KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

05 Bezpečnosť sieťových protokolov IPv4 a IPv6

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnosť sieťových protokolov IPv4 a IPv6

- možné útoky a ochrana
- protokol IPsec
- bezpečnostné asociácie a politiky
- výmena kryptografických informácií

Sieťová vrstva a jej úloha

- protokol IP zabezpečuje adresovanie a doručovanie paketov medzi sieťami
- IPv4 – 32-bitové adresy, dominantný protokol desaťročia
- IPv6 – 128-bitové adresy, riešenie vyčerpania adresného priestoru
- pôvodný návrh IP neobsahoval bezpečnostné prvky (dôvera v sieť)
- dôvernosť, integrita a autentizácia sa pridávali až dodatočne

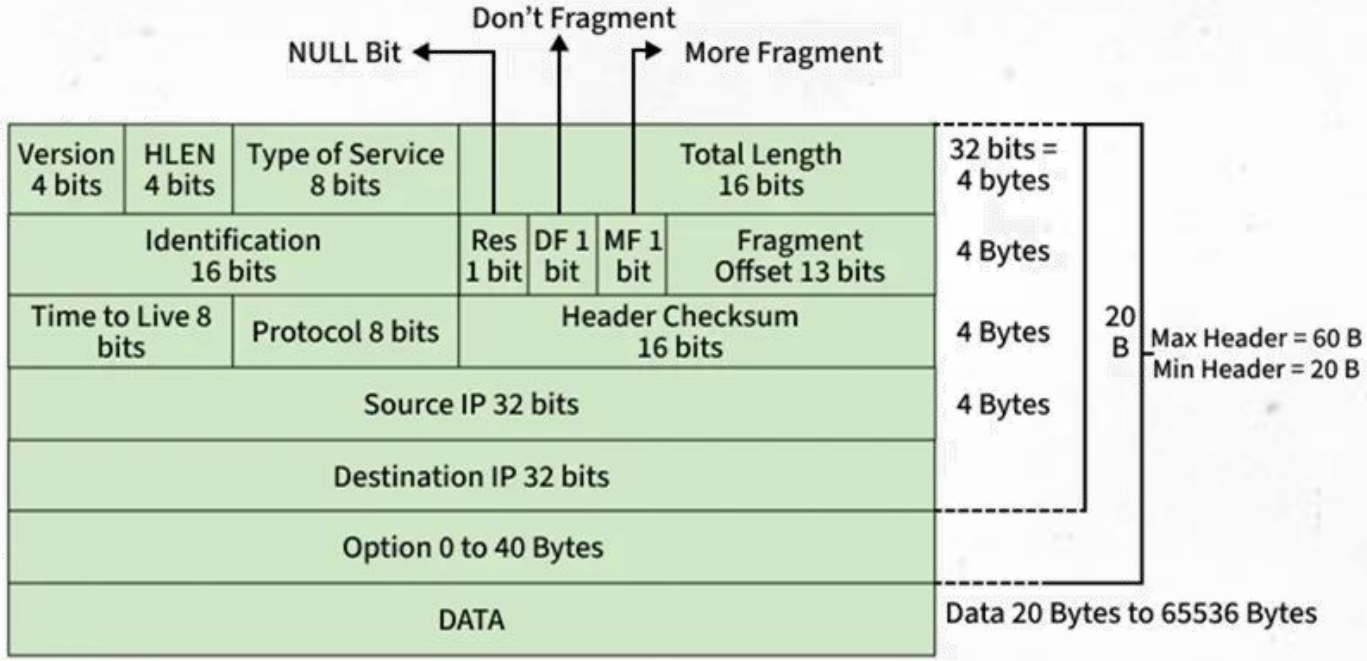
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnosť IP

- hlavička IP nie je chránená proti modifikácii
- zdrojová adresa sa dá ľahko sfalšovať (spoofing)
- dáta sa prenášajú v otvorenej forme (bez šifrovania)
- chýba overenie pôvodu paketu (autentizácia odosielateľa)
- smerovanie možno ovplyvniť podvrhnutými správami

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

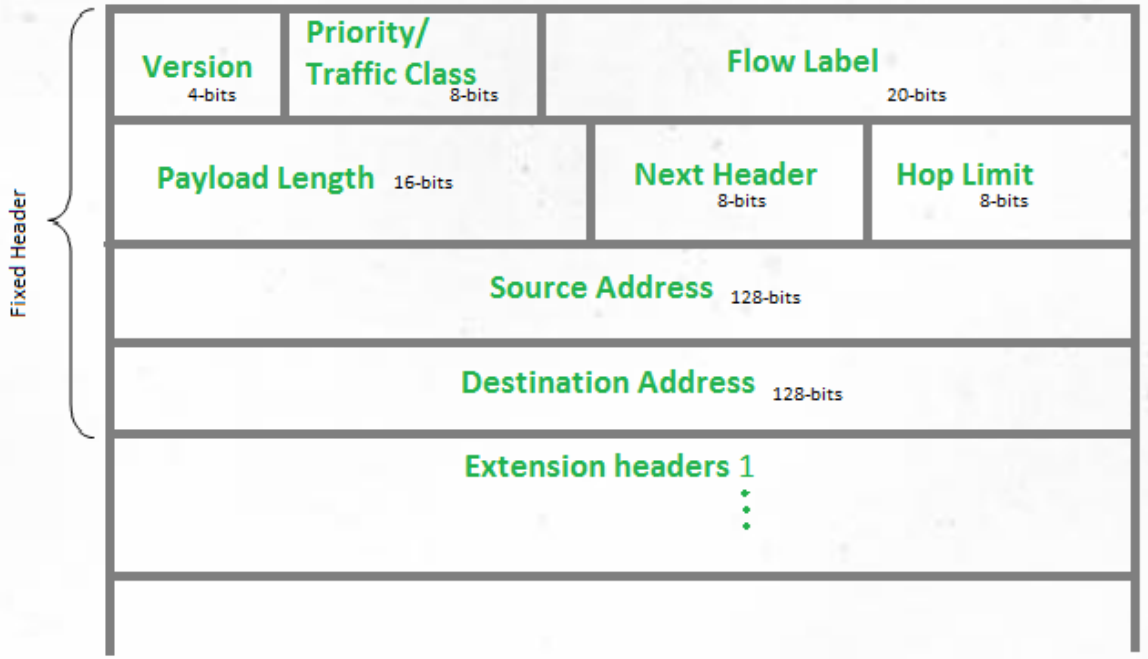
IPv4 vs. IPv6 – bezpečnostné rozdiely (I.)



Zdroj: https://www.geeksforgeeks.org/computer-networks/what-is-ipv4/

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

IPv4 vs. IPv6 – bezpečnostné rozdiely (II.)



Zdroj: https://www.geeksforgeeks.org/computer-networks/internet-protocol-version-6-ipv6-header/

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

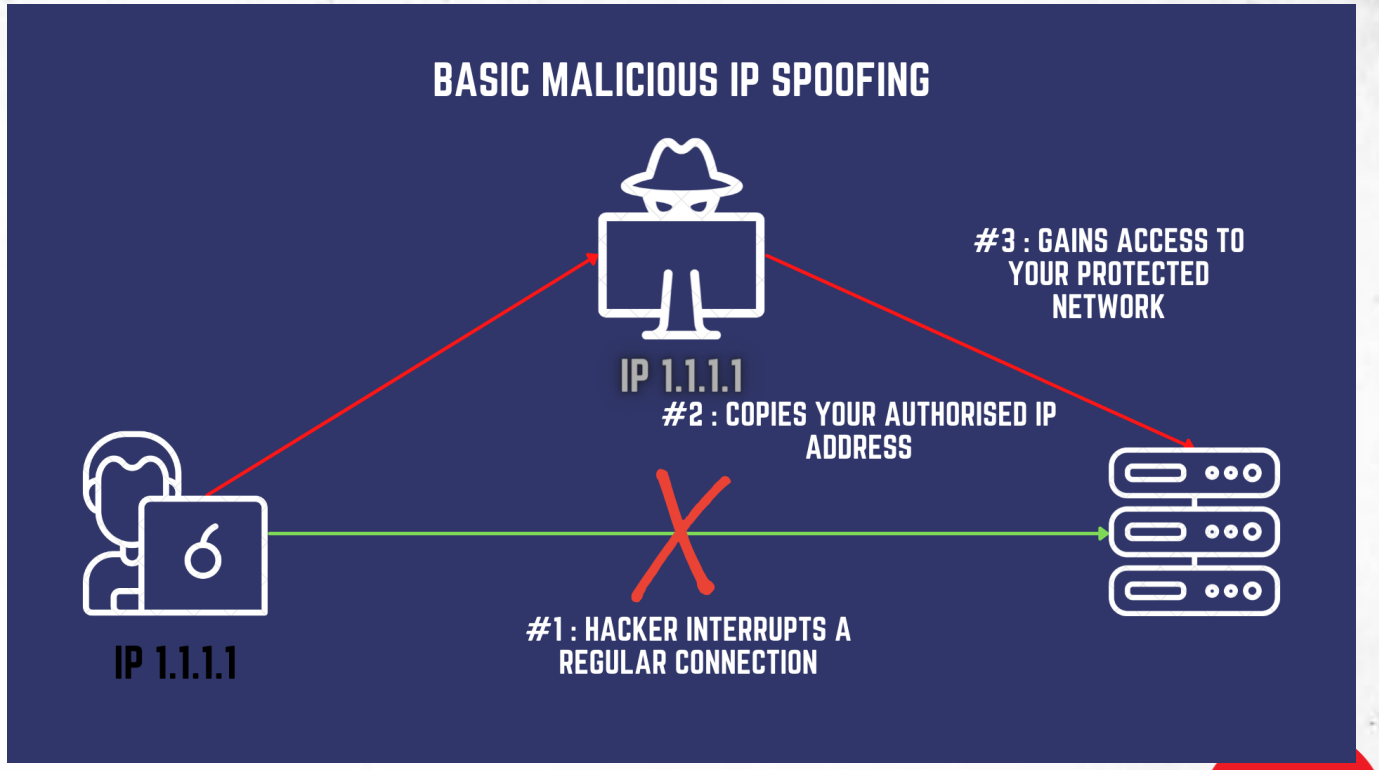
IPv4 vs. IPv6 – bezpečnostné rozdiely (III.)

- IPv6 má povinnú podporu IPsec v štandarde (v praxi voliteľná)
- IPv6 nepoužíva ARP, ale protokol NDP (Neighbor Discovery)
- IPv6 ruší fragmentáciu na medziľahlých uzloch
- väčší adresný priestor sťažuje skenovanie siete
  - ale prináša nové vektory: RA spoofing, SLAAC útoky
- prechodné mechanizmy (tunelovanie) zvyšujú útočnú plochu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

IP spoofing

- **IP spoofing**
  - podvrhnutie zdrojovej adresy paketu
  - obchádzanie filtrov, zneoprávnený prístup, zahladenie stôp
  - základ pre reflexné a amplifikačné DDoS útoky

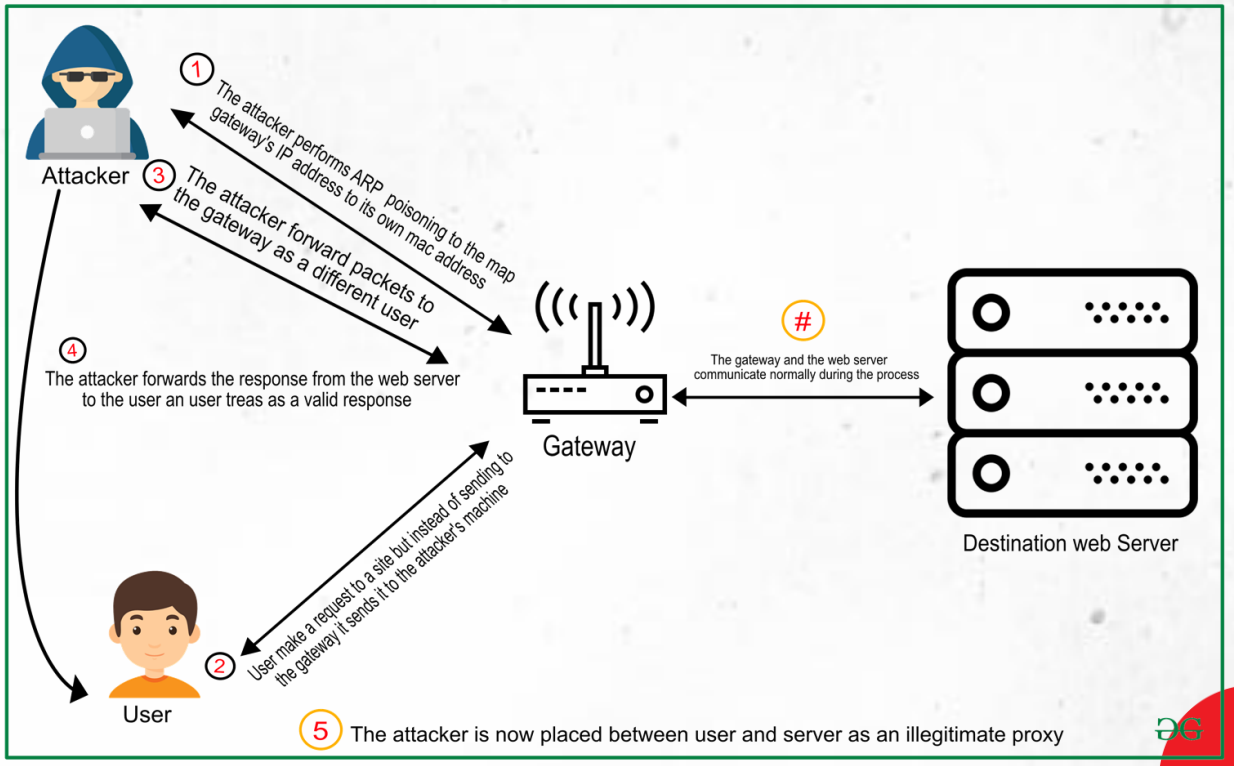


Zdroj: https://bhaifi.ai/blog/what-is-ip-spoofing-attack-2020/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Man-in-the-Middle útok

- **Man-in-the-Middle (MITM)**
  - útočník medzi komunikujúcimi stranami
  - odpočúvanie aj aktívna modifikácia prevádzky
  - často kombinovaný s ARP/NDP spoofingom alebo DNS útokom



Zdroj: https://www.geeksforgeeks.org/blogs/how-to-prevent-man-in-the-middle-attack/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Útoky špecifické pre IPv6

- RA (Router Advertisement) spoofing – podvrhnutie falošného smerovača
- NDP spoofing – obdoba ARP spoofingu na vrstve IPv6
- útoky cez prechodové tunely (6to4, Teredo)
- zneužitie rozširujúcich hlavičiek na obchádzanie filtrov
- ochrana:
  - RA Guard,
  - SEND (Secure Neighbor Discovery),
  - filtrovanie ICMPv6

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Možnosti ochrany

- filtrovanie a kontrola na hranici siete (firewall, ACL)
- anti-spoofing pravidlá (uRPF – Unicast Reverse Path Forwarding)
- segmentácia siete a princíp najmenších oprávnení
- šifrovanie a autentizácia prevádzky – IPsec
- monitoring a detekcia anomálií v prevádzke

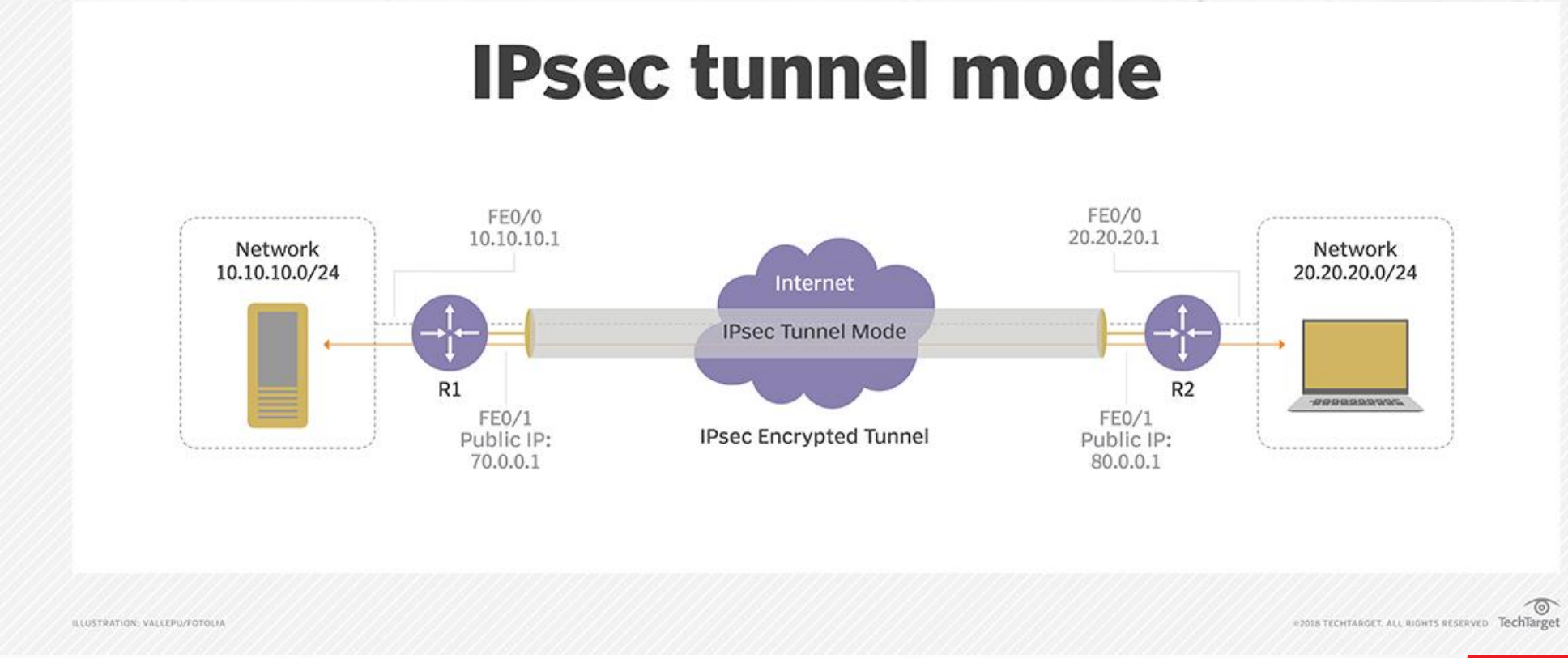
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Protokol IPSec (I.)

- súbor protokolov pre bezpečnosť na sieťovej vrstve (IP)
- poskytuje dôvernosť, integritu a autentizáciu paketov
- funguje transparentne pre aplikácie – chráni celú IP prevádzku
- definovaný v RFC 4301 a súvisiacich dokumentoch IETF
- základ pre site-to-site aj remote-access VPN

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Protokol IPSec (II.)



Zdroj: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

AH a ESP

- **AH (Authentication Header)**
  - integrita a autentizácia pôvodu
  - nezabezpečuje dôvernosť (nešifruje dáta)
  - chráni aj časti IP hlavičky proti modifikácii

- **ESP (Encapsulating Security Payload)**
  - šifrovanie + integrita
  - v praxi najpoužívanejší, poskytuje dôvernosť dát
  - voliteľná autentizácia obsahu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

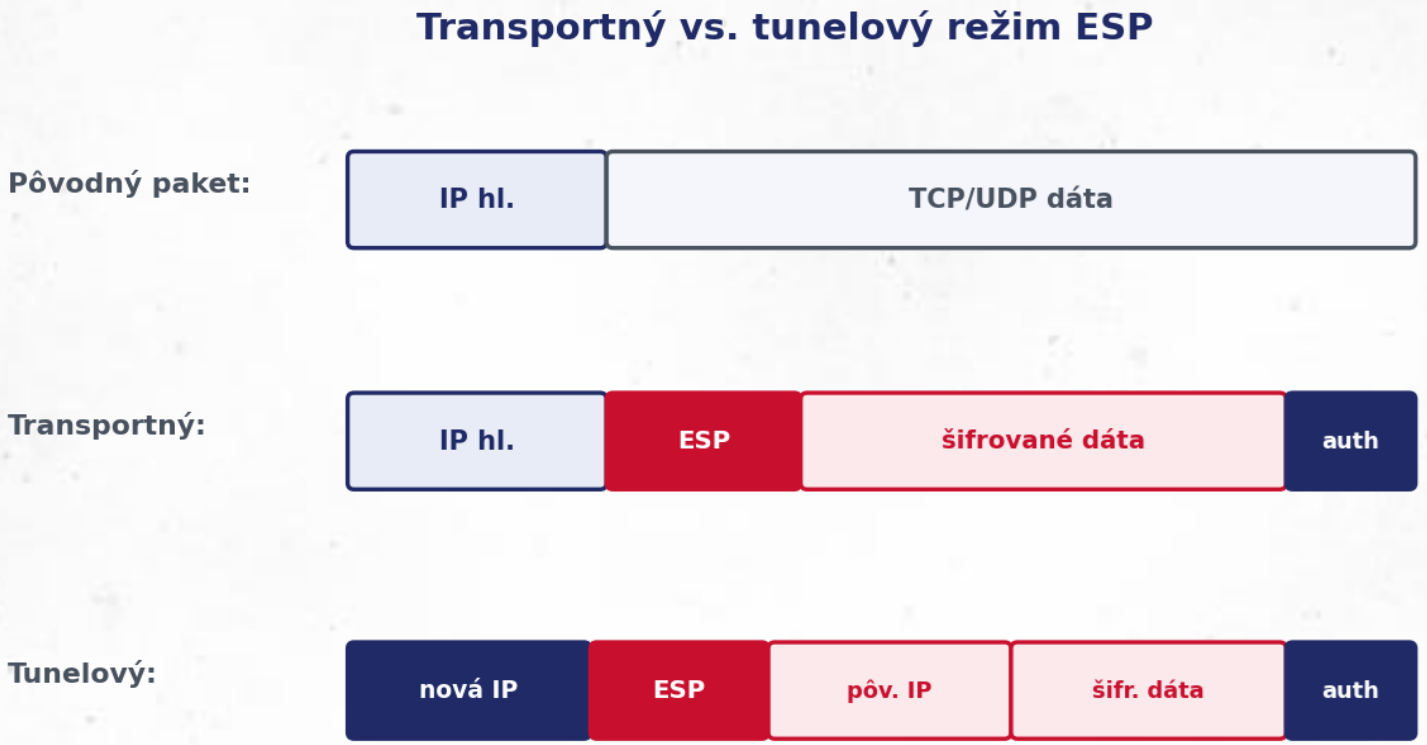
Transportný a tunelový režim (I.)

- **Transportný režim**
  - chráni len užitočné dáta (payload)
  - pôvodná IP hlavička ostáva, komunikácia host-to-host

- **Tunelový režim**
  - chráni celý pôvodný paket
  - pridáva novú IP hlavičku, používa sa pri VPN bránach
  - skrýva pôvodné adresy koncových staníc

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Transportný a tunelový režim (II.)



Zdroj: Claude Opus, spracované podľa RFC 4303 (IETF) – https://datatracker.ietf.org/doc/html/rfc4303

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnostné asociácie (SA)

- SA = jednosmerný „kontrakt“ o ochrane prevádzky medzi dvoma stranami
- definuje protokol (AH/ESP), režim, algoritmy a kľúče
- identifikovaná pomocou SPI, cieľovej adresy a protokolu
- obojsmerná komunikácia vyžaduje dvojicu SA
- aktívne SA sú uložené v databáze SAD (Security Association Database)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnostné politiky (SPD)

- SPD (Security Policy Database) určuje, ako naložiť s prevádzkou
- tri možné rozhodnutia: PROTECT, BYPASS, DISCARD
- selektory: zdrojová/cieľová adresa, port, protokol
- SPD prepája konkrétnu prevádzku s príslušnou SA
- politiky a SA spolu tvoria jadro fungovania IPsec

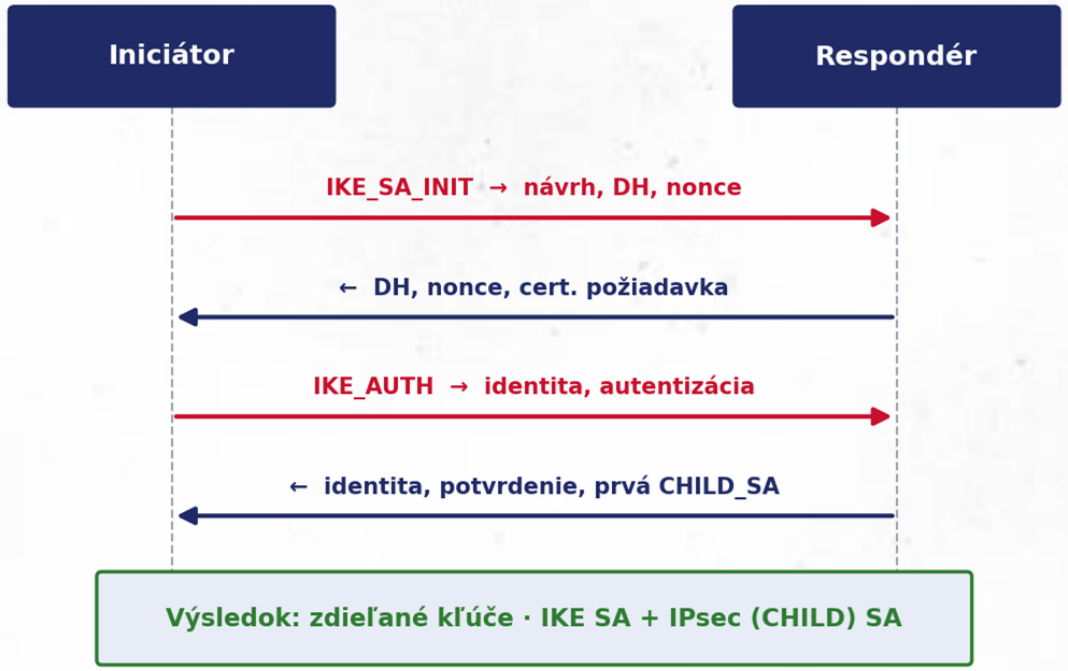
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Výmena kryptografických informácií – IKE (I.)

- **IKE (Internet Key Exchange)** automatizuje dohodu kľúčov a SA
- Využíva Diffie-Hellman na bezpečné odvodenie zdieľaného kľúča
- **IKEv2 (RFC 7296)**
  - dnešný štandard, jednoduchší a robustnejší
  - Fáza 1: vznik IKE SA a autentizácia (certifikát alebo PSK)
  - Fáza 2: vznik IPsec (CHILD) SA pre samotnú prevádzku
- Perfect Forward Secrecy – kompromitácia kľúča neohrozí staré relácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Výmena kryptografických informácií – IKE (II.)



Zdroj: Claude Opus, spracované podľa RFC 4303 (IETF) – https://datatracker.ietf.org/doc/html/rfc4303

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť