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

06 Bezpečnosť transportných protokolov TCP a UDP

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 transportných protokolov TCP a UDP

- protokol TLS
- zabezpečenie údajov v TLS relácii
- vytváranie tunelov
- VPN

Transportná vrstva

- Zabezpečuje komunikáciu medzi procesmi (porty)
- TCP – spoľahlivý, spojovo orientovaný prenos
- UDP – nespojový, rýchly prenos bez záruk doručenia
- ani TCP, ani UDP samé o sebe nešifrujú prenášané dáta
- bezpečnosť sa rieši nadstavbou - najmä protokolom TLS

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

Hrozby na transportnej vrstve

- odpočúvanie nešifrovanej prevádzky (sniffing)
- TCP SYN flood - vyčerpanie zdrojov serverom (DoS)
- TCP session hijacking - prevzatie nadviazaného spojenia
- podvrhnutie sekvenčných čísel, RST útoky
- UDP flooding a amplifikačné útoky (DNS, NTP)

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

Protokol TLS (I.)

- **TLS (Transport Layer Security)**
  - nástupca protokolu SSL
  - poskytuje dôvernosť, integritu a autentizáciu komunikácie
  - pracuje nad TCP, pod aplikačnými protokolmi (HTTPS, SMTPS...)
  - aktuálne verzie: TLS 1.2 a TLS 1.3 (RFC 8446)
  - staršie verzie (SSL 3.0, TLS 1.0/1.1) sú považované za nebezpečné

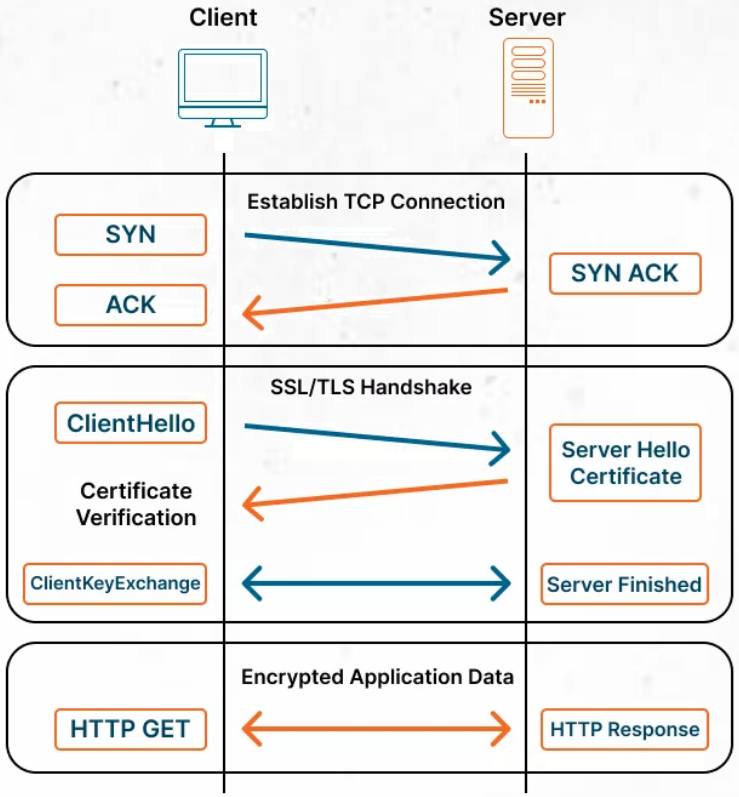
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Protokol TLS (II.)

- Handshake protokol - dohoda parametrov a kľúčov
- Record protokol - šifrovanie a prenos aplikačných dát
- Alert protokol - signalizácia chýb a ukončenia
- Change Cipher Spec - prepnutie na dohodnuté šifrovanie
- Kombinácia asymetrickej (dohoda) a symetrickej (prenos) kryptografie

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

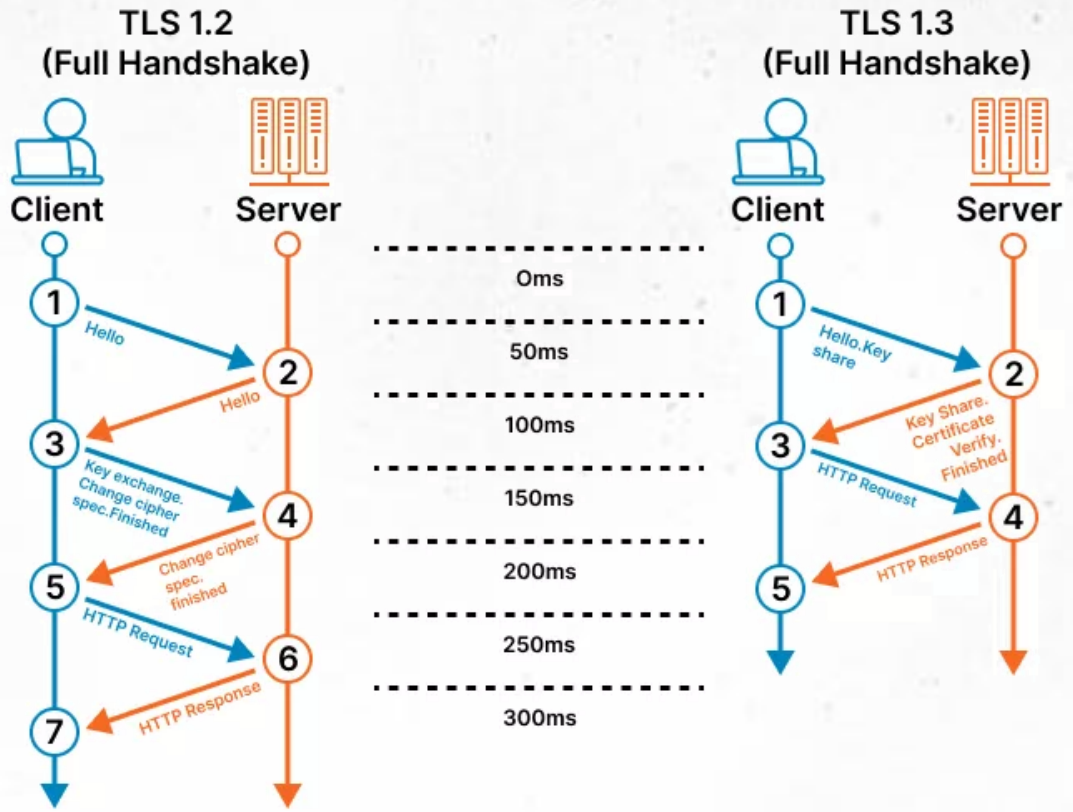
Protokol TLS (III.)



Zdroj: https://cheapsslweb.com/blog/tls-versions-explained-difference-between-tls-1-2-and-1-3/

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

Protokol TLS (IV.)



Zdroj: https://cheapsslweb.com/blog/tls-versions-explained-difference-between-tls-1-2-and-1-3/

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

Bezpečnosť TLS relácie

- dôvernosť - symetrické šifrovanie (AES-GCM, ChaCha20)
- integrita - autentizačné kódy správ (AEAD, HMAC)
- autentizácia servera (a voliteľne klienta) certifikátmi X.509
- dopredná tajnosť (PFS) vďaka efemérnemu ECDHE
- TLS 1.3 odstránil zastarané a slabé šifry a režimy

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

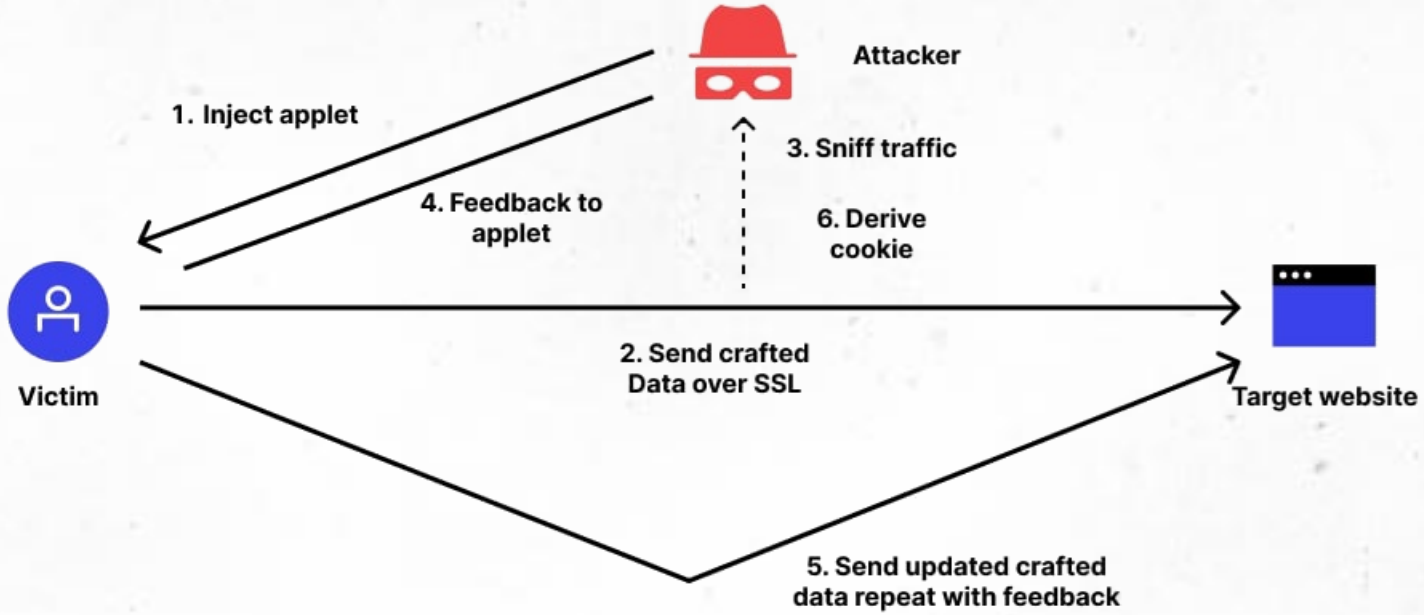
Útoky na TLS (I.)

- downgrade útoky - vynútenie slabšej verzie/šifry
- MITM s podvrhnutým certifikátom (chýbajúce overenie)
- historické zraniteľnosti:
  - BEAST
  - POODLE
  - Heartbleed
- ochrana: aktuálne verzie, HSTS, certificate pinning
- pravidelná aktualizácia knižníc (napr. OpenSSL)

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

Útoky na TLS (II.)

- **BEAST**

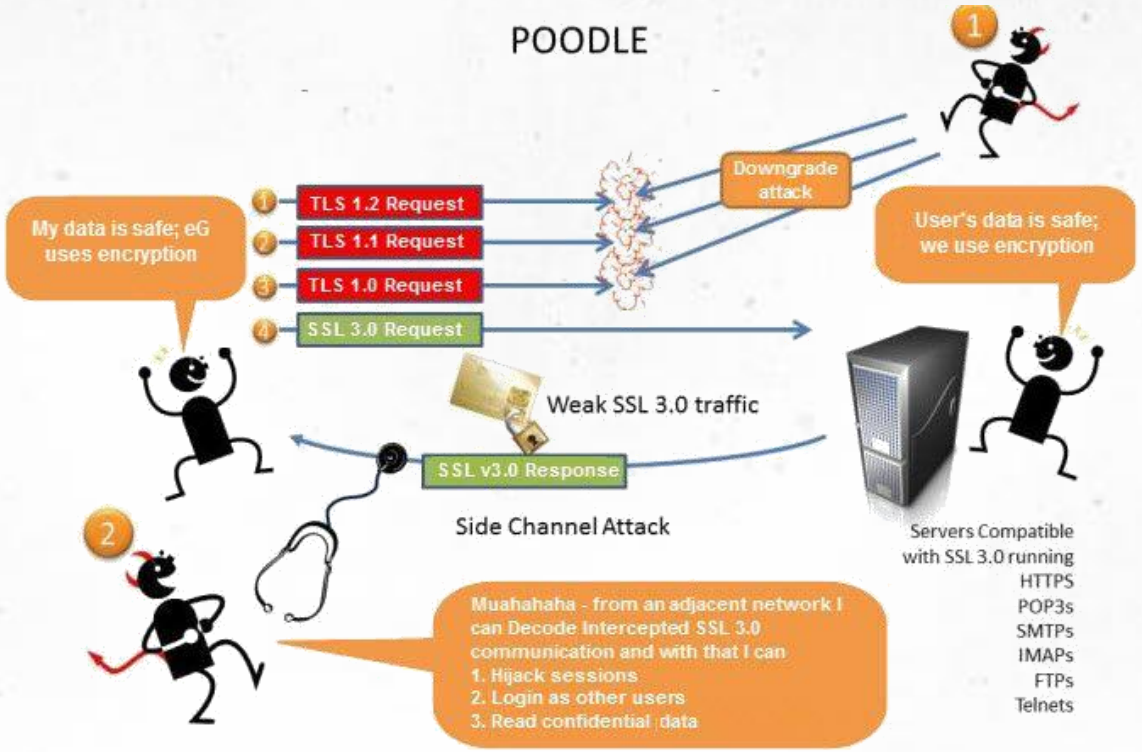


Zdroj: https://www.wallarm.com/what/what-is-a-beast-attack

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

Útoky na TLS (III.)

- **POODLE**

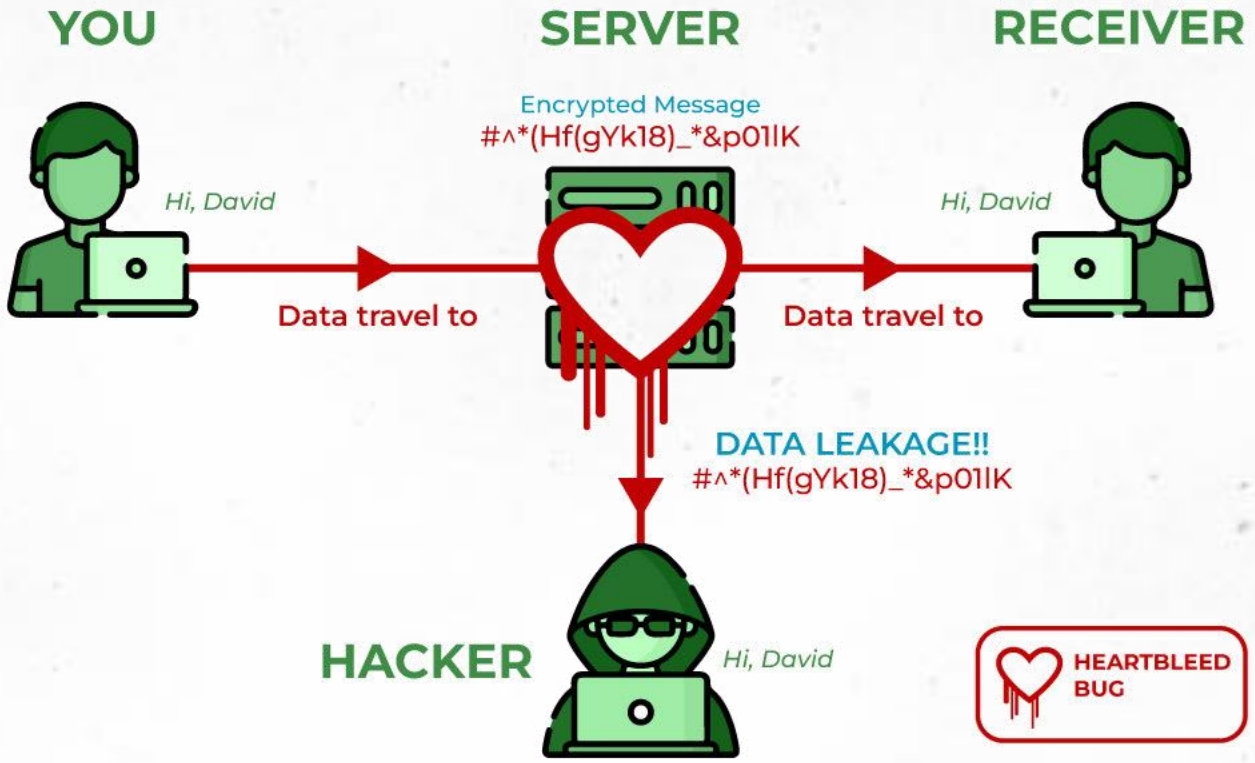


Zdroj: https://www.eginnovations.com/blog/poodle-attack-vulerability/

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

Útoky na TLS (IV.)

- **Heartbleed**



Zdroj: https://www.geeksforgeeks.org/ethical-hacking/what-is-heartbleed-bug-in-ethical-hacking/

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

Vytváranie tunelov

- **tunelovanie** = zapuzdrenie jedného protokolu do druhého
- umožňuje bezpečný prenos cez nedôveryhodnú sieť
- príklady: IPsec tunel, TLS tunel, SSH tunel, GRE
- zabezpečuje dôvernosť a integritu prenášaných dát
- základný stavebný prvok virtuálnych privátnych sietí (VPN)

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

VPN – virtuálna privátna sieť (I.)

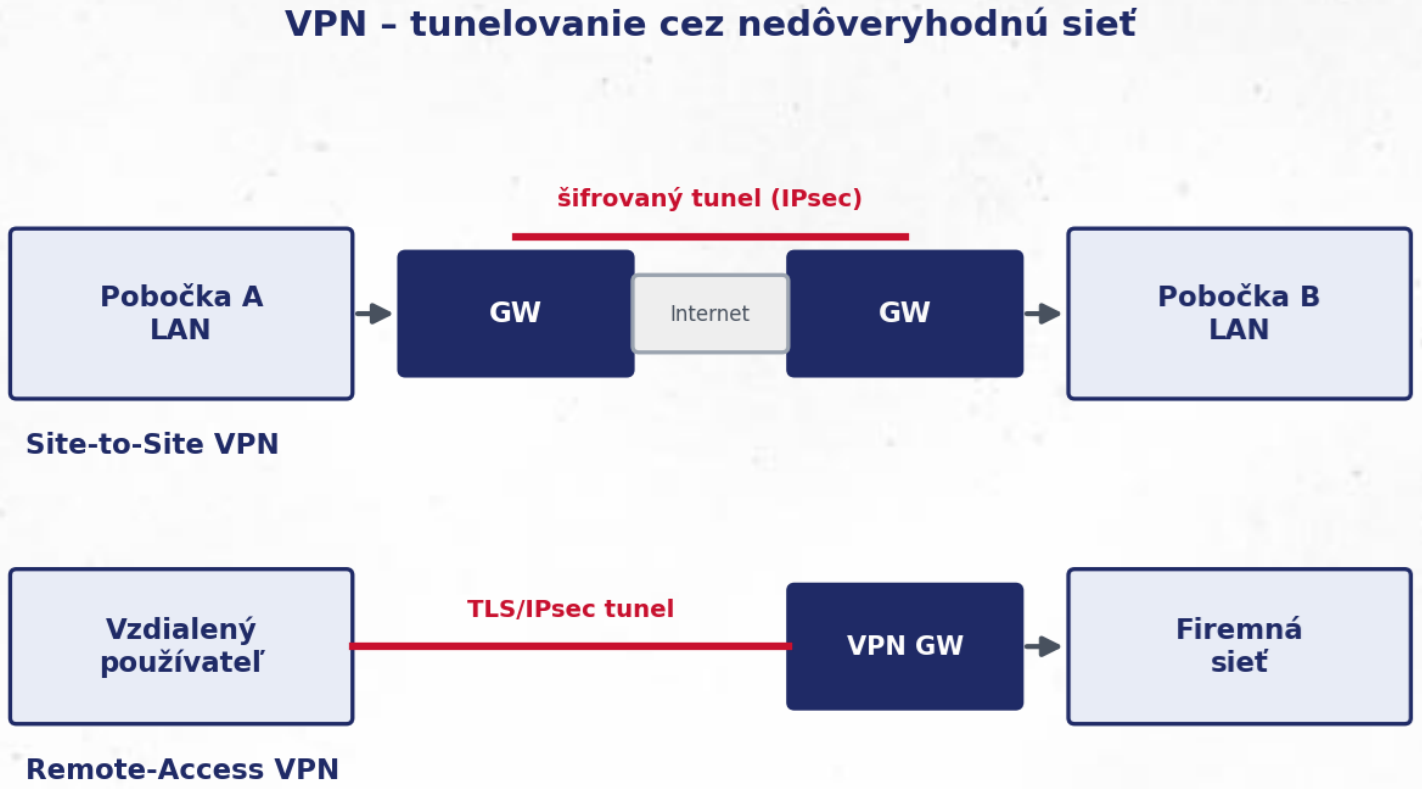
- vytvára šifrované spojenie cez verejnú sieť (Internet)
- zaisťuje dôvernosť, integritu a autentizáciu komunikácie

- **Site-to-Site VPN** - prepojenie celých sietí (pobočiek)
- **Remote-Access VPN** - pripojenie jednotlivého používateľa

- implementácie: IPsec, OpenVPN, WireGuard, SSL/TLS VPN

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

VPN – virtuálna privátna sieť (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

VPN – virtuálna privátna sieť (III.)

- IPsec - štandard na sieťovej vrstve, site-to-site aj remote
- OpenVPN - TLS-based, flexibilný, pracuje v užívateľskom priestore
- WireGuard - moderný, jednoduchý, vysoký výkon
- L2TP/IPsec, PPTP - staršie riešenia (PPTP je nebezpečné)
- SSL/TLS VPN - prístup cez prehliadač, jednoduché nasadenie

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