Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečná komunikácia

Kryptografia, ochrana dát a bezpečná komunikácia (Blok III.)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Pavel Segeč

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk

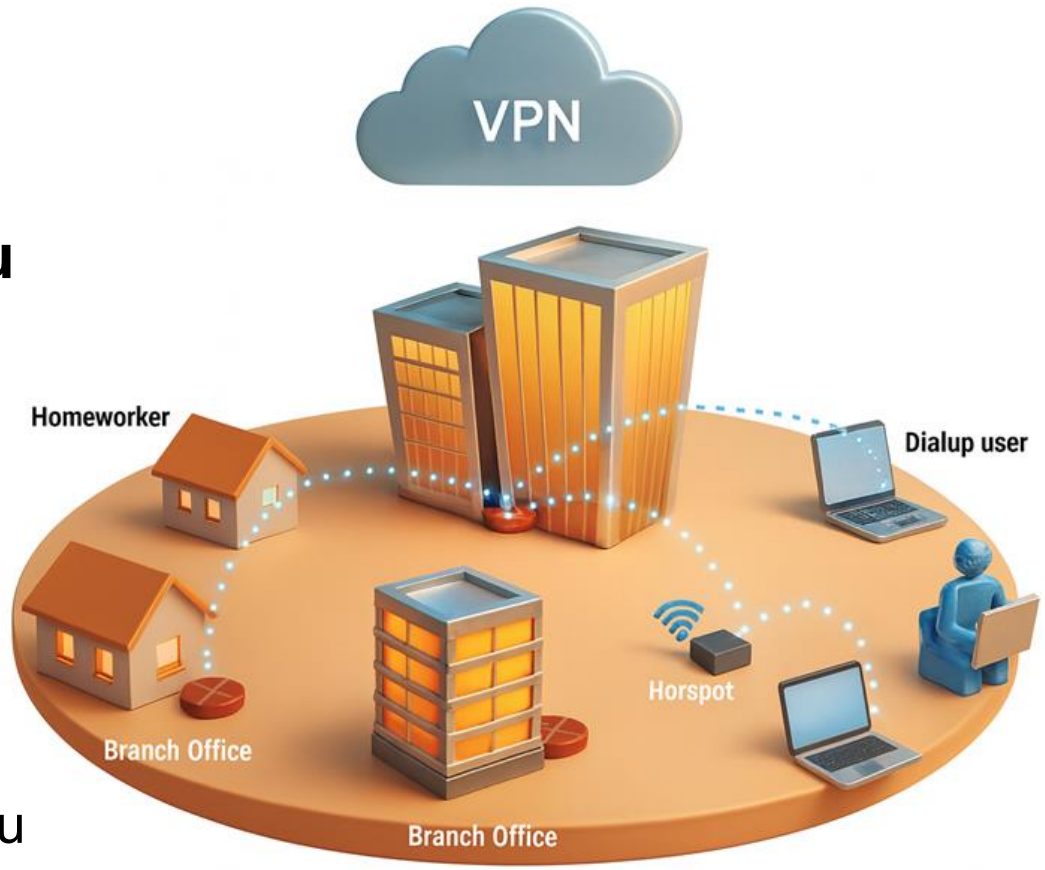
Čo nás čaká ...

- Čo je VPN
- Typy VPN
- GRE tunely
- IPsec

VPNs - Virtual Private Networks

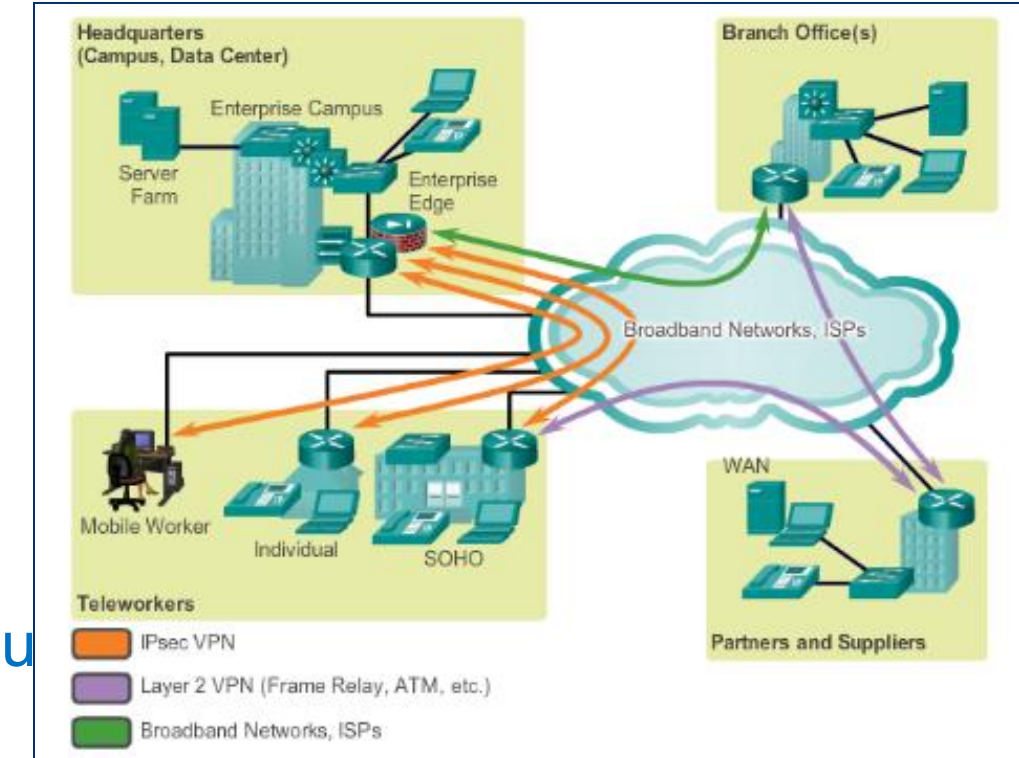
VPN – riešenie vzdialeného prístupu

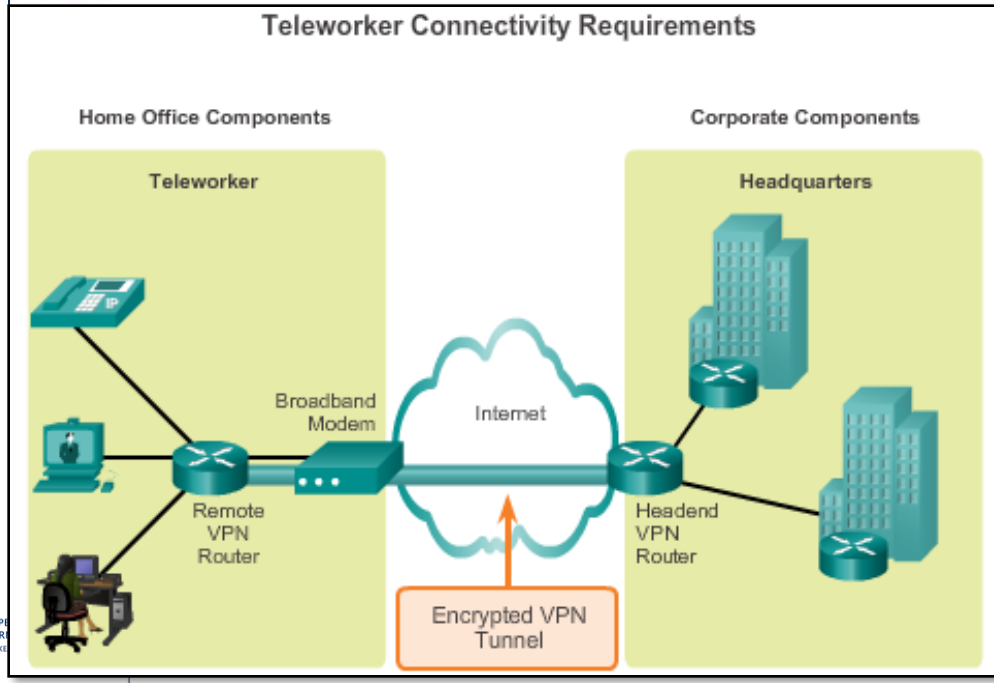
- Prečo treba vzdialený prístup?
  - Firmy potrebujú typicky riešiť vzdialený prístup do siete spoločnosti z dôvodov:
    - **Integrácia sietí pobočiek s centrálou**
      - Napr. prístup zo siete/sietí pobočky k službám centrály (interné služby a servery)
    - **Prístup zákazníkov k interným službám firmy**
      - Napr. rôzne systémy výroby pri dodávkach tovarov a služieb
    - **Teleworking/Homeworking**
      - Umožnenie pracovať zamestnancom z domu
      - Freelancing



Požiadavky na riešenie

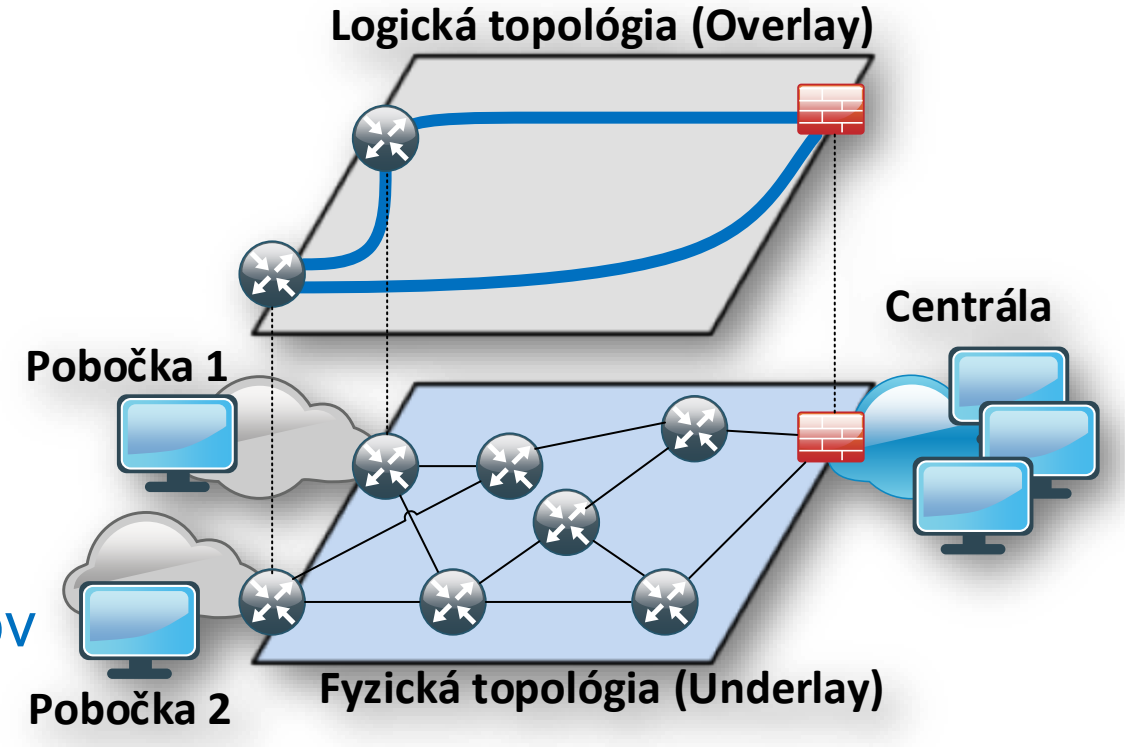
- Každé riešenie z predchádzajúcich možností vyžaduje:
  - Širokopásmový/rýchly prístup
    - Rôzne služby (VoIP, TelePresence, zdieľanie apod.)
  - Bezpečný prístup
- Riešenia širokopásmového a rýchleho prístupu
  - Rýchlosť vyššia 200kbps
    - Cable / DSL / WiFi / WiMAX / Fiber („Always-on“ technológie)
  - Je potrebné pri výbere zvažovať
    - Cena, rýchlosť
    - Bezpečnosť
    - Jednoduchosť a spoľahlivosť
- Riešenie bezpečného prístupu
  - **Privátne VPN služby ISP**
    - napr. VPLS cez MPLS na SK, Frame Relay a podobne
  - L3 VPN cez verejný internet
    - Takto to chápe aj CCNA





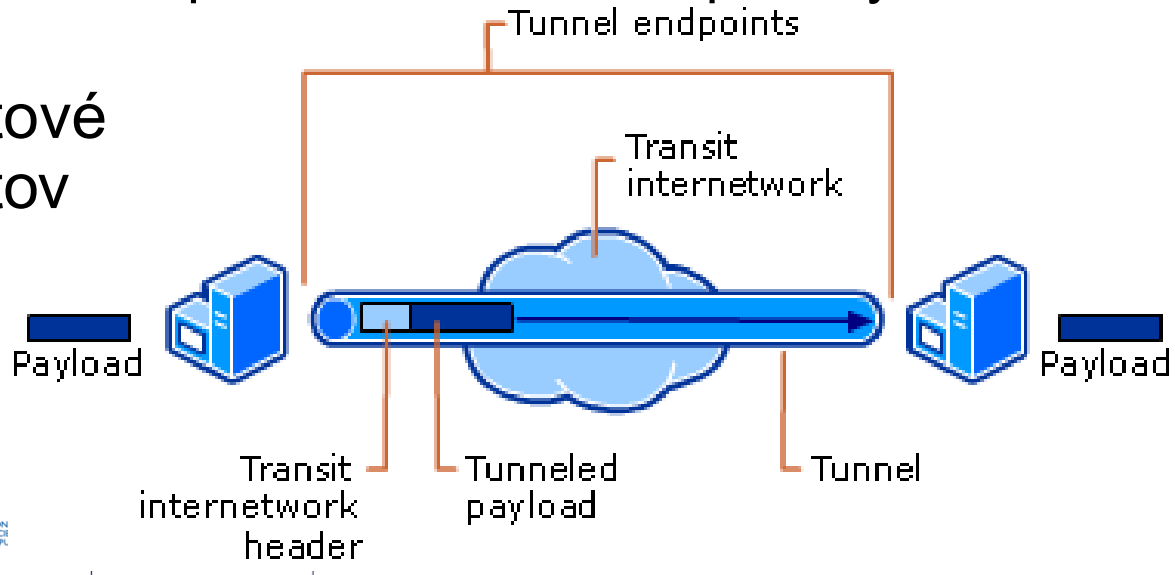
VPN základy

- **Virtual Private Networks**
  - Technicky privátna end-to-end sieť, ktorou si organizácie prepájajú svoje privátne časti (napr. pobočky)
    - Typicky cez siete iných poskytovateľov (third-party networks)
- **Realizácia** => cez vytvorenie virtuálneho prepoja – sieťového tunela – nad existujúcimi sieťami ISP poskytovateľov
  - Vytvorenie tzv. **Overlay** (sieť VPN tunelov)
  - Nad tzv. **Underlay** (siete ISP)
  - Poznámka:
    - *V súčasnosti je VPN už hlavne chápaná ako zabezpečená (šifrovaná) sieť vytvorená cez IPSec formou tunela*



Čo je to tunelovanie protokolov?

- Mnohokrát je potrebné nad existujúcou sieťou vytvoriť ilúziu novej siete
  - Existujúca sieť nepozná protokol, ktorý cez ňu potrebujeme preniesť, alebo službu, ktorú chceme využiť
  - Existujúcu sieť chceme využívať iba ako transport, avšak z pohľadu našej internej siete má byť takmer neviditeľná
  - Potrebujeme prepojiť viaceré lokality, potenciálne s privátnym adresovým rozsahom
  - Existujúcej sieti nedôverujeme a chceme cez ňu preniesť dáta zabezpečeným spôsobom
- Tunelovanie je technika, pri ktorej sa hotové pakety opätovne obalia do nových paketov
  - Z pôvodných paketov sa stáva payload, do ktorého sa existujúca sieť nepozerá

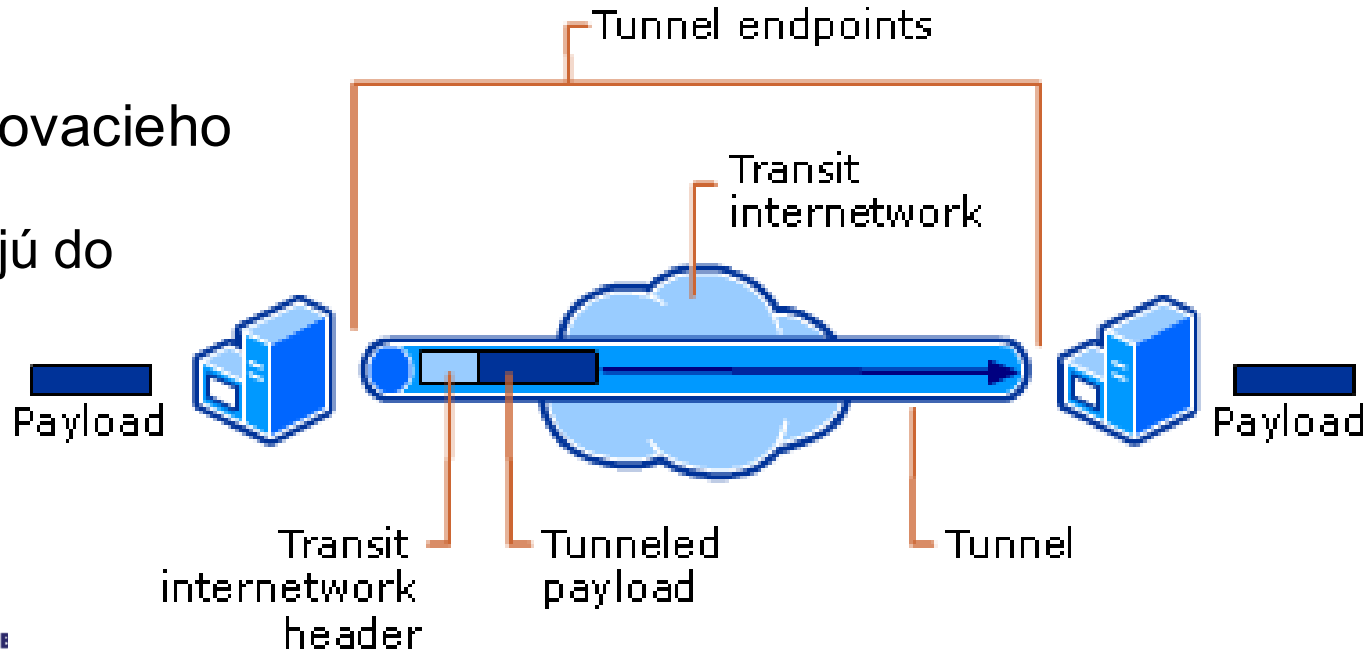


Protokoly pri tunelovaní - terminológia

- Prenášaný protokol (passenger protocol)
  - Protokol, ktorého datagramy potrebujeme tunelovaním preniesť cez existujúcu sieť
    - IPv4 or IPv6
- Pomocný tunelovací protokol (carrier protocol)
  - Protokol, ktorého hlavička sa prikladá k datagramom prenášaného protokolu
  - Umožňuje identifikovať prenášaný protokol, realizovať zabezpečenie, autentifikáciu a ďalšie funkcie
    - U nás GRE
- Nosný protokol (transport protocol)
  - Protokol, na ktorom pracuje existujúca sieť a vo vnútri ktorého transportujeme datagramy prenášaného protokolu obalené pomocným tunelovacím protokolom
    - IPv4 or IPv6

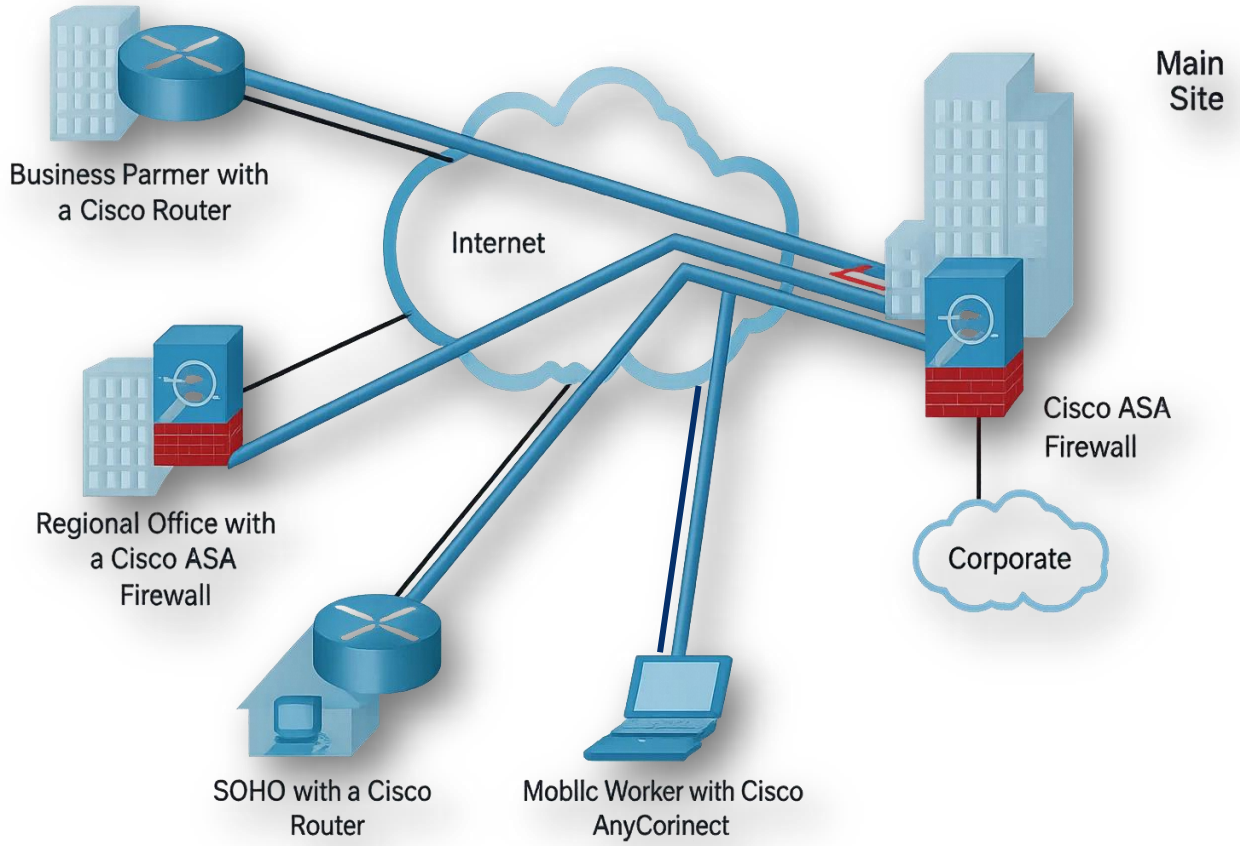
Tunelovacie protokoly

- Tunelovanie je možné realizovať s pomocným tunelovacím protokolom alebo bez neho
- Tunelovanie **s pomocným** tunelovacím protokolom
  - Tunelované (passenger) pakety sa obalia hlavičkou pomocného tunelovacieho protokolu, až potom sa opätovne vkladajú do nových paketov
  - Možnosti pre autentifikáciu, viacnásobné tunely medzi rovnakými zariadeniami, rôzne typy tunelovaných protokolov, šifrovanie
  - Potenciálne vyššia réžia
  - Napríklad: GRE, L2TP ...
- Tunelovanie **bez pomocného** tunelovacieho protokolu
  - Tunelované pakety sa priamo vkladajú do nových paketov
  - Minimálna réžia
  - Obmedzené možnosti
  - Napríklad: IP-in-IP, IPv6-in-IPv4



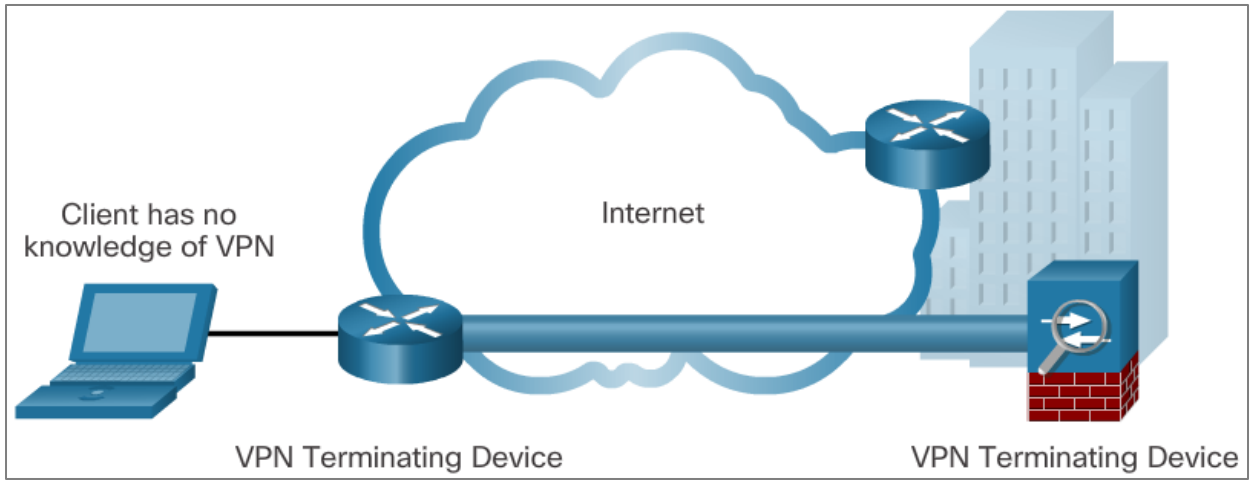
Čo potrebujeme na implementáciu VPN?

