlavného sídla organizácie

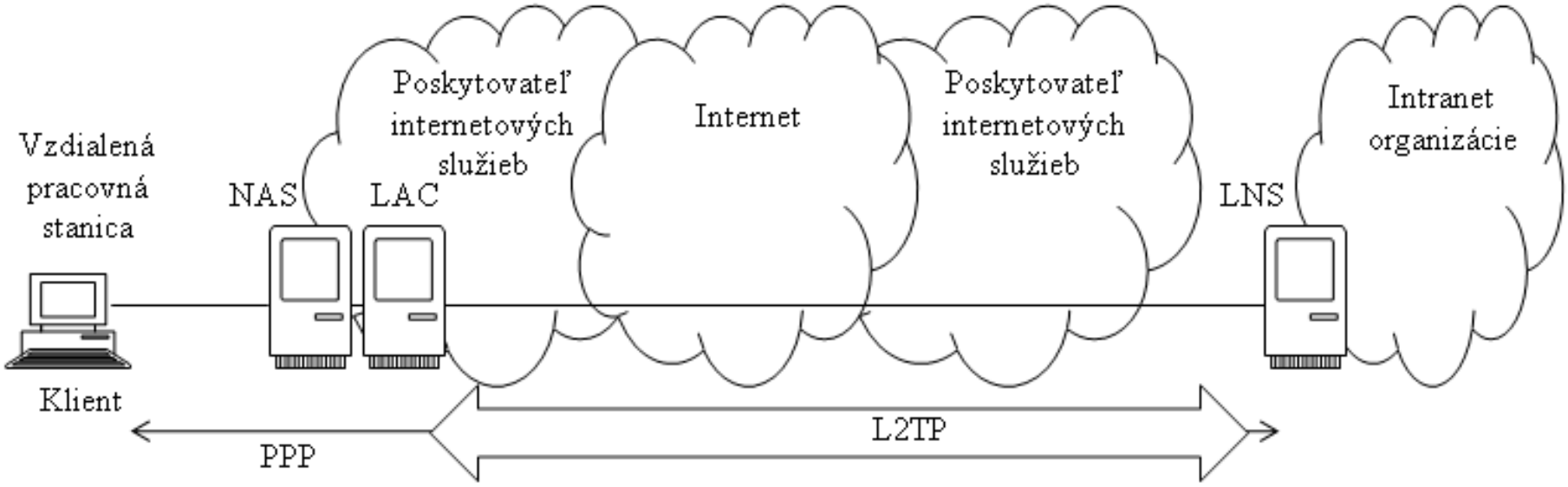


Protokol L2TP

- V tejto časti sa budeme zaoberať protokolmi, ktoré umožňujú spojenie **na druhej vrstve** (podľa sieťového referenčného modelu ISO/OSI). Štandardne ide o protokol PPP (Point to Point Protocol) **tunelovaný cez iné siete, bežne siete IP**. Zdá sa to ako zložitý prístup obsahujúci veľkú réžiu, ale tento prístup prináša niekoľko užitočných výhod pre budovanie VPN. V skutočnosti by bol počet internetových scenárov VPN alebo možností bez použitia tunelovacích techník pre druhú vrstvu dosť obmedzený.
- Protokol L2TP (Layer 2 Tunneling Protocol) je **jednou zo štandardných techník** na zabezpečenie vzdialeného pripojenia do sieti intranet organizácie. Protokol L2TP vznikol zlúčením dvoch rôznych protokolov: Point-to-Point Tunneling Protocol (PPTP) a Layer 2 Forwarding (L2F).
- L2TP zabezpečuje techniku na zriadenie tunela PPP.
  - Namiesto toho, aby protokol PPP bol ukončený najbližšom mieste POP ISP (Point Of Presence, prístupové miesto do siete ISP), protokol **L2TP zabezpečí ukončenie protokolu PPP na poslednej prístupovej bráne intranetu organizácie**.
  - Tunel môže **začať buď na vzdialenom hoste alebo na prístupovej bráne ISP**. L2TP zabezpečuje spoľahlivý spôsob pripojenia vzdialených používateľov do VPN, ktorý **podporuje premávku s viacerými protokolmi**. To znamená, že podporuje všetky protokoly sieťovej vrstvy podporované protokolom PPP. Okrem toho, pre spojenia cez Internet L2TP zabezpečuje podporu všetkých privátnych adresovacích schém na sieťovej vrstve.

Protokol L2TP

- Koncepcia protokolu L2TP predpokladá tieto entity:
  - **Prístupový koncetrátor LAC** (L2TP Access Concentrator) sa nachádza na POP ISP a zabezpečuje fyzické spojenie vzdialeného používateľa. Z koncentrátora LAC sú ďalej zriadené spojenia L2TP, ktoré LAC smeruje na jeden alebo viaceré servery LNS, na ktorých tunely L2TP končia.
  - **Sieťový server LNS** (L2TP Network Server). Na serveri LNS je ukončené spojenie L2TP. Na ukončenie spojení vzdialených používateľov na LNS môže byť použité iba jedno spojenie.
  - **Sieťový prístupový server NAS** (Network Access Server) je point-to-point prístupové zariadenie, ktoré na požiadanie zabezpečuje prístup vzdialených používateľov cez linky PSTN (Public Switched Telephone Network) alebo ISDN (Integrated Services Digital Network).
- Na obrázku je schematicky dokumentovaná základná koncepcia protokolu L2TP.



Protokol L2TP

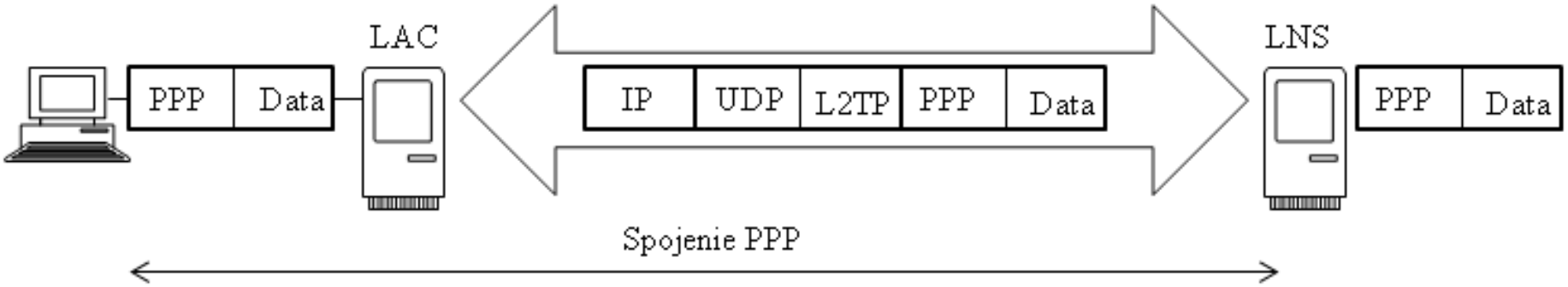
- **Zriadenie relácie a tunela L2TP** sú zabezpečené v týchto krokoch:
  1. Vzdialený používateľ iniciuje pripojenie protokolom PPP na NAS.
  2. Server NAS akceptuje pripojenie.
  3. Autentizácia koncového používateľa je vykonaná na NAS prostredníctvom autorizačného servera (štandardne server RADIUS).
  4. Koncetrátor LAC je spustený pokusom koncového používateľa otvoriť spojenie s LNS na vytvorenie tunela s LNS, ktorý je umiestnený na hranici intranetu organizácie. Každý pokus o pripojenie otvára spojenie a je riadené koncentrátorom LAC. Datagramy sú posielané cez tunel od koncentrátora LAC na server LNS. Zariadenie LAC a LNS evidujú stav pripojeného používateľa.
  5. Vzdialený používateľ je autentizovaný tiež autentizačným serverom na bráne LNS predtým, než je akceptované vytvorenie tunela.
  6. Server LNS akceptuje pripojenie a vytvorí tunel L2TP.
  7. Server NAS zaprotokoluje akceptovanie.
  8. Server LNS si so vzdialeným používateľom dohaduje protokolom PPP podmienky prenosu.
  9. Odteraz môžu byť tunelované údaje medzi vzdialeným používateľom a serverom LNS.
- Protokol L2TP podporuje dva typy tunelov a to **povinný a dobrovoľný tunel**.
  - **Povinný tunel L2TP** je zriadený od LAC cez ISP až k LNS na sieti organizácii.
    - Tento koncept si vyžaduje **spoluprácu poskytovateľa** internetových služieb, ktorý musí podporovať protokol L2TP a musí stanoviť na základe autentizačných informácií, či môže byť L2TP použitý pre konkrétnu reláciu a kam má byť tunel smerovaný.
    - Takýto prístup **nevyžaduje žiadne zmeny na strane vzdialeného klienta** a umožňuje centralizované prideľovanie adresy IP vzdialenému klientovi sieťou organizácie.
    - Takisto vzdialenému klientovi ISP **neposkytne prístup na Internet**, okrem prístupu cez bránu zo sieti organizácie. Takto organizovaný prístup vzdialeného používateľa na Internet umožňuje organizácii lepšie riadenie bezpečnosti.

Protokol L2TP

- **Zriadenie povinného tunela L2TP** sa vykoná podľa tejto postupnosti krokov:
  1. Vzdialený používateľ iniciuje spojenie PPP do ISP.
  2. ISP akceptuje spojenie a tým je zriadená linka PPP.
  3. ISP vykoná čiastočnú autentizáciu a zistí meno používateľa.
  4. ISP udržiava databázy mapujúce používateľov na služby a na koncové body tunelov LNS.
  5. LAC potom inicializuje tunel L2TP na LNS.
  6. Ak LNS akceptuje spojenie, potom LAC zapúzdri PPP do L2TP a odovzdá ho príslušnému tunelu.
  7. LNS akceptuje tieto rámce, odstráni obal protokolu L2TP a ďalej ich spracováva ako normálne prichádzajúce rámce PPP.
  8. LNS potom použije autentizáciu PPP na potvrdenie používateľa a priradí mu adresu IP.
- **Dobrovoľný tunel L2TP** je zriadený medzi vzdialeným klientom (ktorý efektívne funguje ako LAC) a serverom LNS v počítačoveh sieti organizácie.
  - Táto metóda je podobná PPTP a je v podstate pre ISP transparentná, ale vyžaduje podporu L2TP na strane klienta.
  - Tento prístup umožňuje vzdialenému klientovi prístup na Internet, takisto ako jedno alebo viacero pripojení VPN súčasne.
  - Klient však nakoniec skončí pridelením viacerých adries IP, jedna adresa IP od ISP pre pôvodné PPP spojenie a jedna adresa IP pridelená sieťou organizácie pre tunel VPN L2TP. Tým sa otvorí klient a rovnako aj sieť organizácie na potenciálne útoky zvonku. Táto skutočnosť vyžaduje potrebu klientskych aplikácií na určenie správnych cieľov pre ich údajové premávky.
- **Zriadenie dobrovoľného tunela L2TP** sa vykoná podľa tejto postupnosti krokov:
  1. Vzdialený používateľ má už zriadené spojenie do ISP.
  2. Klient L2TP (LAC) iniciuje tunel L2TP do LNS.
  3. Ak LNS akceptuje spojenie, potom LAC zapúzdri PPP do L2TP a pošle ho tunelu.
  4. Server LNS akceptuje tieto rámce, odstráni obal protokolu L2TP a spracuje ich ako normálne prichádzajúce rámce.
  5. LNS potom použije autentizáciu PPP na potvrdenie používateľa a priradí mu adresu IP.

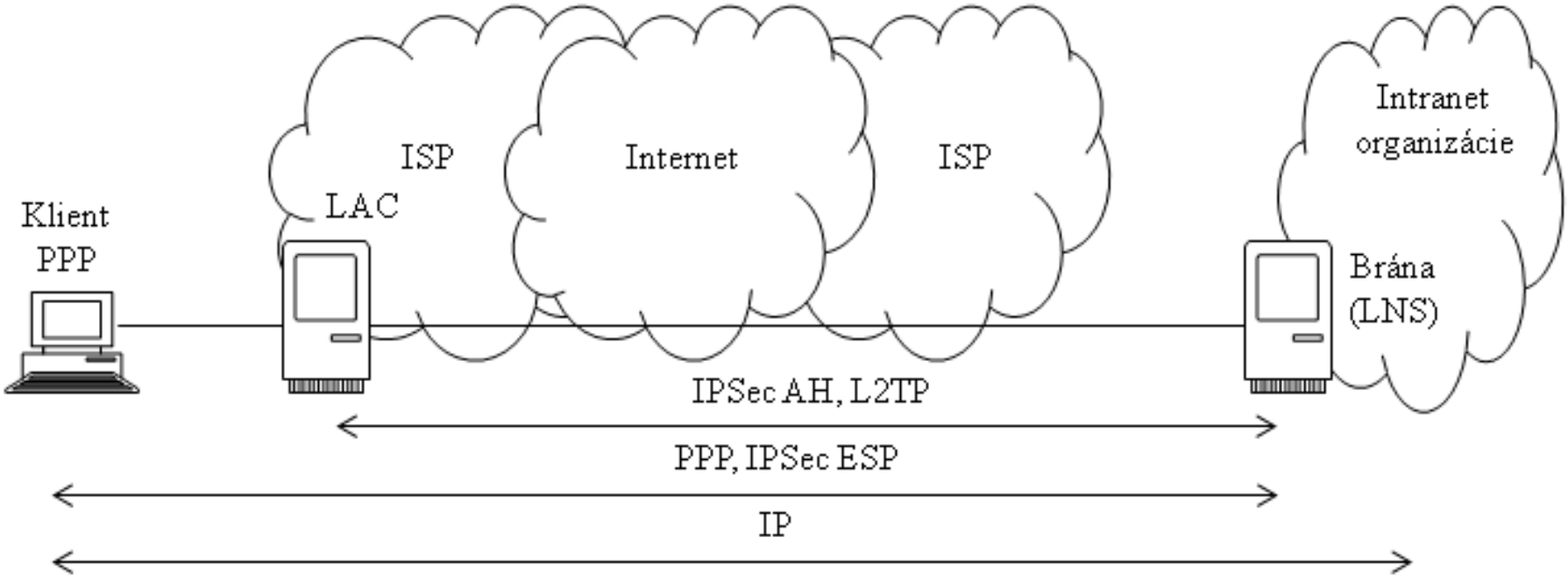
Protokol L2TP

- **Vytvorenie tunela** prostredníctvom protokolu L2TP **ešte neznamená**, že prenášané údaje sú **pred útočníkom skryté a pôvod údajov je autentický**.
  - Tunel L2TP je vytvorený **zapúzdrením rámca L2TP do datagramu UDP a následným zapúzdrením do paketu IP**.
  - Zdrojová a cieľová adresa paketu IP spoločne určujú **koncové body tunela**.
  - Táto koncepcia je dokumentovaná na obrázku a predpokladá, že LAC a LNS sú vybavené príslušným softvérom na vytvorenie a ukončenie L2TP tunela, prípadne LNS je vybavené softvérom smerovača.
  - Pretože vonkajšie zapúzdrenie je protokolom IP, môže byť jednoducho namiesto protokolu IP použitá jeho **bezpečnostná verzia IPSec**. Takýmto spôsobom možno bezpečnostne zaistiť údaje prenášané v tuneli L2TP, t.j. môžu byť priamočiaro použité protokoly súvisiace s IPSec a to AH (Authentication Header), ESP (Encapsulating Security) a IKE (Internet Key Exchange).



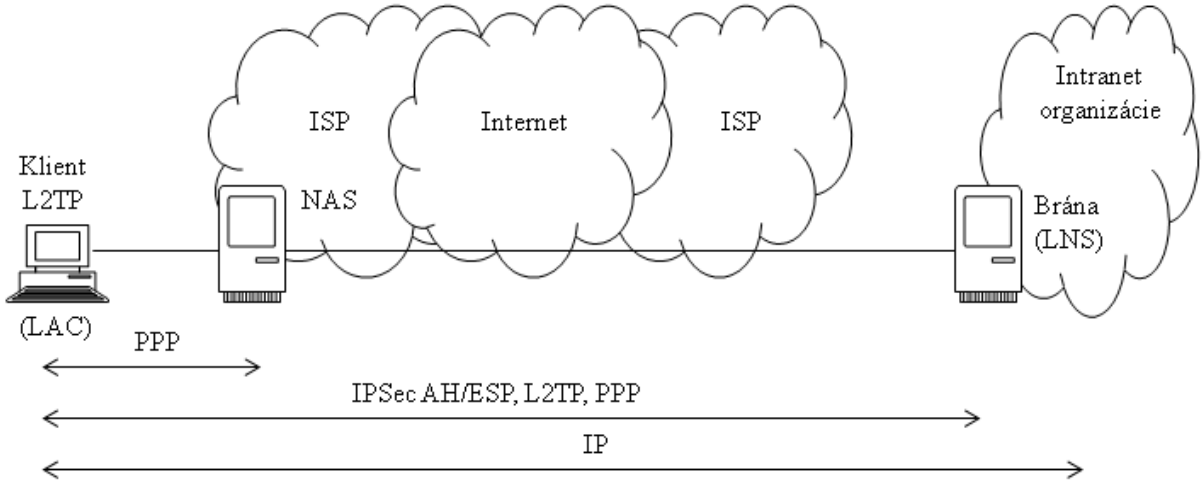
Protokol L2TP

- Použitie technológie **IPsec** v spojení s protokolom L2TP môže poskytnúť **bezpečné spojenie end-to-end** medzi vzdialenými používateľmi a intranetom organizácie.
  - IPSec môže do protokolu L2TP pridať mechanizmus **autentizácie** jednotlivých paketov a **kontroly integrity** namiesto jednoduchej autentizácie koncového bodu tunela, ktorá nie je zabezpečená proti útokom z uzlov nachádzajúcich sa v sieti pozdĺž cesty spojenia tunela.
  - Navyše IPSec pridáva do protokolu L2TP šifrovacie funkcie na **zaistenie dôvernosti údajov** prenášaných v náklade L2TP a na bezpečený spôsob pre automatizované generovanie a výmenu kryptografických kľúčov v rámci spojenia tunela.
- Na obrázku nižšie je **protokol IPSec použitý na zabezpečenie povinného tunela L2TP na bránu VPN**.

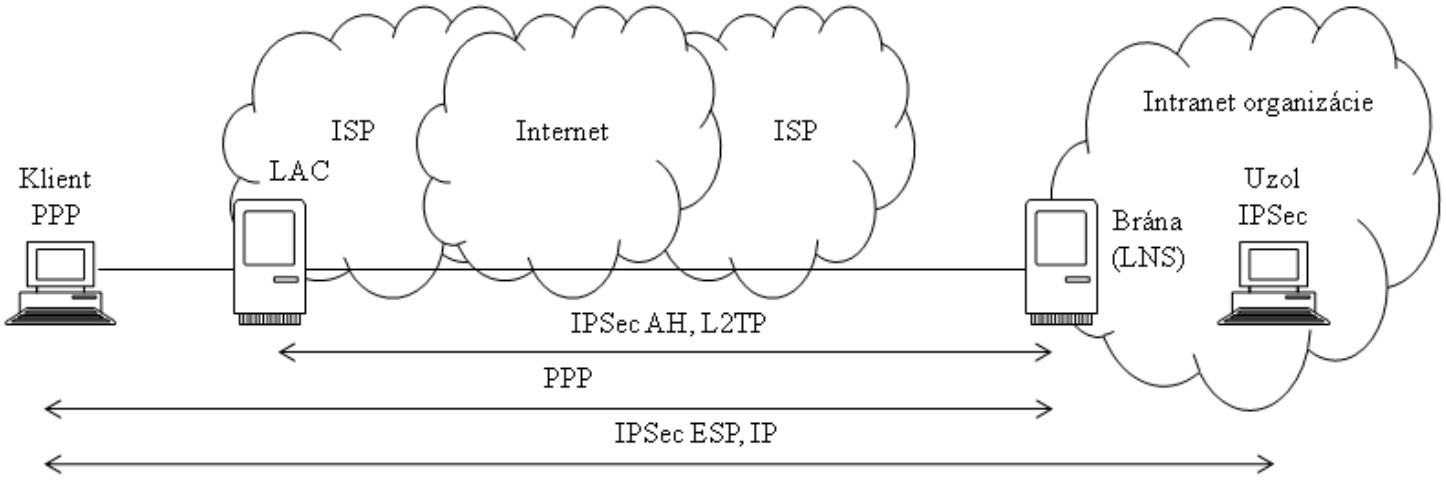


Protokol L2TP

- **Protokol IPSec je použitý na zabezpečenie voliteľného tunela L2TP na bránu VPN**

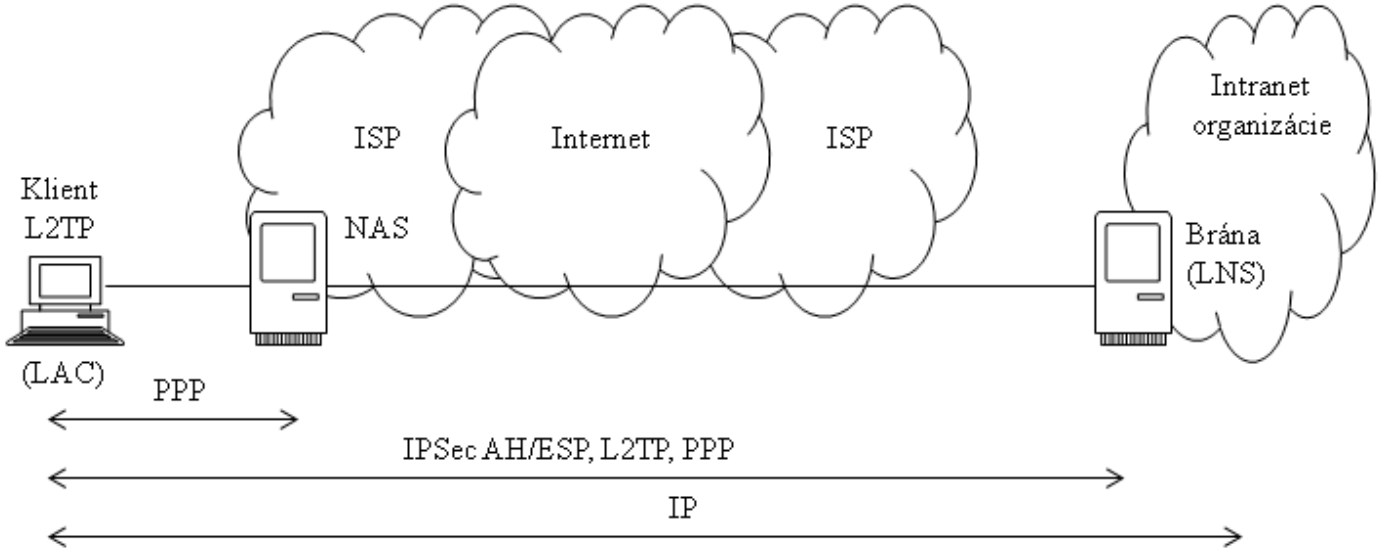


- **Protokol IPSec je použitý na zabezpečenie povinného tunela L2TP end-to-end**



Protokol L2TP

- **Protokol IPSec je použitý na zabezpečenie voliteľného tunela L2TP end-to-end**

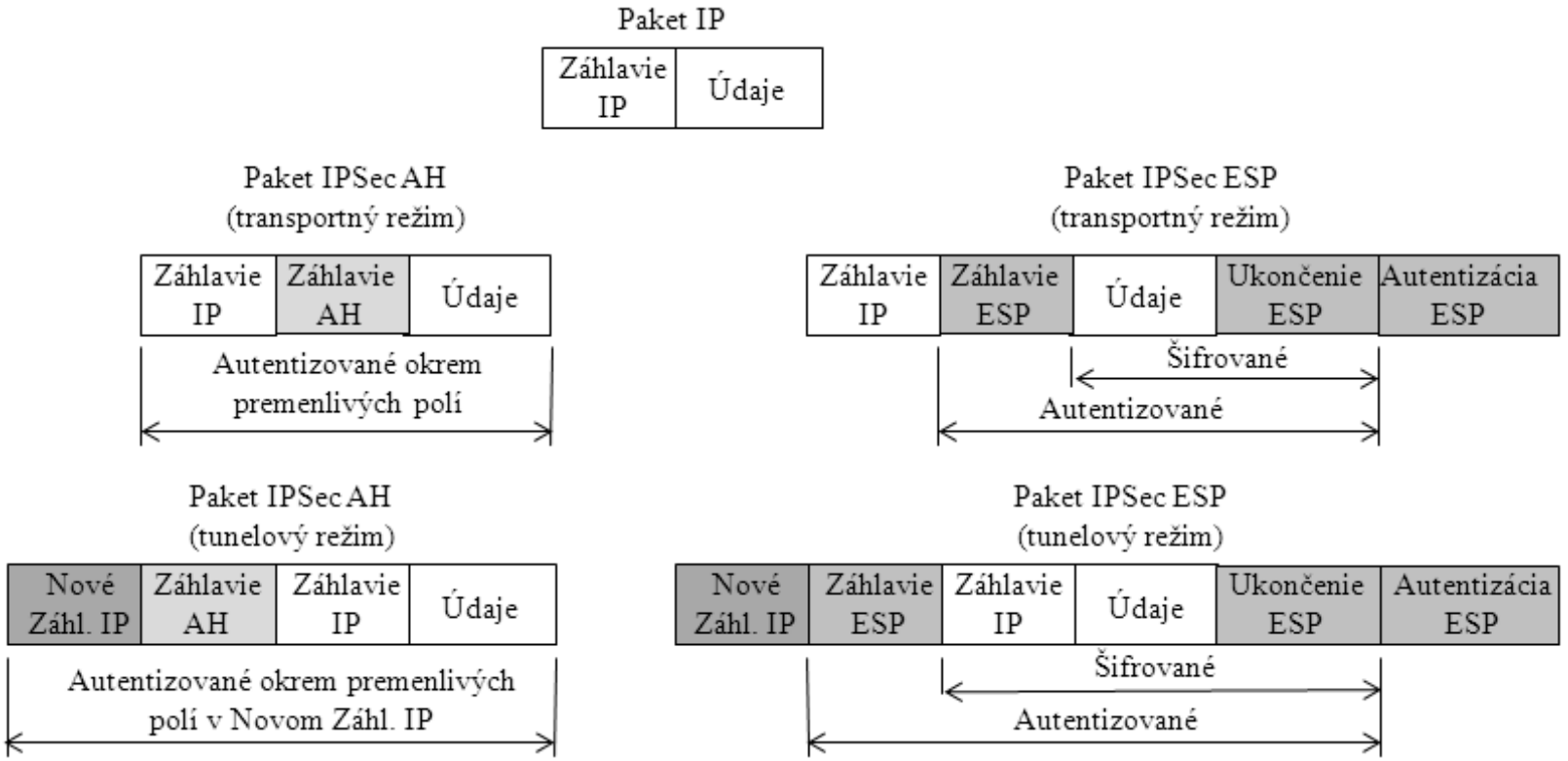


Protokol IPSec

- **Štandard IPSec** poskytuje metódu autentizácie a ochrany údajov pri bezpečnom prenose správy.
  - IPSec obsahuje protokol **ISAKMP/Oakley** (Internet Security Association a Key Management Protocol) a dva protokoly IPSec: **IPSec ESP** (Encapsulating Security Protocol) a **IPSec AH** (Authentication Header).
  - IPSec používa na ochranu údajov. **symetrické šifrovacie algoritmy** (sú časovo efektívnejšie a jednoduchšie sa implementujú v hardvéri).
  - Tieto algoritmy potrebujú na zabezpečenie ochrany dát **bezpečný spôsob zriadenia a výmeny šifrovacích kľúčov**. Túto možnosť zabezpečujú protokoly IKE (Internet Key Exchange) ISAKMP/ Oakley.
  - IPSec tiež obsahuje niekoľko spôsobov vytvorenia **autentizačných kódov správ HMAC** (Hashed Message Authentication Code), z ktorých si je možné vybrať, každý z nich poskytuje rôznu úroveň ochrany pred útokmi ako sú man-in-the-middle, znovuposlanie paketu (packet replay) a útoky na integritu údajov.
- Bezpečnostné rozšírenie protokolu IP protokolom IPSec má dve možnosti: **protokoly IPSec ESP a IPSec AH**.
  - Záhlavie **ESP** (protokol IP 50) **tvorí jadro protokolu IPSec**. Tento protokol, spolu s dohodnutým súborom bezpečnostných parametrov, zabezpečuje **šifrovanie údajovej časti paketu** (náklad paketu) a používa ďalšie ochrany (HMAC) na **zaistenie integrity údajov**, zaistenie proti útoku znovuposlatia paketu a útoku typu man-in-the-middle. Voliteľne môže IPSec ESP tiež zabezpečiť **autentizáciu chránených údajov**.

Protokol IPSec

- Bezpečnostné rozšírenie protokolu IP protokolom IPSec má dve možnosti: **protokoly IPSec ESP a IPSec AH**.
  - **Protokol IPSec AH** (protokol IP 51) tvorí druhú časť IPsec. IPSec AH nezabezpečuje šifrovanie údajov bežným spôsobom, ale **pridáva k údajom v pakete autentizačný kód**, ktorý chráni paket pred neoprávnenou modifikáciou. Medzi chránené údaje paketu tiež možno zahrnúť nemeniteľné polia v záhlaví IP ako sú polia adresy IP. Protokol IPSec AH **nezabezpečuje dôvernosť údajov**, preto nemôže byť iba sám použitý v prípade, že je požiadavka na dôvernosť údajov.



Protokol IPSec

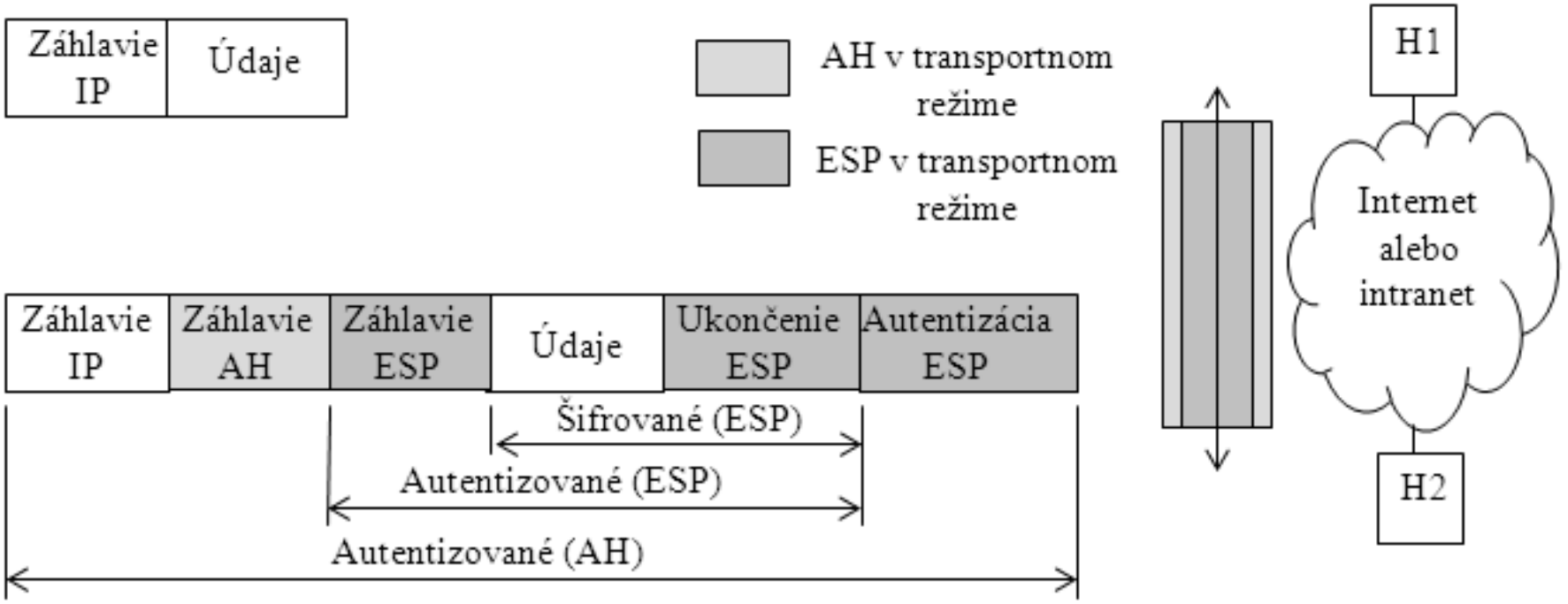
- Protokol IPsec môže fungovať v dvoch režimoch vo vzťahu k prenášaniu údajov cez sieť a to **v transportnom režime a v tunelovom režime**. Jedntlivé režimy sa líšia v spôsobe používania ako aj v množstve vyžadovanej réžie.
  - **Tunelový režim** funguje tak, že **celý paket IP je zapúzdrený a chránený**. Pretože tunelový režim skryje aj záhlavie IP pôvodného paketu IP, pridáva sa nové záhlavie IP, aby mohol byť paket cez tunel úspešne prenesený. Šifrovacie zariadenie pozná adresy IP (začiatok a koniec tunela) v novom záhlaví a tieto adresy bývajú štandardne nastavené pri konfigurácii sieťovej brány (napríklad smerovača). Tunelový režim môže byť zriadený jedným alebo obidvomi protokolmi IPsec (ESP a AH). Výsledkom použitia tunelového režimu je rozšírenie pôvodného **paketu IP asi o 20 bajtov** z dôvodu zavedenia nového záhlavia IP. Tunelový režim je všeobecne považovaný za bezpečnejší a flexibilnejší než transportný režim. Tunelový režim IPSec **šifruje zdrojovú a cieľovú adresu IP pôvodného paketu** a teda skrýva tieto informácie na nechránenej sieti pred potecionálnym útočníkom.
  - **Transportný režim IPSec** sa zriadi tak, že do paketu IP sa za záhlavie IP vloží záhlavie ESP alebo AH. **Obe adresy IP sieťových uzlov**, medzi ktorými je premávka chránená IPsec, **sú viditeľné v IP hlavičke aj po prípadnom šifrovaní paketu**. Tento režim IPSec môže byť citlivý na útoky analýzy premávky. Pretože nie je pridané žiadne ďalšie záhlavie IP, z toho vyplýva menšie rozšírenie veľkosti paketu. Transportný režim môže byť zriadený jedným alebo oboma protokolmi IPSec ESP a AH.

Protokol IPSec

- Protokoly IPSec ESP a ISPSec AH je možné použiť samostatne alebo **v kombinácii**.
  - Vzhľadom k tomu, že **každý protokol má dva režimy**, existuje celý rad možných kombinácií. Aby to bolo ešte komplikovanejšie, **bezpečnostné asociácie SA** (Security Association - bezpečnostná asociácia je dohoda medzi dvoma entitami zapojenými do používania kryptografických prostriedkov) **IPSec AH a IPSec ESP nemusia mať rovnaké koncové body**.
- Prakticky používané sú však iba niektoré scénare. Kombinácie protokolov IPSec sú realizované s balíčkami SA a existujú dva prístupy na ich vytvorenie a to:
  - **transportná priľahlosť** (transport adjacency) a
  - **vnorené tunelovanie** (nested tunneling).

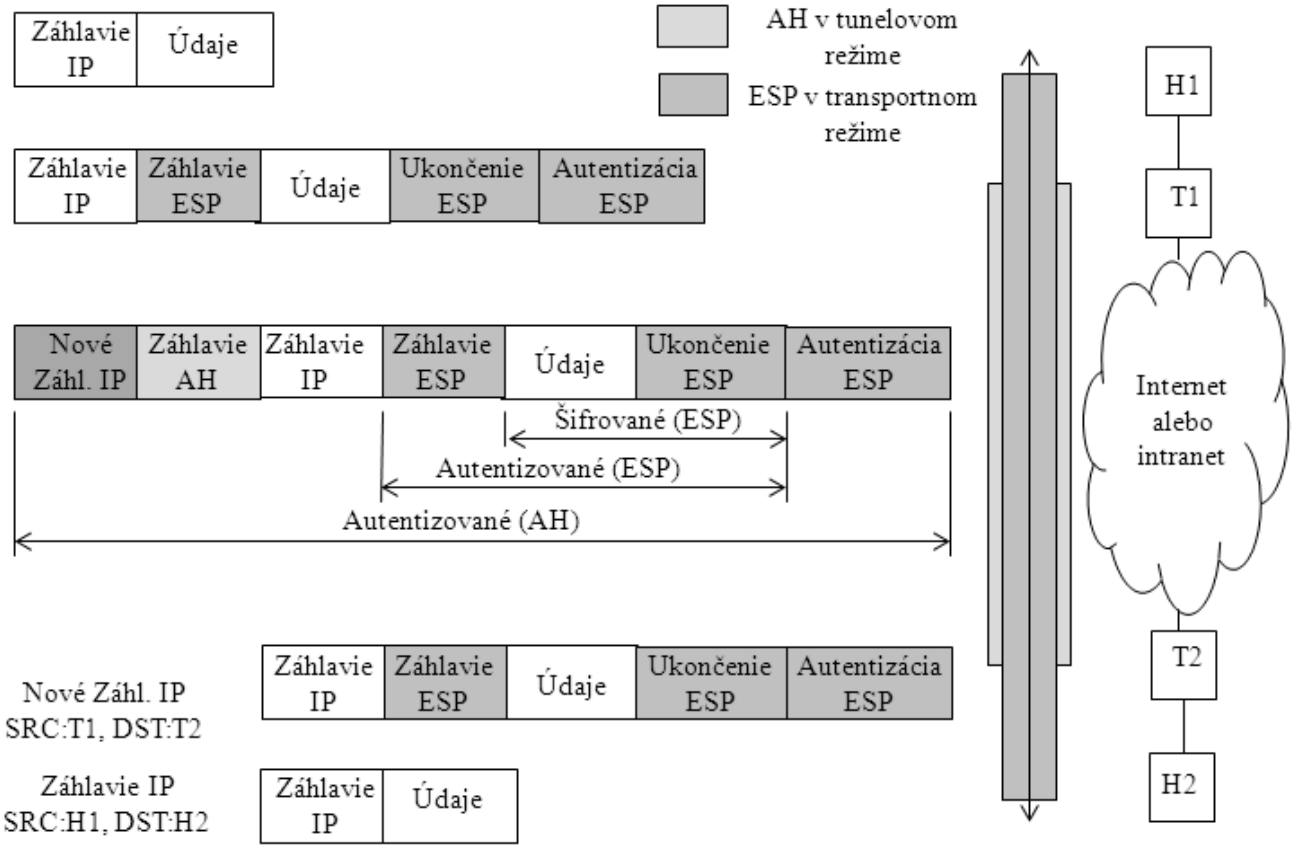
Protokol IPSec

- V prístupe **transportnej priľahlosti** sú **oba bezpečnostné protokoly použité v transportnom režime toho istého paketu IP**. Táto metóda je praktická iba pre jednu úroveň kombinácie. Štandard IPSec stanovuje, že transportná priľahlosť susedov môže byť použitá iba spôsobom uvedeným na obrázku. To znamená, že pre **odchádzajúce pakety** musí byť vykonané **šifrovanie** (vnútorná SA) **pred autentizáciou** (vonkajšia SA), zatiaľ čo pre **prichádzajúce pakety** sa musí autentizácia **vykonať pred šifrovaním**. Toto je logická následnosť a tiež šetrí zaťaženie systému dešifrovaním v prípade, keď skorej zlyhá autentizácia paketu (a teda dešifrovanie sa nemusí vykonať).



Protokol IPSec

- V prístupe **vnoreného tunelovania** (nested tunneling) sú **oba bezpečnostné protokoly aplikované za sebou**. Po každom aplikovaní je vytvorený nový paket IP a na tento paket je aplikovaný ďalší protokol. **Táto metóda nemá žiadne obmedzenia na počet vnorených úrovní. Ale viac ako tri úrovne vnorenia sú nepraktické**. Na obrázku je príklad vnoreného tunelovania. Najprv sa na paket IP aplikuje protokol IPSec ESP v transportnom režime a následne protokol IPSec AH v tunelovom režime.



Protokol IPSec

- Na implementáciu riešenia VPN so šifrovaním je nevyhnutná **pravidelná výmena relačných šifrovacích kľúčov**.
  - **Zanedbanie výmeny** relačných kľúčov môže spôsobiť **zraniteľnosť šifrovaných údajov** prenášaných VPN na útok hrubou silou.
  - IPsec rieši tento problém **protokolom IKE**, ktorý využíva ďalšie dva protokoly na autentizáciu entít využívajúce kryptografické prostriedky (krypto entity) a na generovanie kľúčov.
  - IKE využíva matematický algoritmus **Diffie-Hellmanovej výmeny kľúčov** na generovanie symetrických relačných kľúčov, ktoré sú potom použité krypto entitami.
- **Bezpečnostná asociácia SA** (Security Association) je dohoda **medzi dvomi krypto entitami**. Táto dohoda zahrňuje typ a silu šifrovacieho algoritmu použitého na ochranu údajov. SA zahrňuje metódu a silu autentizácie údajov a metódu vytvárania nových kľúčov pre túto ochranu údajov. Krypto entity sú vytvorené podľa ďalej uvedeného opisu.
- Každá SA má **stanovenú dobu životnosti**, počas ktorej je SA považovaná za platnú.
  - Životnosť je meraná v **jednotkách času existencie SA** (v sekundách) a v **jednotkách objemu** prenesených údajov (počet bajtov). Životnosť je dohodnutá pri vytvorení SA. Tieto dve životnosti sú kontrolované a **vypršanie jednej z nich zneplatní aktuálnu SA**.
  - Za bežných okolností **časová životnosť uplynie skorej** ako objemová životnosť. V prípade, že sledovaný paket vyhovuje SA v záverečných 120 sekundách životnosti aktuálneho SA, je štandardne vyvolaný proces vytvorenia nových relačných kľúčov.
  - Proces vytvorenia nových relačných kľúčov zriadi **novú aktuálnu SA predtým než sa zruší stará SA**. Výsledkom je plynulý prechod zo starej SA na novú SA s minimálnou stratou paketov v novej SA.

Protokol IPSec

- ISAKMP SA je **jeden obojsmerný bezpečný dojednávací kanál** používaný oboma krypto entitami na poslanie dôležitých bezpečnostných parametrov entity, ako sú bezpečnostné parametre pre IPSec SA (údajový tunel). **Štandardné politiky ISAKMP SA** majú predvolenú hodnotu **životnosti 86.400 sekúnd** (24 hodín) **bez limitu na objem prenesených údajov**.
- **IPsec SA je jednosmerný komunikačný kanál** od jednej krypto entity do druhej krypto entity. Skutočné údaje zákazníka prechádzajú iba IPSec SA a nikdy nie cez ISAKMP SA. Každá strana IPSec tunela má pár IPSec SA na spojenie: jeden do vzdialenej krypto entity a druhý zo vzdialenej krypto entity. Tieto informácie o páre IPSec SA sú uložené lokálne v databáze SA. Štandardné politiky IPsec SA majú predvolenú životnosť 3.600 sekúnd (1 hodinu) a objemovú životnosť 4608000 kB.
- **Prvá fáza IKE** predstavuje počiatočné dojednanie obojsmerného ISAKMP SA medzi dvoma krypto entitami.
  - Prvá fáza IKE začína **vzájomnou autentizáciou krypto entít**. Po úspešnej autentizácii sa krypto entity **dohodnú na šifrovacom algoritme, hešovacej funkcii a ďalších parametroch, potrebných na vytvorenie ISAKMP SA**. Komunikácia medzi dvomi krypto entitami môžu byť predmetom odchytenia útočníkom, ale útočník má minimálnu šancu odhaliť šifrovací kľúč. ISAKMP SA je použitá procesom IKE na dojednanie bezpečnostných parametrov pre IPsec SA. Tieto informácie ISAKMP SA sú uložené lokálne v databáze SA každej krypto entity.

Protokol IPSec

- **Prvá fáza IKE má tri možné autentizačné metódy**:
  - **Predvolený spoločný kľúč PSK** (Pre-Shared Key). Predvolený spoločný kľúč je administrátorom preddefinovaný reťazec kľúča vložený ručne do každej krypto entity a slúži na vzájomnú identifikáciu. Pomocou PSK sú schopné dve krypto entity dojednať a vytvoriť ISAKMP SA. PSK zvyčajne obsahuje adresu IP hosta alebo podsiete a masku, ktorá je platná pre daný PSK.
  - **Infraštruktúra verejného kľúča PKI** (Public Key Infrastructure) pomocou digitálnych certifikátov X.509. Súčasťou certifikátu je názov, sériové číslo, doba platnosti a ďalšie informácie, ktoré môže zariadenie IPSec použiť na určenie platnosti certifikátu. Certifikáty môžu byť tiež zrušené, čo zariadenie IPSec odmietne na možnosť úspešnej autentizácie.
  - **Náhodné čísla šifrované RSA**.
- Na podporu premávky **medzi krypto entitami cez NAT** (Network Address Translator) alebo PAT (Port Address Translator) zariadenia **sa v sieti zavádza uzol IPSec NAT-T** (Network Address Translator - Transparency), **ktorý zapúzdruje krypto pakety do obalu UDP** a takto umožňuje paketom prejsť zariadeniami NAT alebo PAT. **NAT-T je automaticky dojednané** medzi dvoma krypto entitami **počas dojednávania ISAKMP** s cieľovým portom UDP 4500. Za zdrojový port sa používa nasledujúci vyšší dostupný port. Ak je použitý port UDP 4500, potom sa cieľový port posunie na port UDP 4501, 4502 a tak ďalej, až pokiaľ nie je zriadená relácia ISAKMP.

Protokol IPSec

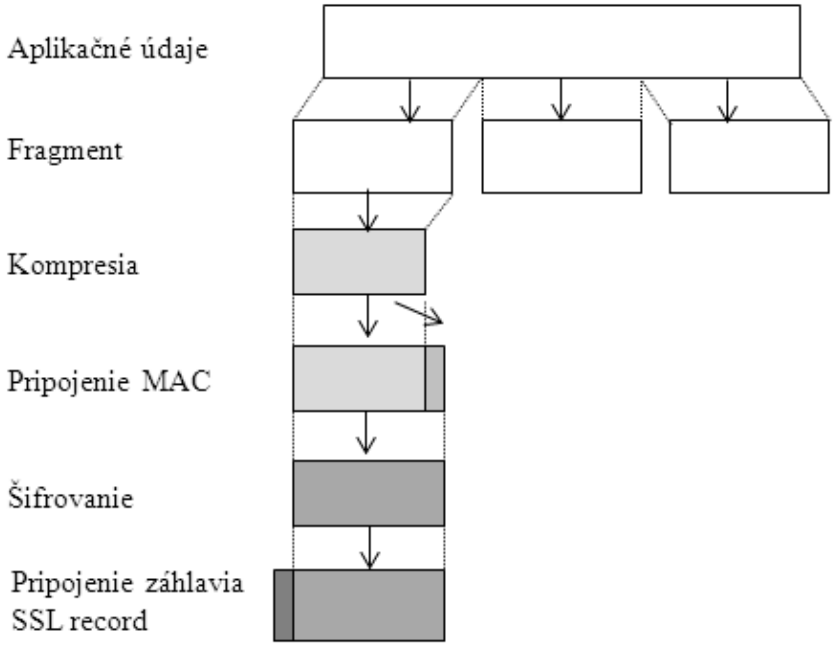
- **V druhej fáze IKE** sú procesom IKE pomocou obojsmernej ISAKMP SA dojednané asociácie IPSec SA.
  - Asociácie IPsec SA sú vo svojej podstate **jednosmerné,** čo spôsobuje, že je oddelená výmena kľúča pre tok údajov od krypto entity a pre tok údajov do krypto entity.
  - Výhodou tejto stratégie je to, **že údaje prenášané jedným smerom sú šifrované iným kľúčom ako údaje prenášané opačným smerom**.
  - To pre potenciálneho útočníka znamená **dvojnásobnú námahu pri snahe dešifrovať odchytené zašifrované údaje**.

Protokol SSL/TLS

- **Protokol SSL** vyvinula spoločnosť Netscape. Jeho verzia 3 bola publikovaná ako predbežný internetovýdokument. Následne vznikla v rámci IETF pracovná skupina TLS (Transport Layer Security) a navrhla spoločný štandard. Prvú publikovanú verziu TLS možno chápať v podstate ako SSL v3.1, ktorá je spätne kompatibilná s SSL v3. V tejto časti bude opísaná základná charakteristika protokolu SSL v3 a na záver hlavné rozdiely medzi SSL v3 a TLS.
- Protokol TCP **nezabezpečuje spoľahlivú bezpečnostnú službu** medzi komunikujúcimi koncovými entitami (end-to-end security). Preto bolo nevyhnutné nad protokolom TCP v transportnej vrstve navrhnúť ďalší protokol SSL tak, aby protokol TCP bol schopný zabezpečovať spoľahlivú bezpečnú komunikáciu dvoch koncových entít.
- Samotný protokol SSL **nie je jediný protokol**, ale predstavuje dve vrstvy protokolov.
  - Na nižšej vrstve je protokol **SSL Record Protocol** (poskytuje základné bezpečnostné služby rôznym protokolom na vyššej úrovni, ako je napríklad protokol HTTP).
  - Na vyššej vrstve sú protokoly **SSL Alert Protocol, SSL Change Cipher Spec Protocol a SSL Handshake Protocol** (špecifické protokoly SSL a sú využité pri manažmente SSL výmen).
- Koncepcia protokolu SSL predpokladá **reláciu SSL a spojenie SSL**, ktoré sú definované takto:
  - **Spojenie SSL** je transport (podľa definície vrstvového modelu OSI), ktoré zabezpečuje vhodný typ služieb. Pre SSL toto spojenie zodpovedá spojeniu odpovedajúcich si entít (správy medzi koncovými uzlami SSL). Spojenia sú dočasné. Každé spojenie je asociované s jednou reláciou.
  - **Relácia SSL** je asociácia medzi klientom a serverom. Relácie sú vytvárané prostredníctvom protokolu SSL Handshake Protocol. Relácie definujú množinu kryptografických bezpečnostných parametrov, ktoré môžu byť spoločné medzi viacerými spojeniami. Relácie sa využívajú na to, aby sa zamedzilo náročnému dohadovaniu nových bezpečnostných parametrov pre každé spojenie.

Protokol SSL/TLS

- **SSL Record Protocol** je protokol, ktorý zabezpečuje dve služby pre spojenia SSL a to **dôvernosť a integritu správy**.
  - SSL Handshake Protocol **definuje spoločné tajné kľúče**, ktoré sú využité pri konvenčnom šifrovaní údajov nákladu SSL a pri tvobe autentizačného kódu správy MAC (Message Authentication Code).
  - Na obrázku je zobrazená celková funkcionalita protokolu SSL Record Protocol. Tento protokol pri vysielaní v začiatočnom uzle SSL zabezpečuje **prevzatie aplikačnej správy**, **vykoná fragmentáciu** správy do zvládnuteľných blokov, **voliteľne vykoná kompresiu údajov** bloku, **určí autentizačný kód** bloku MAC, blok s pripojeným autentizačným kódom **zašifruje**, **pridá záhlavie SSL** a vyšle ho v TCP segmente. Prijatý TCP segment v koncovom uzle SSL je potom podľa protokolu SSL Record Protocol spätne dešifrovaný, je verifikovaný MAC bloku, voliteľne je blok dekompresovaný a fragmenty sú zložené do správy pre aplikáciu.

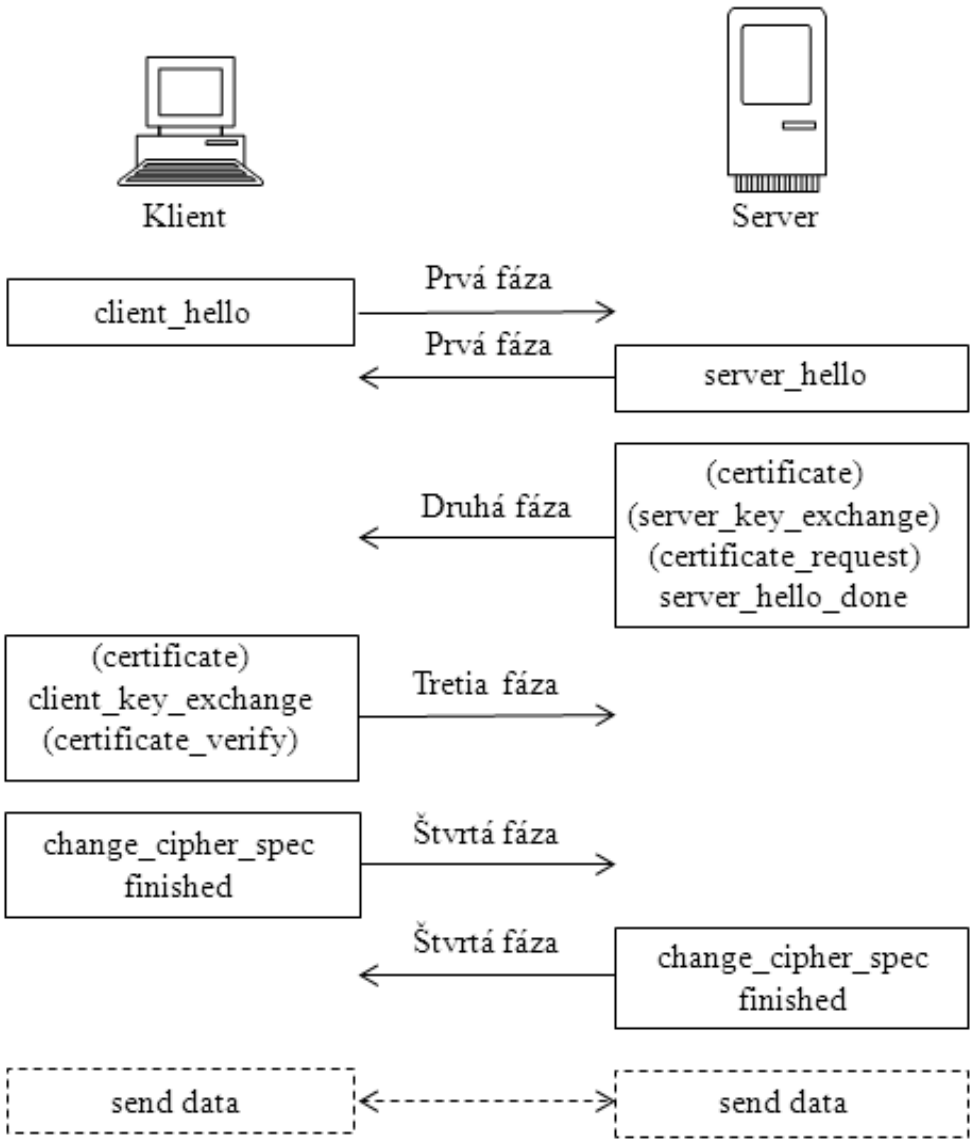


Protokol SSL/TLS

- **Change Cipher Spec Protocol** je najjednoduchší zo špecifických protokolov SSL a používa ho protokol SSL Record Protocol.
  - Pozostáva z **jedinej** správy a z jediného bajtu s hodnotou 1. Účelom tejto správy je spôsobiť preklopenie pripravenej množina šifrovacích nástrojov (predtým dohodnutej protokolom SSL Handshake Protocol) do aktuálneho stavu a začať používať novú množinu šifrovacích nástrojov v danom spojení.
- **Alert Protocol** je využitý pri prenose výstražných správ SSL do odpovedajúcej entity.
  - Podobne ako pri aplikačnej správe aj výstražné správy sú komprimované a šifrované podľa nastaveného aktívneho stavu.
  - Každá správa v tomto protokole sa skladá z dvoch bajtov. Prvý bajt vyjadruje závažnosť správy a má hodnotu **varovanie** (warning) alebo **fatálne** (fatal). Ak je závažnosť správy fatálne, potom **SSL okamžite ukončí spojenie**, v ktorom vznikla situácia fatálne. Ostatné spojenia relácie, v ktorom je spojenie so situáciou fatálne, môžu pokračovať, ale v tejto relácii nemôže byť zriadené žiadne nové spojenie.

Protokol SSL/TLS

- Najkomplexnejšou časťou SSL je protokol **SSL Handshake Protocol**.
  - Tento protokol umožňuje **vzájomnú autentizáciu klienta a servera**, umožňuje **dojednanie šifrovacieho algoritmu**, algoritmu na výpočet **autentizačného kódu správy** a **kryptografických kľúčov** použitých na ochranu údajov v SSL protokole.
  - Protokol SSL Handshake Protocol sa vykoná **pred prenosom aplikačných údajov**.
  - SSL Handshake Protocol pozostáva z **výmeny správ medzi klientom a serverom**. Správy sú zoskupené **do štyroch fáz**. Na obrázku je zobrazená postupnosť výmeny správ. Správy v zátvorkách sa **vymieňajú voliteľne alebo závisia na konkrétnej situácii** a správy nie sú vždy poslané.



Protokol SSL/TLS

- **Prvá fáza SSL Handshake Protocol – Zriadenie bezpečnostných funkcií.**
  - Táto fáza slúži na nadviazanie **logického spojenia a na zriadenie bezpečnostných funkcií**, ktoré budú s ním spojené.
  - Túto fázu inicializuje klient, ktorý posiela správu **client_hello** s parametrami verzia (najvyššia verzia SSL podporovaná klientom) a náhodné číslo (klientom vytvorené náhodné číslo pozostávajúce z 32 bitovej hodnoty času a dátumu a 28 bajtov vytvorených náhodným generátorom, využíva sa pri výmene kľúčov proti útokom typu znovuprehratie).
  - Na správu client_hello odpovedá server správou **server_hello**, ktorá obsahuje rovnaké parametre ako správa client_hello. Interpretácia parametrov správy server_hello je takáto.
    - Pole **verzia** obsahuje **nižšiu verziu z verzií navrhnutej klientom a najvyššou verziou** podporovanou serverom, **náhodné číslo** je vytvorené serverom rovnakým spôsobom nezávisle na náhodnom čísle klientovej správe.
    - Ak pole **ID relácie** (SessionID) **klienta bolo nenulové**, potom takú istú hodnotu použije aj server, v opačnom prípade pole ID relácie servera obsahuje hodnotu pre novú reláciu.
    - Pole **šifrovacia suita** (CipherSuite) obsahuje jednu **serverom vybratú šifrovaciu suitu** zo šifrovacej suity navrhnutej klientom.
    - Pole **kompresie** (Compression) obsahuje **kompresnú metódu** zvolenú serverom z metód navrhnutých klientom.
- **Prvým elementom** v parametroch šifrovacej suity je **metóda výmeny kľúčov** (spôsob, ktorým sa dojedná výmena kryptografických kľúčov pre symetrické šifrovanie a MAC). Sú podporované tieto výmeny kľúčov:
  - **RSA** – tajný kľúč je zašifrovaný verejným RSA kľúčom príjemcu. Musí byť k dispozícii certifikát verejného kľúča príjemcu.
  - **Pevný Diffie – Hellman (D-H)** – táto D-H výmena kľúča predpokladá, že server má certifikát verejného kľúča, ktorý obsahuje verejné D- H parametre (prvočíslo a primitívny koreň) a verejný D-H kľúč. Klient poskytne svoje parametre verejného D-H kľúča v certifikáte, ak sa požaduje autentizácia klienta, alebo v správe výmeny kľúča. Táto metóda poskytuje pevný tajný kľúč medzi komunikujúcimi entitami, nakoľko je tajný kľúč vypočítaný z pevných verejných D-H kľúčov entít.

Protokol SSL/TLS

- **Dočasný D-H** - táto D-H výmena kľúča poskytuje vytvorenie dočasného (jednorázového) tajného kľúča. V tomto prípade sú verejné D-H parametre a verejné D-H kľúče vymenené a podpísané odosielateľovým privátnym kľúčom RSA alebo DSS. Príjemca môže verifikovať podpis pomocou odpovedajúceho verejného kľúča z certifikátu. Táto výmena kľúča je najbezpečnejšia, pretože poskytuje dočasný (jednorázový) autentizovaný tajný kľúč.
- **Anonymný D–H** - používa D-H algoritmus výmeny kľúča bez autentizácie komunikujúcich entít. To znamená, že každá entita posiela svoje D-H parametre bez autentizácie. Tento spôsob výmeny kľúča je zraniteľný na útok man-in-the-middle, pri ktorej útočník realizuje anonymnú výmenu kľúča s obidvomi entitami (sprostredkováva komunikáciu entít).
- **Fortezza** – technika definovaná v schéme Fortezza.

❑ **Druhá fáza SSL Handshake Protocol – Autentizácia servera a výmena kľúča.**

- Túto fázu začne server poslaním svojho certifikátu, ak je potreba jeho autentizácie. Správa **certificate** je vyžadovaná pre každú metódu výmeny kľúčov s výnimkou anonymného D-H.
- Ako ďalšia správa môže byť poslaná správa **server_key_exchange**, pokiaľ sa to požaduje. Nie je to požadované v prípade, keď server poslal certifikát s pevnými D-H parametrami alebo bude použitá výmena kľúčov RSA. Správa server_key_exchange je potrebná v týchto prípadoch:
  - **Anonymný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívne koreň tohto čísla) a verejný D-H kľúč servera.
  - **Dočasný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívny koreň tohto čísla), verejný D-H kľúč servera spolu s podpisom týchto troch parametrov.
  - **Výmena kľúča RSA** (server používa RSA, ale má iba podpisovací kľúč RSA). To znamená, že klient nemôže jednoducho poslať tajný kľúč zašifrovaný verejným kľúčom servera. Namiesto toho musí server vytvoriť dočasný kľúčový pár (verejný a privátny kľúč) RSA a použiť správu server_key_exchange na odoslanie verejného kľúča. Správa obsahuje dva parametre dočasného verejného kľúča RSA (exponent a modul) a podpis týchto parametrov.
  - **Fortezza.**

Protokol SSL/TLS

- Neanonymný server (server nepoužíva anonymný D-H) môže klienta požiadať o certifikát.
  - Správa **certificate_request** obsahuje dva parametre, a to **typ certifikátu a certifikačné autority**. Typ certifikát udáva algoritmus verejného kľúča a jeho použitie. Napríklad RSA (algoritmus)/iba na podpis (použitie), RSA/pre pevný D-H (v tomto prípade je podpis použitý iba na autentizáciu), RSA/dočasný D-H. Druhý parameter v správe certificate_request je zoznam názvov akceptovateľných certifikačných autorít.
  - Záverečná správa v druhej fáze, ktorá sa vždy vyžaduje, je správa servera **server_done**. Po odoslaní tejto správy bude server čakať na klientovu odpoveď. Táto správa neobsahuje žiadne parametre.
- **Tretia fáza SSL Handshake Protocol – Autentizácia klienta a výmena kľúča.**
  - Po prijatí správy **server_done** by klient mal overiť, či **server predložil platný certifikát** (ak sa požaduje) a skontrolovať, či sú akceptovateľné parametre správy **server_hello**. Ak je všetko akceptovateľné, klient pošle späť serveru jednu alebo viacero správ. Ak server požadoval certifikát, klient začne túto fázu zaslaním správy **certificate**. Ak klient nemá k dispozícii vhodný certifikát, pošle serveru namiesto certifikátu varovanie **no_certificate**.
- Ďalej nasleduje správa **client_key_exchange**, ktorá musí byť poslaná v tejto fáze. Obsah správy závisí od typu výmeny kľúča takto:
  - **RSA.** Klient vygeneruje 48 bajtové pre-master tajomstvo a zašifruje ho pomocou verejného kľúča zo serverovho certifikátu alebo dočasného kľúča RSA zo správy server_key_exchange.
  - **Dočasný alebo anonymný D-H.** Sú poslané klientove verejné parametre D-H.
  - **Pevný D-H.** Verejné parametre D-H klienta boli poslané v správe certificate, takže obsah tejto správa je prázdny.
  - **Fortezza.** Pošlú sa klientove parametre Fortezza.

Protokol SSL/TLS

- Nakoniec v tejto fáze môže klient poslať správu **certificate_verify** na potvrdenie explicitnej verifikácie klientovho certifikátu.
  - Táto správa je poslaná **iba ako následná** po akomkoľvek klientskom certifikáte, ktorý má **funkciu podpisovania** (t.j. všetky certifikáty s výnimkou tých, ktoré obsahujú pevné D-H parametre). Táto správa obsahuje **podpis zreťazených predchádzajúcich správ**.
  - Ak privátny kľúč klienta je pre algoritmus DSS, potom sa používa algoritmus SHA-1 na vypočítanie hešovacej hodnoty zreťazených predchádzajúcich správ. Ak privátny kľúč klienta je pre algoritmus RSA, potom sa za hešovaciu hodnotu zoberie zreťazenie hešovacích hodnôt vypočítaných zo zreťazených predchádzajúcich správ algoritmom MD5 a SHA-1.
  - V každom prípade je účelom overiť, že **klient vlastní súkromný kľúč pre verejný kľúč z certifikátu klienta**. Aj keby niekto zneužíval certifikát klienta, nie je schopný zabezpečiť podpis, pretože nemá súkromný kľúč klienta.
- **Štvrtá fáza SSL Handshake Protocol – Ukončenie.**
  - Táto fáza ukončí vytvorenie bezpečeného spojenia.
  - Klient pošle správu **change_cipher_spec** a skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity. Stojí za zmienku, že táto správa nie je súčasťou protokolu SSL Handshake Protocol, ale je poslaná pomocou protokolu Change Cipher Spec Protocol.
  - Po tejto správe klient bezprostredne pošle správu **finished** podľa novej šifrovacej suity. Táto správa potvrdzuje, že výmena kľúča a autentizačné procesy boli úspešné.
  - Ako odpoveď na tieto dve správy klienta pošle server vlastnú správu **change_cipher_spec,** skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity, a pošle správu **finished**. V tomto bode je dohodnutie šifrovacej suity ukončené a klient a server môžu začať výmenu údajov na aplikačnej vrstve.

Protokol SSL/TLS

- **Protokol TLS** je štandardizačná iniciatíva IETF, ktorej cieľom je vytvorenie verzii Internetového štandardu protokolu SSL. Súčasná verzia TLS je definovaná v Internetovom štandarde [RFC 5246], ktorý je veľmi podobný SSL v3. Ďalej sa poukáže na niektoré ich **rozdiely**. **Formát správy** protokolu SSL Record Protokol je v TLS rovnaký.
  - Jediný **rozdiel je v hodnotách verzií**, pre aktuálnu verziu TLS je hodnota vyššej verzie 3 a hodnota nižšej verzie je tiež 3.
  - Pri výpočte **autentizačného kódu správy MAC** existujú medzi SSL v3 a TLS dva rozdiely, a to v používanom algoritme a rozsahu údajov, z ktorých sa počíta autentizačný kód. TLS používa algoritmus HMAC definovaný v [RFC 2104].
  - TLS podporuje **všetky výstražné kódy protokolu Alert Protocol** definované vo SSLv3 s výnimkou varovania no_certificate. V TLS sú definované ďalšie výstražné kódy najmä typu fatálne.
  - V **šifrovacích suitách** existuje niekoľko malých rozdielov medzi SSL v3 a TLS. Pri výmene kľúča TLS podporuje všetky výmeny kľúča definované v SSL v3 s výnimkou Fortezza. Pri symetrických šifrovacích algoritmoch TLS obsahuje všetky symetrické šifrovacie algoritmy definované v SSLv3 s výnimkou Fortezza.
  - V **klientskych typoch certifikátu** TLS definuje len tieto typy certifikátu, o ktoré je možno požiadať v správe certificate_request: rsa_sign, dss_sign, rsa_fixed_dh a dss_fixed_dh. TLS nepodporuje systém Fortezza. V **správach certificate_verify a finished** TLS zahrňuje do výpočtu hešovacej hodnoty menší počet položiek.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™