slovensky

MOVET

Modernisation of VET through
Collaboration with the Industry

Ivan Pravda

Sieťová bezpečnosť

Erasmus+

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

Názov: Sieťová bezpečnosť
Autor: Ivan Pravda
Preložil: Peter Trúchly
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, Česká republika
Tel.: +420 224352084
Tlač: (iba elektronická)
Počet strán: 42
Edícia (vydanie): 1. vydanie, 2019

MoVET
Modernisation of VET through
Collaboration with the Industry

https://movet.fel.cvut.cz

Tento projekt bol financovaný s podporou Európskej Komisie.

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
	Výhody
	Nevýhody

ANOTÁCIA

Modul sa zaoberá možnosťami zabezpečenia premávky v sietí so zameraním na oblasť virtuálnych privátnych sietí (VPN). Definuje súbor základných pojmov, obsahuje opis základných komponentov a koncepcií sietí VPN. Ďalej je venovaná pozornosť charakteristike protokolu IPsec a mechanizmom umožňujúcim implementáciu zabezpečenia premávky privátnych sietí, medzi ktoré patrí metóda ISAKMP/IKE a mechanizmus výmeny kľúčov Diffie-Hellmann. Modul obsahuje v neposlednom rade aj niekoľko praktických príkladov a ich riešenie. Záver modulu je venovaný problematike elektronického podpisu.

CIELE

Štúdiom modulu získajú študenti prehľad o problematike zabezpečenia počítačových sietí prostredníctvom virtuálnych privátnych sietí. Táto problematika je dnes veľmi aktuálna, lebo pojem bezpečnosti veľmi úzko súvisí s kyberkriminalitou. Dôraz je kladený nielen na objasnenie terminológie v danej oblasti, ale aj na vysvetlenie princípu základných postupov a je vhodne doplnený o konkrétne príklady implementácie. Záverečná časť objasňuje záležitosti týkajúce sa elektronického podpisu a možnosti jeho implementácie v každodennom živote.

LITERATÚRA

[1] Deal, Richard. The Complete Cisco VPN Configuration Guide. Cisco Press, 2005. 1032 pages. ISBN: 978-1-58705-204-0.

[2] Cisco Systems. Clientless SSL VPN (WebVPN) on Cisco IOS with SDM Configuration Example. 2009. https://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70663-webvpn.html [online]

[3] RFC4301 - Security Architecture for the Internet Protocol http://tools.ietf.org/html/rfc4301 [online]

[4] RFC4302 - IP Authentication Header http://tools.ietf.org/html/rfc4302 [online]

[5] RFC4303 - IP Encapsulating Security Payload (ESP) http://tools.ietf.org/html/rfc4303 [online]

[6] RFC4308 - Cryptographic Suites for IPsec http://tools.ietf.org/html/rfc4308 [online]

[7] RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs). http://tools.ietf.org/html/rfc4364 [online]

[8] RFC4835 - Cryptographic Algorithm Implementation Requirements forEncapsulating Security Payload (ESP) and Authentication Header (AH) http://tools.ietf.org/html/rfc4835 [online]

[9] RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2. http://tools.ietf.org/html/rfc5246 [online]

Obsah

1 Virtuálna privátna sieť - definícia základných pojmov 7

2 Komponenty VPN 9

3 Rozdelenie VPN podľa RM OSI 11

4 Protokol IPsec 13

5 Výmena kľúčov pri protokole IPsec - metóda ISAKMP/IKE 16

6 Algoritmus Diffie-Hellmann 20

7 Útoky v lokálnych sieťach - príklady a riešenie 22

8 Budovanie VPN pomocou IPsec - príklady a riešenia 27

8.1 Príklad konfigurácie IPsec VPN na zariadeniach firmy Cisco 30

9 Budovanie VPN pomocou SSL/TLS - príklady a riešenia 32

9.1 Typy prístupov SSL VPN 34

10 Elektronický podpis 36

10.1 Zaručený elektronický podpis 38

10.2 Kvalifikovaný elektronický podpis 40

10.3 Elektronická pečať 41

10.4 Časová pečiatka 42

1 Virtuálna privátna sieť - definícia základných pojmov

FORMÁLNA DEFINÍCIA

Virtuálna privátna sieť **VPN** (*Virtual Private Network*) je komunikačné prostredie, v ktorom je riadený prístup ku komunikácii medzi jednotlivými entitami. Komunikačné prostredie je vytvorené na báze vopred definovanej formy rozdelenia spoločného komunikačného média, ktoré je následne schopné poskytovať sieťové služby na neexkluzívnej báze.

NEFORMÁLNA DEFINÍCIA

Virtuálna privátna sieť **VPN** je neverejná (počítačová) sieť, vybudovaná v rámci verejnej sieťovej infraštruktúry, akou je napr. Internet. Táto sieť typicky poskytuje zabezpečené pripojenie vzdialených pobočiek alebo účastníkov k materskej sieti.

Z predchádzajúcich definícií je možné stručne povedať, že VPN je vo svojej podstate logická sieť v rámci zdieľanej verejnej infraštruktúry. Poskytuje rovnaký výkon a pravidlá ako ktorákoľvek súkromná sieť typu **LAN** (*Local Area Network*).

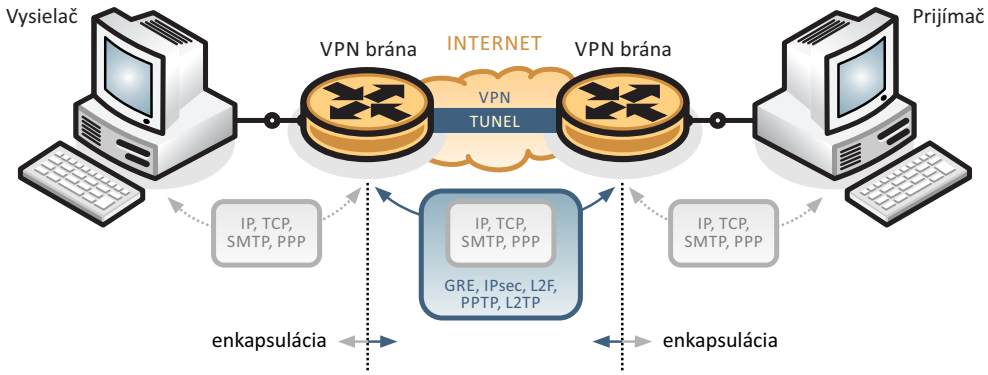
Úplne zásadným problémom pri použití VPN je zaistenie jej bezpečnosti a poskytovanie služieb v požadovanej kvalite s ohľadom na parametre **QoS** (*Quality of Service*). Obe tieto požiadavky nerieši infraštruktúra siete založená na protokoloch **TCP/IP** (*Transmission Control Protocol/Internet Protocol*).

Požiadavky na bezpečnosť sa z hľadiska návrhu VPN riešia pomocou:

- tunelovania,
- šifrovania,
- autentizácie (autentifikácie) a
- riadenia prístupu.

Pojmom tunelovanie je chápaný proces zapuzdrenia pôvodného paketu do iného. Pôvodný paket je pre všetky medziľahlé zariadenia nečitateľný počas celej doby jeho prenosu.

Dôvodom pre implementáciu tunelovania je zaistenie bezpečnosti a vytvorenie transportného mechanizmu medzi geograficky odľahlými lokalitami. Na zapuzdrenie sa používajú napr. protokoly **GRE** (*Generic Routing Encapsulation*), **IPsec** (*Internet Protocol Security*), **L2F** (*Layer 2 Forwarding*), **PPTP** (*Point-to-Point Tunneling Protocol*), **L2TP** (*Layer 2 Tunneling Protocol*).



Mechanizmus tunelovania v sieti VPN

Tunelovanie je tiež možné využiť na prispôsobenie navzájom nekompatibilných protokolov, napr. prepojenie LAN s **NetBEUI** (*NetBIOS Extended User Interface*) alebo **IPX** (*Internetwork Packet Exchange*) cez Internet (protokol IP).

Reálne je možné implementovať aj tzv. rozdelené tunelovanie (Split Tunneling), kedy má klient možnosť súčasnej komunikácie nielen vo vnútri VPN, ale aj s Internetom.

Pod pojmom šifrovanie rozumieme proces na zaistenie dôvernosti aj integrity dát. Čisto technicky ide o zapuzdrenie dát do bezpečnej obálky, t.j. šifrovanie tajným kľúčom.

Autentizácia v rámci VPN zaisťuje proces overovania pravosti, resp. zabezpečí, že dáta prichádzajú zo zdroja, z ktorého tvrdia, že prichádzajú.

Používajú sa schémy založené na systémoch so zdieľaným kľúčom, ako je **CHAP** (*Challenge Handshake Authentication Protocol*), signatúra **RSA** (*Rivest-Shamir-Adleman*) a ďalšie. Nad rámec zabezpečenia zaisťujú tieto systémy tiež integritu dát, t.j. ich celistvosť.

Riadenie prístupu, resp. kontrola prístupu umožňuje obmedzovanie prístupu či vniknutia neautorizovaných používateľov v spojitosti s procesom kontroly práv jednotlivých používateľov.

2 Komponenty VPN

Siete VPN používajú na zabezpečenie šifrovacie tunelovacie protokoly a poskytujú ochranu proti odpočúvaniu paketov (Packet Sniffing), zaručujú zodpovedajúcu autentizáciu a deklarujú úplnosť správ, t.j. ich integritu.

Komponenty potrebné na vybudovanie VPN spojenia sú:

- existujúca sieť typu LAN alebo samostatný terminál (napr. PC, notebook, netbook, a pod.),
- dostupné pripojenie do Internetu,
- VPN brány, tzv. VPN Gateways (napr.: smerovače, firewally, VPN koncentrátory) a
- zodpovedajúce programové vybavenie (software) potrebné na budovanie a spravovanie VPN tunelov.

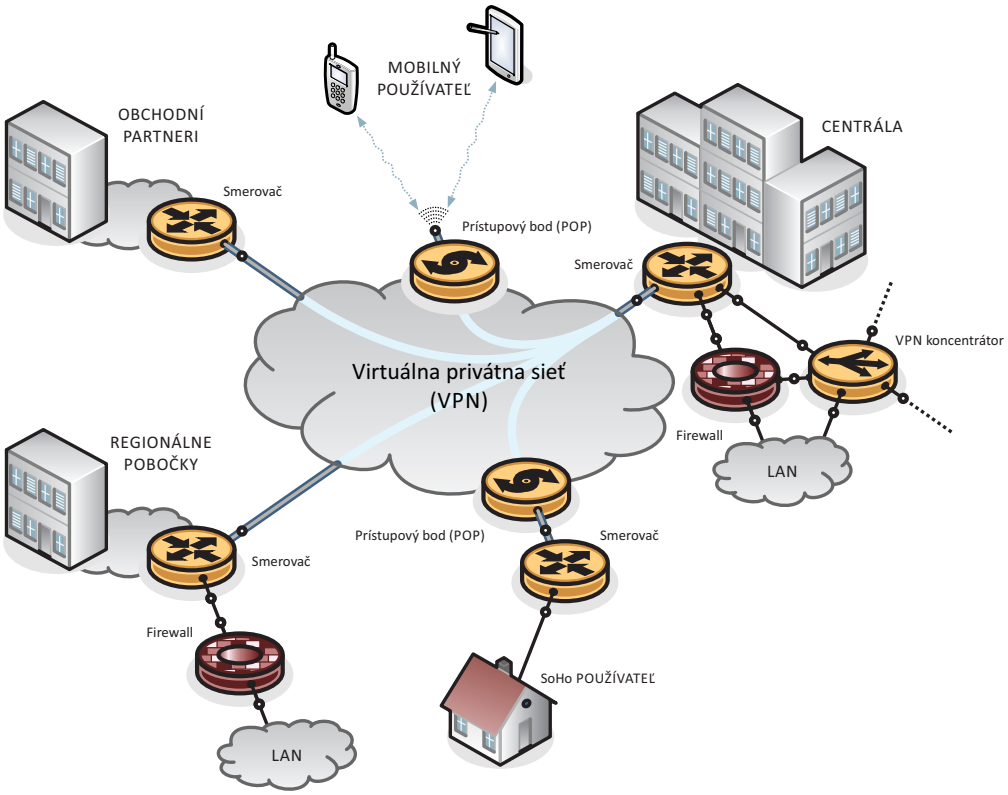
1. Spojenie sieť-sieť (Site-to-Site alebo LAN-to-LAN)

Tento typ spojenia sietí cez VPN je využívaný na prepojenie geograficky rozptýlených miest obdobným spôsobom, ako keby boli tieto lokality prepojené prenajatou linkou alebo inou **WAN** (*Wide Area Network*) technológiou (napr. Frame Relay, **ATM** (*Asynchronous Transfer Mode*)). Výhodou takéhoto prepojenia je zdieľanie podnikového intranetu alebo extranetu s pracovným partnerom. V tejto topológii používatelia posielajú a prijímajú dáta prostredníctvom VPN brány, ktorou býva zvyčajne smerovač alebo server. VPN brána je zodpovedná za šifrovanie odchádzajúcej premávky a jej smerovanie do VPN tunela v Internete k protiľahlej VPN bráne cieľovej siete. Táto VPN brána odoberie hlavičku paketu, dešifruje jeho obsah a následne doručí paket cieľovému používateľovi vo vnútri cieľovej siete.

2. Spojenie typu vzdialený prístup (Remote-Access)

Pracovníci v teréne alebo domáci pracovníci využívajú vzdialený prístup VPN pripojením veľmi často. V minulosti boli títo vzdialení pracovníci pripájaní telefónnymi linkami, čo znamenalo nízku rýchlosť prenosu spojenú s vysokými nákladmi na prevádzku. V súčasnosti ale už väčšina z nich disponuje rýchlym prístupom do Internetu priamo z domu prostredníctvom širokopásmových technológií a môžu tak vybudovať kvalitné VPN spojenie.

Každý používateľ má zvyčajne nainštalovaného VPN klienta, t.j. software, ktorý zapuzdruje a šifruje pakety pred tým, ako ich odošle cez Internet do cieľovej VPN brány. Tento software tak významne uľahčuje pripojenie, keďže používateľovi stačia iba základné znalosti na vybudovanie kvalitného VPN spojenia.



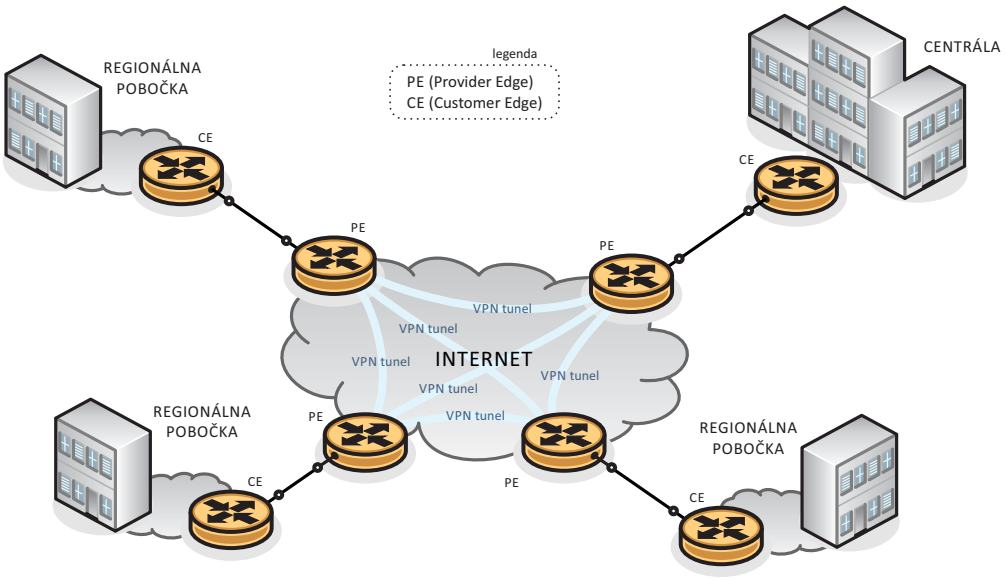
Možnosti prepojenia pomocou VPN

3 Rozdelenie VPN podľa RM OSI

1. VPN založené na zariadení prevádzkovateľa (PE-based VPN)

Zariadenia **PE** (*Provider Edge*) sú hraničné zariadenia poskytovateľa pripojenia a patria medzi ne smerovače **ISP** (*Internet Service Provider*), prepínače alebo zariadenia, ktoré sú kombináciou obidvoch.

Zariadenie typu PE sa zúčastní smerovania a preposielania premávky na základe adresného priestoru zákazníka. Dáta sú zvyčajne prenášané medzi zariadeniami PE prostredníctvom VPN tunelov vytvorených pomocou technológie **MPLS** (*Multi Protocol Layer Switching*), IPsec, L2TPv3 alebo GRE. V tomto prípade zariadenia **CE** (*Customer Edge*) nie sú vnímané ako súčasť VPN.



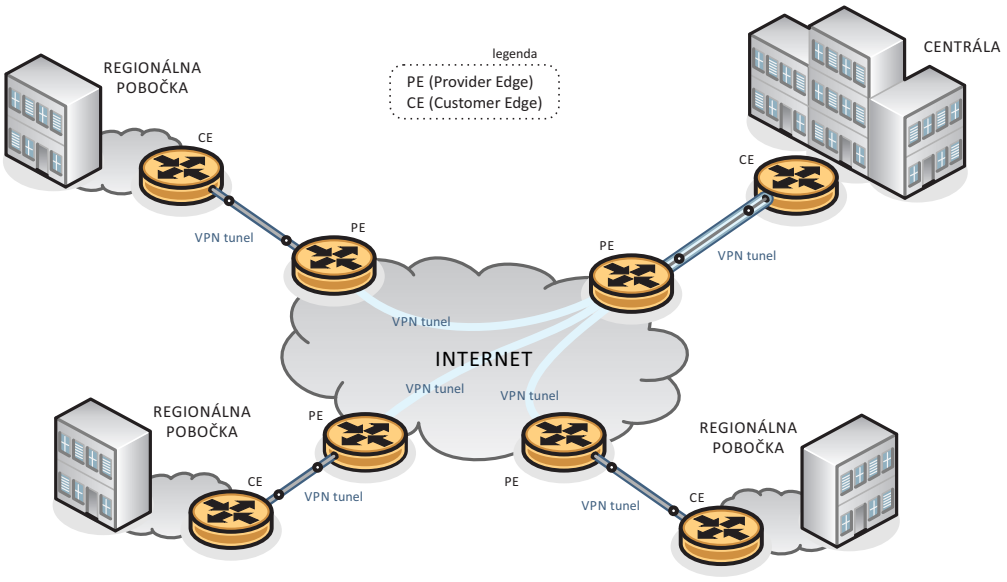
Usporiadanie VPN založené na zariadeniach prevádzkovateľa

VPN tunely sú ukončené na hraničnom smerovači PE a sú obyčajne konfigurované ako permanentné.

2. VPN založené na zariadení zákazníka (CE-based VPN)

Zariadenie CE je hraničné zariadenie zákazníka prepojené so zariadením PE prevádzkovateľa.

Zariadenia PE v tomto móde nerozlišujú typ premávky, o VPN spojenia sa starajú zariadenia CE, ktoré vykonávajú smerovanie a posielanie premávky používateľa. Tunely sú vytvorené medzi zariadeniami CE na základe protokolu IPsec alebo GRE.



Usporiadanie VPN založené na zariadeniach zákazníka

Zariadenie CE (VPN brána) väčšinou plní aj ďalšie funkcie pre VPN klientov (napr. server **DHCP** (*Dynamic Host Configuration Protocol*), doménový server **DNS** (*Domain Name Server*)). Toto riešenie všeobecne kladie vyššie nároky na autentizáciu klientov, keďže sa pripájajú kedykoľvek a odkiaľkoľvek.

4 Protokol IPsec

Protokol IPsec je komplexným súborom protokolov riešiacich šifrovanie, autentizáciu, integritu dát a proces tunelovania. Zabezpečenie je realizované na sieťovej vrstve referenčného modelu **OSI** (*Open System Interconnection*), a preto poskytuje transparentne bezpečnosť akémukoľvek prenosu, resp. ľubovoľnej sieťovej aplikácii.

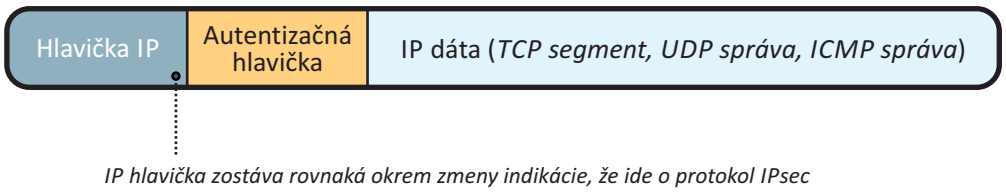
Medzi základné komponenty protokolu IPsec patria:

- bezpečnostné protokoly - **AH** (*Authentication Header*), **ESP** (*Encapsulating Security Payload*),
- protokoly pre výmenu kľúčov - **ISAKMP** (*Internet Security Association and Key Management Protocol*), **IKE** (*Internet Key Exchange*),
- pomocné databázy - **SPD** (*Security Policy Database*), **SAD** (*Security Association Database*) a
- **DOI** (*Domain Of Interpretation*) - obsahuje rôzne hodnoty ako napr. identifikátory a ukazovatele pre **SA** (*Security Association*)

Protokol IPsec podporuje dva pracovné režimy:

1. transportný režim - určený pre spojenie typu Host-to-Host

V transportnom režime je zvyčajne zašifrovaný alebo overený iba obsah daného IP paketu. Smerovacie informácie zostávajú nezmenené, pokiaľ nie je hlavička IP paketu upravená ani šifrovaná. Pri použití autentizačnej hlavičky **AH** (*Authentication Header*) nemôžu byť IP adresy preložené, pretože sa vždy stratí právo na hodnotu hash. Transportné a aplikačné vrstvy sú vždy zabezpečené hashovacou funkciou, takže nemôžu byť nijako upravované (napr. zmenou čísla portu).

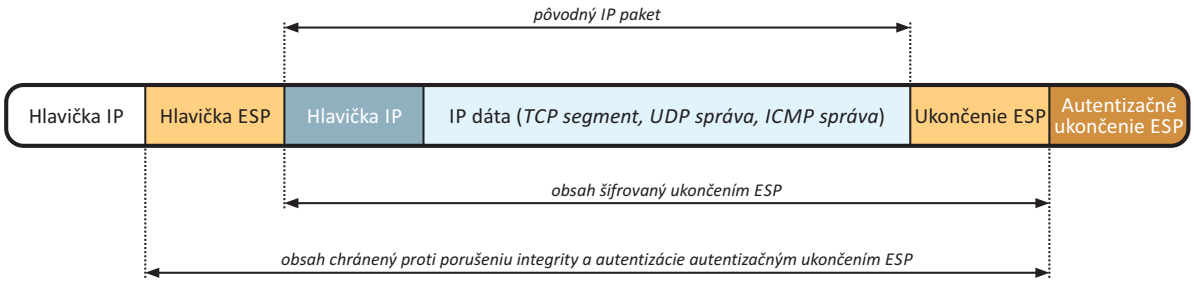


Štruktúra paketu IPsec v transportnom režime s využitím hlavičky AH

2. tunelovací režim - určený primárne pre spojenie typu Site-to-Site

V tunelovacom režime je šifrovaný alebo overovaný celý IP paket pomocou **ESP** (*Encapsulating Security Payload*). Následne je zapuzdrený do nového IP paketu s úplne novou hlavičkou. Tento režim sa používa na tvorbu sietí VPN určených na

komunikáciu medzi jednotlivými sieťami Site-to-Site (napr. medzi smerovačmi prepájajúcimi rôzne siete), Host-to-Site komunikáciu (napr. vzdialený prístup používateľa) a Host-to-Host komunikáciu (napr. súkromný chat).



Štruktúra paketu IPsec v tunelovacom režime s využitím ESP

Tunelovací režim protokolu IPsec podporuje **NAT** (*Network Address Translation*) a **PAT** (*Port Address Translation*).

Protokol IPsec neobsahuje v hlavičke žiadne pole určujúce typ režimu. Pracovný režim je nastavený podľa hodnoty poľa *Next Header* (hodnota „IP“ špecifikuje tunelovací režim, hodnoty „TCP, UDP, ICMP“ alebo čokoľvek iné identifikujú transportný režim).

Medzi výhody protokolu IPsec patrí jeho transparentnosť, tzn. nie je potrebné nijako modifikovať protokoly vyšších vrstiev, protokol IPsec môže zabezpečiť ľubovoľný protokol využívajúci protokol IP, zabezpečuje aj „staré“ protokoly, ktoré sú nezabezpečené a je široko podporovaný výrobcami **HW** (*Hardware*) a **SW** (*Software*).

K nevýhodám protokolu IPsec patrí zvýšenie systémovej réžie (overhead), nutnosť inštalácie klienta v prípade vzdialeného prístupu, sám nerieši autentizáciu používateľa, komplikácie s NAT a PAT (možný iba v tunelovacom režime) a s prenosom premávky typu multicast a broadcast.

Protokol IPsec:

- zabezpečuje premávku na sieťovej vrstve,
- je univerzálny na zabezpečenie ľubovoľnej TCP/IP premávky,
- chráni pred analýzou premávky na úrovni sieťovej vrstvy tzv. Packet Sniffing,
- je vhodný pre pevné pripojenie vzdialených používateľov,

- nepodporuje prenos multicastu a broadcastu,
- má problémy s prekladom adries (NAT a PAT) - mení sa adresné pole chránené **HMAC-SHA1** (*Hash Message Authentication Code* - *Secure Hash Algorithm*), riešením je zabaliť IPsec paket do segmentu **UDP** (*User Datagram Protocol*) -> metóda **NAT-T** (*NAT-Traversal*) a
- v prípade vzdialeného prístupu je vyžadovaná inštalácia klienta (môžu však vzniknúť problémy s kompatibilitou rôznych implementácií).

5 Výmena kľúčov pri protokole IPsec - metóda ISAKMP/IKE

Výmena kľúčov medzi klientmi pred začatím vlastnej zabezpečenej komunikácie je dôležitá hneď z niekoľkých hľadísk. Objavuje sa tu však otázka: Ako vlastne riešiť bezpečnú výmenu kľúčov? Pred vlastnou komunikáciou je nutné zaistiť:

1. dohodu o type kľúča a spôsobe jeho tvorby, t.j. stanoviť zdieľaný kľúč **PSK** (*Pre-Shared Key*)
2. autentizáciu účastníkov, t.j. vzájomné overenie identity účastníkov komunikácie
3. ochranu identity účastníkov, t.j. pasívny útočník nemá byť schopný odhaliť identitu účastníkov obyčajným sledovaním komunikácie
4. ochranu proti **DoS** (*Denial of Service*), t.j. zlomyseľný používateľ by nemal byť schopný zneužiť protokol tak, aby nútil protistranu plytvať zdrojmi (**CPU** (*Central Processing Unit*), pamäťou, kapacitou úložiska,…)

Protokol ISAKMP je definovaný odporúčaním RFC 2408. Na svoju činnosť využíva transportný protokol UDP na porte 500.

Protokol ISAKMP je všeobecným protokolom na vytváranie SA, t.j. nerieši, ako konkrétne sa majú autentizované kľúče vymeniť. To je práca protokolu IKE. Protokol ISAKMP slúži na autentizáciu komunikujúcich strán a výmenu dát pre šifrovacie kľúče.

Nejedná sa o komunikáciu typu klient - server, ale typu výzva (požiadavka) - odpoveď. Strana, ktorá chce vytvoriť nové SA, iniciuje komunikáciu protokolom ISAKMP.

Protokol IKE je flexibilný vyjednávací protokol definovaný odporúčaním RFC 2409. Umožňuje dojednanie konkrétnej metódy autentizácie, šifrovania, dĺžok kľúčov a ich bezpečnú výmenu. Pre svoju činnosť používa Diffie-Hellmanov algoritmus (D-H algoritmus).

Protokol IKE je využívaný na výmenu relačných kľúčov, tzv. Session Keys. Správy protokolu IKE sú zapuzdrené do paketov protokolu ISAKMP.

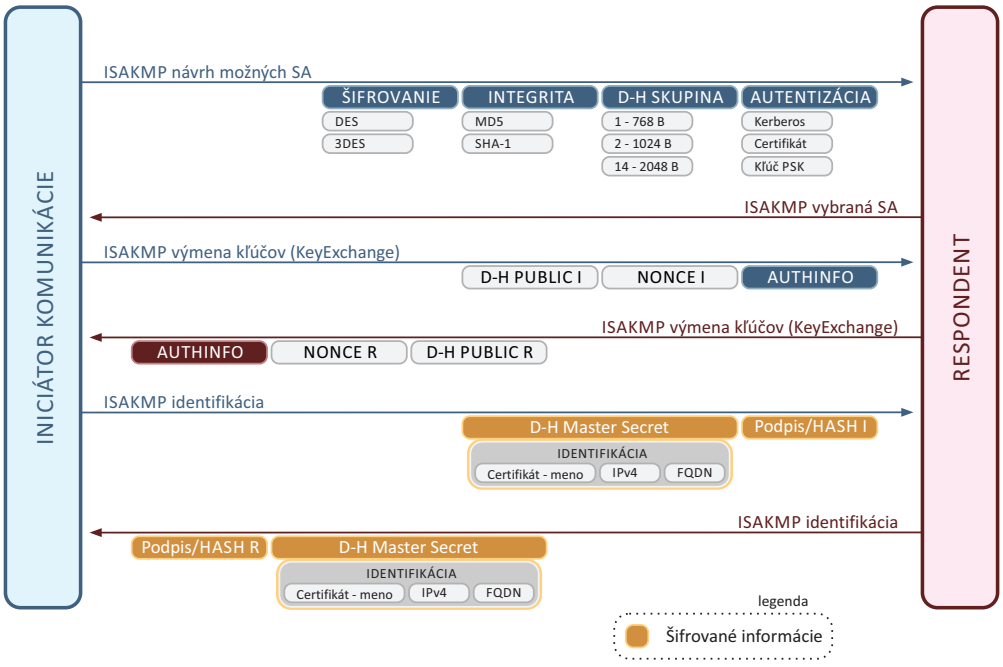
Činnosť protokolu IKE je možné rozdeliť na dve nezávislé fázy. Prvá fáza realizuje zostavenie bezpečného autentizovaného kanála medzi komunikujúcimi entitami (počítačmi). V rámci tejto fázy je chráneným spôsobom autentizovaná identita

komunikujúcich strán. Obe komunikujúce strany sa dohodnú, aké použijú SA a ako vykonajú autentizovanú výmenu zdieľaných kľúčov PSK. Následne je zostavený bezpečný tunel pre druhú fázu. Na postavenie tunela sú k dispozícii dva režimy:

- hlavný režim (Main Mode)
  - dojedná algoritmy a hashovacie funkcie, vygeneruje zdieľané tajomstvo pomocou D-H algoritmu a overí identitu protistrany. Celkovo ide o 6 správ.
- agresívny režim (Agressive Mode)
  - skráti vyjednávanie do menšieho množstva paketov. Celkovo ide o 3 správy.

Výhodou agresívneho režimu je úspora prenosového pásma a času nutného pre prenos správ.

Nevýhodou agresívneho režimu je výmena dôležitých informácií ešte pred postavením šifrovaného spojenia, čo je náchylné na odpočúvanie (Sniffing).



Procesný diagram fázy 1 protokolu IKE (hlavný režim)

V prvej fáze je možné využiť štyri rôzne spôsoby výmeny kľúča PSK:

- asymetrické šifrovanie verejným kľúčom (pôvodná verzia)
- asymetrické šifrovanie verejným kľúčom (zdokonalená verzia)
- digitálny podpis

- tajný kľúč (podľa symetrického algoritmu)

Každú variantu výmeny kľúča je možné využiť v hlavnom alebo agresívnom režime, t.j. dohromady existuje osem rôznych variant prvej fázy protokolu IKE !!! Hlavný režim musí byť implementovaný vždy, agresívny režim je voliteľný, t.j. mal by byť implementovaný.

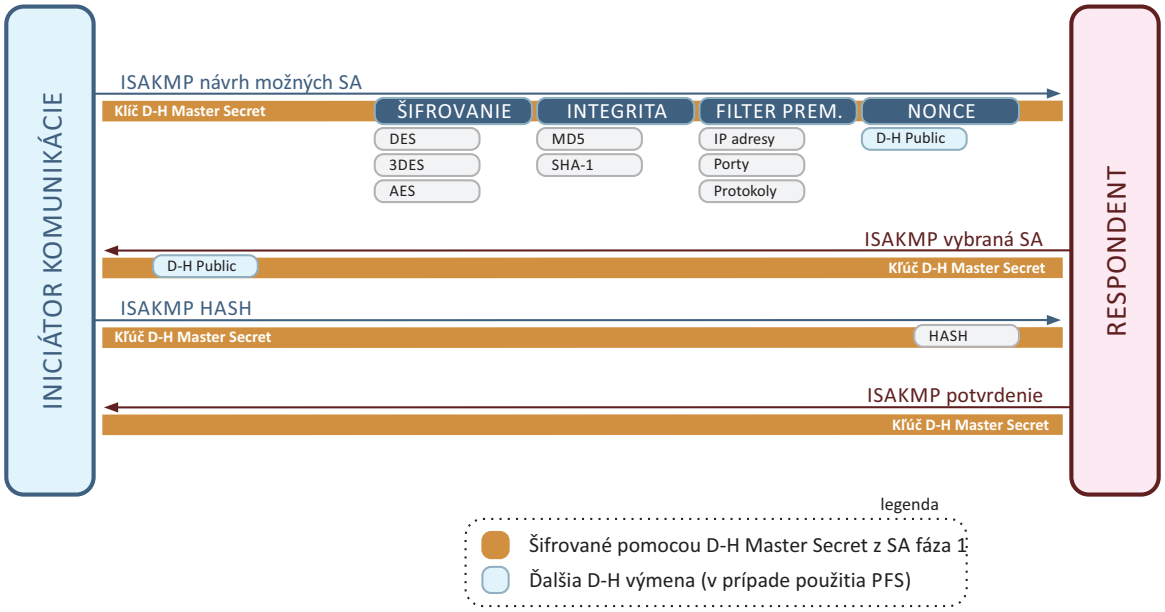
Výsledkom prvej fázy protokolu IKE je vzájomná autentizácia komunikujúcich strán, výmena zdieľaného symetrického kľúča PSK a ustanovenie IKE SA (Security Association).

Druhá fáza (Quick Mode) vytvorí SA pre IPsec reláciu, t.j. dojednávajú sa parametre SA IPsec spojenia, dochádza k zostaveniu IPsec SA pre konkrétne spojenie (napr.: FTP, telnet, a pod.), vykonáva sa periodická obnova IPsec SA, voliteľne sú realizované ďalšie D-H výmeny a špecifikuje sa ďalší kľúčový materiál pre vlastnú komunikáciu.

Táto komunikácia je od začiatku chránená pomocou algoritmov a kľúčov získaných počas prvej fázy.

Na šifrovanie bežnej komunikácie sa použije relačný kľúč (Session Key), ktorý je odvodený z D-H Master kľúča získaného z SA v hlavnom režime prvej fázy a z Nonce hodnoty SA generovanej v druhej fáze.

Využitie **PFS** (*Perfect Forward Secrecy*) označuje stav, kedy nie sú aktuálne kľúče použité na generovanie ďalších kľúčov. Ak je totiž náhodou konkrétny kľúč rozšifrovaný, t.j. prezradený, umožní to útočníkovi jednoduché prelomenie ďalších kľúčov. Ak je PFS použité, potom sa v druhej fáze znovu generuje pomocou D-H nová zdieľaná tajná informácia. Využitie PFS je bezpečnejšie, ale trochu náročnejšie na výkon a čas pri zostavovaní spojenia. Relačný kľúč sa získa z nového D-H tajného kľúča a hodnoty Nonce, ktoré sa získajú v druhej fáze budovania SA. Aplikáciou PFS je tak zabezpečené, že relačný kľúč nie je nikdy generovaný z rovnakého materiálu.



Procesný diagram fázy 2 protokolu IKE (Quick Mode)

Porovnanie so SSL/TLS - SSL relácia zodpovedá prvej fáze činnosti protokolu IKE, SSL spojenie zodpovedá druhej fáze činnosti protokolu IKE.

6 Algoritmus Diffie-Hellmann

Diffie-Hellmanov algoritmus (D-H algoritmus) je kryptografický protokol, ktorý umožňuje vytvoriť medzi komunikujúcimi stranami šifrované spojenie cez nezabezpečený kanál, a to bez nutnosti si dopredu dohodnúť šifrovací kľúč. Výsledkom algoritmu je symetrický šifrovací kľúč, ktorý môže byť následne použitý na šifrovanie zvyšnej komunikácie.

Výhodou je, že prípadný útočník odpočúvajúci komunikáciu tento kľúč nezachytí. Kľúč je totiž vytvorený všetkými účastníkmi komunikácie a nikdy nie je poslaný v otvorenej forme. Resp. tento algoritmus zaručí výmenu spoločného kľúča takým spôsobom, že ak túto komunikáciu odpočúva útočník, potom nie je schopný spoločný kľúč na základe odpočutých informácií zrekonštruovať.

Nevýhodou tohto protokolu je bezbrannosť proti útoku **MITM** (*Man in the Middle*), pretože neumožňuje autentizáciu účastníkov. Tento protokol bez kombinácie s inými metódami autentizácie je teda vhodný iba tam, kde útočník nemôže aktívne zasahovať do samotnej komunikácie.

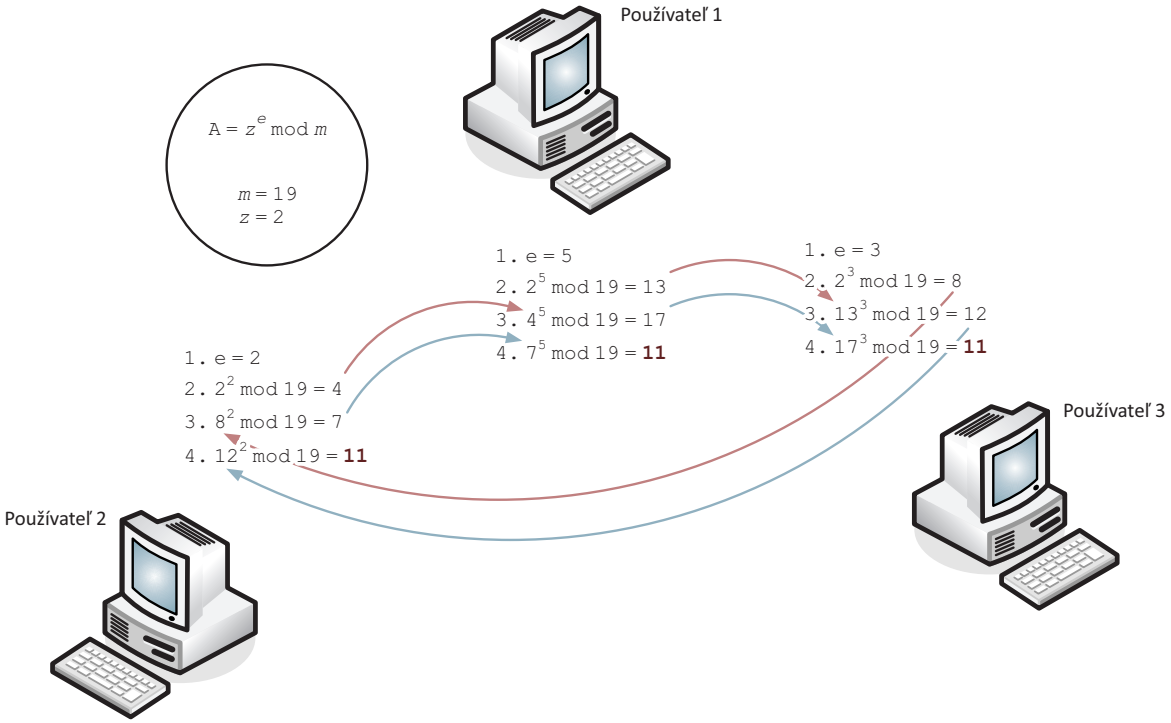
Princíp D-H algoritmu definovaný odporúčaniami RFC 2409, RFC 3526 a RFC 5114 je založený na umocňovaní čísiel $(A^B)^C = (A^C)^B$, resp. na modulárnej variante tohto vzorca $(A^B)^C|m = (A^C)^B|m$.

Veľkosť modulu potom špecifikuje typ skupiny. Obyčajne sa používajú skupiny 1, 2 a 5. Číslo skupiny udáva dĺžku kľúča - DH-1 (768 bitov), DH-2 (1024 bitov), DH-5 (1535 bitov), DH-14 (2048 bitov).

Výpočet výslednej hodnoty je veľmi jednoduchý (rýchly), ale len veľmi ťažko sa dá zistiť niektorá z hodnôt, ktorú pozná iba iný účastník. Tomuto princípu, na ktorom stojí bezpečnosť tohto algoritmu, sa hovorí problém diskrétneho logaritmu.

Komunikácia s využitím D-H algoritmu prebieha nasledujúcim spôsobom:

- Účastníci sa verejne dohovoria na použitom module *m*, resp. type skupiny a základe *z*.
- Každý z účastníkov si zvolí svoj exponent *e* (nesúdeliteľný s modulom *m*).
- Každý z účastníkov umocní modulárne základ na svoj exponent a výsledok pošle ďalšiemu účastníkovi.
- Algoritmus končí, keď je každý z pôvodných základov spracovaný každým účastníkom.



Princíp komunikácie troch účastníkov pomocou Diffie-Hellmanovho algoritmu

7 Útoky v lokálnych sieťach - príklady a riešenie

Bezpečnosť sieťových prvkov bola veľmi dlho podceňovaná a firmami odsúvaná do pozadia. V poslednom čase sa ale trend mení a veľa podnikov si uvedomuje význam a dôsledky potenciálnych hrozieb. Počet útokov zvnútra siete rapídne prevažuje počet útokov zvonka siete. Preto sa budeme venovať zabezpečeniu prístupových prepínačov (Access Switch), ku ktorým majú používatelia priamy prístup, a kde tak vzniká vysoké potenciálne riziko rôznych typov útokov.

Príklady možných útokov na prepínače:

- MAC-Address Flooding - preplnenie tabuľky **CAM** (*Content Addressable Memory*) -> prepínač sa potom chová ako obyčajný rozbočovač (HUB)
- DHCP Spoofing - podvrhnutie DHCP adresy útočníkovým DHCP serverom
- zneužitie Trunk portu - útočník má potom prístup k premávke z ďalších prenášaných **VLAN** (*Virtual LAN*)
- útoky prostredníctvom správ **CDP** (*Cisco Discovery Protocol*) - správy protokolu CDP nie sú šifrované, odosielajú sa periodicky a poskytujú detailné informácie o type zariadenia, verzii IOS, atď.
- ďalšie útoky - napr. útoky na heslá vzdialeného prístupu, DoS útoky, a pod.
- inštalácia neautorizovaných bezdrôtových prístupových bodov (Rogue AP), ktoré si zamestnanec nainštaluje, aby mal na pracovisku napr. dostupný Internet pre svoje **PDA** (*Portable Digital Assistant*), a ktorý tak kvôli svojmu nedostatočnému zabezpečeniu môže sprístupniť vnútornú sieť firmy.

Možné riešenia:

1. Port Security

Port Security je najjednoduchší spôsob zabezpečenia portov, ktorý slúži na kontrolu adries **MAC** (*Medium Access Control*) pripojených na dané porty. V prípade porušenia definovaného pravidla sa vykoná akcia podľa toho, ako bol port nastavený.

Existujú tri reakcie na narušenie bezpečnosti:

- Protect - povolené MAC adresy môžu naďalej komunikovať, komunikácia z nepovolených MAC adries je zablokovaná
- Restrict - správanie je rovnaké ako v režime Protect, ale navyše sa vygeneruje chybové hlásenie do logu zariadenia a ak je nakonfigurovaný protokol **SNMP** (*Simple Network Management Protocol*), odošle sa SNMP trap správa na SNMP server

- Shutdown - všetka komunikácia (aj z povolených adries) je zablokovaná. Port je prepnutý do špeciálneho stavu Error-Disable, kedy je nutný zásah správcu a opätovné manuálne zapnutie portu.

Takto nastaveným spôsobom zabezpečenia previažeme daný fyzický port s pevne pridelenou virtuálnou sieťou (VLAN). Tým vznikne pevná väzba skupiny MAC adries a jednej VLAN na daný prístupový port.

Pre rozsiahle podnikové siete nie je predchádzajúce riešenie dostatočné a používajú sa komplexné integrované riešenia ako sú napr. riešenia založené na protokole (odporúčaní) IEEE 802.1X.

Zabezpečenie Port Security sa na Cisco prepínači vykoná nasledovne. Najskôr je potrebné na zvolenom porte zapnúť funkciu Port-Security pomocou príkazu „switchport port-security“. Prednastavenou hodnotou je 1, čo znamená, že k danému portu je možné pripojiť iba jedno zariadenie. Túto hodnotu, t.j. povolený počet MAC adries, ktoré môžu na daný port pristupovať, je možné zmeniť. Adresy sa prepínač môže tiež učiť buď dynamicky, alebo je možné ich nastaviť ručne. Ručné nastavenie sa realizuje pomocou príkazu „switchport port-security mac-address MAC-ADRESA“. Tento príkaz je možné rozšíriť parametrom „sticky“, ktorý zabezpečí, aby sa dynamicky naučená MAC adresa uložila do konfigurácie zariadenia. Ako už bolo uvedené skôr, teraz je potrebné nastaviť akciu, ktorú prepínač vykoná v prípade porušenia pravidiel pomocou príkazu „switchport port-security violation“. Všetko je možné názorne vidieť na nasledujúcom výpise.

```
Switch(config)#interface fastethernet 0/1
switch(config-if)#switchport mode access //nastaví port do príslušného režimu
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum POČET_ADRIES
Switch(config-if)#switchport port-security mac-address MAC_ADRESA_ZARIADENIA //manuálne vloženie adresy
Switch(config-if)#switchport port-security mac-address sticky //dynamické učenie MAC adresy
Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Ukážka konfigurácie Port Security na prepínači Cisco

2. DHCP Snooping

DHCP Spoofing je druh sieťového útoku, kedy útočník v lokálnej sieti falšuje správy protokolu DHCP (napr. spustením vlastného DHCP servera s pozmenenými sieťovými parametrami) s cieľom podvrhnúť obete napr. inú predvolenú bránu. Tým môže útočník docieliť presmerovanie premávky od obete na svoj počítač. Následne je potom schopný odpočúvať všetku odchádzajúcu premávku od obete.

Iným typom útoku na DHCP server je vyčerpanie adresných rozsahov DHCP servera (DHCP Starvation). V tomto prípade útočník generuje veľké množstvo sfalšovaných žiadostí o pridelenie adresy, čím dôjde k ich vyčerpaniu.

DHCP Snooping je označenie postupov, ktorými je možné brániť sa proti DHCP Spoofingu. Konfiguruje sa na prepínačoch, ktoré sú priamo pripojené ku koncovým staniciam (tzv. prístupové prepínače - Access Switches). Celý proces obrany proti DHCP spoofingu spočíva v odpočúvaní DHCP požiadaviek na portoch prepínača a blokovaní odosielaných podvrhnutých odpovedí žiadajúcim staniciam. Tým je vplyv útočníkovho podvrhnutého DHCP servera eliminovaný. Odosielanie odpovedí z DHCP servera je povolené iba na dôveryhodných (Trusted) portoch prepínačov. To, ktorý port je „dôveryhodný“, nastavuje ručne administrátor a obvykle to je iba jeden port, ku ktorému je pripojený pravý DHCP server. Cisco prepínače umožňujú nastaviť DHCP Snooping pre ľubovoľný počet VLAN, umožnujú nastaviť dôveryhodné porty, na ktorých sú pripojené DHCP servery, a umožňujú obmedziť počet požiadaviek **PPS** (*Packet Per Second*) na DHCP server a zabrániť tak jeho preťaženiu. Ukážka konfigurácie DHCP Snoopingu je na nasledujúcom výpise.

```
Switch(config)#ip dhcp snooping
switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping vlan JEDNA_VLAN_ALEBO_ROZSAH
Switch(config)#interface fastethernet ČÍSLO
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate PPS //vypne option 82 - používa sa pre DHCP Relay
```

Ukážka konfigurácie DHCP Snoopingu na prepínači Cisco

Zapnutím funkcie DHCP Snooping Binding Database (viď nasledujúci výpis) je možné sa navyše chrániť aj pred ďalšími typmi útokov v lokálnych sieťach. Po zapnutí tejto funkcie si totiž prepínač vytvára tabuľku obsahujúcu väzby medzi MAC adresou stanice, IP adresou, dobou zapožičania IP adresy, portom z ktorého komunikuje, virtuálnou sieťou (VLAN) v ktorej sa nachádza a spôsobom akým bola položka do tabuľky pridaná (ručne alebo automaticky). Tieto informácie potom využíva funkcia **DAI** (*Dynamic ARP Inspection*), ktorá chráni pred útokmi typu ARP Cache Poisoning.

```
Switch(config)#ip dhcp snooping database flash:/dhcpbind.txt
```

Zapnutie funkcie DHCP Snooping Binding Database na prepínači Cisco

3. Dynamic ARP Inspection

ARP Cache Poisoning je veľmi jednoducho realizovateľný a ťažko odhaliteľný útok spočívajúci vo falšovaní odpovedí správ protokolu **ARP** (*Address Resolution Protocol*). Protokol ARP zabezpečuje zisťovanie väzieb IP adresa - MAC adresa v lokálnej sieti. Útočník pomocou sfalšovaných odpovedí dokáže spôsobiť presmerovanie komunikácie napadnutého PC na útočníka. Následne potom môže odpočúvať kompletnú komunikáciu obete s ostatnými stanicami v sieti.

Tento útok je možné detekovať (a zabrániť mu) priamo na prepínači, ktorý podporuje funkciu DAI.

Útok je možné jednoducho realizovať na PC napr. nástrojom Cain&Abel (www.oxid.it) alebo Ettercap (http://ettercap.sourceforge.net/).

Funkcia DAI je spôsob obrany proti ARP Cache Poisoningu. Využíva sa tabuľka vytvorená pomocou DHCP Snoopingu. Ak na prepínač príde ARP paket z dôveryhodného (trusted) portu, je poslaný ďalej. Ak ale na prepínač príde ARP paket z nedôveryhodného (untrusted) portu, je ďalej analyzovaný. Ak sa jedná o správu ARP Request, sieťový procesor v pakete zistí, či MAC a IP adresa počítača žiadajúceho o preklad patria k sebe. Ak áno, je paket preposlaný ďalej do siete. V opačnom prípade je zahodený. V prípade, že sa jedná o odpoveď na požiadavku (ARP Reply), tak sa navyše kontroluje, či k sebe patrí MAC a IP adresa počítača odpovedajúceho na správu ARP Request. Kombinácie IP a MAC adries sú brané z databázy vytvorenej funkciou DHCP Snooping. Príkaz na zapnutie DAI je na nasledujúcom výpise.

```
Switch(config)#ip arp inspection vlan Vlan_ID //zapnutie funkcie DAI
Switch#show ip arp inspection vlan Vlan_ID //zobrazenie sledovaných VLAN
```

Zapnutie funkcie DAI na prepínači Cisco

Na ďalšom výpise je príkaz na vypnutie kontroly DAI na dôveryhodných rozhraniach.

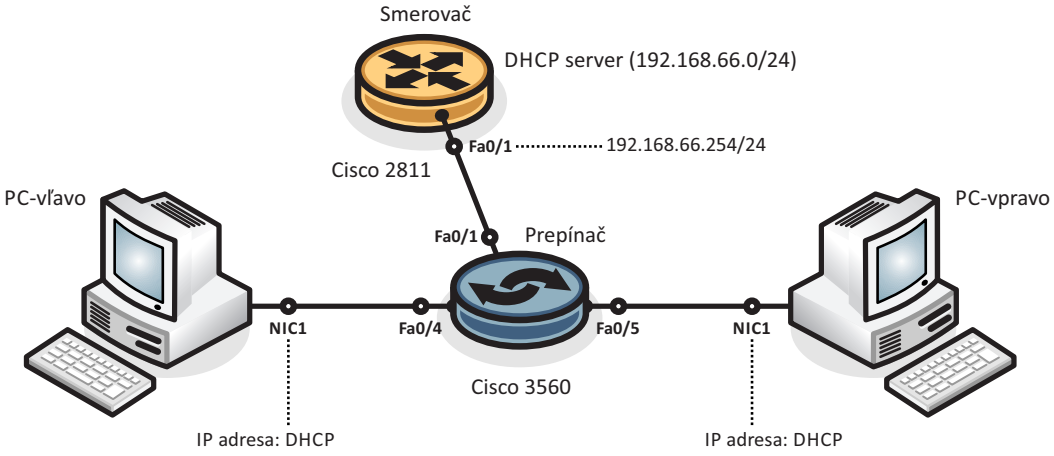
```
Switch(config)#interface fastethernet 0/1
Switch(confid-if)#ip arp inspection trust //označenie rozhrania ako dôveryhodného
```

Vypnutie kontroly DAI na dôveryhodnom rozhraní prepínača Cisco

IP Source Guard má podobnú funkciu ako DAI, ale namiesto sfalšovaných MAC adries sa detekujú sfalšované zdrojové IP adresy. Umožňuje blokovanie nepovolených IP adries na portoch. Nastavuje sa na konkrétny port. Táto funkcia tiež využíva DHCP Snooping Binding Database. Príkaz pre zapnutie funkcie IP Source Guard je na nasledujúcom výpise.

```
Switch(config)#interface MENO_ROZHRANIA
Switch(confid-if)#ip verify source port-security //filtruje podľa zdrojovej IP a MAC adresy
```

Zapnutie funkcie IP Source Guard na prepínači Cisco



Príklad zapojenia topológie úlohy na simuláciu útokov v lokálnej sieti

8 Budovanie VPN pomocou IPsec - príklady a riešenia

Vzdialený prístup je dnes úplne neoddiskutovateľnou súčasťou správy sieťových zariadení ľubovoľne veľkej lokálnej siete, a to predovšetkým s ohľadom na nutnosť pohotového zásahu správcu siete v prípade neočakávanej situácie a v spojitosti so znížením celkových nákladov na takú akciu. Stačí teda, aby bol správca siete pripojený k Internetu a môže tak vzdialene monitorovať a prípadne rekonfigurovať jednotlivé sieťové prvky.

V minulosti sa na vzdialený prístup na správu sieťových prvkov používal protokol Telnet. Ten ale nijako nechránil vlastnú komunikáciu, takže bolo relatívne jednoduché premávku odpočúvať a zachytiť prihlasovacie informácie. Rozšírením prístupu do Internetu teda vznikla potreba takého protokolu, ktorý by všetku komunikáciu zabezpečil pred potenciálnymi útočníkmi. Vznikol tak protokol **SSH** (*Secure Shell*), ktorý štandardne komunikuje transportným protokolom TCP na porte 22, poskytuje zabezpečenú autentizáciu oboch strán, zabezpečuje ich integritu, transparentné šifrovanie prenášaných dát a voliteľne aj bezstratovú kompresiu (viac informácií je možné nájsť v odporúčaní RFC 4252 [https://www.ietf.org/rfc/rfc4252.txt]).

Potreby veľkých spoločností vzájomne bezpečne prepojiť oddelené pobočky dali vzniknúť virtuálnym privátnym sieťam zabezpečujúcich prepojenie dvoch a viac sieťových zariadení v prostredí nedôveryhodnej verejnej siete Internet. Ďalším dôvodom bola aj cena za prepojenie. V prípade využitia vyhradených okruhov by totiž boli náklady neporovnateľne vyššie. VPN je možné vo všeobecnosti deliť podľa vrstvy, na ktorej pracujú z pohľadu referenčného modelu OSI. Najpoužívanejšie VPN technológie prehľadne uvádza nasledujúca tabuľka.

Typ VPN	Vrstva RM OSI	Opis
Frame Relay	linková	Vyžaduje homogénne prostredie Frame Relay. Spoľahlivejšie, bezpečnejšie, ale aj drahšie v porovnaní s IP VPN.
ATM	linková	Vyžaduje homogénne prostredie ATM. Podobne ako FR poskytuje virtuálne kanály s dohodnutými parametrami.
L2TP/PPTP	linková	L2TP ako náhrada PPTP, ktorý odvádza kľúče z hesla používateľa (potenciálna slabina). PPTP využíva na šifrovanie **MPPE** (*Microsoft Point-to-Point Encryption*) a L2TP IPsec. Definované sú odporúčaniami RFC 2637 [https://www.ietf.org/rfc/rfc2637.txt] a RFC 2661 [https://www.ietf.org/rfc/rfc2661.txt] .
BGP/MPLS	linková/sieťová	Slúži na bezpečnú výmenu informácií medzi hraničnými smerovačmi **BGP** (*Border Gateway Protocol*) v chrbticových sieťach pomocou MPLS tunelov. Definovaný odporúčaním RFC 4364 [https://www.ietf.org/rfc/rfc4364.txt] a ďalšími.
IPsec	sieťová	Bezpečnostné rozšírenie klasického protokolu IP. Šifrovaním každého paketu vzniká transparentný zabezpečený prenos (tzv. tunel). Definované niekoľkými RFC odporúčaniami.
SSL/TLS	transportná a vyššie	**SSL** (*Secure Sockets Layer*) je technológia nezávislá (transparentná) od použitej technológie sieťovej vrstvy. Od SSL je následne odvodený protokol **TLS** (*Transport Layer Security*) definovaný v odporúčaní RFC 5246 [https://www.ietf.org/rfc/rfc5246.txt] .

Najčastejším spôsobom prepojenia pobočiek je dnes spojenie pomocou protokolu IPsec VPN, kedy je postavený šifrovaný jednosmerný logický (virtuálny) kanál, tzv. SA medzi smerovačmi/firewallmi umiestnenými na okraji lokálnej siete.

Pre duplexnú (obojsmernú) komunikáciu je teda potrebné zriadiť dve nezávislé jednosmerné SA.

Protokol IPsec je povinnou súčasťou IPv6 a dodatočne bol implementovaný aj do IPv4.

Dokáže pracovať v dvoch režimoch (tunelovacom - plne zapuzdrený pôvodný IP paket do nového IP paketu, a transportnom - hlavička protokolu IPsec je vložená medzi pôvodnú IP hlavičku a hlavičku protokolu vyššej vrstvy) a využíva pre zabezpečenie dva protokoly AH a ESP. Obidva protokoly podporujú buď nulové šifrovanie (NULL), alebo algoritmy **DES** (*Data Encryption Standard*), **3DES**

(*Triple DES*), **AES** (*Advanced Encryption Standard*) a Blowfish. Protokol IPsec je definovaný mnohými odporúčaniami **RFC** (**Request For Comments**), ale najzákladnejšie je odporúčanie RFC 4301 [https://www.ietf.org/rfc/rfc4301.txt] . Na zabezpečenie integrity sú použité HMAC algoritmy **MD5** (*Message-Digest 5*) a SHA-1.

8.1 Príklad konfigurácie IPsec VPN na zariadeniach firmy Cisco

V prvej fáze je potrebné nastaviť politiky IKE protokolu ISAKMP. Politika IKE slúži protokolu IPsec na zriadenie SA. Pre ich zriadenie je však potrebné dojednať zdieľaný kľúč PSK medzi obomi stranami, od ktorého budú odvodené vlastné šifrovacie kľúče. Na výmenu kľúčov sa obyčajne využíva mechanizmus DH. Protokol ISAKMP používa transportný protokol UDP na porte 500. Príklad konfigurácie politík (typ autentizácie, šifrovací a hashovací algoritmus, DH skupiny a doby životnosti SA v sekundách) je možné vidieť na nasledujúcom obrázku.

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption {des | 3des | aes 128 | aes 192 | aes 256}
Router(config-isakmp)#hash {md5 | sha}
Router(config-isakmp)#group {1 | 2 | 5}
Router(config-isakmp)#lifetime 86400
```

Konfigurácia IKE politík protokolu ISAKMP na smerovači Cisco

Ďalej je potrebné nastaviť zdieľaný kľúč PSK, ktorým sa strany vzájomne autentizujú. V rámci príkazu je taktiež definovaná IP adresa druhej strany. Príklad je opäť uvedený na nasledujúcom obrázku.

```
Router(config)#crypto isakmp key TUjeTENtajnyKLUC address 192.168.0.2
```

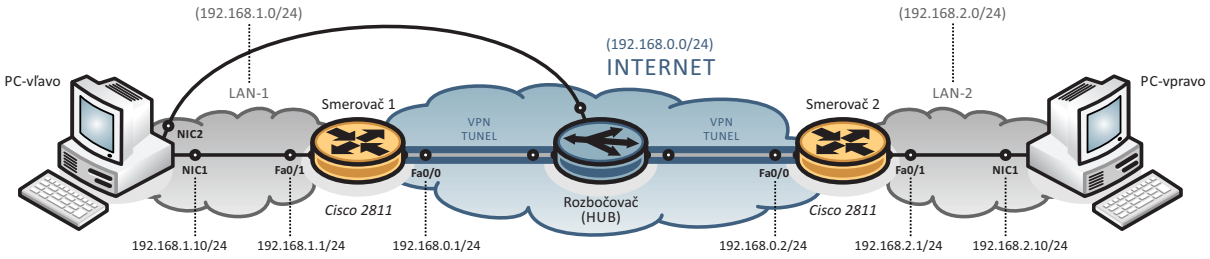
Konfigurácia zdieľaného kľúča PSK na smerovači Cisco

V druhé fáze sa konfigurujú vlastné nastavenia protokolu IPsec. Definuje sa množina použitých algoritmov na šifrovanie a zabezpečenie integrity dát, tzv. **TS** (*Transform Set*). Ako príklad použijeme protokol ESP v kombinácii s HMAC algoritmom SHA-1. Smerovač začne príslušnú premávku šifrovať až vtedy, ak má nastavenú tzv. zaujímavú premávku (Interresting Traffic) pomocou klasického firewallového pravidla **ACL** (*Access List*). Takto definované parametre spojí objekt, tzv. kryptomapa (Crypto Map), ktorá je spolu s ďalšími dodatočnými parametrami ako predvolená adresa druhej strany (všeobecne je možné definovať viacej adries) a nepovinnými parametrami ako DH skupina, doba životnosti IPsec SA (v sekundách) následne aplikovaná na príslušné rozhranie **WAN** (*Wide Area Network*). Všetko je vidieť na príklade v nasledujúcom obrázku.

```
Router(config)#crypto ipsec transform-set ESP-AES esp-aes 256 esp-sha-hmac
Router(config)#ip access-list extended ZAUJIMAVA-PREMAVKA
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#crypto map IPSEC-MAPA 1 ipsec-isakmp
Router(config-crypto-map)#match address ZAUJIMAVA-PREMAVKA
Router(config-crypto-map)#set peer 192.168.0.2 default
Router(config-crypto-map)#set transform-set ESP-AES
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 86400
Router(config)#interface fastethernet 0/0
Router(config-if)#crypto map IPSEC-MAPA
```

Konfigurácia protokolu IPsec VPN na smerovači Cisco

Analogicky je nutné obe IPsec fázy nastaviť aj na druhej komunikujúcej strane (smerovači) !!!



Príklad zapojenia topológie úlohy na IPsec VPN

9 Budovanie VPN pomocou SSL/TLS - príklady a riešenia

Pomocou VPN nie je možné len prepájať jednotlivé pobočky, ale tiež je možné kontrolovane sprístupňovať klientom zdroje umiestnené v neprístupnej časti podnikovej siete pomocou protokolu **HTTPS** (*HyperText Transfer Protocol for Secure*) - protokol **HTTP** (*HyperText Transfer Protocol*) s podporou SSL/TLS. Klient sa pripojí pomocou bežného webového prehliadača podporujúceho SSL/TLS na vstupnú webovú stránku, kde zadá svoje prihlasovacie údaje. V prípade, že sú správne, je mu sprístupnená stránka so zdieľanými sieťovými zdrojmi. Akékoľvek spojenie je pritom zabezpečené pomocou SSL/TLS.

Prístup SSL VPN rieši tiež niektoré nevýhody klasickej IPsec VPN. IPsec VPN má problémy pri prechode cez NAT. To je síce možné obísť mechanizmom NAT-T, ktorý spočíva v zabalení paketov IPsec resp. ESP paketov do datagramov UDP, avšak to zvyšuje celkovú réžiu protokolu. Ďalšou nevýhodou je v prípade vzdialeného prístupu k VPN nutnosť špeciálneho programového vybavenia na strane účastníka. Implementácia IPsec klientov rôznych výrobcov tiež nemusí byť vzájomne kompatibilná, tunel sa nemusí dať zriadiť kvôli bezpečnostným pravidlám v cudzích sieťach (napr. filtrovaním odchádzajúcej premávky, použitím proxy serverov), …

Mnohým týmto problémom je možné sa vyhnúť použitím VPN využívajúcich protokol SSL/TLS. Tento VPN prístup je označovaný ako SSL VPN alebo tiež Clientless VPN, pretože používateľ nepotrebuje špeciálne programové vybavenie na prístup do VPN, resp. využije bežný webový prehliadač s podporou protokolu HTTPS.

Termínom SSL VPN je často označovaný rad vzájomne nekompatibilných technológií. Všetky sú postavené na rovnakej základnej myšlienke a tou je využitie asymetrickej kryptografie a knižníc SSL/TLS pre zabezpečenú komunikáciu. Technológia protokolov rodiny SSL/TLS je dnes značne využívaná pri šifrovanom prístupe k webovému serveru schémou HTTPS.

Cieľom SSL VPN je vytvorenie transparentného šifrovaného tunelu založenom na protokole SSL/TLS. Vzhľadom na prítomnosť SSL v bežných webových prehliadačoch nie je nutné na dosiahnutie väčšiny ponúkanej funkčnosti inštalovať na klientske počítače žiadny špeciálny klientsky software. Na rozšírenie možností SSL VPN riešení sú ďalej používané malé aplikácie v podobe Java appletov alebo ActiveX komponentov. Práve bohatosť nadštandardnej výbavy významne ovplyvňuje úžitkovú hodnotu implementácií SSL VPN od rôznych výrobcov.

Základná funkcionalita SSL VPN spočíva v zabezpečenom prístupe k vnútorným informačným zdrojom organizácie. Je vytvorený šifrovaný SSL tunel medzi SSL VPN bránou a webovým prehliadačom na klientskom počítači. V tejto podobe teda môže SSL VPN veľmi dobre poslúžiť ako implementačne jednoduchý spôsob, ako v rámci Internetu zabezpečene sprístupniť webové portály informačných systémov organizácie. Ďalšou bežnou vlastnosťou SSL VPN riešenia je možnosť s pomocou webového rozhrania na bráne pracovať so súbormi zdieľanými v rámci vnútornej

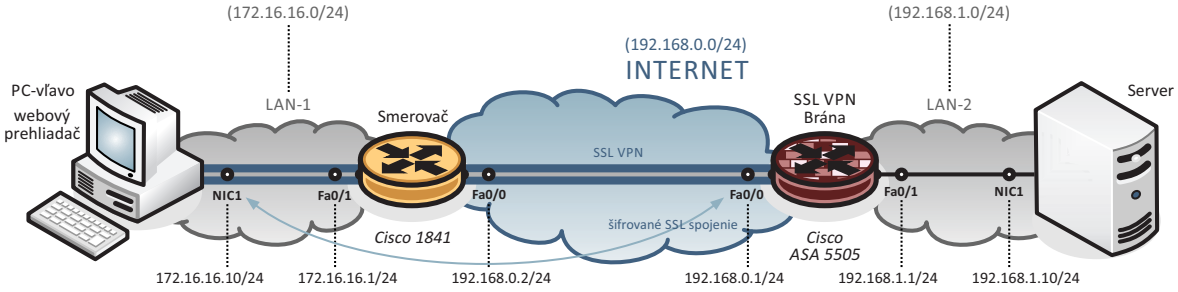
siete pomocou **CIFS** (*Common Internet File System*), čiže zdieľanie súborov novších systémov Windows alebo unixového **NFS** (*Network File System*).

9.1 Typy prístupov SSL VPN

1. Clientless VPN

V tomto režime vzdialený používateľ pristupuje do internej siete použitím internetového prehliadača (FireFox, Chrome, Internet Explorer, Edge, Safari,…) na klientskom počítači (viď obrázok nižšie). Vzdialený používateľ má dostupné aplikácie:

- internetové prehliadanie (používajúce HTTPS) - stránka portálu poskytuje zoznam URL webových serverov, ktoré môže vzdialený používateľ prehliadať
- zdieľanie súborov (používajúce súborový systém CIFS) - stránka portálu poskytuje zoznam súborových serverov, kde môže vzdialený používateľ:
  - prehliadať a sťahovať zdieľané súbory,
  - premenovávať a mazať súbory,
  - nahrávať a sťahovať súbory a
  - vytvárať a premenovávať nové súbory a adresáre.



Príklad zapojenia topológie úlohy na IPsec VPN

2. ThinClient

Zásadnou podmienkou je, že počítač vzdialeného používateľa musí tento spôsob komunikácie podporovať. Vzdialený používateľ si zo stránky portálu stiahne Java applet. Tento applet funguje na klientovi ako TCP proxy server pre služby, ktoré sú nakonfigurované na stránke portálu. Tento typ umožňuje vzdialený prístup ku štandardným aplikáciám založených na TCP ako sú **POP3** (*Post Office Protocol 3*), **SMTP** (*Simple Mail Transfer Protocol*), **IMAP** (*Internet Message Access Protocol*) alebo Telnet, ako aj prístup do podnikových informačných systémov typu **SAP** (*System Application Products*). Klientske aplikácie musia byť nakonfigurované tak, aby komunikovali cez TCP spojenie na známy server a port. Ako adresa servera obvykle slúži loopback (127.0.0.1), kde je komunikácia zachytávaná TCP proxy serverom a ďalej smerovaná do SSL tunela.

3. Tunnel

V tomto režime má vzdialený používateľ najväčšie možnosti. Používateľ si po prihlásení na VPN server stiahne (ručne alebo automaticky) plnohodnotného SSL VPN klienta. V prípade technológie Cisco ide o „Cisco AnyConnect VPN klient“. Tento program vytvorí virtuálne sieťové rozhranie, ktoré poskytuje prístup k sieťovej vrstve rôznym aplikáciám. Tento typ SSL VPN poskytuje možnosti porovnateľné s VPN založenej na technológii IPsec (v režime vzdialeného prístupu - Remote Access). Po ukončení spojenia sa Cisco AnyConnect VPN klient odstráni z klientskej stanice alebo môže zostať na stanici nainštalovaný.

Klasické SSL VPN nie je možné použiť na vytváranie Site-to-Site VPN, používajú sa väčšinou ako Remote-Access VPN. Výnimkou z tohto pravidla je projekt OpenVPN, ktorý umožňuje vytvárať Site-to-Site VPN zabezpečené pomocou SSL/TLS.

10 Elektronický podpis

Dôvodov pre zavedenie elektronického podpisu je hneď niekoľko. Jednak vznikla nutnosť zavedenia ekvivalentu ku klasickému podpisu, za druhé dnes vzniká veľký počet dokumentov v elektronickej podobe, resp. niektoré dáta dokonca existujú iba v digitálnej podobe a predovšetkým svojou podstatou výrazne obmedzujú ich jednoduché falšovanie.

Všeobecne je pri elektronickom podpise nutné zaistiť identifikáciu podpisujúcej osoby/subjektu, neporušenosť doručeného dokumentu (dátovú integritu), nepopierateľnosť a právnu akceptovateľnosť.

Pri elektronicky podpísanom dokumente môžeme ďalej vyžadovať utajenie vlastného obsahu správy (t.j. šifrovanie) a zistenie, či dokument existoval v konkrétnom čase (t.j. časová pečiatka).

Čo je to vlastne elektronický podpis? Definícia elektronického podpisu vychádza z nariadenia Európskeho parlamentu a Rady EU č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom európskom trhu (v skratke **eIDAS** (*electronic IDentification, Authentication and trust Services*)).

Nariadenie eIDAS definuje v čl. 3 odst. 10 elektronický podpis ako údaje v elektronickej podobe, ktoré sú pripojené k dátovej správe alebo sú s ňou logicky spojené. Elektronický podpis teda slúži ako metóda jednoznačného overenia totožnosti podpísanej osoby vo vzťahu k dátovej správe.

Tejto veľmi všeobecnej definícii vyhovuje aj podpis obyčajného e-mailu vo forme textu.

Elektronický podpis má hneď niekoľko možných variant:

- elektronický podpis,
- zaručený elektronický podpis,
- uznávaný elektronický podpis a
- kvalifikovaný elektronický podpis.

Pojem uznávaný elektronický podpis je české špecifikum (do 09/2018). Ide o zaručený elektronický podpis založený na kvalifikovanom certifikáte. Je teda použiteľný na komunikáciu s orgánom verejnej moci **OVM** (avšak iba v ČR!) a nie je tu vyžadovaná podmienka na zabezpečené HW úložisko. Pri kvalifikovanom elektronickom podpise musia byť kľúče naopak uložené na „bezpečnom“ prostriedku.

V spojitosti s elektronickým podpisom je vhodné zmieniť ešte pojem digitálny podpis. Digitálny podpis využíva prostriedky asymetrickej kryptografie. Ide teda o konkrétne technické riešenie elektronického podpisu.

Digitálne podpisovanie chápeme dnes ako bezpečnostne najlepší spôsob realizácie elektronického podpisovania.

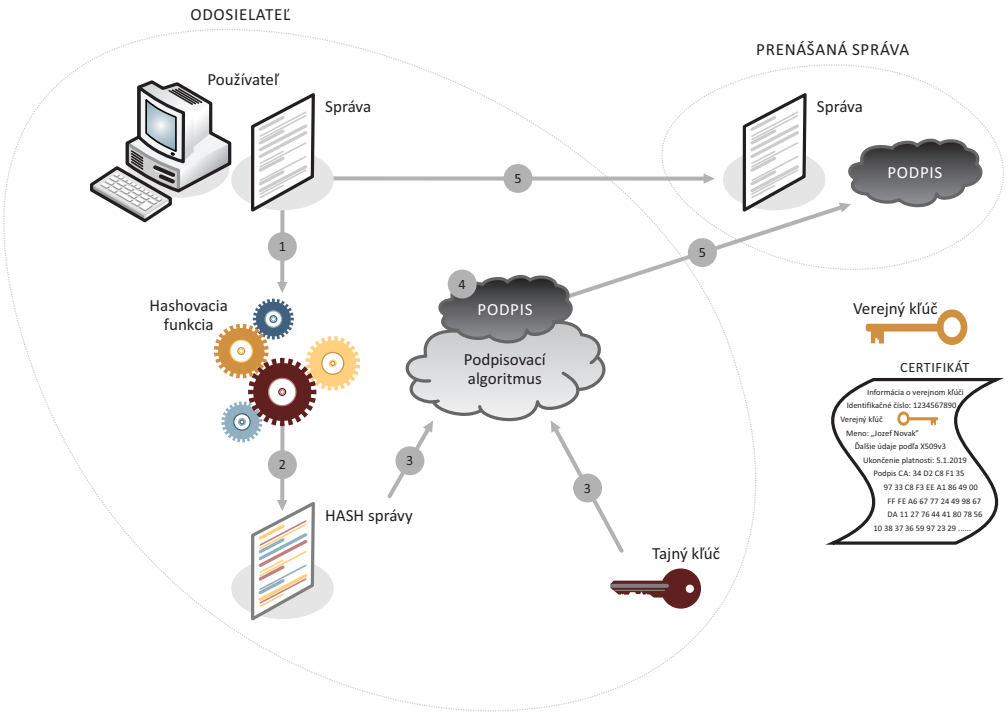
Pojem elektronický podpis je v kontexte digitálneho podpisu pojmom všeobecnejším, je teda technologicky neutrálny. Zahŕňa v sebe okrem digitálneho podpisu aj všetky ostatné metódy zabezpečujúce požadované vlastnosti (napr. biometrické metódy). Z tohto dôvodu je použiteľný aj pre legislatívne dokumenty.

1. Digitálny podpis je pojem kryptologický, resp. matematický.
2. Elektronický podpis je pojem najmä právny a normotvorný.
3. Samotná definícia elektronického podpisu stanovuje požiadavky ale nerieši, ako ich dosiahnuť.
4. Nástroje pre digitálny podpis sa naopak plne sústredia na plnenie stanovených požiadaviek.

10.1 Zaručený elektronický podpis

Z kryptografického hľadiska je elektronický podpis chápaný ako sústava čiastkových kryptografických funkcií zabezpečujúcich identifikáciu, autentizáciu, integritu a nepopierateľnosť. Matematicky je elektronický podpis svojim vyjadrením iba jedno veľké číslo.

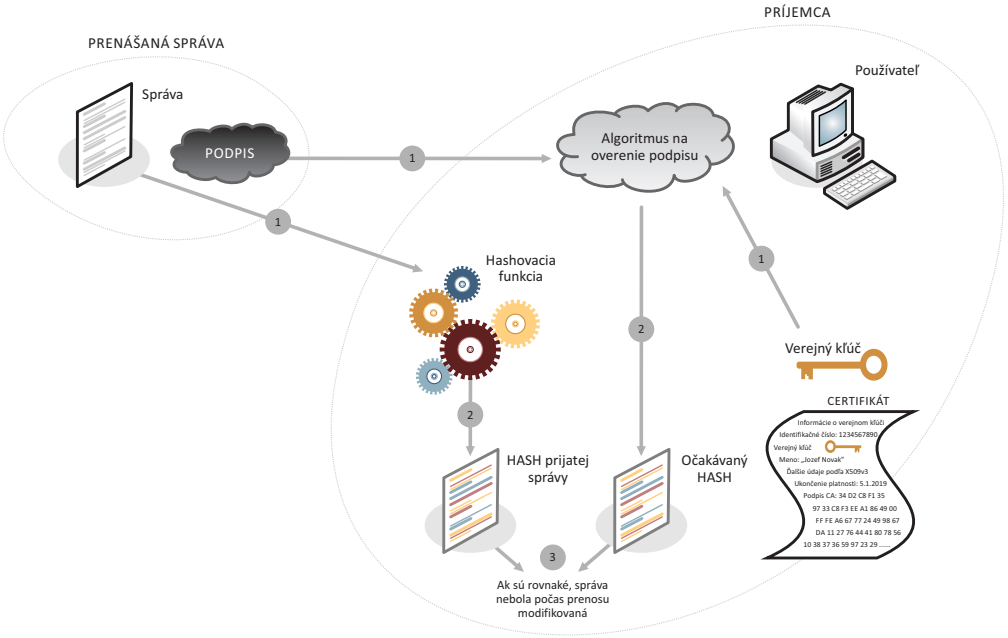
Na nasledujúcom obrázku je znázornený proces vytvorenia zaručeného elektronického podpisu. Čísla v obrázku indikujú jednotlivé kroky procesu tvorby zaručeného elektronického podpisu.



Proces vytvorenia zaručeného elektronického podpisu

Elektronicky je možné podpísať ľubovoľné digitálne dáta ako je napr. text (PDF, TXT, DOCX, RTF, XLSX,…), obrázok (BMP, JPG, GIF, PNG,…), audio (WAV, MP3, FLAC,…), video (AVI, MPG,…), spustiteľné súbory (EXE, COM,…) a ďalšie. Vo svojej podstate teda čokoľvek.

Na nasledujúcom obrázku je znázornený proces overenia zaručeného elektronického podpisu. Čísla v obrázku indikujú jednotlivé kroky procesu overenia zaručeného elektronického podpisu.



Proces overenia zaručeného elektronického podpisu

+

Zaručený elektronický podpis zabezpečuje integritu prenášaných správ a dokumentov, identifikáciu komunikujúcich strán, autentizáciu komunikujúcich strán (t.j. overenie ich identifikácie) a nepopierateľnosť, resp. neodmietnuteľnosť.

−

Zaručený elektronický podpis naopak nezabezpečuje právnu akceptovateľnosť podpísaných dokumentov.

$E=m \cdot c^2$

Nariadenie eIDAS definuje zaručený elektronický podpis v čl. 3 odst. 11 ako podpis, ktorý spĺňa podmienky uvedené v čl. 26:

1. Je jednoznačne spojený s podpisujúcou osobou.
2. Umožňuje identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe.
3. Bol vytvorený a pripojený k dátovej správe pomocou prostriedkov, ktoré podpisujúca osoba môže udržať pod svojou výhradnou kontrolou.
4. Je k dátovej správe, ku ktorej sa vzťahuje, pripojený takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dát.

10.2 Kvalifikovaný elektronický podpis

Nariadenie eIDAS definuje kvalifikovaný elektronický podpis v čl. 3 odst. 12 ako zaručený elektronický podpis, ktorý je vytvorený kvalifikovaným prostriedkom pre vytváranie elektronických podpisov, a ktorý je založený na kvalifikovanom certifikáte pre elektronické podpisy.

Má rovnakú platnosť ako vlastnoručný podpis.

Kvalifikovaný certifikát je definovaný nariadením eIDAS v čl. 3 odst. 15 ako certifikát pre elektronický podpis, ktorý je vydaný kvalifikovaným poskytovateľom služieb vytvárajúcim dôveryhodné certifikáty a spĺňa požiadavky stanovené v prílohe I daného nariadenia.

Technicky je kvalifikovaný certifikát rovnaký ako ľubovoľný „bežný“ certifikát.

10.3 Elektronická pečať

Technologicky ide o to isté ako v prípade zaručeného elektronického podpisu. Rozdiel je v oblasti jej využitia, ktorá je zameraná na právnu rovinu.

Elektronický podpis používa výhradne fyzická osoba, elektronická pečať môže byť využitá výlučne právnickou osobou alebo organizačnou zložkou štátu.

Predtým bol pre elektronickú pečať používaný termín elektronická značka. Vo svojej podstate ide o ekvivalent úradnej pečiatky, ktorá garantuje integritu a pôvod dokumentu.

Kvalifikovaná pečať je založená na kvalifikovanom elektronickom podpise, resp. je jeho ekvivalentom s ohľadom na oblasť jeho využitia (výlučne pre právnické osoby). Ďalej vyžaduje špecifický HW modul **HSM** (*Hardware Security Module*) na uloženie súkromného (tajného) kľúča.

Druhy certifikátov z hľadiska elektronického podpisu:

1. osobné, t.j. určené iba pre fyzické osoby
   a) komerčné - zákon nešpecifikuje ich obsah, využívané napr. na prihlasovanie do dátových schránok
   b) kvalifikovaný - určený na podpisovanie správ a dokumentov
2. systémový, t.j. určený pre právnické osoby, organizačné zložky štátu alebo orgány verejnej moci
   a) komerčné - využitie napr. na prihlásenie do spisovej služby
   b) kvalifikovaný - určený na vytváranie elektronických pečatí

10.4 Časová pečiatka

Časová pečiatka preukazuje existenciu dokumentu v danej podobe v pevne špecifikovanom čase, to znamená, nerieši sa, kedy dokument vznikol a kto dokument vlastnil.

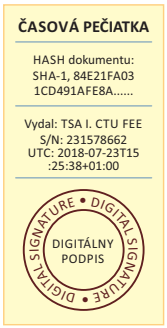
Dátová štruktúra časovej pečiatky je obdobná ako štruktúra certifikátu. Technicky je časová pečiatka realizovaná ako ďalší elektronický podpis odvodený od autority časových pečiatok **TSA** (*Time Stamp Authority*).

Existuje aj tzv. kvalifikovaná časová pečiatka ako ekvivalent kvalifikovanej elektronickej pečiatky, resp. kvalifikovaného elektronického podpisu. Kvalifikovanú časovú pečiatku vytvára kvalifikovaný poskytovateľ služby časových pečiatok.

Elektronicky podpísaná štruktúra časovej pečiatky okrem iného obsahuje:

- meno vydavateľa,
- jedinečné sériové číslo pečiatky,
- kontrolný súčet (tzv. HASH) odvodený z dokumentu a
- čas.

Autorita časových pečiatok TSA preukazuje synchronizáciu svojho časového zdroja s celosvetovým časovým štandardom **UTC** (*Universal Time Coordinated*).



Ukážka časovej pečiatky