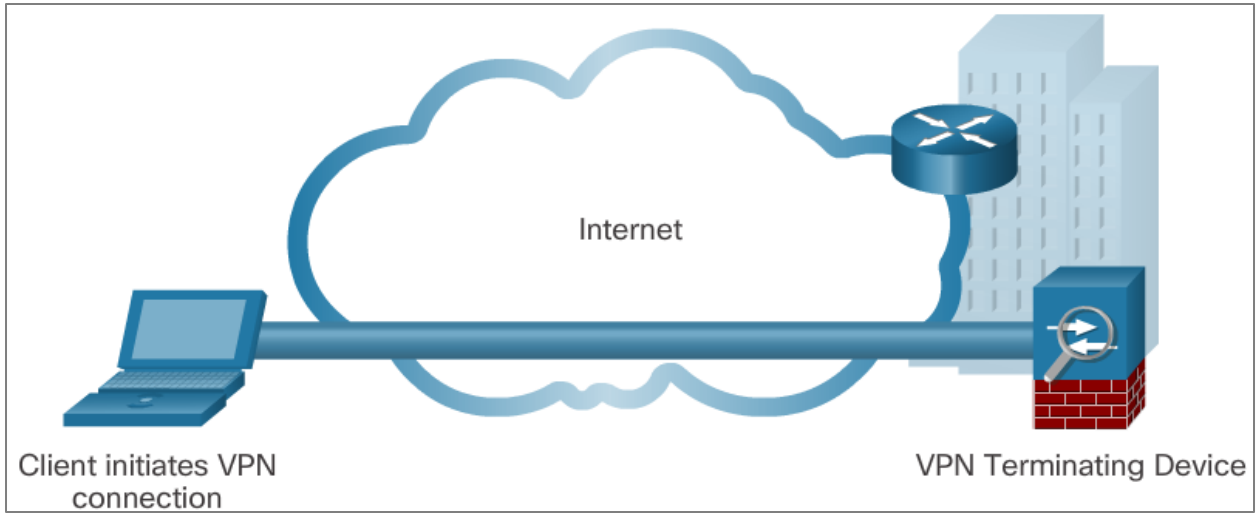
- Čo potrebujeme na implementáciu VPN?
  - **VPN bránu/brány (VPN gateway)**
    - Sieťové zariadenia, medzi ktorými alebo voči ktorým, sa vytvárajú VPN tunely
      - V svojom OS implementujú podporu potrebných VPN protokolov
    - Príklad:
      - Smerovač, Firewall, Cisco Adaptive Security Appliance (ASA), VPN Server, VPN koncentrátor apod.
      - Ideálne aby mala VPN brána hardvérovú podporu šifrovania
  - **VPN klienta**
    - VPN softvér bežiaci v OS počítača/koncového zariadenia



Typy VPN z pohľadu možností nasadenia

- **Site-to-Site VPN**
  - Prepája VPN bránu s VPN bránou navzájom
    - Teda celé siete, napr. pobočky s centrálou
  - Všetky činnosti implementované na VPN bránach
    - Na koncových PC nie je požadovaný žiaden softvér, nemajú zdanie o nejakej VPNke
- **Remote Access VPN**
  - Použitá na pripájanie individuálnych PC k VPN bráne,
    - napr. pre prístup do centrály
  - Klientske alebo bez klientske
- VPN brána
  - Router, firewall, VPN koncentrátor
  - Ideálne aby mal hw podporu šifrovania





Typy VPN z pohľadu kto ich manažuje

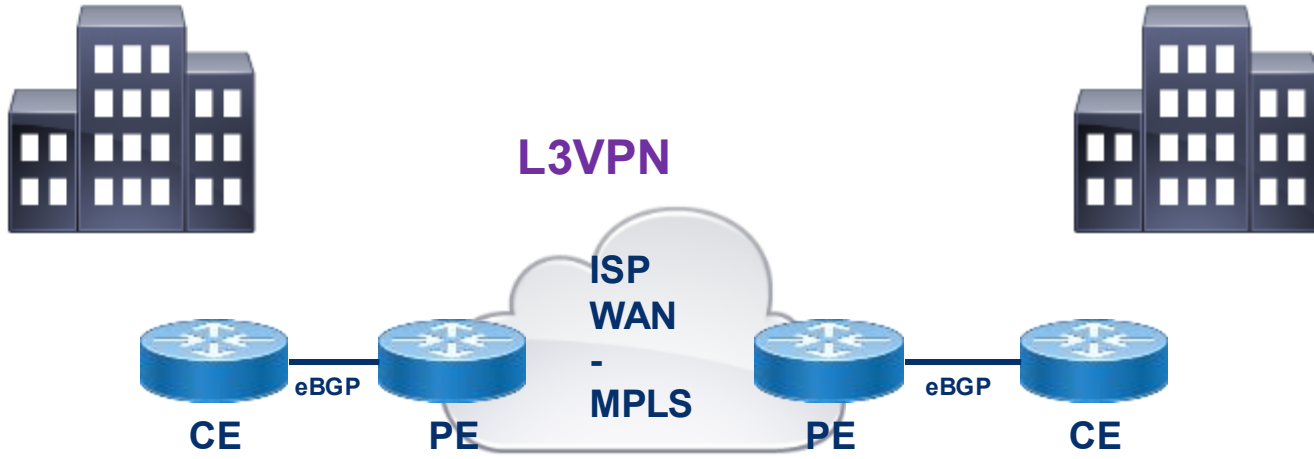
- **Podnikové VPN**
  - Zriadenie a odobratie VPN si manažuje firma sama
    - Svojimi zamestnancami na svojich VPN zariadeniach
  - Technológie riešenia Site-to-site VPN
    - GRE (nešifrovaná)
    - IPSec (šifrovaná)
    - GRE over IPSec (šifrovaná)
    - Cisco Dynamic Multipoint Virtual Private Network (DMVPN)
    - Cisco IPsec Virtual Tunnel Interface (VTI)
  - Technológie riešenia Remote-access VPN
    - Využívajúce VPN klienta
    - Nevyužívajúce VPN klienta
    - L3 VPN: IPSec VPN
    - L4 VPN: SSL VPN

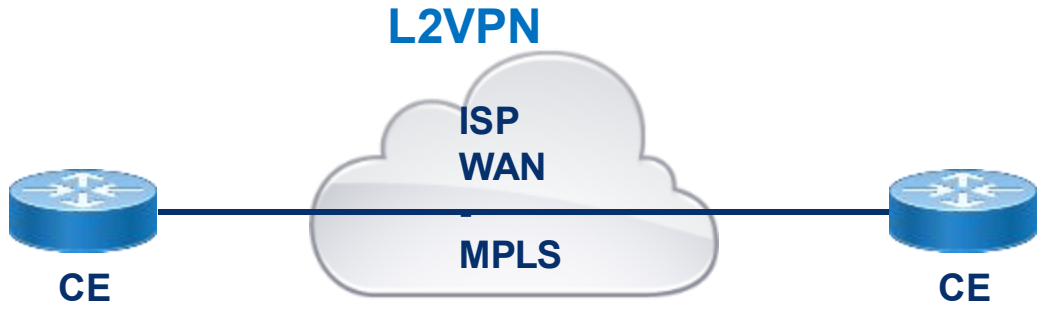
- **Privátne VPN služby poskytované SP/ISP**
  - Zriadenie a manažovanie VPN služby sa objednáva ako produkt na kľúč od konkrétneho ISP poskytovateľa
  - Aktuálne rozlišujeme
    - Layer 2 MPLS VPN
    - Layer 3 MPLS VPN
  - Pôvodné, dnes zastaralé riešenia
    - Frame Relay, ATM Asynchronous Transfer Mode

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Privátne VPN služby SP (CCNA nepokrýva)

- Garantovaná služba ISP
  - Stabilita, rýchlosť, stratovosť, bezpečnosť apod.
    - ISP za týmto účelom buduje vlastnú WAN len pre zákazníkov tejto služby
  - Skôr pre firmy => cena
    - Napr. len zriadenie služby 34Mbps MPLS
      - Aproxim. 9950 Euro s DPH
      - Aproxim 3Mbps / 200E
      - Pozri price listy ISP
- Typy privátnych VPN služieb
  - **L3VPN (cez MPLS)**
    - Smerovače zákazníka si vymieňajú updates zo smerovačom ISP
  - L2VPN (cez MPLS)
    - Smerovače zákazníka si vymieňajú updates napriamo





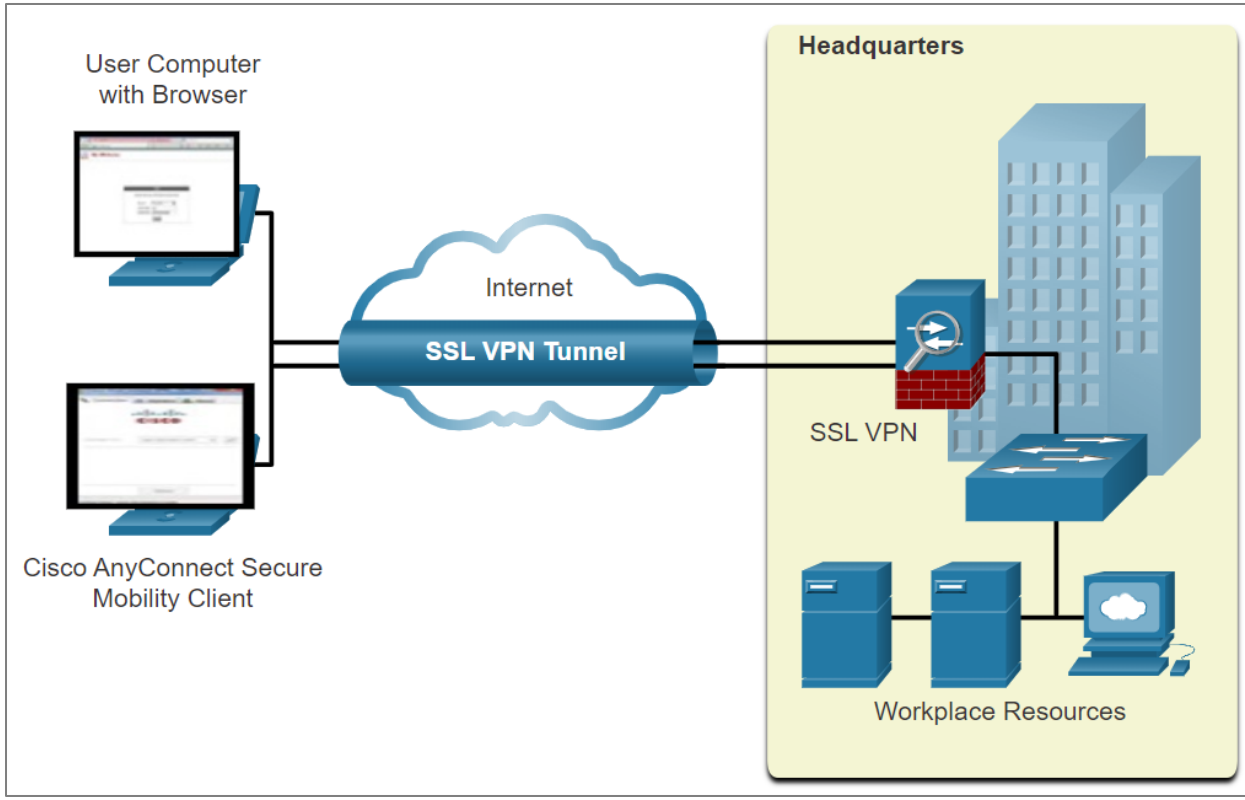
VPN základy

- **Výhody VPN**
  - Šetrenie nákladov
    - Teleworking, mobilita, využitie lacného Internetu na bezpečný prístup do korporátnej siete
  - Škálovateľnosť
    - Jednoduché riadenie pridávania/odobernia používateľov a sietí cez vytvorenie nového tunela
  - Kompatibilita, resp. nezávislosť od širokopásmových technológií pripojenia do Internetu
  - Bezpečnosť
    - Pri použití šifrovaných riešení s autentntifikáciou (alebo riešení od ISP) vysoká úroveň zabezpečenia komunikácie

Remote-Access VPN

Remote-Access VPN

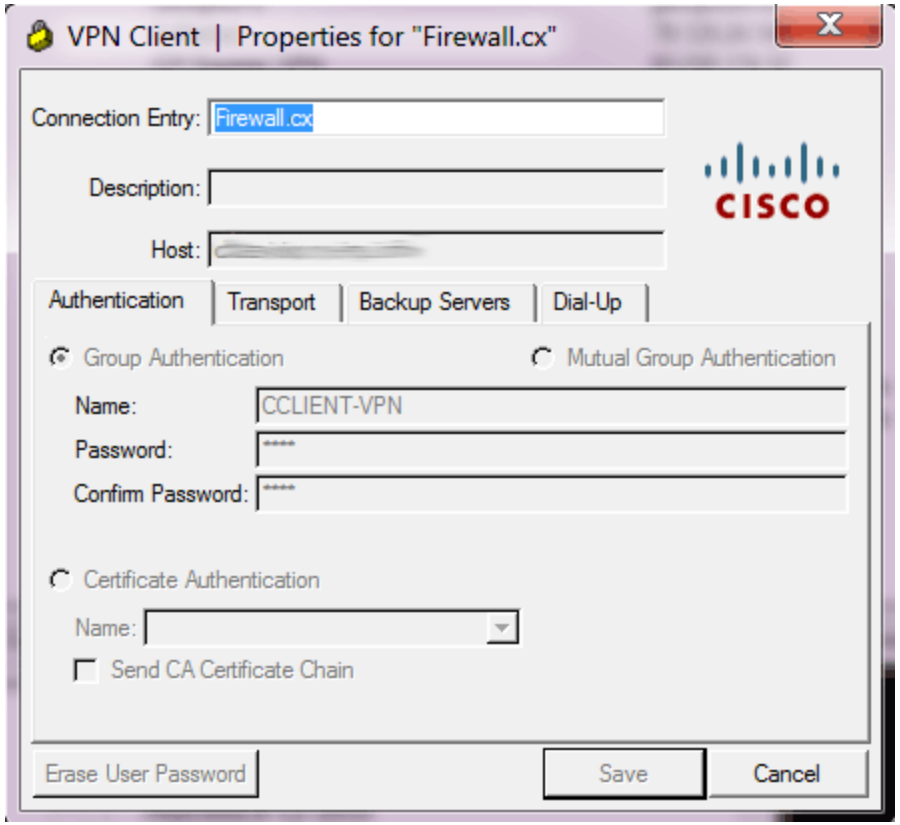
- Primárne určená pre mobilných pracovníkov / homeworkerov / partnerov spoločnosti
  - Používateľ sa pripája zo svojho NB/mobilu/tabletu do siete zamestnávateľa
  - Vytvára tunel zo svojho zariadenia na nakonfigurovanú VPN bránu
    - Spustením IPsec klientskej aplikácie
  - VPN ponúka prístup k špecifickým službám za VPN bránou
    - Prístup k web/file server apod.

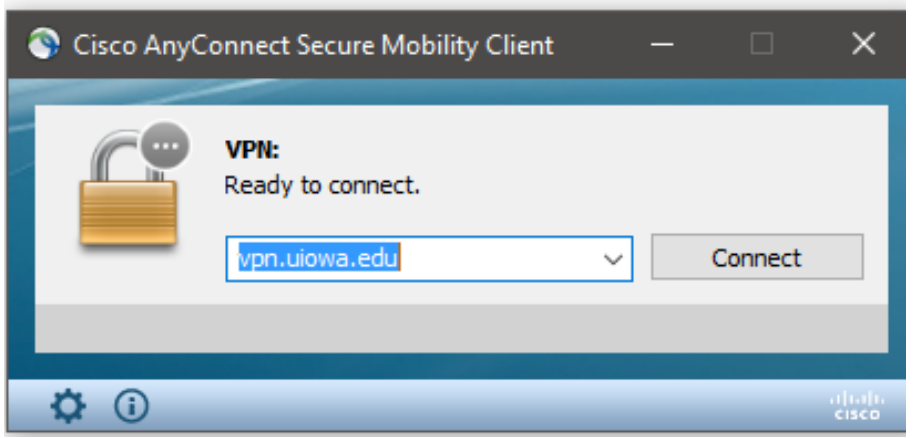


- Zabezpečený typ dynamickej VPN
  - Vytváraná len na určitý čas
  - Po skončení požadovanej činnosti ju používateľ vypne

Možnosti pripojenia k VPN bráne

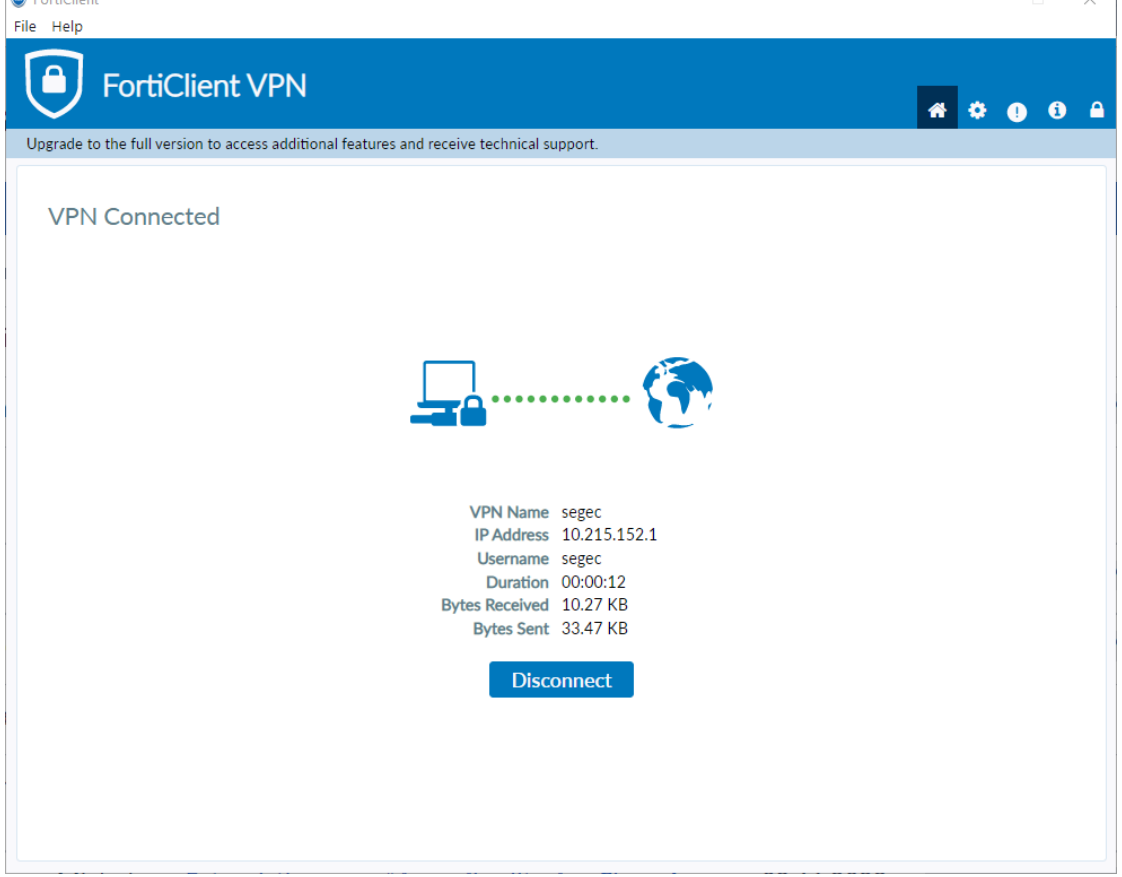
- Dve rozdielne riešenia Remote Access VPN
  - **Client-based VPN - L3 IPsec VPN and L4 SSL VPN**
    - Na koncovom zariadení => nainštalovaný a nakonfigurovaný klientský softvér
      - IPSec klient: Cisco IPSec client (older version), Cisco AnyConnect Secure Mobility Client (current software), built-in IPSec in Win 10 (KIS) (L2TP over IPsec)
      - SSL VPN klient: Cisco AnyConnect, FortiClient, OpenVPN iný
    - Nevýhody:
      - Musí byť nainštalovaný a správne nakonfigurovaný VPN klient
      - Vždy, keď sa používateľ chce pripojiť, musí spustiť klienta
    - Výhody:
      - Pracuje pre všetky služby od L3/L4 nahor
  - **Client-less VPN - L4 VPN – SSL VPN**
    - Bez potreby inštalovať klienta => SSL VPN (TLS – Transport Layer Security)
      - Používa HTTPS, pomenovaný Web mode SSL VPN
      - Prístup a relay cez Jump Portal
    - Využíva PKI infraštruktúru kľúčov a certifikátov
    - V súčasnosti už menej populárne, až potláčané
      - Vhodné len pre niektoré služby od L4 nahor, primárne prístupné cez Web prehliadač

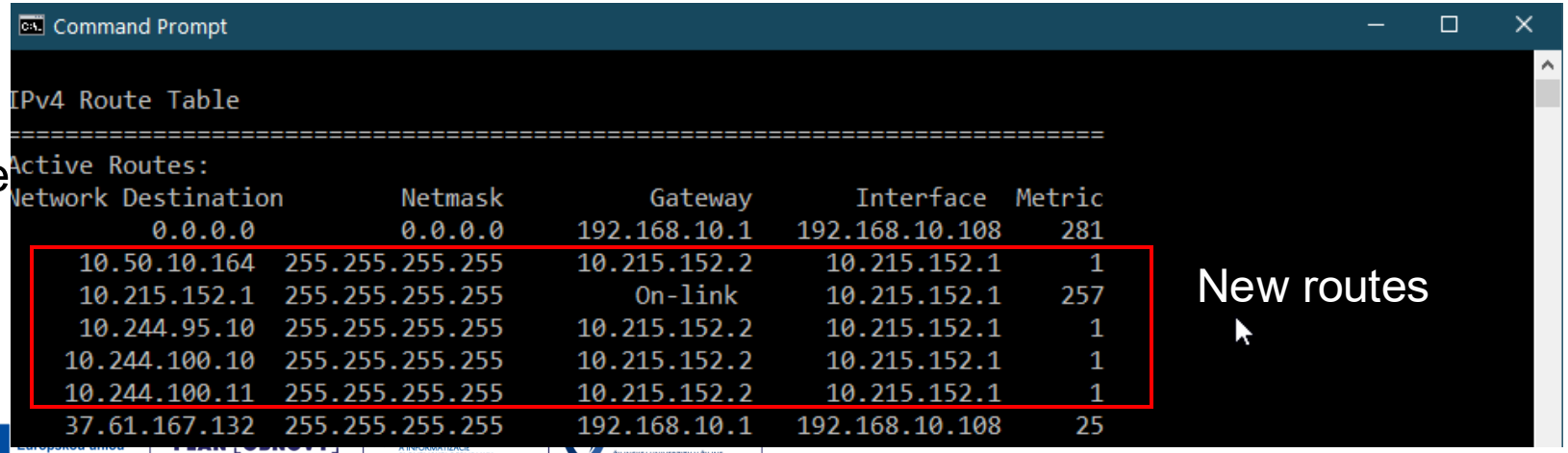




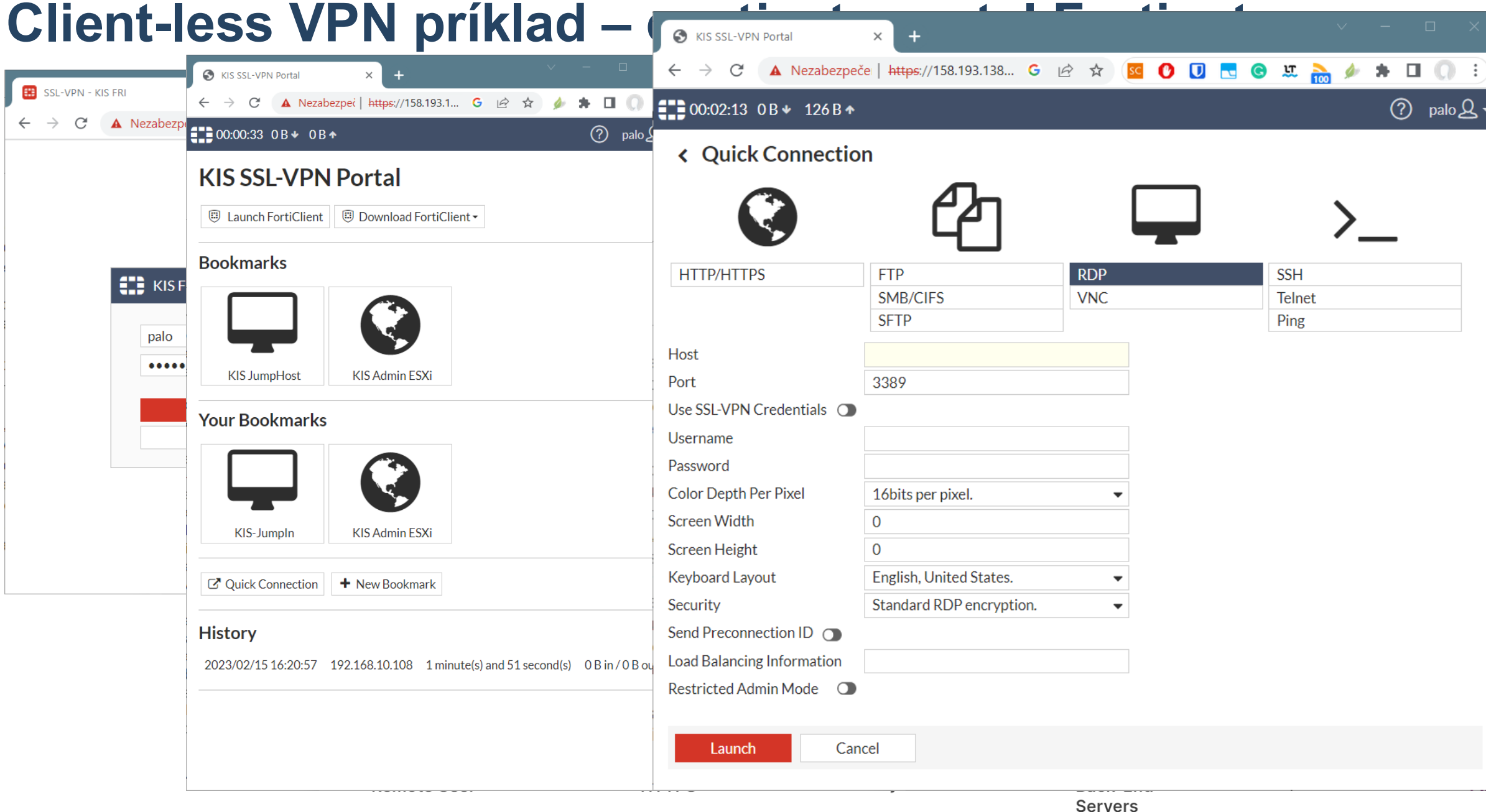
Konektivita klienta

- Týka sa najmä klientských SSL VPN
  - Klient obsahuje virtuálny sieťový adaptér
  - Získava IP adresu
  - Spolu s informáciami o smerovaní
- Smerovanie
  - **Plné smerovanie**
    - Celá komunikácia je smerovaná cez vzdialenú bránu (GW) a následne von
    - Vhodné na vynucovanie firemných politík
  - **Rozdelené smerovanie (Split routing)**
    - Umožňuje lokálny breakout.
    - Len vybrané prefixy sú smerované na vzdialenú lokalitu
    - Ostatný prístup na internet ide priamo lokálne
      - Obzvlášť dôležité v ére cloudu
      - Získava si popularitu





Client-less VPN príklad –



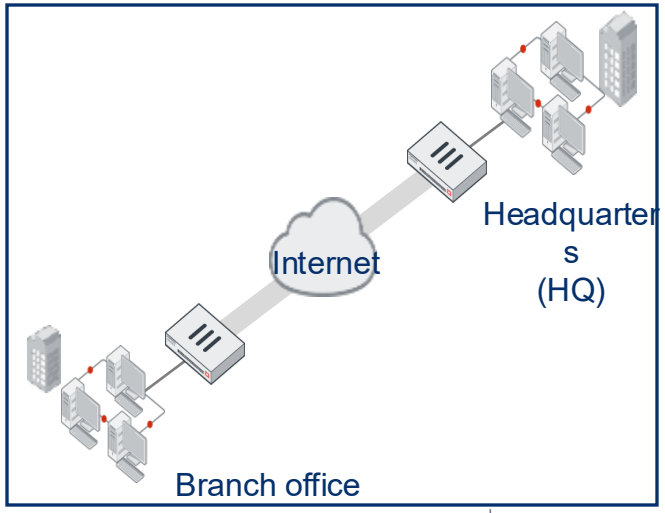
Porovnanie IPsec vs. SSL VPN

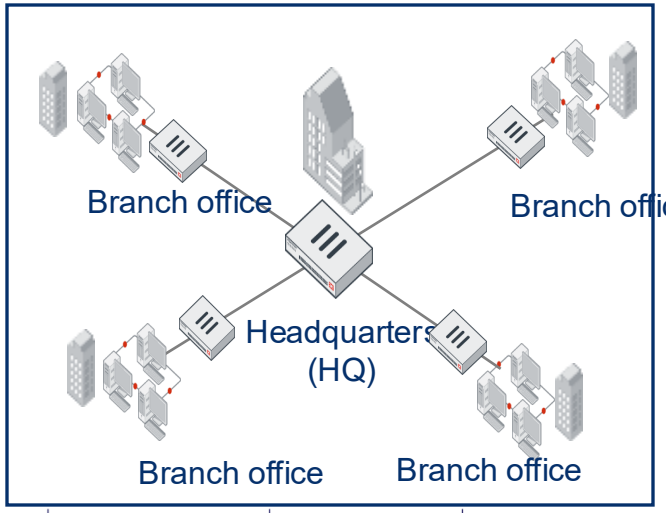
Vlastnosť	IPsec VPN	SSL VPN	ZTNA
Ktorú vrstvu OSI modelu zabezpečuje?	Sieťová vrstva	Transportná až aplikačná vrstva	Transportná až aplikačná vrstva
Aká implementácia je potrebná na strane klienta?	Aplikácia VPN klienta	Webový prehliadač alebo aplikácia SSL VPN klienta	ZTNA klient
Aká kontrola prístupu k sieťovým zdrojom existuje po nadviazaní relácie?	Žiadna kontrola prístupu po nadviazaní VPN relácie	Čiastočne granulárna kontrola – SSL pripája používateľov k špecifickým aplikáciám a službám (napr. e-mailová aplikácia)	Granulárna kontrola prístupu ku konkrétnym aplikáciám. Prístup je riadený rolami/politikou používateľa a priebežnými bezpečnostnými kontrolami pripojených zariadení
Autentifikácia	Autentifikácia prebieha medzi VPN klientom a privátnou sieťou	Autentifikácia prebieha cez prihlasovací formulár v prehliadači po nadviazaní SSL relácie	Autentifikácia používateľa aj zariadenia, znovu overované pri každej požiadavke na prístup k aplikácii
Typ tunela	Iba IPsec tunel	Relácia alebo tunel	Iba relácia
Kategória	Priemyselný štandard	Vendor-špecifické	Vendor-špecifické
Konfigurácia	- Vyžaduje inštaláciu- Flexibilné nastavenie ◦ Mesh a star topológie ◦ Pre klientov alebo partnerské brány	- Nepotrebuje inštaláciu (pri použití webovej verzie)- Jednoduchšie nastavenie ◦ Len klient k FortiGate ◦ Bez používateľských nastavení	- Vyžaduje inštaláciu ZTNA klienta- Jednoduchšie nastavenie ◦ Len klient k FortiGate ◦ Bez používateľských nastavení

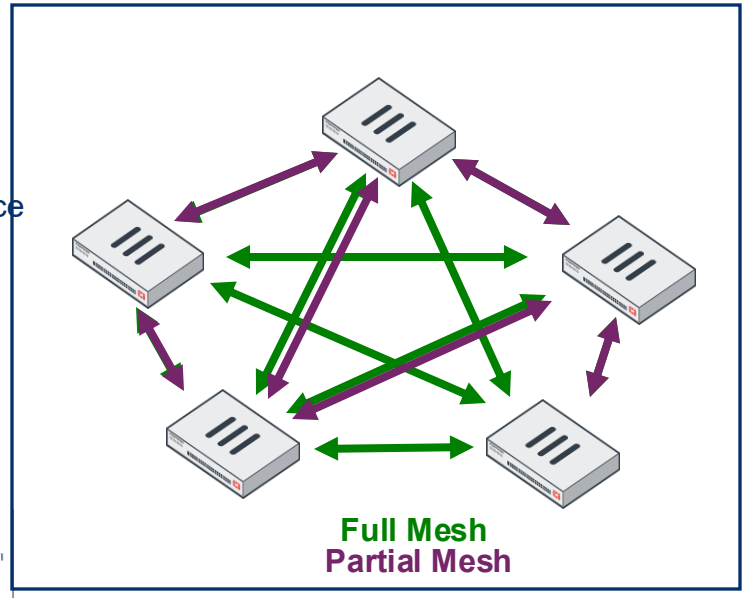
Site – to – Site VPN

Site – to – Site VPN

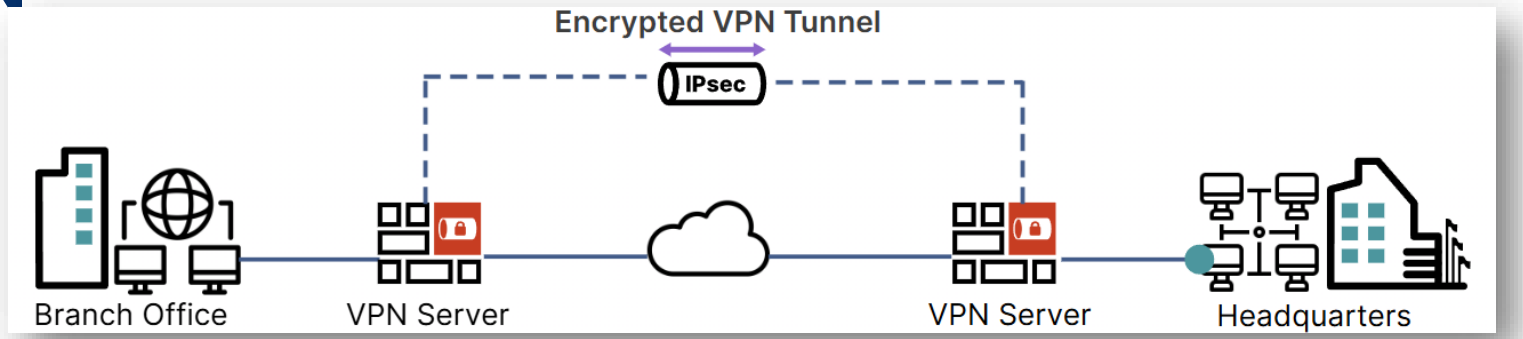
- Využíva koncept tunelovania medzi dvomi sieťovými VPN bránami
- Site to Site topológie
  - Point to point
    - Najjednoduchšia
  - Full mesh
    - Najflexibilnejšia, redundantná, priamy spoj medzi pobočkami
    - Najzložitejšia, veľa zdrojov,
  - Partial mesh
    - Lacnejší variant Full mesh
  - Hub and Spoke
    - Medzi tým všetko prechádza cez centrálny bod — pozor na SPoF (Single Point of Failure)
- Poznámka: Všetky pripojenia môžu mať „lokálny breakout“







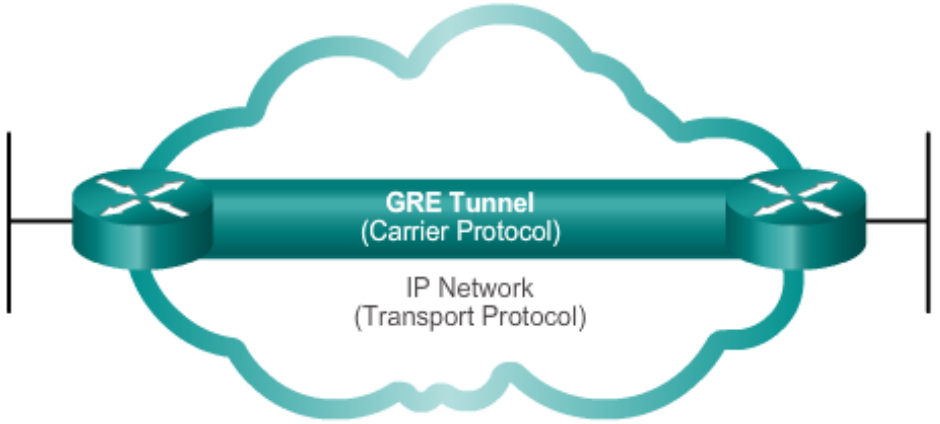
Site – to – Site VPN

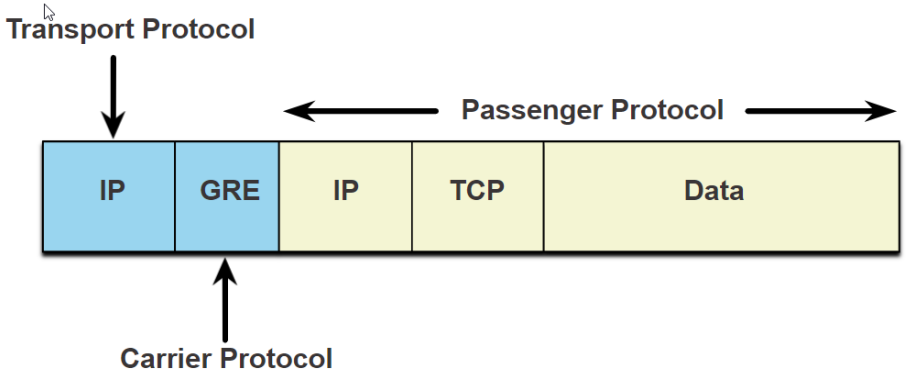


- **Cisco riešenia Site–to–Site VPN**
  - **Statické**
    - GRE
      - Nešifrovaná, preto sa už neodporúča
      - Alternativa:
        - DC siete: nvGRE, VxLAN, GENEVE
    - IPSec – venujeme sa extra
      - šifrovaná VPN, problém so smerovaním
    - GRE over IPSec
      - rieší problém so smerovaním, konfig. Overhead
    - IPsec Virtual Tunnel Interface (VTI)
    - Other
      - L2TP, L2TP over Ipsec, PPTP,
  - **Dynamické**
    - Cisco Dynamic Multipoint Virtual Private Network (DMVPN):
      - rieší overhead GREoverIPsec konfigurácie
    - SD-WAN

Generic Routing Encapsulation

- GRE je pomocný tunelovací protokol na 3. vrstve
  - Podporuje rôzne typy tunelovaných paketov
    - Napr. IPv4, IPv6, IPX...
  - Vytvára virtuálny point-to-point prepoj medzi dvojicou smerovačov
  - Umožňuje prenášať aj multicastovú prevádzku
- GRE charakteristiky
  - je bezstavový, bez riadenia toku dát
  - GRE neposkytuje zabezpečenie
    - žiadna dôvernosť, autentifikácia alebo kontrola integrity
  - Vkladá sa do IP paketov, overhead GRE tunelov je 24B
    - 20B na novú IP hlavičku a 4B na GRE hlavičku
  - Na smerovači vytvára „normálne“ rozhranie
    - Tunnel môže byť vložený do smerovacieho procesu

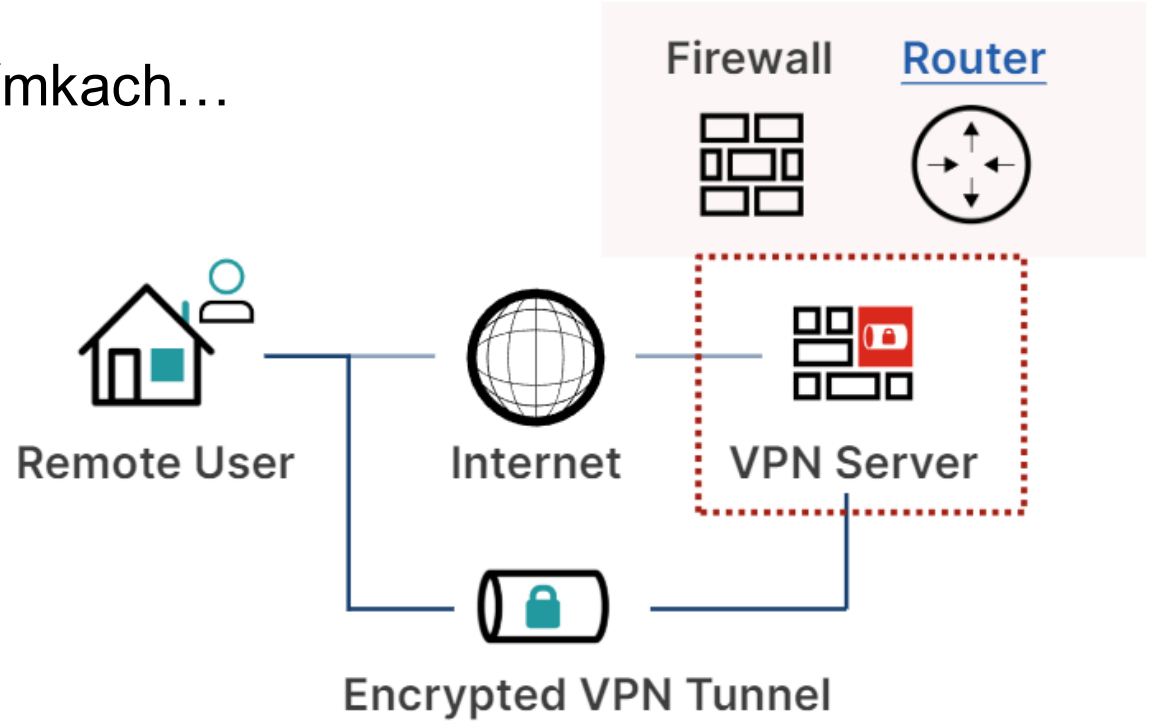





```
Frame 934: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface -, id 0
Ethernet II, Src: ca:01:47:4d:00:08 (ca:01:47:4d:00:08), Dst: ca:03:49:f6:00:08 (ca:03:49:f6:00:08)
Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.17.0.1
Generic Routing Encapsulation (IP)
  Flags and Version: 0x0000
      0... .... .... .... = Checksum Bit: No
      .0.. .... .... .... = Routing Bit: No
      ..0. .... .... .... = Key Bit: No
      ...0 .... .... .... = Sequence Number Bit: No
      .... 0... .... .... = Strict Source Route Bit: No
      .... .000 .... .... = Recursion control: 0
      .... .... 0000 0... = Flags (Reserved): 0
      .... .... .... .000 = Version: GRE (0)
    Protocol Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
Internet Control Message Protocol
```

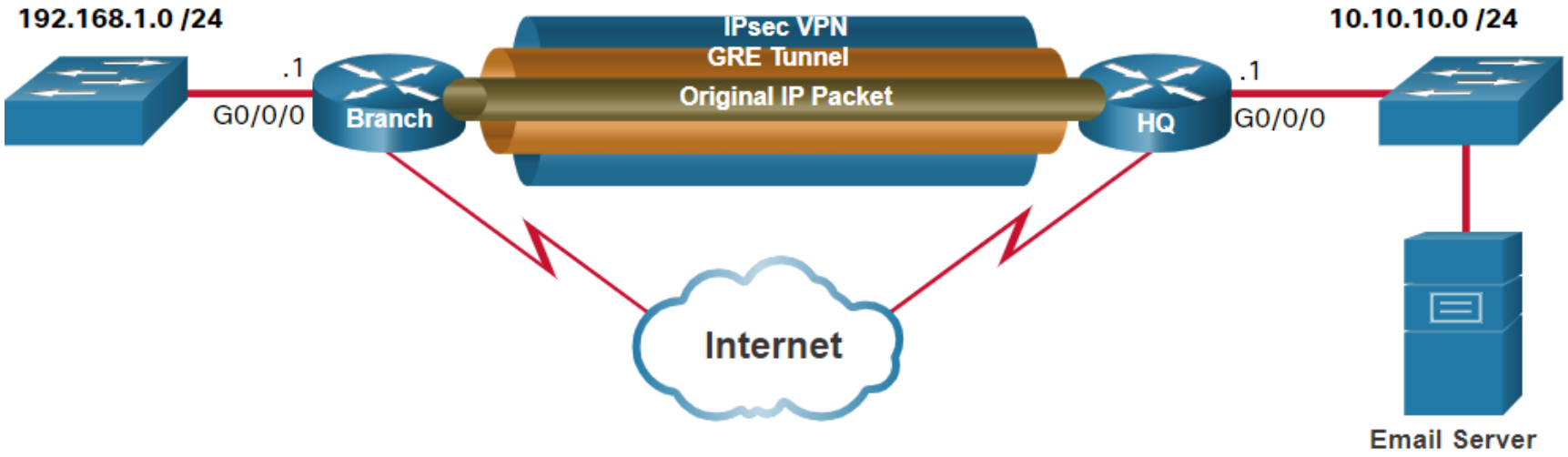
IPsec

- **Podporuje princípy CIA *(Confidentiality, Integrity, Availability)***
  - Nepodporuje smerovanie
  - Chýba sieťové rozhranie
  - Bude predstavené na nasledujúcich snímkach…



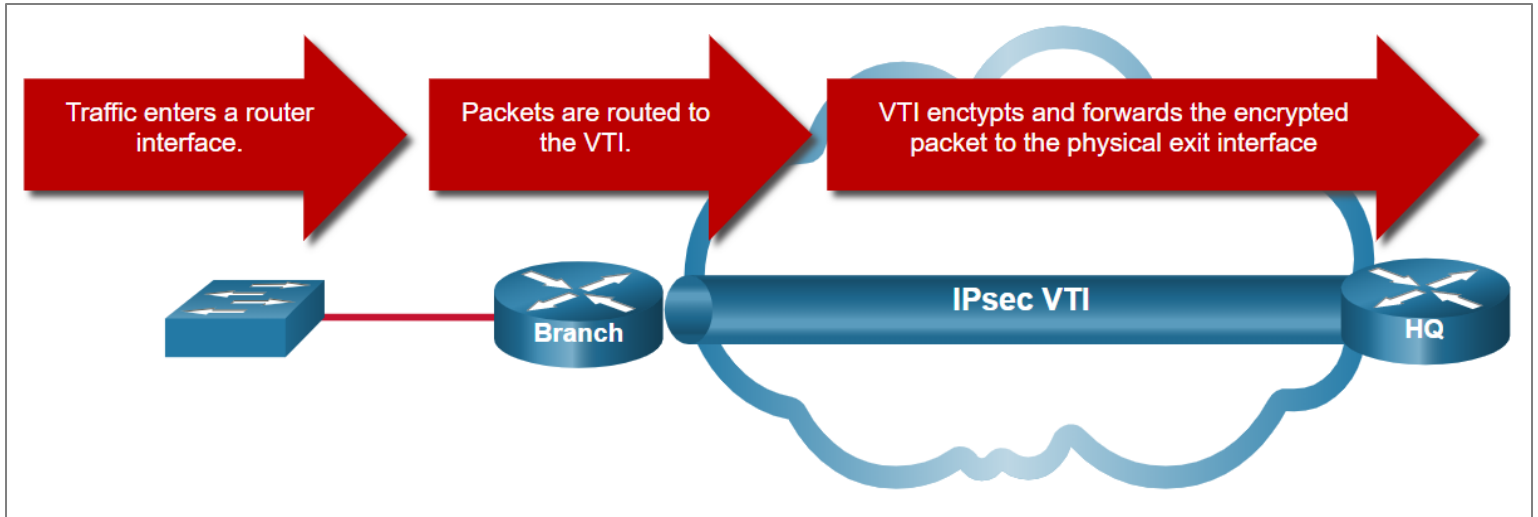
GRE over IPsec

- V realite na sieťových zariadeniach máme nasledovný problém:
  - GRE
    - Podporuje smerovanie cez GRE rozhranie
    - Je všk nešifrovaný => neodporúča sa jeho samostatné nasadenie do „živého” prostredia
  - IPSec
    - je šifrovaný,
    - ale v bežnej konfigurácii nemá v Cisco IOS rozhranie
      - Nedá sa nad ním spustiť smerovanie
  - Riešenie => spojenie a nasadenie oboch => GRE cez IPsec



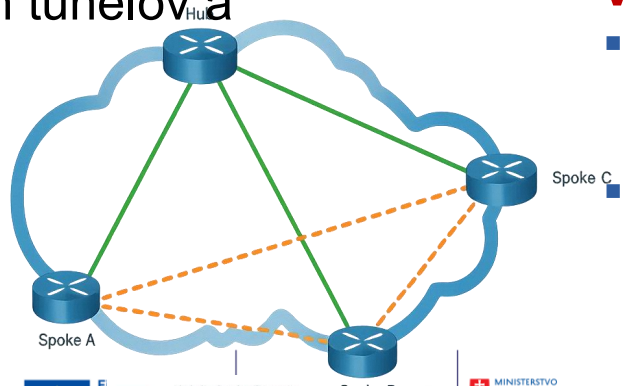
IPsec Virtual Tunnel Interface (VTI) – modernejší IPsec

- **Virtuálne tunelové rozhranie (VTI)**
  - Cisco technológia
  - **Zjednodušuje** konfiguráciu a správu
    - Na rozdiel od tradičných *crypto map* konfigurácií
  - Vytvára logické routovateľné tunelové rozhranie pre každého VPN partnera (**VTI interface**)
    - Rozhrania sú jednoduchšie na správu a konfiguráciu
    - Všetky nastavenia sa aplikujú priamo na rozhranie
- **Typy VTI rozhraní**
  - **Statické VTI**
    - Fixný tunel k špecifickému peerovi (partnerovi)
  - **Dynamické VTI (DVTI)**
    - Automaticky vytvára tunely
    - Vhodné pre dynamické prostredia (napr. hub-and-spoke, dial-up VPN)
- **Routovaná VPN riešenie**
  - Umožňuje prevádzku dynamických smerovacích protokolov (OSPF, EIGRP, BGP, RIP) cez IPsec tunely
  - Podpora pre unicast aj multicast routovanie
  - Nahrádza potrebu GRE tunelov pre podporu dynamického routingu



Dynamické Multipoint VPN (DMVPN)

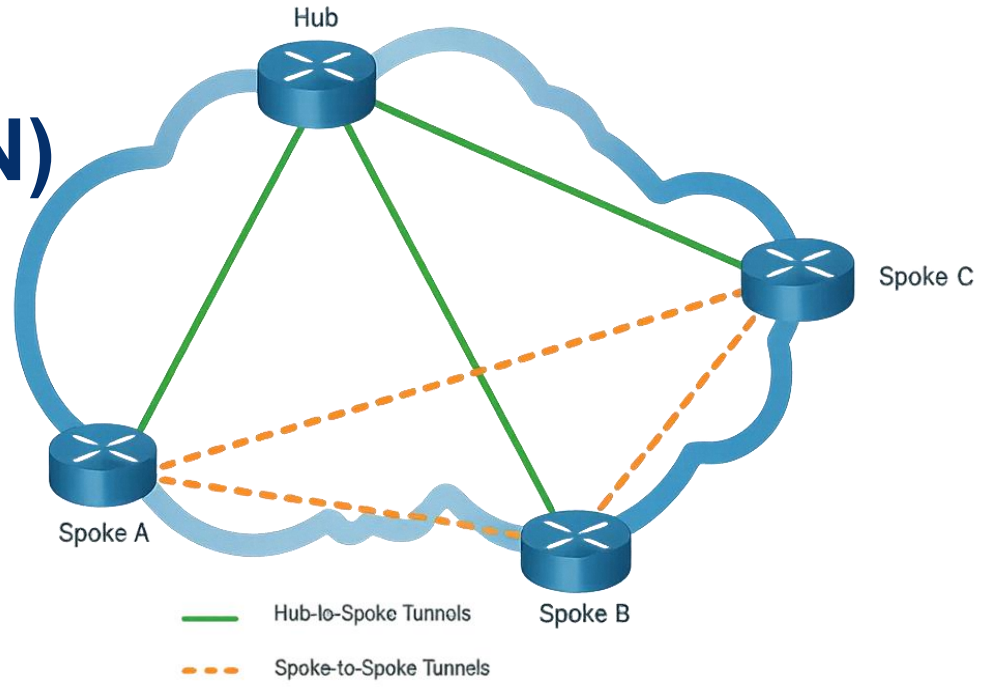
- **Problém s GRE cez IPsec**
  - GRE cez IPsec konfigurácia:
    - Vytvára point-to-point tunely
    - Vytvárajú sa manuálne a staticky
    - ⇒ zdĺhavé, vhodné len pre malé množstvo pobočiek
- **Cisco riešenie ⇒ Dynamic Multipoint VPN (DMVPN)**
  - Cisco VPN riešenie pre podniky s viacerými pobočkami
  - Škálovateľné riešenie pre veľký počet pobočiek
  - Umožňuje dynamické, jednoduchšie vytváranie GRE-over-IPsec VPN, aby sa vyriešil problém mnohých tunelov a routovania
  - Odporúčané nasadenie:
    - Hub-to-Spoke tunely
    - Spoke-to-Spoke tunely



- **Výhody**
  - **Škálovateľnosť**
    - Dynamické tunely medzi spoke bez potreby rekonfigurácie iných prvkov siete
  - **Optimalizovaná prevádzka**
    - Priame tunely spoke-to-spoke
    - Znižuje závislosť od hubu
    - Minimalizuje preťaženie hubu
  - **Zjednodušená konfigurácia**
    - Netreba manuálne vytvárať statické VPN tunely medzi každým párom spoke
  - **Nákladová efektívnosť**
    - Znižuje prevádzkové náklady
    - Optimalizuje využitie liniek
- **Výzvy**
  - **Komplexita pri nasadení**
    - Počiatočné nastavenie môže byť zložité
    - Vyžaduje dobré znalosti technológií
  - **Integrácia smerovacích protokolov**
    - Nasadenie dynamických routovacích protokolov (OSPF, EIGRP, BGP) v DMVPN môže byť náročné vo väčších sieťach

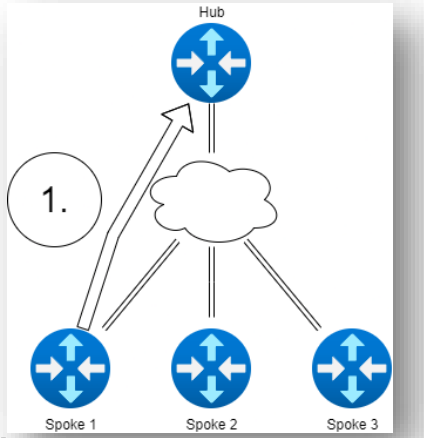
Dynamické Multipoint VPN (DMVPN)

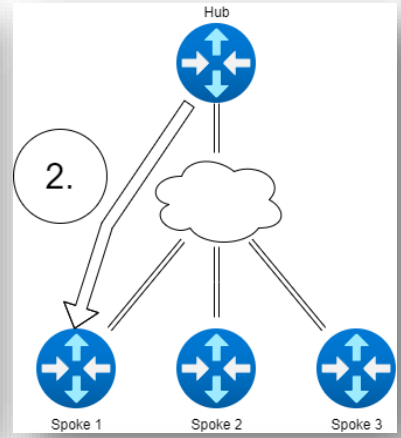
- **Spája tri sieťové technológie:**
  - **1. Multipoint GRE tunely (mGRE)**
    - Jedno rozhranie podporuje viacero GRE tunelov (multipoint)
    - Umožňuje vyhnúť sa potrebe viacerých point-to-point tunelových rozhraní na jednom routeri (napr. hub)
  - **2. NHRP – Next Hop Resolution Protocol**
    - Dynamická detekcia IP adries „next-hop“ routerov pobočiek, kde chcem vytvoriť tunel
    - Mapovanie privátnej IP siete pobočky na verejnú IP adresu „next-hop“
    - Architektúra klient/server:
      - **Klient**: nahlasuje svoje IP adresy, registruje sa a žiada o mapovanie
      - **Server (hub)**: uchováva mapovania klientov
  - **3. IPsec (IP Security)**
    - Šifrovanie prenášaných dát
    - Nie je povinné, ale **odporúčané**

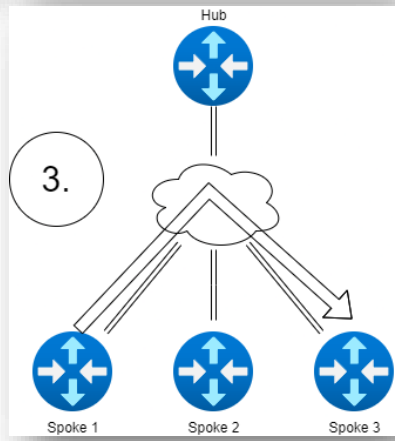


- **Aplikácia v topológii medzi**
  - **Hub Router**
    - Hlavný router v centre siete
    - Všetky spoke (pobočky) sa najskôr pripájajú na hub
    - Zodpovedný za správu dynamického vytvárania tunelov
  - **Spoke Routers (pobočkové routery)**
    - Routery v pobočkách
    - Dynamicky vytvárajú GRE tunely:
      - k hubu
      - k iným spoke routerom (priama komunikácia)
      - ak je to možné, obchádzajú hub

Priebeh DMVPN a nadviazanie tunela







1. **Registrácia spoke routera**
   - Po spustení sa každý **spoke** router zaregistruje so svojou verejnou IP adresou na **hub** routeri pomocou **NHRP**
     - Proces: *NHRP Registration Request / NHRP Registration Reply*
   - Hub si buduje tabuľku: spoke → public IP mapping.
2. **Hub ako sprostredkovateľ**
   - Keď chce **spoke** komunikovať s iným **spoke**
     - Pošle dotaz na **hub**, aby získal IP adresu cieľového spoke
     - Proces: *NHRP Resolution Request / Resolution Reply*
3. **Dynamické vytvorenie tunela**
   - **Hub** odpovie IP adresou cieľového spoke
   - Inicializujúci spoke => vytvorí priamy **mGRE/IPsec tunela** k cieľovému spoke
4. **Priama komunikácia spoke-to-spoke**
   - Dáta potom tečú priamo medzi spoke routermi cez **IPsec tunel**
   - Výhody:
     - zníženie latencie, optimalizácia využitia šírky pásma, odbremenenie hub routera od preťaženia

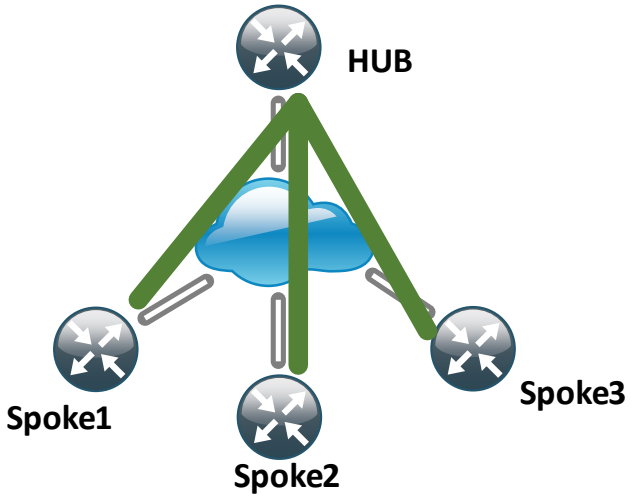
Architektonický spôsob fungovania DMVPN

- **Fungovanie DMVPN**:
  - **Fáza 1:**
    - len hub-and-spoke tunely → všetko ide cez hub
    - jednoduché, statické, menej efektívne
  - **Fáza 2:**
    - Je možné Priame spoke-to-spoke spojenie
      - ale bez redirectu na Hub → môžu vznikať suboptimálne cesty
    - Znižuje záťaž na hub, ale stále nie úplne optimalizované
    - Routing ešte nie je optimálny
  - **Fáza 3:**
    - Plne dynamické tunely s podporou shortcut routing
    - Hub poskytuje redirect informácie, aby spokes vedeli vytvoriť optimálnu trasu
    - moderné, plne dynamické, optimálne

- **Fázy DMVPN**
  - Nie sú konkrétne konfiguračné príkazy
    - Aka dmvpn phase 1
  - Je to „spôsob fungovania siete“:
    - ako sa vytvárajú tunely (len spoke–hub, alebo aj spoke–spoke),
    - ako funguje routovanie (statické / dynamické / redirect),
    - ako sa hub a spoke správajú pri výmene NHRP správ
- Cisco ich definuje ako logické etapy evolúcie DMVPN

DMVPN fázy – Fáza 1 - Iba Hub-and-Spoke

- **Prevádzka (Traffic)**
  - Všetka prevádzka, vrátane komunikácie medzi spoke **musí prechádzať cez hub**
  - Neexistuje žiadne priame spojenie spoke-to-spoke
- **Topológia**
  - Čistý model hub-and-spoke
  - Všetky tunely sú point-to-point
    - Od spoke k hubu
- **Smerovanie (Routing)**
  - Spoke používa statickú trasu smerom na hub
    - Všetky next-hop adresy sú IP adresy hubu
  - Celé smerovanie prebieha na hube
    - Hub má kompletnú smerovaciu tabuľku




```
Hub#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:15:23, expire 00:07:56
   Type: dynamic, Flags: registered
   NBMA address: 172.17.0.2
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:15:27, expire 00:07:52
   Type: dynamic, Flags: registered
   NBMA address: 172.18.0.2
10.0.0.4/32 via 10.0.0.4
   Tunnel0 created 00:15:26, expire 00:07:53
   Type: dynamic, Flags: registered
   NBMA address: 172.19.0.2
```

```
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel0 created 01:48:36, never expire
   Type: static, Flags:
   NBMA address: 172.16.0.2
```

Fáza 2: Spoke-to-Spoke via mGRE (partial mesh)

- **Cieľ:** *priama komunikácia Spoke ↔ Spoke* bez preťaženia Hubu
- **Základná myšlienka**
  - Dynamické **tunely medzi pobočkami (Spokes)**
  - **Hub sprostredkuje signalizáciu (NHRP)**,
    - Potom už **nie je v dátovej ceste** po nadviazaní spojenia
- **Ako to funguje**
  - Každý Spoke má tunel na Hub (mGRE).
  - Ak Spoke A potrebuje komunikovať so Spoke B:
    - Spoke A pošle paket Spoke B → ide cez Hub (má len default route)
    - Spoke A si potom od Hubu vyžiada NBMA adresu Spoke B (NHRP Resolution Request)
    - Hub odpovie (NHRP Resolution Reply)
    - Spoke A vytvorí priame GRE spojenie so Spoke B
    - Ďalšia komunikácia ide priamo A↔B bez Hubu

```
[Spoke A] ---- Registration ----> [Hub]
            (NHRP Reg Req/Reply)

[Spoke A] ---- Resolution Req ---> [Hub] ----> Lookup spoke B
[Hub] ----- Resolution Reply ----> [Spoke A] (IP of Spoke B)

[Spoke A] ============================> [Spoke B]
            (mGRE/IPsec tunnel established)

Dáta teraz tečú priamo medzi Spoke A a Spoke B
```

- **Výhody**
  - Priama komunikácia *Spoke ↔ Spoke* po inicializácii
  - Nižšia záťaž na Hub
- **Nevýhody**
  - Prvé pakety idú cez Hub
  - Vyžaduje presnú konfiguráciu routingu (next-hop)

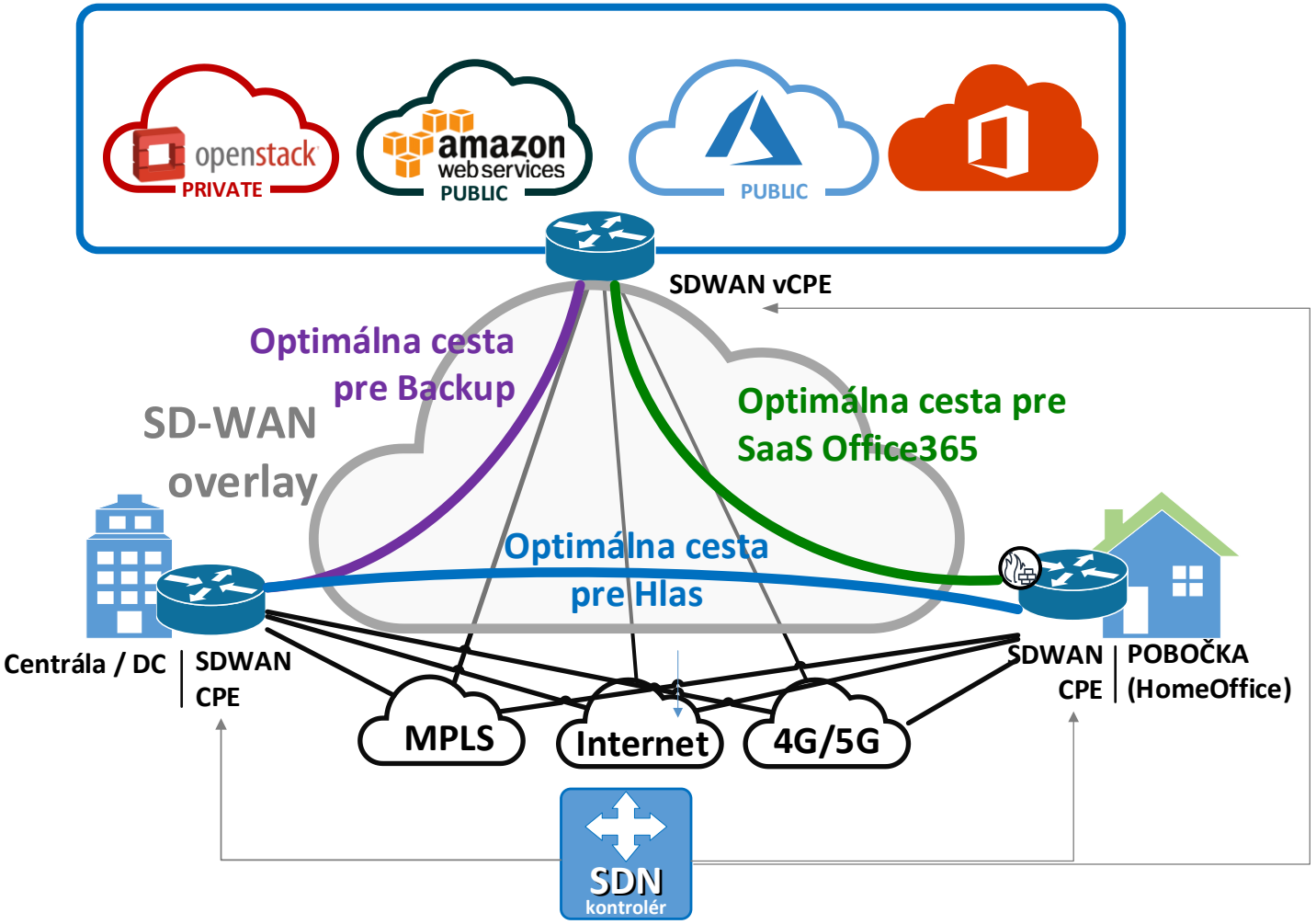
Fáza 3 - Dynamické Spoke-to-Spoke s NHR

- **Idea**
  - Najefektívnejšia a najmodernejšia verzia DMVPN.
  - Odstraňuje „**trombónovanie**“ z Fázy 2.
  - **Hub aktívne pomáha** Spokes vytvárať priame spojenia cez **NHRP Redirect / Shortcut**.
- **Ako to funguje**
  - Spoke A pošle paket na Spoke B → prvý paket ide cez Hub
  - Hub zistí, že cieľ aj zdroj sú Spokes v tom istom DMVPN.
  - Hub pošle **NHRP Redirect** → „Choď priamo na Spoke B“
  - Spoke A pošle Hubu **NHRP Resolution Request** → Hub odpovie s adresou B
  - Spoke A vytvorí **priame GRE spojenie so Spoke B**
  - Ďalšia komunikácia ide **priamo A↔B**,
    - Hub už nie je v dátovej ceste
- **Routing**
  - NHRP Redirect / Shortcut automaticky optimalizuje trasy
  - Routing protokoly (EIGRP, OSPF, BGP) fungujú bez úprav

- **Výhody**
  - Plne automatická optimalizácia trás
  - Žiadne „trombónovanie“ cez Hub
  - Najlepšia škálovateľnosť a efektivita
- **Nevýhody**
  - Vyžaduje príkazy ip nhrp redirect (Hub) a ip nhrp shortcut (Spoke)
  - O niečo zložitejšia signalizácia (NHRP Redirect + Reply)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SD-WAN – application and „*cloud-centric*“ solution



- **SD-WAN**
  - **Oddelenie dátovej a riadiacej roviny** (data plane vs. control plane)
  - **Centralizovaný management** – orchestrátor riadi politiku siete
  - **Aplikáciami riadené smerovanie** – prevádzka podľa SLA/QoS, nie len podľa IP prefixov
  - **Podpora multicloud a hybridných prostredí**
  - **Zabudovaná bezpečnosť** (IPsec, FW, segmentácia)

- **SD-WAN = SDN + cloud + WAN siete + virtualizácia + automatizácia + bezpečnosť**
  - Autonómne riadenie siete podľa požiadaviek aplikácii (SLA a kvalitu služby (QoS))

Architektonické vrstvy SD-WAN

- **Data Plane (Forwarding Layer)**
  - Prenos dát cez WAN (MPLS, Internet, LTE/5G)
  - IPsec tunely medzi edge zariadeniami
- **Control Plane (Routing & Policies)**
  - Dynamické vytváranie tunelov
  - Politiky pre smerovanie podľa aplikácií
- **Management & Orchestration Layer**
  - Centralizovaná správa (vCloud Director, vManage, DNA Center…)
  - Monitorovanie výkonu, automatizácia a reporting

Kľúčové časti SD-WAN

- **Kľúčové komponenty**
  - **Edge zariadenia (SD-WAN CPE / routery)** – v pobočkách, dátových centrách, cloude
  - **Controllers**
    - Orchestrátor (Zero-Touch Provisioning, management)
    - Control (výmena routing informácií, politika)
    - Data (tunelovanie, distribúcia dát)
  - **Security funkcionality**
    - Šifrovanie, NGFW, IDS/IPS, URL filtering, CASB integrácia
  - **Analytics a Telemetria**
    - Viditeľnosť nad aplikáciami, SLA monitoring

- **Kľúčové technologické súčasti**
  - **Overlay tunely (IPsec/GRE/DTLS/TLS)**
    - bezpečný prenos
  - **Application-Aware Routing**
    - výber linky podľa aplikácie, SLA a stavu siete
  - **Path Conditioning**
    - FEC, packet duplication, jitter buffering
  - **Cloud OnRamp**
    - optimalizácia prístupu do SaaS (O365, Salesforce, AWS, Azure, GCP)
  - **Zero-Touch Provisioning (ZTP)**
    - rýchle nasadenie bez manuálneho nastavovania

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Iné súčasné open prístupy k VPN

OpenVPN

- **Charakteristika**
  - Open-source, multiplatformový protokol
  - Pracuje na **transportnej/aplikačnej vrstve (SSL/TLS)**
  - Prenáša dáta cez TCP alebo UDP (často port 443)
    - vyzerá ako HTTPS prevádzka
- **Bezpečnosť**
  - Šifrovanie: AES (128/256), ChaCha20
  - Autentifikácia: certifikáty (X.509), PSK, LDAP/RADIUS integrácia, podpora MFA
  - Podpora TLS 1.2 a vyššie, HMAC pre integritu

- **Výhody**
  - Prejde cez väčšinu firewallov a NAT (využitie portu 443)
  - Veľká flexibilita a vysoká kompatibilita (Windows, Linux, macOS, mobilné OS, appliance)
  - Open-source, auditovaný a široko podporovaný v komerčných VPN riešeniach
- **Nevýhody**
  - Komplexnejšia konfigurácia a správa (PKI infraštruktúra, certifikáty)
  - Nižší výkon v porovnaní s WireGuard (väčší kód, vyšší overhead)
  - Závislosť od TLS stacku (potenciálne zraniteľnosti, ak sa nepoužívajú moderné knižnice)

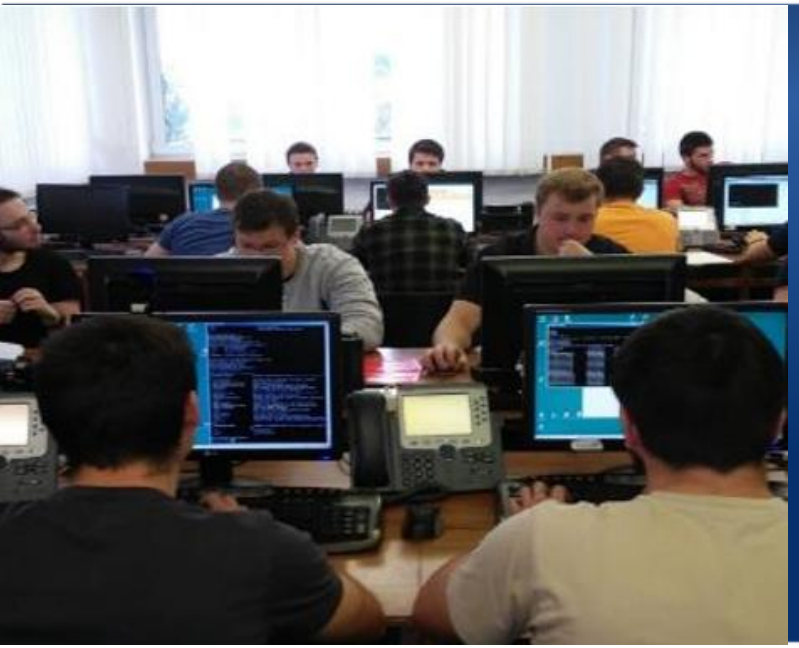
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

WireGuard a SSTP

- **WireGuard**
  - **Charakteristika**
    - Moderný, minimalistický VPN protokol (~4000 riadkov kódu)
    - Pracuje na **sieťovej vrstve (Layer 3)**, podobne ako IPsec
    - Vstavaný do Linux jadra, dostupný aj na Windows, macOS, mobilné OS
  - **Bezpečnosť a výkon**
    - Moderná kryptografia: ChaCha20, Poly1305, Curve25519, BLAKE2s
    - Rýchly handshake, nízky overhead, vysoký výkon aj v mobilných sieťach
    - Automatický roaming IP adries – vhodný pre mobilné zariadenia
- **Výhody**
  - Jednoduchá konfigurácia (ako nastaviť IP tunel)
  - Malý kód = ľahko auditovateľný, nižšie riziko chýb
  - Vysoká efektivita → vhodné pre cloud a kontajnerové prostredia
- **Nevýhody**
  - Menej enterprise funkcionalít než IPsec (QoS, granularita politiky)
  - Ešte nie je plne štandardizovaný (IETF draft, ale široko adoptovaný)

Porovnanie VPN protokolov

Protokol	Vrstva OSI	Šifrovanie / bezpečnosť	Výhody	Nevýhody	Použitie
IPsec	Sieťová (L3)	AES, 3DES, SHA, DH/ECDH, PFS	Štandardizovaný, enterprise funkcionality, podpora dynamického routingu, QoS	Zložitejšia konfigurácia, NAT traversal problémy	Site-to-Site VPN, enterprise remote access
OpenVPN	Transportná/aplikačná (L4–7, SSL/TLS)	TLS 1.2/1.3, AES, ChaCha20, HMAC	Flexibilita (UDP/TCP, port 443), open-source, široká podpora, MFA integrácia	Komplexnejšia PKI správa, vyšší overhead, slabší výkon	Remote access VPN, prechod cez firewally/proxy
WireGuard	Sieťová (L3)	ChaCha20, Poly1305, Curve25519, BLAKE2s	Minimalistický kód, veľmi rýchly, jednoduchá konfigurácia, vhodný pre mobilné siete a cloud	Menej enterprise funkcií (QoS, granularita), nie plne štandardizovaný	Mobilné VPN, cloud prostredia, kontajnery



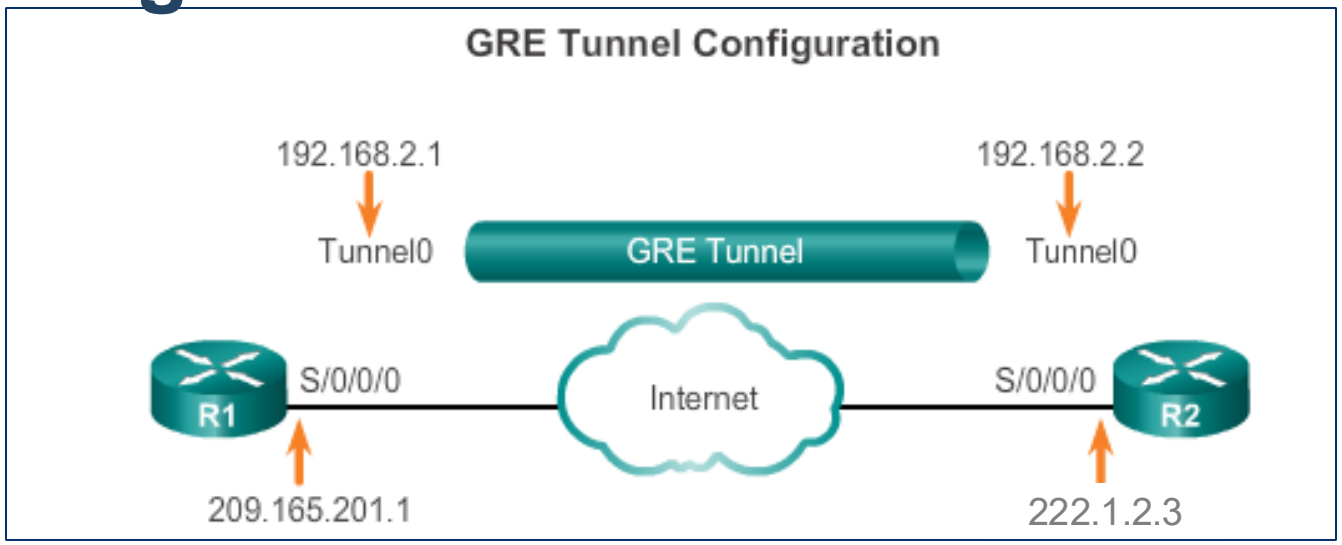
Jednoduchá konfigurácia GRE (Generic Routing Encapsulation)

Site-to-site GRE tunnely

Konfigurácia GRE tunelov

- GRE tunely sú na smerovači reprezentované virtuálnym rozhraním Tunnel
- Rozhranie Tunnel musí mať definované
  - Vlastnú IP adresu (ako každé iné rozhranie)
  - IP adresu odosielateľa
    - Odosielajúce rozhranie or IP adresa odosielajúceho rozhrania
  - IP adresu príjemcu nosných (carrier) paketov
  - Režim tunelovania
- Dvojica rozhraní Tunnel na rôznych smerovačoch, ktoré komunikujú, musí spĺňať tieto kritériá:
  - Vlastné IP adresy rozhraní Tunnel musia byť v tej istej sieti (rovnako ako na dvojici vzájomne prepojených rozhraní)
  - IP adresy odosielateľa a príjemcu musia navzájom korešpondovať (IP odosielateľa na jednom routeri musí zodpovedať IP príjemcu na druhom routeri a obrátene)
- Predvolený bandwidth rozhrania Tunnel je 9 Kbps
  - Mysli na EIGRP či OSPF metriku
  - Odporúča sa zvýšiť ho na realistickú hodnotu

Príklad konfigurácie GRE tunela




```
hostname Bratislava
!
interface Serial0/0/0
 ip address 209.165.201.1 255.255.255.0
 no shut
!
interface Tunnel0
 bandwidth 1000
 tunnel source s0/0/0
 ! Or
 ! tunnel source 209.165.201.1
 tunnel destination 223.1.2.3
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
```

```
hostname Kosice
!
interface Serial0/0/0
 ip address 222.1.2.3 255.255.255.0
 no shut
!
interface Tunnel7
 bandwidth 1000
 tunnel source s0/0/0
 ! Or
 ! tunnel source 222.1.2.3
 tunnel destination 209.165.201.1
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 192.168.2.2 255.255.255.0
!
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
```

Stav rozhraní Tunnel

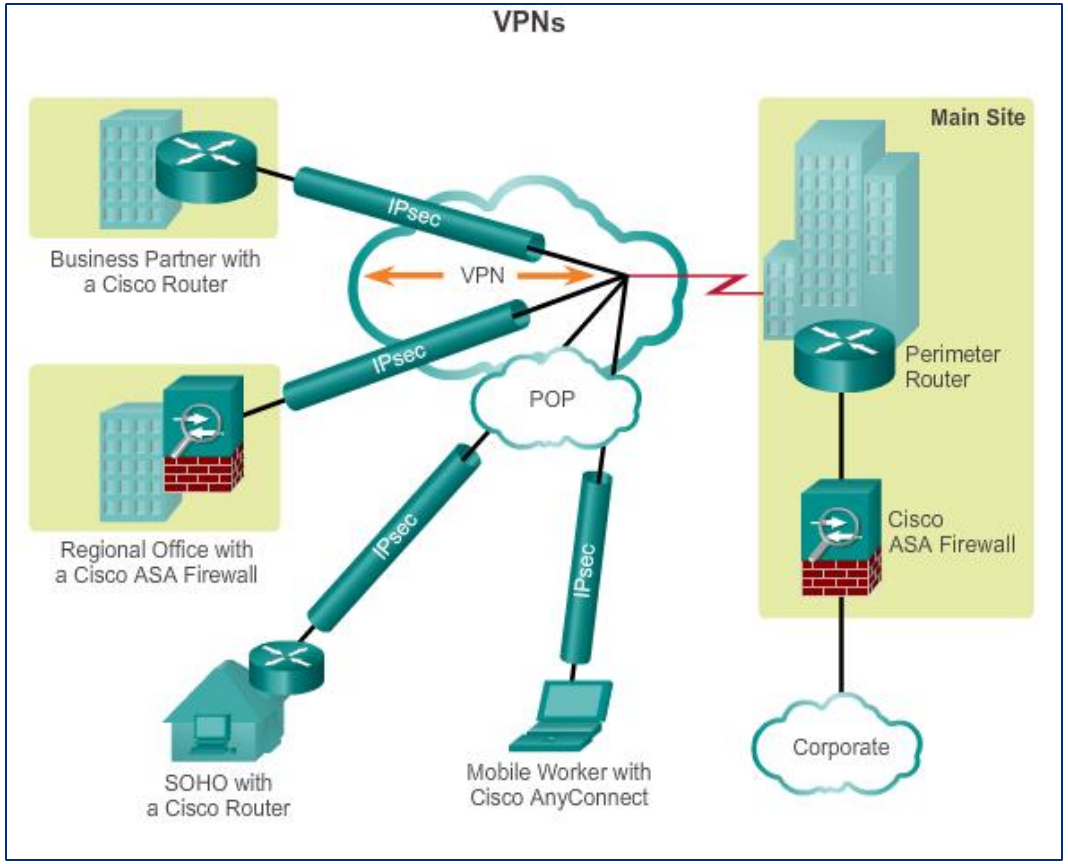
- Rozhrania Tunnel pri GRE budú „up, protocol up“, ak sú splnené súčasne všetky nasledujúce podmienky
  - Rozhranie má definovaný zdroj a cieľ príkazmi **tunnel source**, **tunnel destination**
    - Tunel má definovanú platnú zdrojovú a cieľovú IP
  - Skutočné rozhranie, z ktorého si požičiavame zdrojovú IP v príkaze **tunnel source**, je v stave „up, protocol up“
    - Zdrojová IP adresa musí byť živá
  - V smerovacej tabuľke vieme vyhľadať cestu k náprotivnému koncu tunela definovanému príkazom **tunnel destination**
    - Cieľová IP adresa musí byť podľa našej RT dosiahnuteľná
  - Ak je zapnuté použitie GRE Keepalive, druhá strana odpovedá na naše Keepalive pakety
    - Vnútro transportnej siete musí byť schopné doručovať pakety medzi koncami tunela

IPsec VPN - Komponenty a činnosť

Úvod do IPsec

IPsec VPNs

- IPsec je séria IETF štandardov popisujúcich spôsob bezpečného prenosu IP paketov
  - Pracuje na L3
- Neviaže sa na konkrétny algoritmus/mechanizmus
  - Šifrovací, autentifikačný či iný bezpečnostný algoritmus/mechanizmus
  - Schopná využívať rôzne existujúce aj budúce mechanizmy
- Pracuje na L3 ako tunelovací machanizmus
  - Zabezpečuje tak L3 pakety
    - v IPv4 doplnené, vyžaduje klienta
    - v IPv6 natívna súčasť
  - Zabezpečuje spojenie
    - Site-to-site, remote



Technológia IPsec

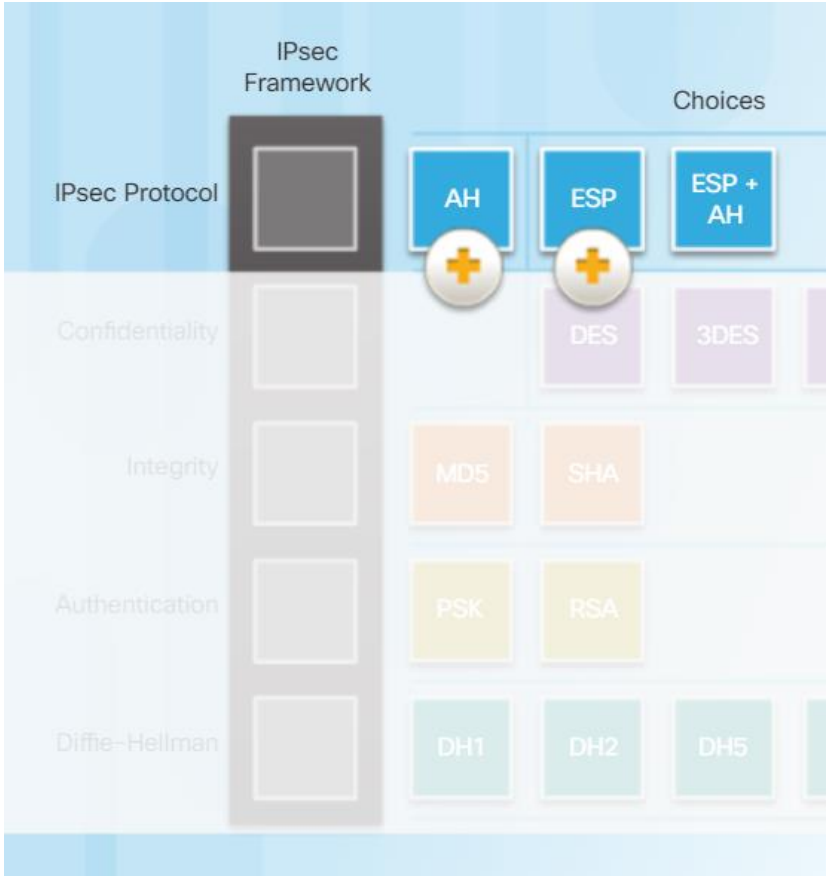
- Je to Framework viacerých otvorených štandardov pre poskytnutie spoľahlivej komunikácie
- IPsec poskytuje CIA vlastnosti
- Štyri stavebné bloky IPsec
  - IPsec framework protokol
    - Riešenie prenosu paketov (ESP, AH, ESP+AH)
  - Utajenie údajov (**Confidentiality**)
    - Šifrovaním, aby nebolo možné správu dešifrovať a prečítať (DES, 3DES, AES ...)
  - Integritu dát (**Integrity**)
    - Dôkaz že správa nebola zamenená.
    - Dosiahnuté hešovaním (MD5 or SHA).
  - Autentifikáciu odosielateľa (**Authenticity**)
    - Dôkaz. že správa nie je podvod a prišla od toho, kto si myslím že je.
    - Dosiahnuté autentifikáciou (PSK or RSA)
  - Diffie-Hellman
    - Bezpečná výmena šifrovacích kľúčov

Sada použitých parametrov vytvára tzv. Security association (SA)

IPsec – protocol framework

IPsec Protokol Framework (cont.)

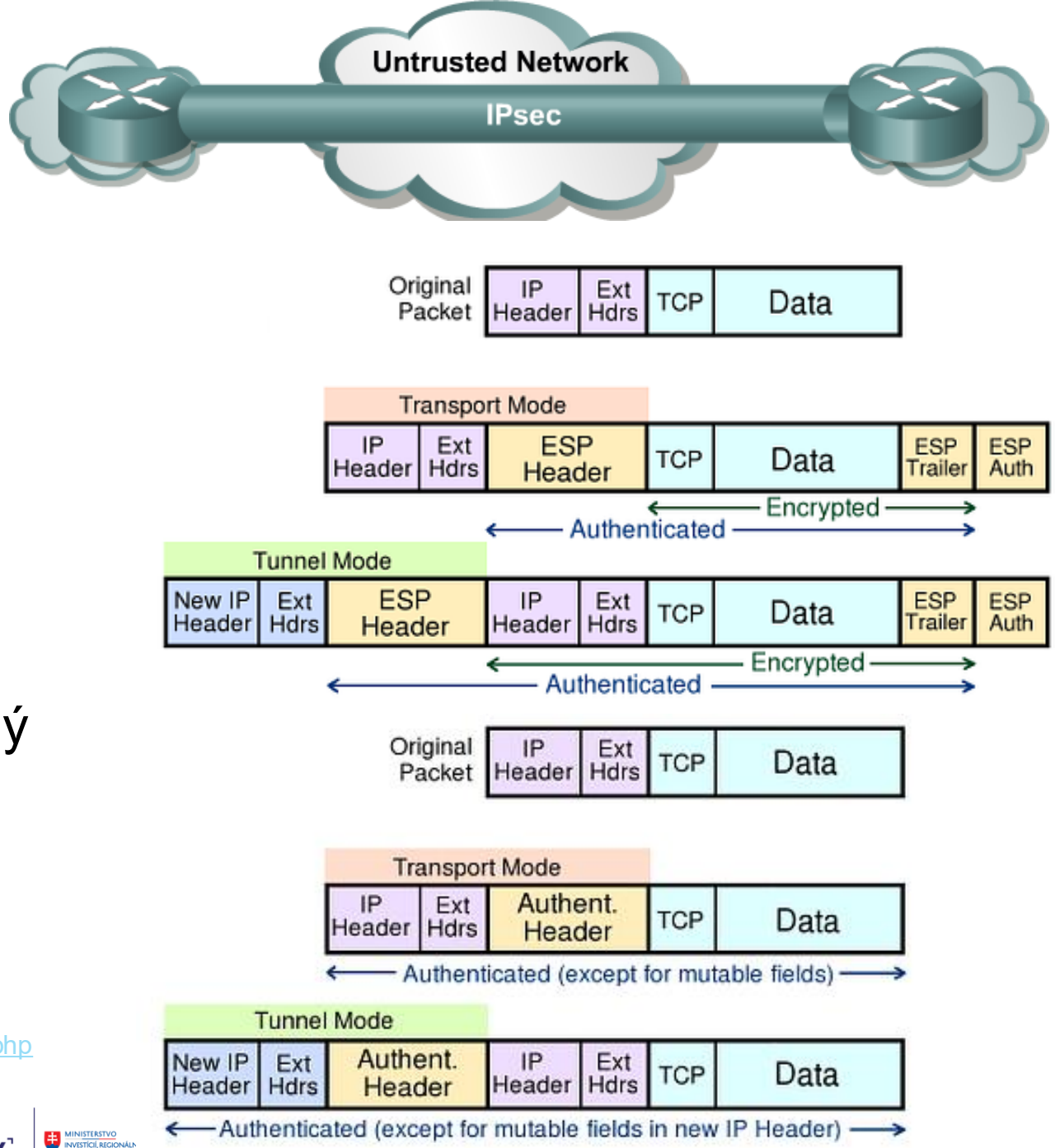
- Definuje spôsob činnosti IPsec,
- Sú dva základné modely:
  - Authentication header (AH)
    - Chráni kompletný obsah paketu vrátane nemenných častí IP hlavičky autentifikačnými mechanizmami
    - Nezabezpečuje však šifrovanie
    - Nemá rada NAT (prepisuje IP adresy v hlavičke)
  - Encapsulation Security Payload (ESP)
    - Chráni payload paketu šifrovaním
    - V transport režime nezabezpečuje hlavičku paketu
    - Autenticitu chráni dodatočne
- Pozn.
  - Použitie AS či ESP určuje aké ďalší CIA možnosti budú v ponuke
  - AH je v súčasnosti používaný zriedkavo, ESP veľmi často (firewally ASA AH vôbec nepodporujú)
  - AH a ESP možno použiť súčasne



Režimy práce IPsec protokolov

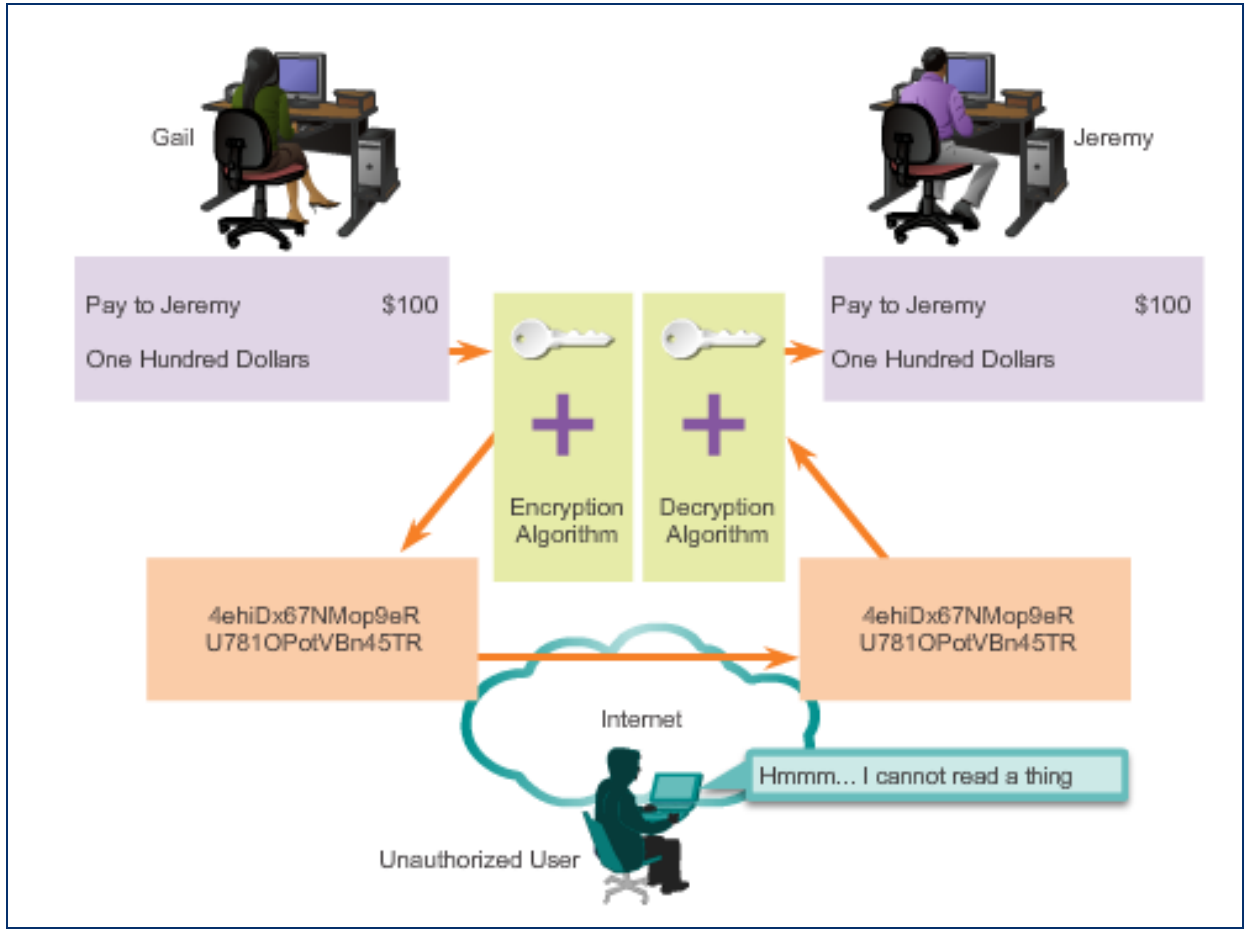
- Tunelový režim
  - Prikladá novú IP hlavičku a tuneluje pôvodný IP paket
  - Preferovaný
- Transportný režim
  - Ponecháva pôvodnú IP hlavičku
  - Na Cisco routeroch sa transportný režim využije len vtedy, ak je odosielateľom (autorom) paketu sám router

- Pozn. Obr. Z http://www.ipv6now.com.au/primers/IPv6PacketSecurity.php



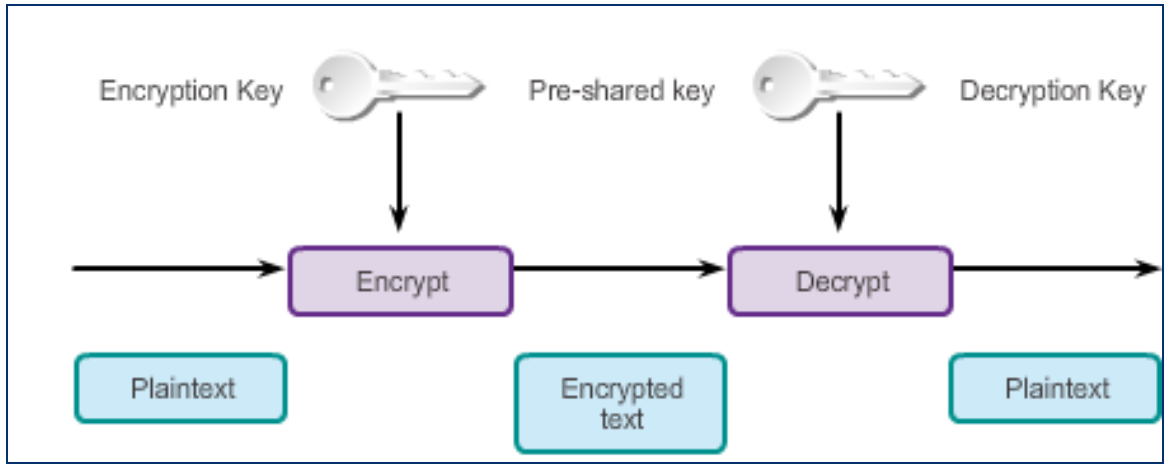
Utajenosť šifrovaním (Confidentiality with Encryption)

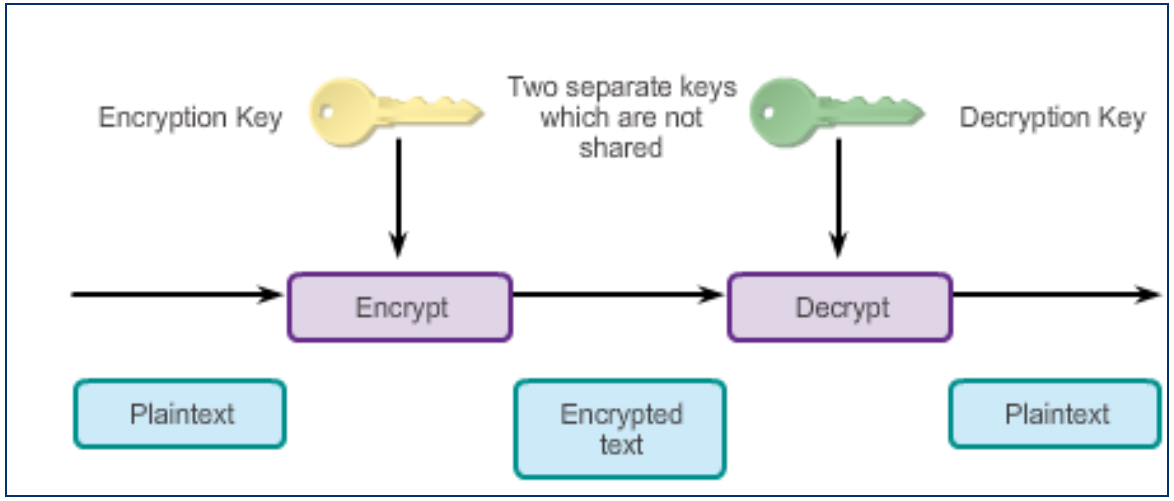
- Využíva techniky symetrického šifrovania
  - Konverzie pôvodnej správy do jej zameneného variantu
- Aby šifrovanie pracovalo správne
  - Musí odosielateľ aj príjemca poznať pravidlá použité na transformáciu pôvodnej správy do jej kódovanej podoby a späť.
- Pravidlá sú založené na algoritmoch a pridružených kľúčoch.
  - Dešifrovanie je bez správneho kľúča mimoriadne ťažké (alebo nemožné)



Šifrovacie Algoritmy

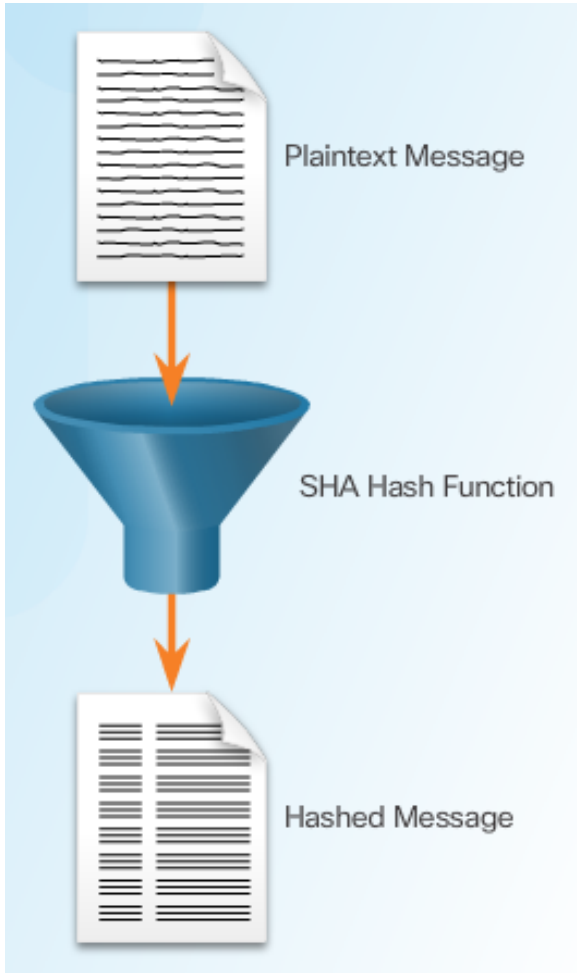
- Dva hlavné typy:
  - **Symetrické algoritmy**
    - **Rovnaký** kľúč pre šifrovanie aj dešifrovanie
    - DES, 3DES, AES, SEAL, RC šifry
    - Líšia sa rýchlosťou, silou kľúča (56-256b)
    - Nižšia bezpečnosť, veľká rýchlosť
  - **Asymetrické algoritmy**
    - Iný kľúč pre šifrovanie, iný pre dešifrovanie
    - Využíva RSA a PKI
      - Privátny a verejný kľúč
    - Vyššia bezpečnosť, sú však pomalšie, či chcú viac zdrojov
- Oba používajú šifrovacie kľúče
  - Balans medzi dĺžkou (bezpečnejšie) a spotrebou zdrojov a časom
  - Problém: ako si vymeniť kľúče?
- Výber algoritmu
  - Odolnosť, rýchlosť, dôveryhodnosť, sila kľúča

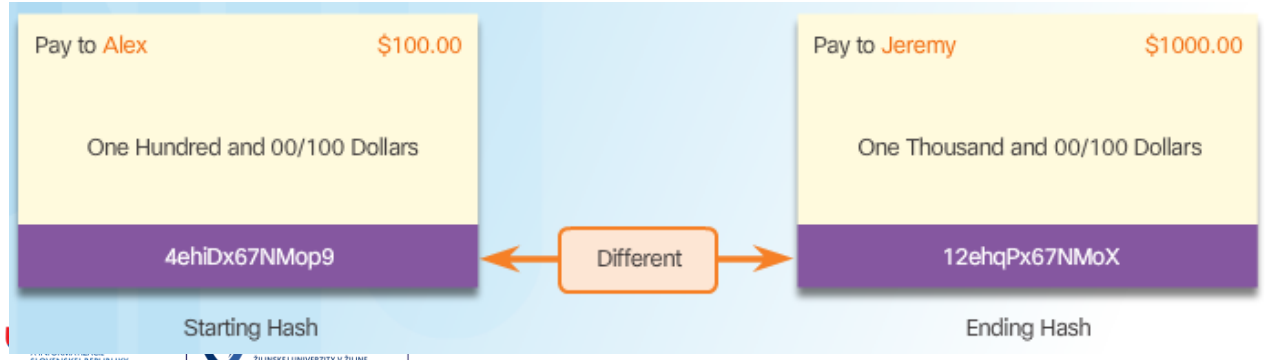




Dátová Integrita (Integrity)

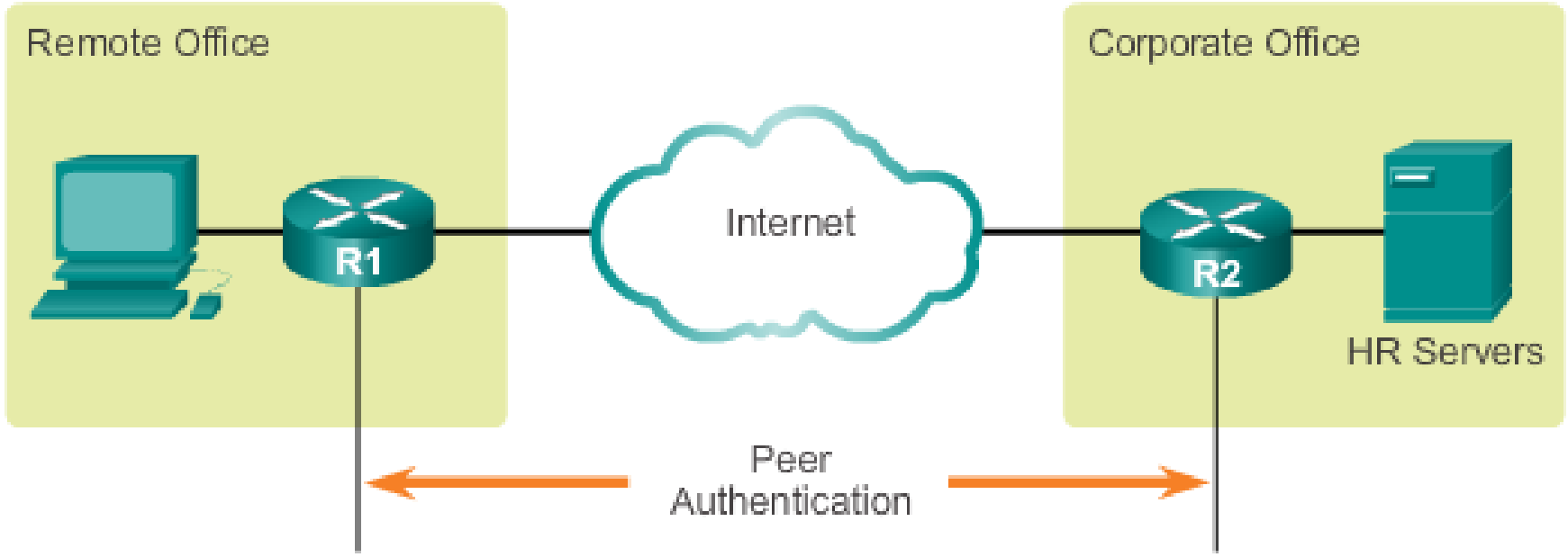
- Prostriedok na dosiahnutie, aby prijímateľ vedel, že so správou sa nemanipulovalo
  - Pôvodný odosielateľ
    - Generuje hash odosielanej správy
    - Ktorú pošle so samotnou správou.
  - Príjemca
    - Z prijatej správy vytvorí vlastný hash
    - Analyzuje správu a prijatý hash
    - Ak sú rovnaké, príjemca si môže byť primerane istý integritou pôvodnej správy.
  - Problém:
    - Nedá sa overiť či sa nemanipulovalo s hashom samotným
- Mechanizmy => Hashing
  - MD5 (kľúč 182-bit)
    - rýchly, ale prelomiteľný, už sa neodporúča
  - alebo SHA (160/256/512-bit)
- Autenticita hash-u sa dá dosiahnúť jeho zaśifrovaním





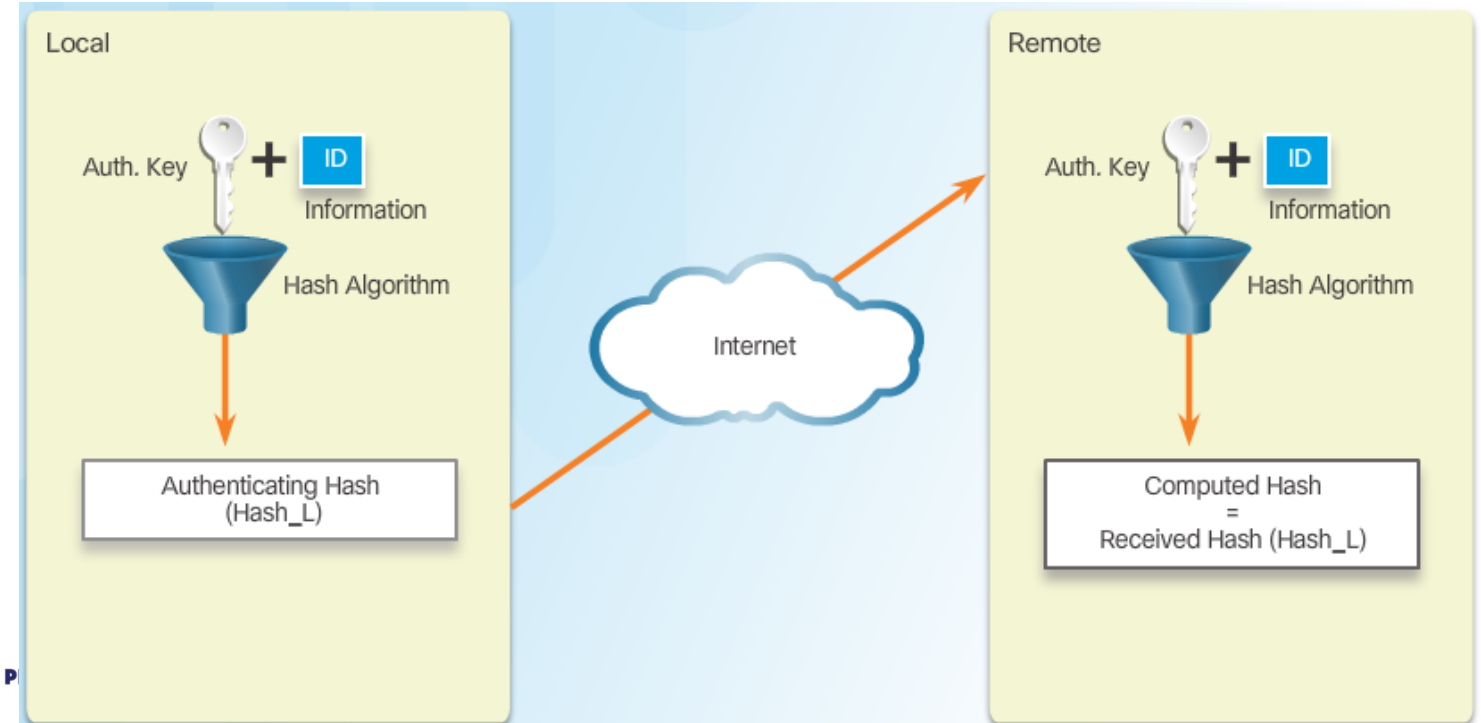
IPsec Autentifikácia (Authentication)

- Je druhá strana tým, kto si myslím že je?
  - Predtým, ako sa komunikačná cesta môže považovať za bezpečnú, musí sa zariadenie na druhom konci tunela VPN overiť
- IPsec podporuje dve autentifikačné metódy
  - **Pre-shared key (PSK) (zdieľaný kľúč)**
  - **Signatúry Rivest, Shamir a Adleman (RSA)**



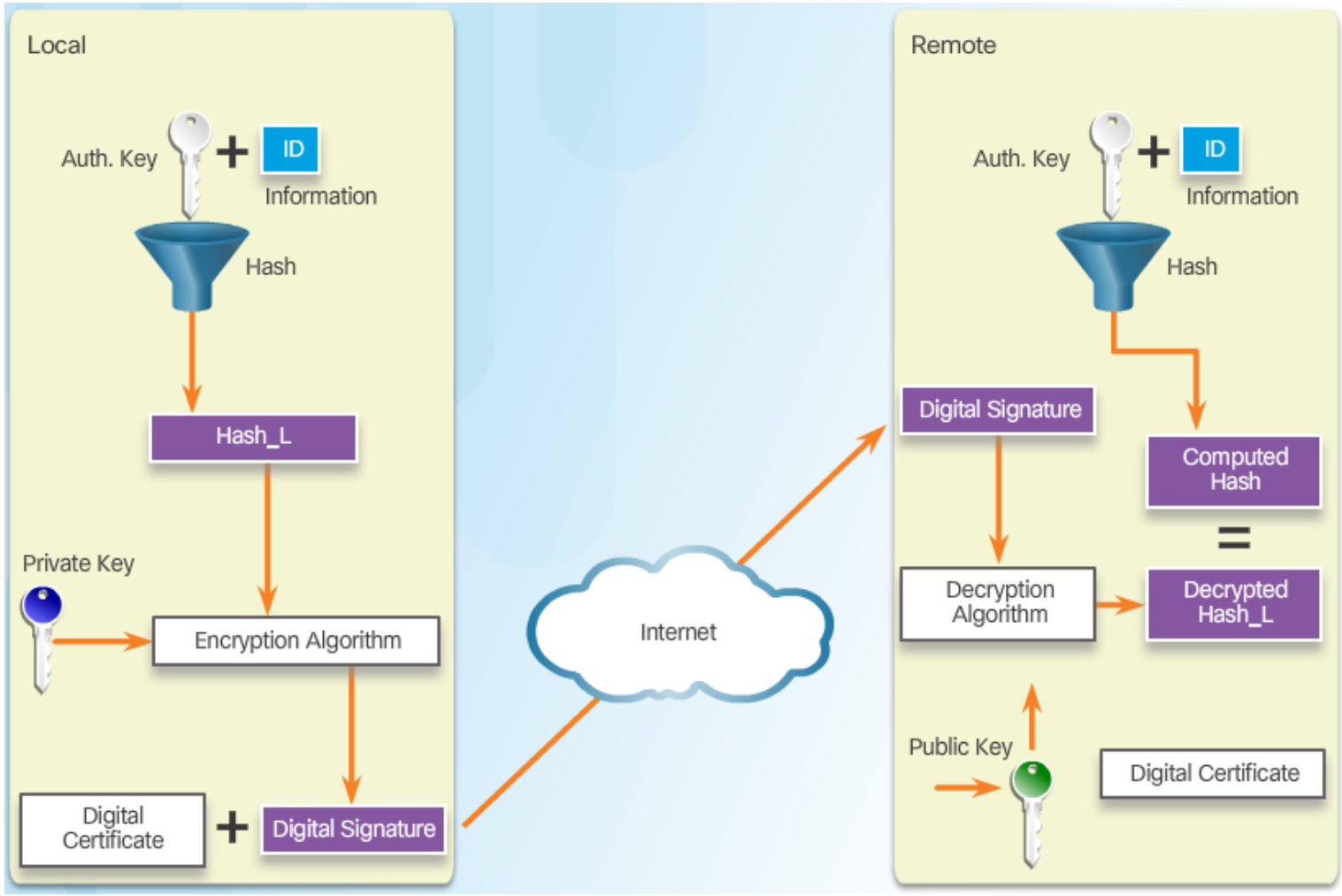
IPsec PSK autentifikácia

- **Pre-shared key (PSK) (zdieľaný kľúč)**
  - Využíva kľúčovo-založené hashovanie HMAC (Hash-based Message Authentication Code)
    - Zlepšenie hashovania pridaním tajného kľúča
    - Využíva symetrické šifrovanie
  - Kľúč sa zadáva na každom susedovi ručne adminom, jednoduchá manuálna konfigurácia
    - Riešenie nie je veľmi škálovateľné (kľúč na každom susedovi, veľa susedov, veľa kľúčov)



IPsec RSA autentifikácia

- **Signatúry Rivest, Shamir a Adleman (RSA)**
  - Na autentifikáciu susedov sa používajú digitálne certifikáty, vymenené medzi susedmi
  - Na zabezpečenie certifikátov používa digitálny podpis
  - Na šifrovanie používa asymetrické algoritmy



Výmena kľúčov cez Diffie-Hellman

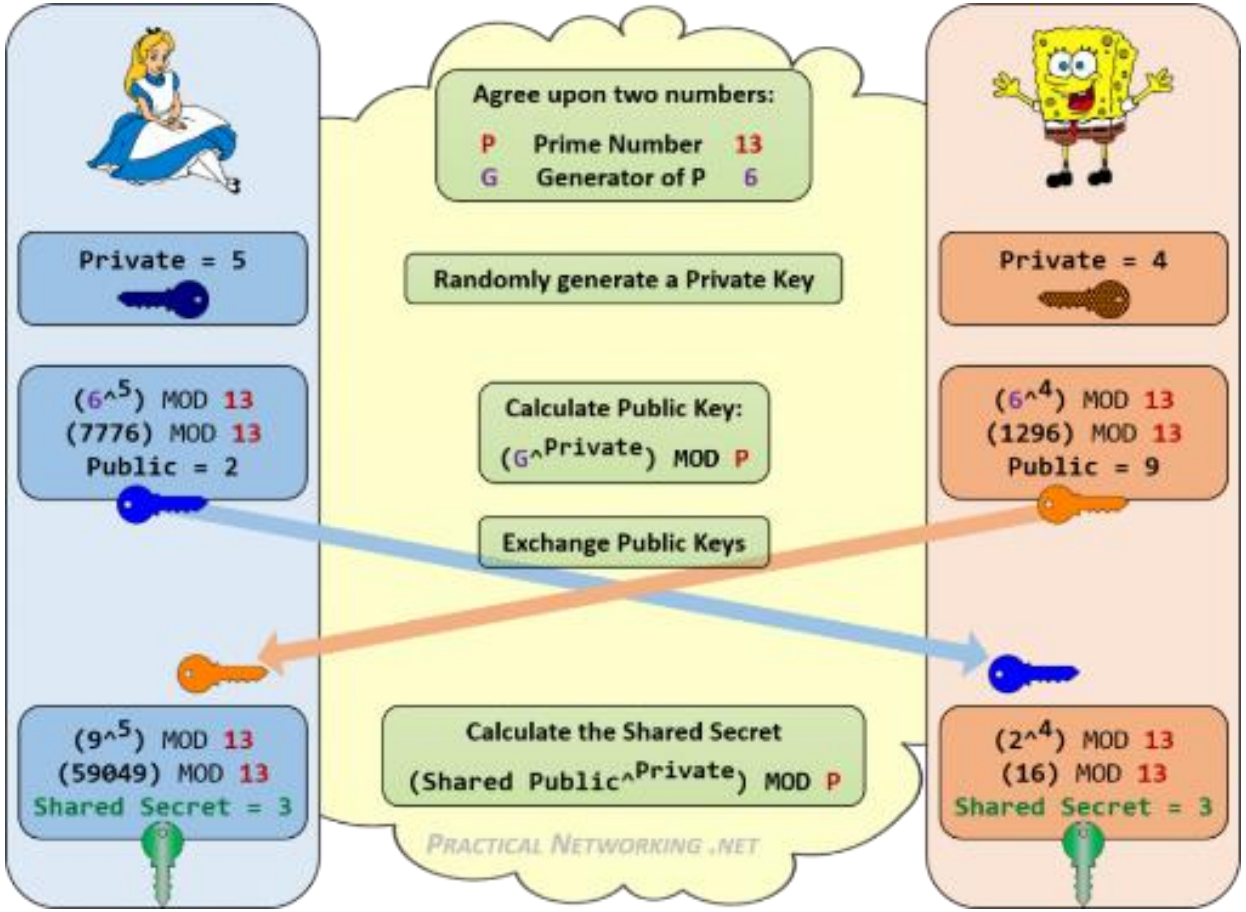
- Symetrické šifrovacie algoritmy (DES, 3DES a AES) ako aj algoritmy hashovania (MD5 a SHA-1)
  - Vyžadujú na vykonanie šifrovania a dešifrovania symetrický zdieľaný tajný kľúč.
  - Ako však preniesť kľúč cez nedôveryhodné prostredie?
- Rieši **Diffie Hellman** (DH) algoritmus
  - DH nie je šifrovací algoritmus
  - Je to metóda ako si dve strany môžu bezpečne dohodnúť šifrovacie kľúče bez toho aby boli samotné kľúče prenášané
    - Algoritmus umožňuje obom susedom si vygenerovať rovnaké heslo, bez toho aby pred tým kedykoľvek komunikovali
  - Existuje viacerré skupiny podľa dĺžky kľúča = DH groups
  - Je súčasť IPsec pre zostavovaciu fázu

Description	Diffie-Hellman Algorithm
Timeline	1976
Type of Algorithm	Asymmetric
Key Size (in bits)	512, 1024, 2048, 3072, 4096
Speed	Slow
Time to Crack (Assuming a computer could try 255 keys per second)	Unknown but considered safe using keys of 2048 or higher
Resource Consumption	Medium

Financované Európskou úniou NextGenerationEU

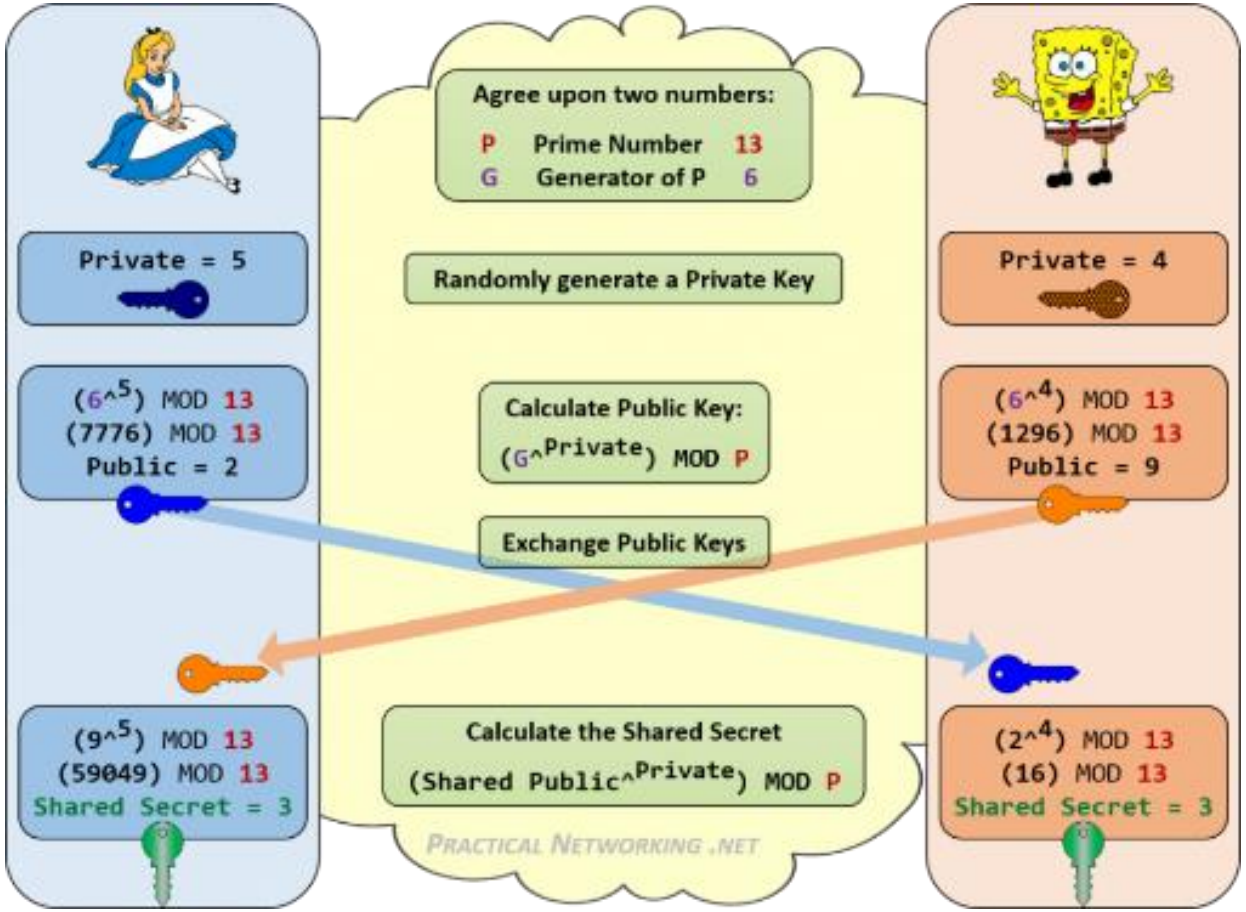
Diffie-Hellman Key Exchange

- Postup vo viac krokoch
  - 1) Obe strany sa najprv musia dohodnúť na dvoch číslach, ktoré si budú zdieľať
    - Čísla sa nemusia utajovať
    - P: prvočíslo, zvyčajne veľké
    - G: základ mocniny (mocnenec), zvyčajne malé
  - 2) Každá zo strán si lokálne vygeneruje náhodné privátne číslo PRIVATE
  - 3) Každá strana s použitím G, P a privátneho čísla si vypočíta svoje verejné číslo ***Public*** (kľúč)
    - $(G^{PRIVATE})$ MOD P = SHARED PUBLIC KEY
  - 4) Strany si vymenia svoje verejné *Public* kľúče cez nezašifrovanú sieť
  - 5) Každá zo strán s použitím G, P a prijatého verejného čísla vypočíta tajný kľúč (secret)
    - $(SHARED\_PUBLIC^{PRIVATE})$ MOD P = SECRET KEY
    - Ten je rovnaký na oboch stranách
    - Môže sa použiť pri symetrickom šifrovaní



Diffie-Hellman skupiny

- V praxi existujú očíslované tzv. DH grupy
  - Číslo grupy určuje s akou dĺžkou kľúča DH bude pracovať
  - DH grupy číslo 1, 2 a 5 by sa už nemali používať
  - Dh grupy
    - DH groups 1 (768), 2 (1024) a 5 neodporúča sa
    - Dh groups
      - **14, key: 2048biys**
      - 15, key: 3072bits
      - 16, key: 4096bits
      - ...
      - 19: (Elliptic Curve DH - ECDH): 256bits
      - 20: (Elliptic Curve DH - ECDH): 384bits
      - ...
      - 24: key: 2048bitov, longer P as DH14



Jednoduchá konfigurácia IPsec

Vytvorenie spojenia medzi IPsec susedmi

- Je potrebné si uvedomiť:
  - Nastavujeme šifrovaný IPsec VPN tunel cez nezabezpečený Internet s „neznámou“ vzdialenou bránou
- VPN brány preto musia vyriešiť viacero otázok:
  - Ako viem, že vzdialený sused je ten správny a nie útočník
    - Rieši sa **autentifikáciou**
  - Ako si vymeníme šifrovacie kľúče cez nezabezpečený Internet
    - Potrebujeme **bezpečný kanál**
    - Ale bezpečný kanál ešte nemáme
  - Aký symetrický algoritmus použijeme na šifrovanie dát
    - Aké heslo/kľúč použijeme pre **šifrovanie/dešifrovanie**
  - Ktorá prevádzka bude **šifrovaná** a ktorá nie
  - Ktorý IPsec protokol a režim použijeme pre VPN (AH, ESP, transport, tunnel)
  - A mnoho ďalších parametrov
- Tieto parametre sú definované v **Security Association (SA)**
  - SA = základ bezpečnostných funkcií IPsec
  - Zoskupenie algoritmov a parametrov, na ktorých sa musia obe strany zhodnúť
  - SA sa vytvárajú a používajú vo dvojiciach

Internet Key Exchange (IKE) protokol

- Protokol používaný na vytvorenie **zabezpečeného a autentifikovaného komunikačného kanála** medzi dvomi peer zariadeniami v IPsec VPN
- Vytvára **riadiaci kanál (Control channel)** pre IPsec
- Používa porty **500** a **4500** (pri prechode cez NAT)
- Slúži na vyjednanie **Security Association (SA)**
  - Výmene kľúčov pomocou **Diffie-Hellman**
  - Autentifikácia peer zariadení
  - Vyjednanie šifrovacích algoritmov a kontrolu integrity

- Založený na protokole **ISAKMP (Internet Security and Key Management Protocol)**
- Funguje v dvoch fázach:
  - **Fáza 1 – IKE SA**
    - Prebieha v dvoch režimoch
  - **Fáza 2 – IPsec SA**
- Verzie:
  - **IKEv1** (staršia, „legacy“)
  - **IKEv2** (novšia, vylepšená)

Protocol	NAT	No NAT
IKE RFC 2409 (IKEv1) RFC 4306 (IKEv2)	IP protocol 17: UDP port 500 (UDP 4500 for rekey, quick mode, mode-cfg)	IP protocol 17: UDP port 500

Vytvorenie spojenia medzi IPsec susedmi

1. Host A sends interesting traffic to Host B.

2. Routers A and B negotiate an IKE Phase 1 session.

=> Vytvorí IKE SA

3. Routers A and B negotiate an IKE Phase 2 session.

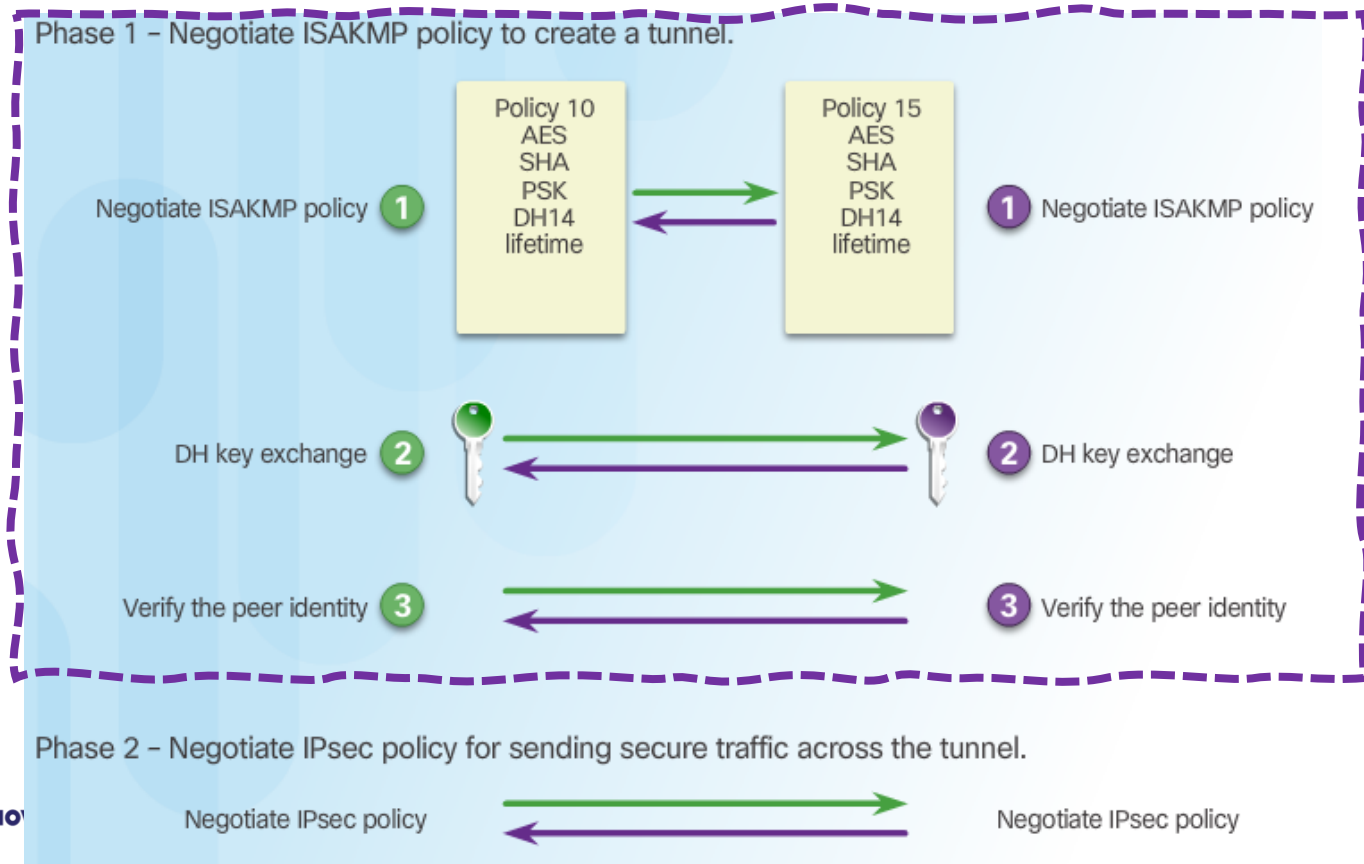
=> Vytvorí IPsec SA

4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

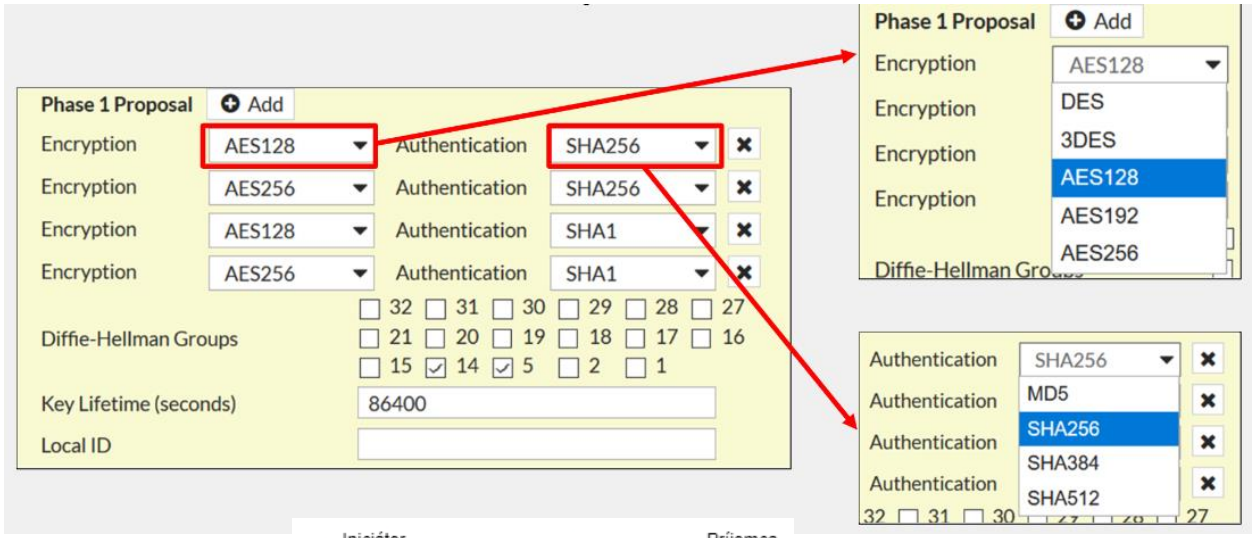
Vytvorenie spojenia: IKE fáza 1 (IKE SA) – main mode

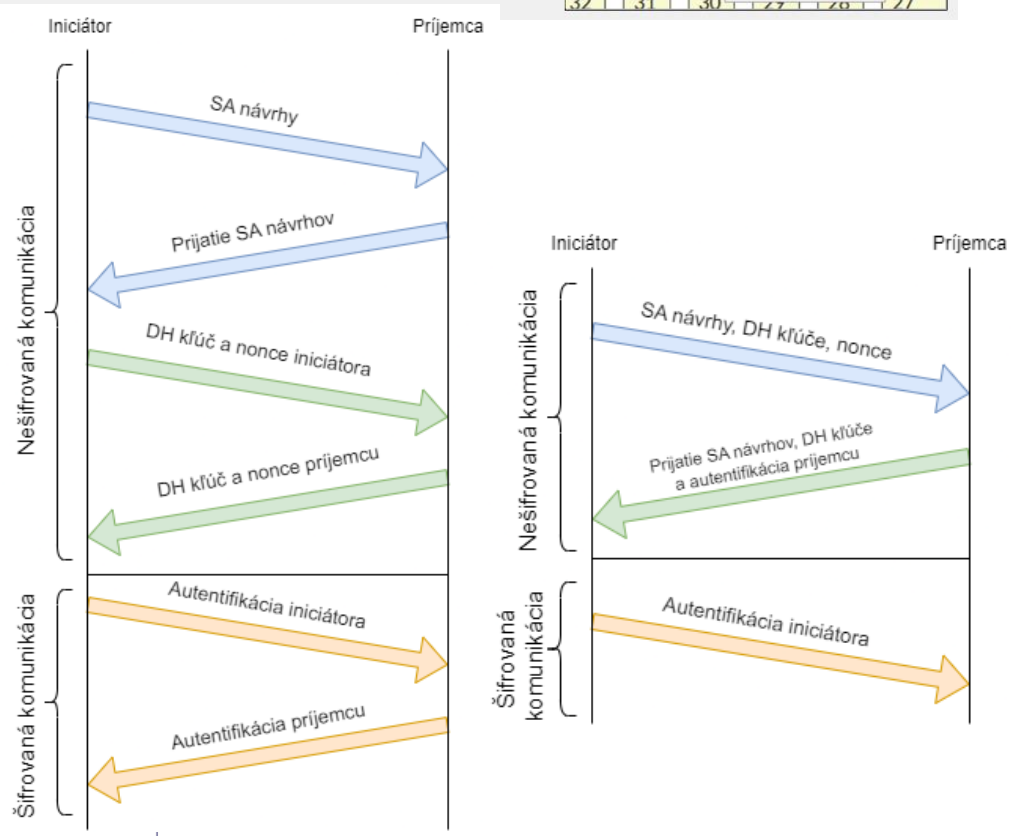
- IKE fáza 1
  - Autentifikuje susedov a riadi ISAKMP politiky (ISAKMP SA)
  - Vytvára zabezpečený kanál per IKE Phase 2
  - Nedohaduje samotné vlastnosti pre činnosť IPsec tunela
  - Má dva módy: **Main a Agressive**
- IKE fáza 1 má tri kroky:
  - Dohodnutie ISAKMP politík
  - Výmenu šifrov./hash kľúčov pomocou Diffie-Hellmanovho algoritmu
    - Tvorba master kľúča
  - Overenie totožnosti susedov
  - Musí byť zhoda na oboch stranách
  - 6 správ
- Čo sú ISAKMP politiky?
  - Aký šifrovací algoritmus? (confident.)
  - Aký hashovací algoritmus? (integr.)
  - Aká Diffie-Hellmanova grupa?
  - Aký spôsob overenia totožnosti? (auth.)
- Overenie totožnosti
  - Podľa spôsobu dohodnutého v prvom kroku



IKE v1 - fáza 1 - módy

- Sú rozdielne z pohľadu bezpečnosti, výkonu a nasadenia
- **Má dva režimy:**
  - **Main – 6 správ**
    - Viac bezpečný
    - Hash predzdieľaného kľúča sa prenáša šifrovane
    - Pomalšia dohodovacia fáza (šesť paketov)
    - Vhodný, ak majú peer zariadenia známe (nie dynamické) IP adresy
  - **Aggressive – 3 správy**
    - Menej bezpečný
    - Rýchlejšia dohodovacia fáza (tri pakety)
    - Vhodnejší pre nasadenie s viacerými tunelmi terminovanými lokálne





Main mód

- **Initiator → Responder:**
  - **Správa 1:** [SA] [KE] [Nonce]
    - **SA (Security Association):** Špecifikuje parametre bezpečnostnej asociácie
    - **KE (Key Exchange):** Obsahuje verejný parameter Diffie-Hellman
    - **Nonce:** Náhodné číslo vygenerované iniciátorom
- **Responder → Initiator:**
  - **Správa 2:** [SA] [KE] [Nonce] [IDr]
    - **IDr (Responder's Identity):** Identifikátor odpovedajúceho (responder)
- **Initiator → Responder:**
  - **Správa 3:** [IDi] [CERTi] [CERTREQ] [AUTH]
    - **IDi (Initiator's Identity):** Identifikátor iniciátora
    - **CERTi (Initiator's Certificate):** Certifikát iniciátora
    - **CERTREQ (Certificate Request):** Žiadosť o certifikát od respondera
    - **AUTH (Authentication):** Obsahuje podpis alebo iný spôsob overenia identity iniciátora
- **Responder → Initiator:**
  - **Správa 4:** [IDr] [CERTr] [AUTH]
    - **IDr (Responder's Identity):** Identifikátor respondera
    - **CERTr (Responder's Certificate):** Certifikát respondera
    - **AUTH (Authentication):** Obsahuje podpis alebo iný spôsob overenia identity respondera
- **Initiator → Responder:**
  - **Správa 5:** [AUTH]
    - **AUTH (Authentication):** Obsahuje podpis alebo iný spôsob overenia identity iniciátora
- **Responder → Initiator:**
  - **Správa 6:** [AUTH]
    - **AUTH (Authentication):** Obsahuje podpis alebo iný spôsob overenia identity respondera

Packet Capture

Msg 1: [SA] [KE] [Nonce]

```
Payload: Security Association (1)
    Next payload: Vendor ID (13)
    Reserved: 00
    Payload length: 60
    Domain of interpretation: IPSEC (1)
  > Situation: 00000001
  v Payload: Proposal (2) # 1
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 48
      Proposal number: 1
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 1
    v Payload: Transform (3) # 1
        Next payload: NONE / No Next Payload  (0)
        Reserved: 00
        Payload length: 40
        Transform number: 1
        Transform ID: KEY_IKE (1)
        Reserved: 0000
      > IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
      > IKE Attribute (t=14,l=2): Key-Length: 128
      > IKE Attribute (t=2,l=2): Hash-Algorithm: SHA
      > IKE Attribute (t=4,l=2): Group-Description: 2048 bit MODP group
      > IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
      > IKE Attribute (t=11,l=2): Life-Type: Seconds
      > IKE Attribute (t=12,l=4): Life-Duration: 86400
```

Msg 3: [IDi] [CERTi] [CERTREQ] [AUTH]

```
  Initiator SPI: f8546d46ab52d005
  Responder SPI: 26da58732815ad53
  Next payload: Key Exchange (4)
> Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
> Flags: 0x00
  Message ID: 0x00000000
  Length: 412
> Payload: Key Exchange (4)
> Payload: Nonce (10)
> Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
> Payload: Vendor ID (13) : Unknown Vendor ID
> Payload: Vendor ID (13) : XAUTH
> Payload: NAT-D (RFC 3947) (20)
> Payload: NAT-D (RFC 3947) (20)
```

Nadviazanie spojenia medzi IPsec susedmi

- Vytvorenie IPsec tunela sa nerobí vopred
- Tunelovanie sa vždy spustí príchodom prvého paketu (tzv. **packet of interest**) preneseného z jednej siete do druhej
  - Jedna strana je **initiator**
  - Druhá strana je **responder**
- Po príchode takéhoto paketu (identifikovaného pomocou ACL):
  - Prebehnú obe fázy a vytvoria sa bezpečnostné asociácie spojenia
  - Ich používanie je viazané na **lifetime** určenú konfiguráciou
  - IPsec sa ukončí po období nečinnosti alebo po vypršaní lifetime
  - A následne sa znovu vytvorí pri ďalšej komunikácii

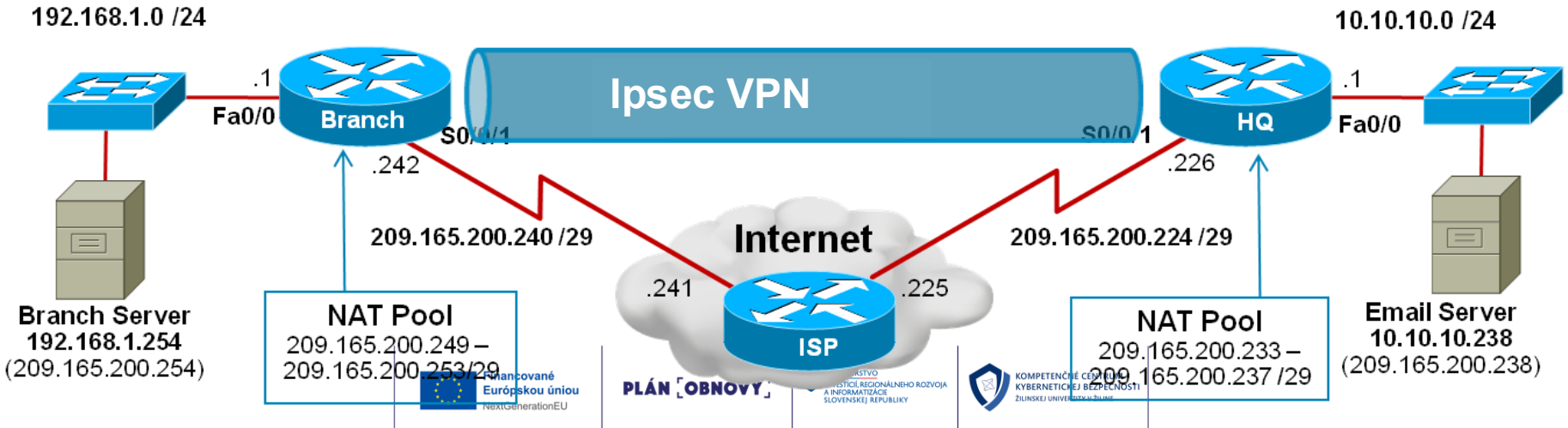
Vytvorenie spojenia: IKE fáza 2 (IPsec SA)

- Cez zabezpečený tunel sa dohodnú pravidlá pre šifrovanie dát (SA)
- IKE fáza 2 teda zodpovedá za dojednanie spôsobu použitia IPsec medzi susedmi
  - Aký protokol IPsec – AH, ESP, AH+ESP?
  - Aký režim – tunelový alebo transportný?
  - Aký šifrovací algoritmus?
  - Aký hashovací algoritmus
  - Aké šifrovacie kľúče (DH)?

  transformačná sada
  - Aká bude životnosť dohodnutých informácií?

Kroky pri konfigurácii IPsec

- Postup pri konfigurácii IPsec
  - Vytvoriť aspoň jednu ISAKMP politiku pre fázu 1
  - Vytvoriť aspoň jednu transformačnú sadu pre fázu 2
  - Vytvoriť ACL, ktoré určí, čo sa má zabezpečiť pomocou IPsec
    - Až príchod paketu spúšťa IPSec processing
  - Vytvoriť kryptovaciu mapu, ktorá s ACL určí čo sa má zabezpečiť pomocou IPsec a ako
    - Až príchod paketu spúšťa IPSec processing
  - Aplikovať kryptovaciu mapu na výstupné rozhranie
- Poznámka:
  - Internet je v príklade použitý len ako záložne spojenie pre private WAN



Kompletná konfigurácia Branch Router IPsec VPN

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes 256
Branch(config-isakmp)# hash sha
Branch(config-isakmp)# lifetime 3600
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 24
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.226
! Specifikuj IPSec transformacnu sadu
Branch(config)# crypto ipsec transform-set MOJA_TR_SADA esp-aes esp-sha-hmac esp-3des
Branch(cfg-crypto-trans)# exit
! Specifikuj prevadzku, ktora bude sifrovana
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Branch(config)#
Branch(config)#
Branch(config)# crypto map MOJA_MAPA 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
! Mapa spoji kroky dokopy, t.j. na akeho suseda aku Tr.Sadu + ake ACL
! Moze mat viac blokov pre viac susedov
Branch(config-crypto-map)# set transform-set MOJA_TR_SADA
Branch(config-crypto-map)# set peer 209.165.200.226
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# int s0/0/1
Branch(config-if)# crypto map MOJA_MAPA
Branch(config-if)# ^Z
Branch#
```

1 ISAKMP Policy
Specifies the initial VPN security details

2 IPsec trans. set
Specifies how the IPsec packet will be encapsulated

3 Crypto ACL
Specifies the traffic that will trigger the VPN to activate

4 VPN Tunnel Information
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL

5 Apply the Crypto Map
Identifies which interface is actively looking to create a VPN

Kompletná konfigurácia HQ Router IPsec VPN

```
HQ# conf t
HQ(config)# crypto isakmp policy 1
HQ(config-isakmp)# encryption aes 256
HQ(config-isakmp)# hash sha
HQ(config-isakmp)# authentication pre-share
HQ(config-isakmp)# group 24
HQ(config-isakmp)# exit
HQ(config)# crypto isakmp key cisco123 address 209.165.200.242
HQ(config)#
HQ(config)# crypto ipsec transform-set MOJA_TR_SADA esp-aes esp-sha-hmac esp-3des
HQ(cfg-crypto-trans)# exit
HQ(config)#
HQ(config)# access-list 110 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
HQ(config)#
HQ(config)#
HQ(config)# crypto map MOJA_MAPA 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
HQ(config-crypto-map)# set transform-set MOJA_TR_SADA
HQ(config-crypto-map)# set peer 209.165.200.242
HQ(config-crypto-map)# match address 110
HQ(config-crypto-map)# exit
HQ(config)# int s0/0/1
HQ(config-if)# crypto map MOJA_MAPA
HQ(config-if)# ^Z
```

❶ **ISAKMP Policy**
Specifies the initial VPN security details

❷ **IPsec Details**
Specifies how the IPsec packet will be encapsulated

❸ **Crypto ACL**
Specifies the traffic that will trigger the VPN to activate

❹ **VPN Tunnel Information**
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL

❺ **Apply the Crypto Map**
Identifies which interface is actively looking to create a VPN

Verifikácia IPsec (Cisco IOS)

- Displays configured ISAKMP policies
  - **`Show crypto isakmp policy`**
- Display PSK key
  - **`sh crypto isakmp key`**
- Display IKE phase 1 SA
  - It can be seen only when phase **`1`** is over
  - **`Sh crypto isakmp sa`**
- View config and status of Sapre Ipsec
  - **`Sh crypto ipsec sa`**
- Show crypto map
  - **`Show crypto map`**

  - **`Show crypto session`**

KEv2 protokol pre Ipsec – aktuálny prístup

- **Charakteristika**
  - Najnovšia verzia protokolu IKE (RFC 7296)
  - Používa sa na vyjednávanie IPsec Security Associations (SA)
  - Pracuje na **vrstve riadenia (control plane)**, port UDP 500/4500 (NAT-T)
- **Vylepšenia oproti IKEv1**
  - Menej správ → rýchlejší handshake
  - Lepšia podpora NAT traversal
  - Podpora mobility a multihomingu (MOBIKE, RFC 4555)
  - Lepší rekeying (obnova kľúčov bez prerušenia spojenia)
  - Zjednodušená správa chýb a retransmisií
- **Bezpečnosť**
  - Podpora moderných algoritmov (AES-GCM, ChaCha20, SHA-2, ECDH)
  - Zabudované Perfect Forward Secrecy (PFS)
  - Podpora certifikátov, PSK aj EAP autentifikácie (vhodné pre remote access VPN)
- **Výhody v praxi**
  - Rýchlejšie a stabilnejšie než IKEv1
  - Odolnejšie voči DoS útokom
  - Vhodné pre mobilné zariadenia (dynamické IP, zmena siete WiFi/LTE)
  - Dnes štandard v enterprise VPN riešeniach (Cisco, Fortinet, Microsoft, atď.)

IKEv1 vs. IKEv2

Feature	IKEv1	IKEv2
Phases	2 fázy: Phase 1 (ISAKMP SA) a Phase 2 (IPsec SA)	Jednotný a zjednodušený výmenný proces pre obe SA
Negotiation Efficiency	Komplexné vyjednávanie, viacero výmen	Optimalizované, znížený overhead
Message Exchanges	Až 9 správ (Aggressive mode), pomalší setup	Len 4 správy → rýchlejší setup
Mobility Support	Bez natívnej podpory	Podpora **MOBIKE** pre dynamické IP a mobilné zariadenia
Dead Peer Detection	Len cez rozšírenia	**DPD zabudovaný** → spoľahlivejšie odhaľovanie neaktívnych peerov
Reliability	UDP bez retransmisií	Zabudovaný retransmission mechanizmus
Security Improvements	Menej bezpečný, slabá ochrana proti DoS, staršie algoritmy	Moderné algoritmy (AES-GCM, ECDH), vyššia odolnosť proti DoS
Config Payload	Nepodporuje natívne	**Config Payload** → jednoduchšie prideľovanie adries a nastavení
EAP Authentication	Len cez rozšírenia	Natívna podpora **EAP** (LDAP, RADIUS, certifikáty, 2FA)

Najlepšie postupy pre VPN

- **Aktualizácie a bezpečnosť**
  - Firewally musia mať najnovšie bezpečnostné záplaty
  - VPN sú častým cieľom kybernetických útokov
- **Šifrovanie a algoritmy**
  - Používaj AES-GCM (128/256) namiesto starších CBC režimov
  - HMAC-SHA-256 alebo vyššie (SHA-384/512), nepoužívať MD5/SHA-1
  - Minimálne DH Group 14 (2048-bit), preferuj ECDH (Group 19, 20, 31)
  - Zapni **Perfect Forward Secrecy (PFS)** v Phase 2
- **Kompatibilita peer zariadení**
  - Over, že obaja peer podporujú rovnaké IPsec/IKE funkcie
  - Staršie alebo rôzne značky môžu používať iné algoritmy
  - Certifikáty (PKI) sú bezpečnejšie než predzdieľané kľúče (PSK)
- **Porty a komunikácia**
  - IKE používa UDP port 500
  - UDP port 4500 pri NAT traversal
  - Over, že sú povolené na všetkých firewalloch v ceste
- **Prevádzka a výkon**
  - IPsec znižuje priepustnosť → počítaj so záťažou CPU/HW
  - Používaj HW akceleráciu (AES-NI, ASIC, Cavium) pri väčšom počte tunelov
  - Sleduj CPU load a logy (SA renegociácie, chyby)
  - Nastav životnosť: IKE SA 8–24 h, IPsec SA kratšie (~1 h)
- **IKE režim**
  - **Preferuj IKEv2** – rýchlejší, stabilnejší, lepší NAT traversal
  - Ak IKEv1:
    - Main mode = bezpečnejší, ale pomalší (site-to-site VPN)
    - Aggressive mode = rýchlejší, ale menej bezpečný (remote-access VPN)
- **Sieť a architektúra**
  - Nastav ACL/traffic selectors presne, nepovoľuj príliš široké rozsahy
  - Over MTU/MSS, aby sa predišlo fragmentácii
  - Používaj DPD (Dead Peer Detection) a redundanciu (dual ISP, HA)

Odporúčania k typom / sile šifrovania, hashovaniu, DH grupám

Parameter	Minimum odporúčaná úroveň	Odporúčaná silnejšia možnosť (ak HW dovolí)
Šifrovací algoritmus (cipher)	AES-128 v GCM režime (napr. AES-128-GCM) (IETF Datatracker)	AES-256-GCM; ak GCM nie je podporovaný, CBC-256 s silnou integrity kontrolou (SHA-256/SHA-384) (docs.fortinet.com)
Režim (mode)	Preferované AEAD režimy (napr. GCM) pre šifrovanie + integritu v jednom kroku (IETF Datatracker)	Ak GCM nie je možný, tak CBC + samostatné HMAC (SHA-256 alebo SHA-384)
Hash / integrita / HMAC	SHA-256 minimálne; ak potrebné, SHA-384 alebo SHA-512 pre väčšiu robustnosť (IETF Datatracker)	SHA-384/512 pre dôležité spojenia alebo pri dlhšom lifetime SA
Diffie-Hellman (DH) / ECDH group	MODP group 14 (2048-bit), ECP groups ako 19 (256-bit ECDH) minimálne (docs.manage.security.cisco.com)	ECDH group 20 (384-bit), 31 (Curve25519) alebo group 21 (521-bit) ak podporované - vyššia bezpečnosť, nižšia latencia pri offloading karte (docs.fortinet.com)
Perfektné forward secrecy (PFS)	Áno, zapnúť v Phase2 aspoň; zabezpečuje, že ak kľúč v budúcnosti unikne, minulá prevádzka zostáva bezpečná (docs.fortinet.com)	Ako vyššie, s použitím silnejšej DH/ECDH grupy
Lifetime (IKE & IPsec SA)	Nastaviť rozumnú dobu — napr. IKE SA 3600-86400 sekúnd, IPsec SA podobne; kratšia doba ak veľké riziko (NIST Publications)	Zvážiť kratšie intervaly pri dynamických tuneloch alebo pri vyššom riziku
Autentifikácia peerov	PSK (predzdieľaný kľúč) len ak sú IP adresy známe a bezpečne uložené; ideálne certifikáty (RSA/ECDSA) (docs.manage.security.cisco.com)	Certifikáty/ECDSA + CRL/OCSP, alebo iné externé PKI riešenie

Najčastejšie problémy a hrozby pri VPN

- **Slabé autentifikačné mechanizmy**
  - Predzdieľané kľúče (PSK) zdieľané medzi viacerými používateľmi
  - Absencia MFA pri remote access VPN
- **Používanie zastaraných algoritmov**
  - MD5, SHA-1, DES, 3DES
  - Nedostatočne silné Diffie-Hellman skupiny (< Group 14)
- **Zraniteľné VPN brány**
  - Fortinet SSL VPN (CVE-2018-13379, CVE-2022-42475)
  - Pulse Secure, Citrix Gateway – remote code execution
  - Dôsledok: útočníci získali priamy prístup do interných sietí
- **Nedostatočná segmentácia prístupu**
  - VPN používateľ má prístup „do celej siete“
  - Chýba princíp *least privilege* a logovanie prístupu
- **Chýbajúce patchovanie a monitoring**
  - VPN brány bežia s neaktuálnym softvérom
  - Neexistuje alerting na neštandardné prihlasovania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Case Study – Útok na Fortinet SSL VPN

- **Zraniteľnosť:** Fortinet FortiOS SSL VPN (CVE-2018-13379)
  - Path traversal → umožnil stiahnutie súboru sslvpn_websession
  - Útočníci získali plaintext prihlasovacie mená a heslá
- **Dôsledky:**
  - Hromadné kompromitácie prístupov do enterprise sietí
  - Údaje z VPN (kontá, heslá) predávané na darknete
  - Následne použité pre ransomvérove kampane (napr. Cring ransomware 2021)
- **Prečo bol problém kritický:**
  - VPN = vstupná brána do vnútornej siete
  - Mnohé organizácie nepoužívali MFA
  - VPN brány neboli pravidelne patchované
- **Poučenie:**
  - Rýchle patchovanie VPN zariadení je absolútne kľúčové
  - Zavedenie MFA minimalizuje dopady kompromitovaných účtov
  - Monitorovať prihlasovania (geolokácia, anomálie)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Jednoduchá konfigurácia GRE over IPsec

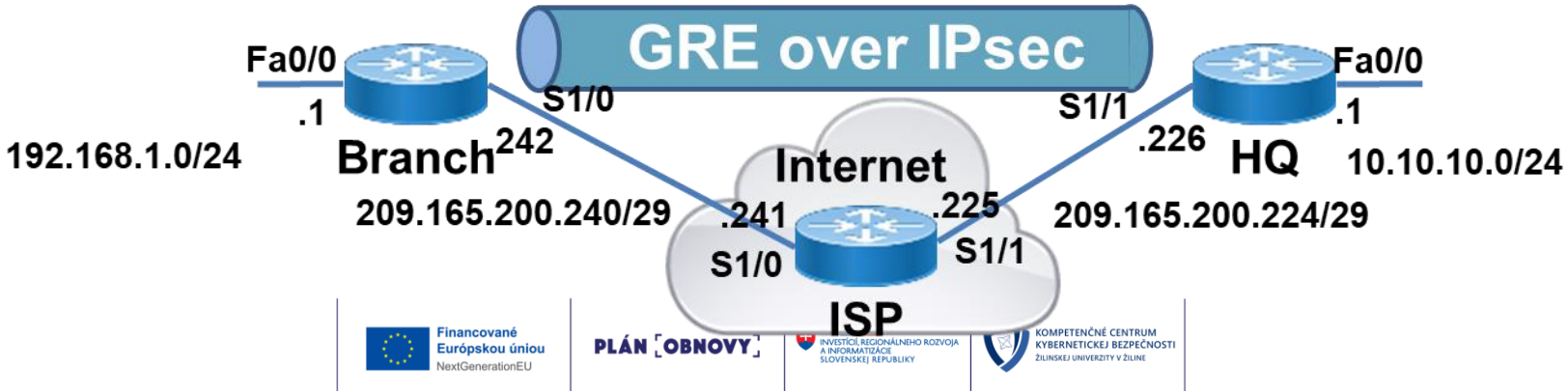
Jednoduchá konfigurácia GRE over IPsec

- Konfiguruj GRE
- Konfiguruj Ipsec
  - ... avšak treba myslieť na to, že výstupným rozhraním už neodchádzajú holé pakety prenášaného protokolu, ale GRE pakety
  - Príkaz **set peer** v kryptomape sa musí zhodovať s adresou uvedenou v príkaze **tunnel destination** na Tunnel rozhraní
  - ACL v kryptomape musí vybrať pakety **typu GRE**, ktorých zdroj zodpovedá príkazu **tunnel source** a cieľ príkazu **tunnel destination**

Konfig smerovačov - GRE

```
! Pobocka
ena
conf t
int tunnel 0
        tunnel source s 1/0
        tunnel destination 209.165.200.226
        tunnel mode gre ip
        ip add 172.16.1.1 255.255.255.0
router ospf 1
        network 192.168.1.0 0.0.0.255 area 0
        network 172.16.1.0 0.0.0.255 area 0
```

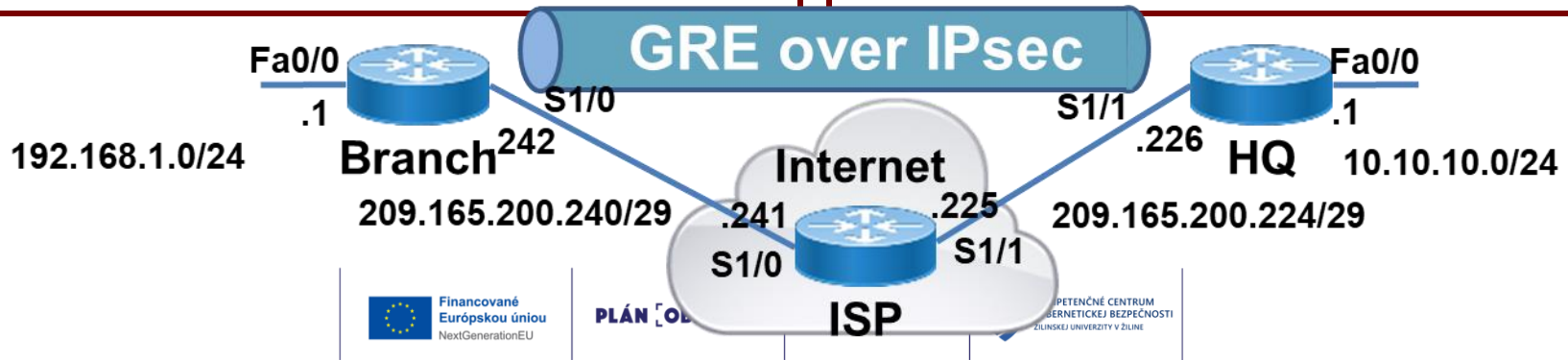
```
!HQ
ena
conf t
int tunnel 0
        tunnel source s 1/1
        tunnel destination 209.165.200.242
        tunnel mode gre ip
        ip add 172.16.1.2 255.255.255.0
router ospf 1
        network 10.10.10.0 0.0.0.255 area 0
        network 172.16.1.0 0.0.0.255 area 0
```



Konfig smerovačov - príprava

```
! Pobocka
ena
conf t
crypto isakmp policy 1
          encryption aes 256
          hash sha
          authentication pre-share
          group 24
          exit
crypto isakmp key cisco123 address 209.165.200.226
crypto ipsec transform-set MOJA_TR_SADA esp-aes esp-
sha256-hmac
access-list 110 permit ip 192.168.1.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit gre host 209.165.200.242 host
209.165.200.226
crypto map MOJA_MAPA 10 ipsec-isakmp
          set transform-set MOJA_TR_SADA
          set peer 209.165.200.226
          match address 110
          exit
int s 1/0
          crypto map MOJA_MAPA
          end
wr mem
```

```
ena
conf t
crypto isakmp policy 1
          encryption aes 256
          hash sha
          authentication pre-share
          group 24
          exit
crypto isakmp key cisco123 address 209.165.200.242
crypto ipsec transform-set MOJA_TR_SADA esp-aes esp-
sha256-hmac
access-list 110 permit ip 10.10.10.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 110 permit gre host 209.165.200.226 host
209.165.200.242
crypto map MOJA_MAPA 10 ipsec-isakmp
          set transform-set MOJA_TR_SADA
          set peer 209.165.200.242
          match address 110
          exit
int s 1/1
          crypto map MOJA_MAPA
          end
wr mem
```



Kvíz

- **Na ktorej vrstve OSI pracuje IPsec?**
  - A) Linková vrstva (Layer 2)
  - **B) Sieťová vrstva (Layer 3)**
  - C) Transportná vrstva (Layer 4)
  - D) Aplikačná vrstva (Layer 7)

- **Na čo sa používa predzdieľaný kľúč (PSK) v IPsec/IKE?**
  - A) Na šifrovanie dátového prenosu v tuneli
  - **B) Na autentifikáciu peerov pri vyjednávaní tunela**
  - C) Na výmenu Diffie-Hellman parametrov
  - D) Na generovanie náhodného čísla (Nonce)

Zhrnutie

- **VPN** umožňuje bezpečný prenos dát cez nezabezpečenú sieť (internet)
- **Site-to-Site vs. Remote Access VPN** – rozdielne scenáre použitia
- **IPsec** – štandard pre enterprise VPN, IKEv1 (Main/Aggressive) vs. IKEv2 (moderný, rýchlejší, bezpečnejší)
- **DMVPN a SD-WAN** – pokročilé riešenia pre škálovateľnosť a centralizované riadenie
- **Moderné VPN protokoly** – OpenVPN, WireGuard (jednoduchosť, výkon, mobilita)
- **Najčastejšie hrozby** – slabé PSK, zastarané algoritmy, zraniteľné VPN brány
- **Best Practices**
  - Silné šifrovanie (AES-GCM, SHA-256, PFS)
  - MFA a princíp *least privilege*
  - Segmentácia a monitoring (SIEM/SOC)
  - Pravidelné patchovanie VPN brán
- **Poučenie z praxe** – známe útoky (Fortinet SSL VPN) ukazujú, že správna konfigurácia a údržba VPN je kritická

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Bezpečná komunikácia

Kryptografia, ochrana dát a bezpečná komunikácia (Blok III)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Pavel Segeč

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk