UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Koncepty Virtuálnych Privátnych Sietí (VPS/VPN) a IPsec-u (IP Security)

Enterprise Networking, Security, and Automation

Pavel Segeč
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Počítačové siete 2 – KIS FRI UNIZA
Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Čo nás čaká ...

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

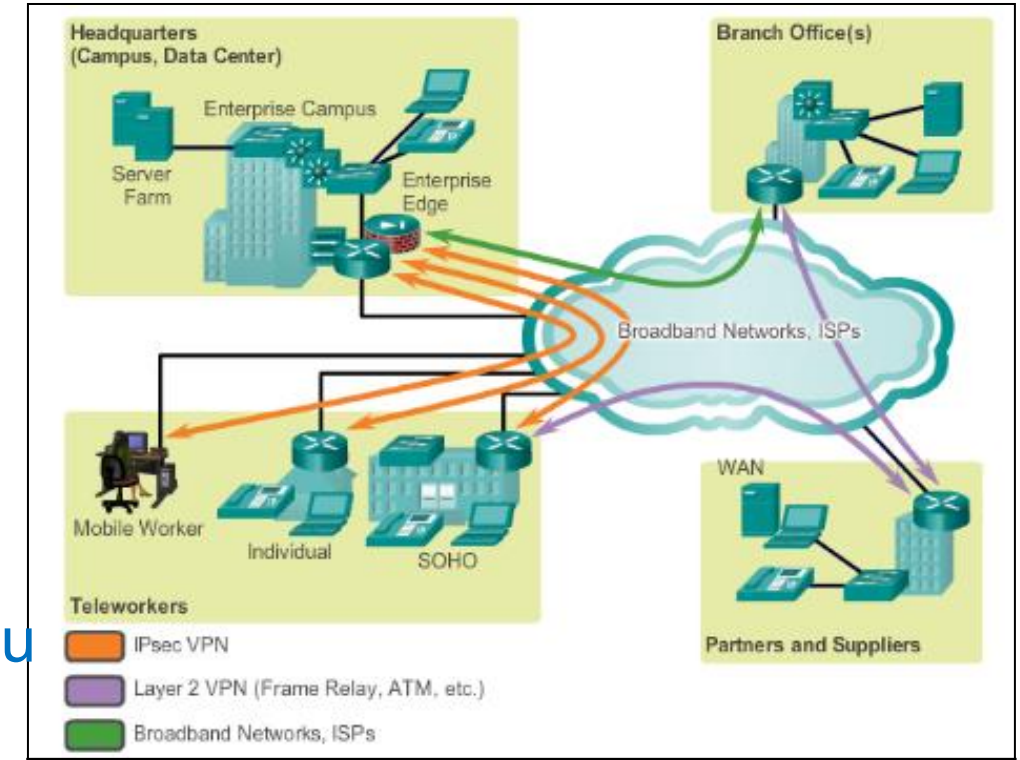
VPNs - Virtual Private Networks

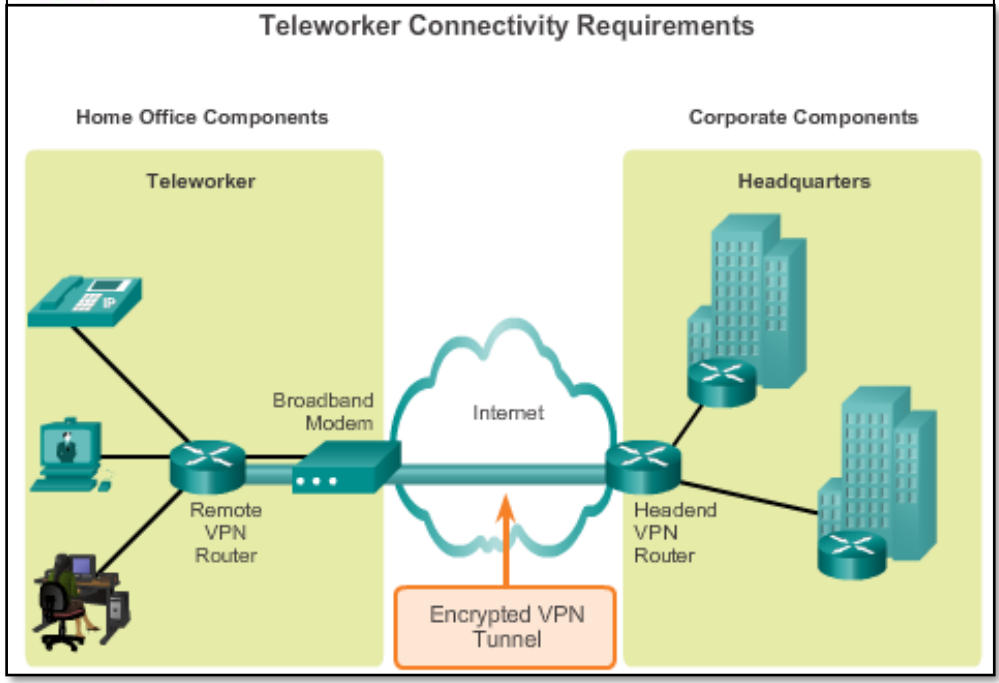
VPN – riešenie vzdialeného prístupu

- 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

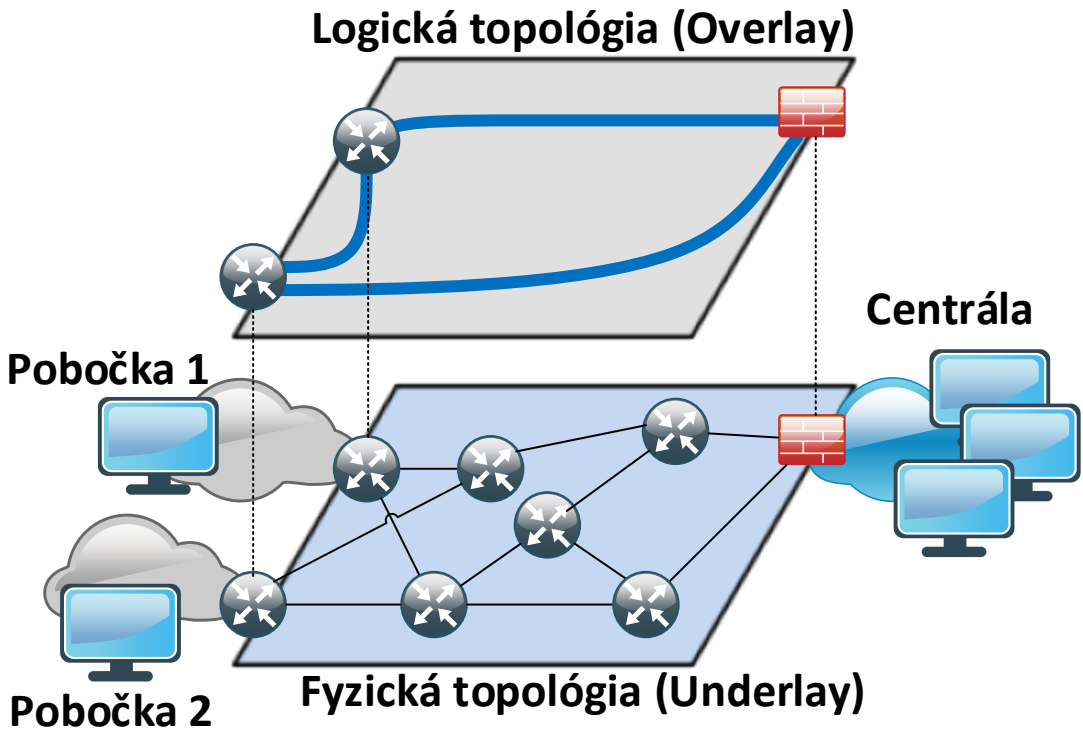
- Každé riešenie z predchádzajúcich možností vyžaduje:
  - Širokopásmový/rýchly prístup
    - Rôzne služby (VoIP, TelePresence, zdieľanie apod.)
  - Bezpečný prístup
- Riešenia širokopásmového a rýchleho prístupu
  - Rýchlosť vyššia 200kbps
    - Cable / DSL / WiFi / WiMAX / Fiber („Always-on“ technológie)
  - 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





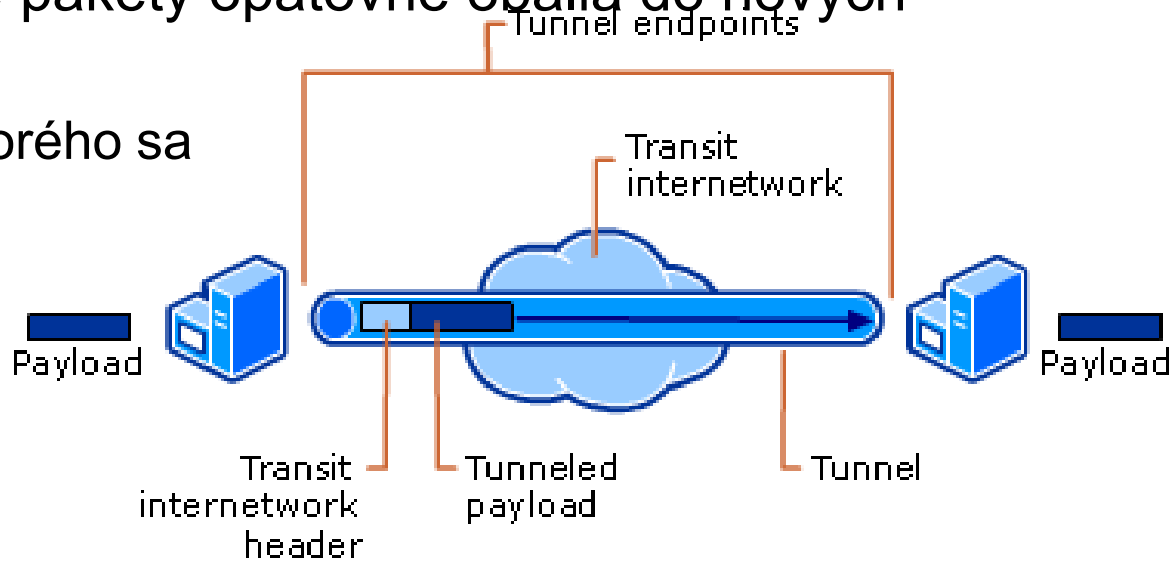
VPN základy

- **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

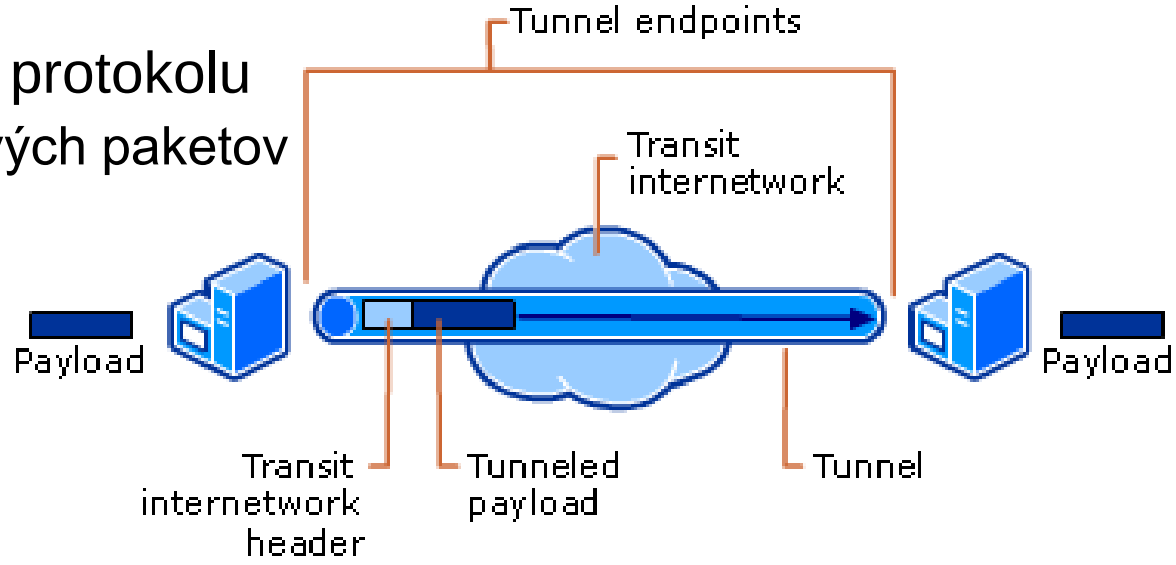


Protokoly pri tunelovaní - terminológia

- 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

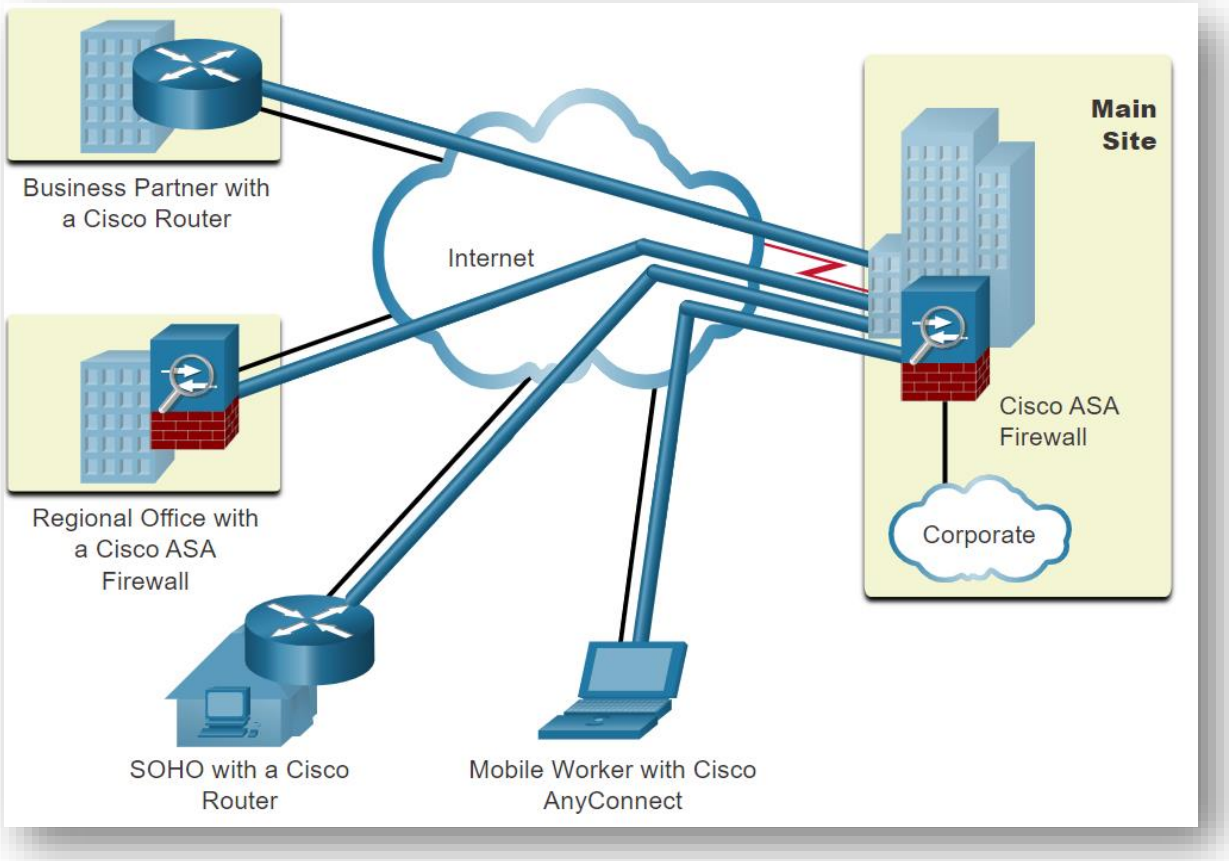
Tunelovacie protokoly

- 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, PPTP
- Tunelovanie bez pomocného tunelovacieho protokolu
  - Tunelované pakety sa priamo vkladajú do nových paketov
  - Minimálna réžia
  - Obmedzené možnosti
  - Napríklad: IP-in-IP, IPv6-in-IPv4



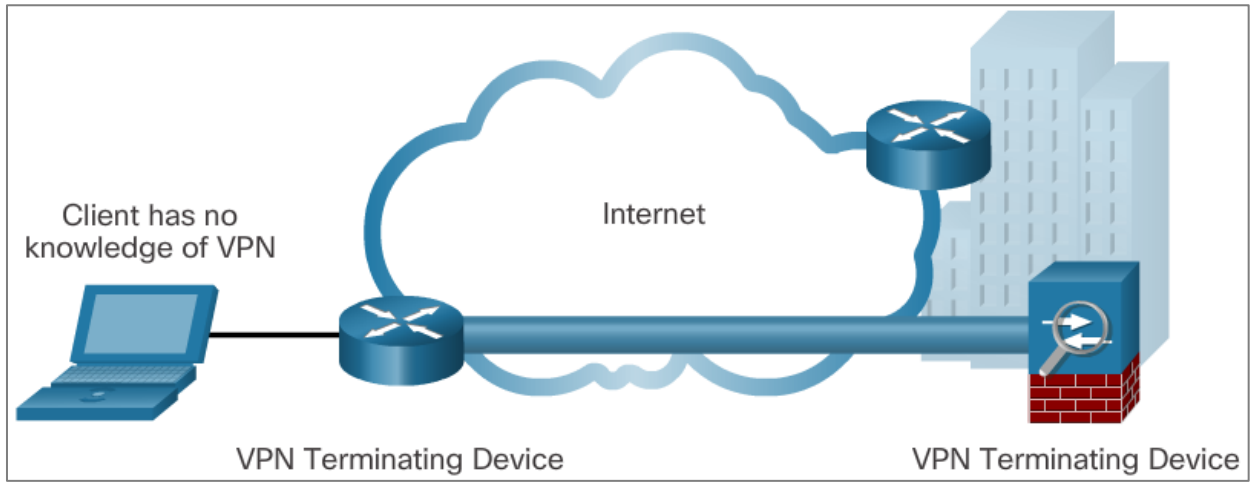
Čo potrebujeme na implementáciu VPN?

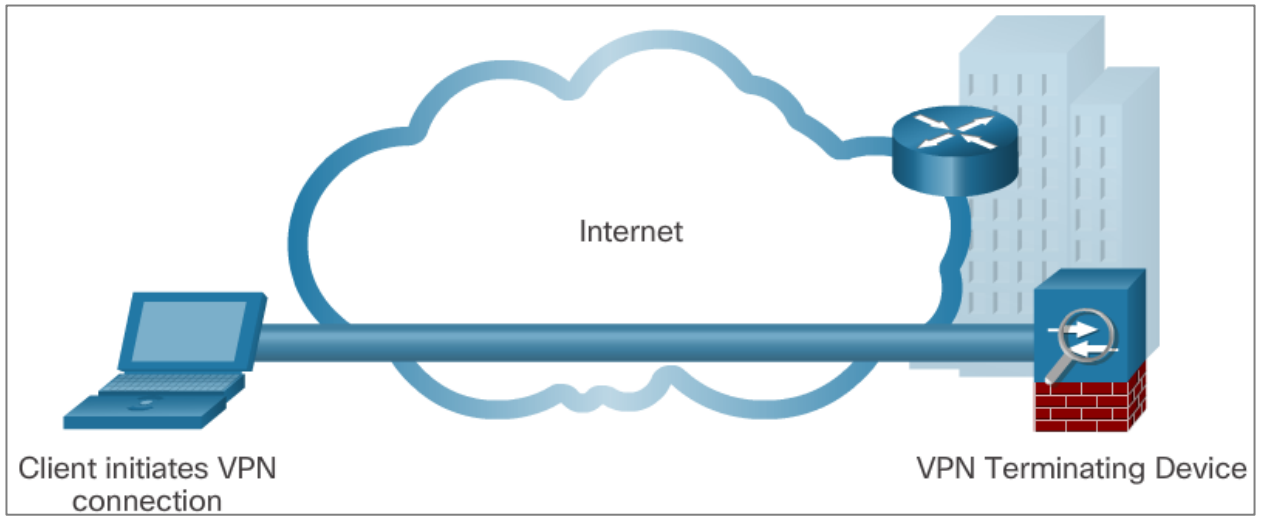
- Čo potrebujeme na implementáciu VPN?
  - VPN bránu/brány (VPN gateway)
    - Sieťové zariadenia, medzi ktorými alebo voči ktorým, sa vytvárajú VPN tunely
      - V svojom OS implementujú podporu potrebných VPN protokolov
    - Príklad:
      - Smerovač, Firewall, Cisco Adaptive Security Appliance (ASA), 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





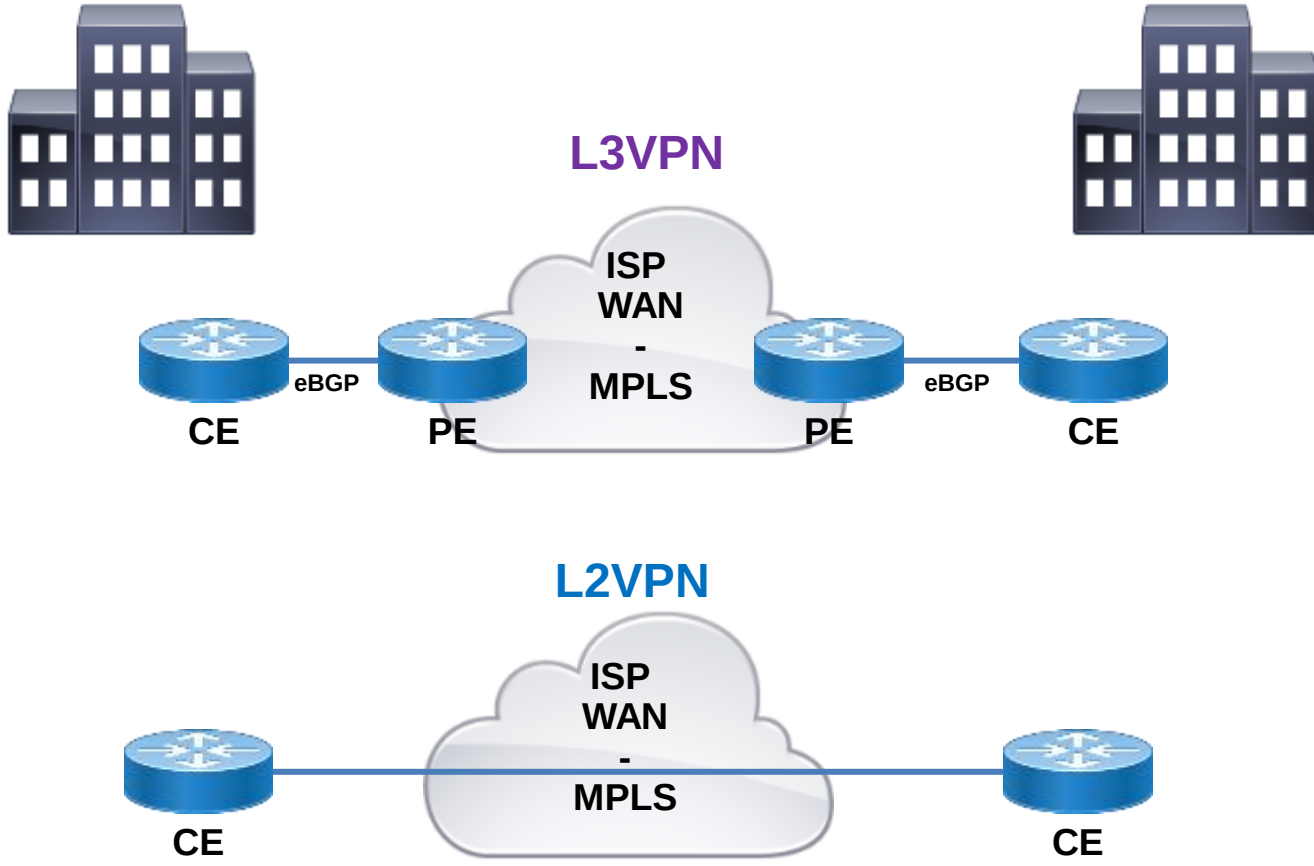
Typy VPN z pohľadu kto ich manažuje

- **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: IPSec VPN
      Nevyužívajúce VPN klienta: 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
    - *Fokus predmetu Projektovanie sietí 1 v* programe ASI
  - Pôvodné, dnes zastaralé riešenia
    - Frame Relay, ATM Asynchronous Transfer Mode

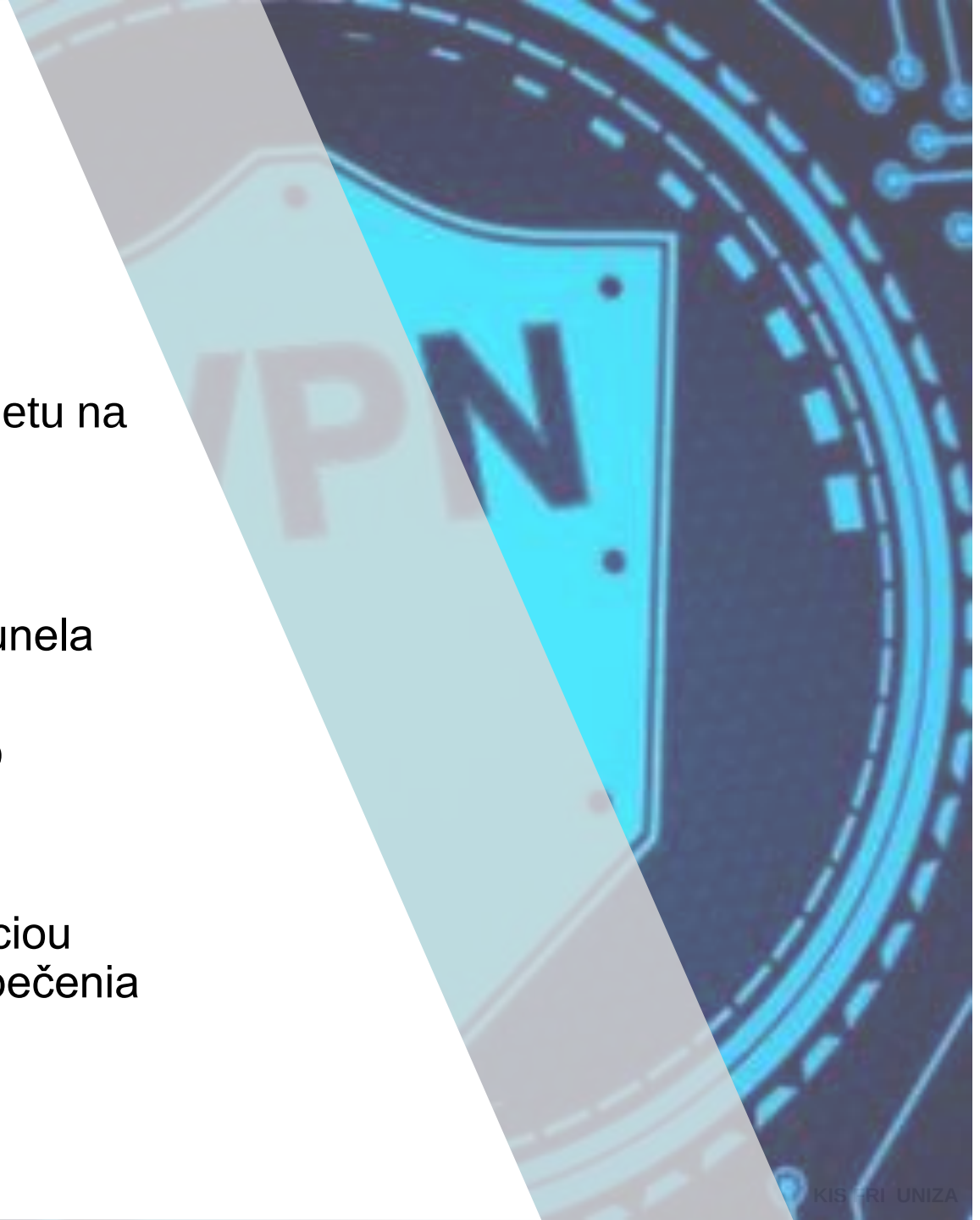
Privátne VPN služby SP (CCNA nepokrýva)

- 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
      - 9950 Euro s DPH
- 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

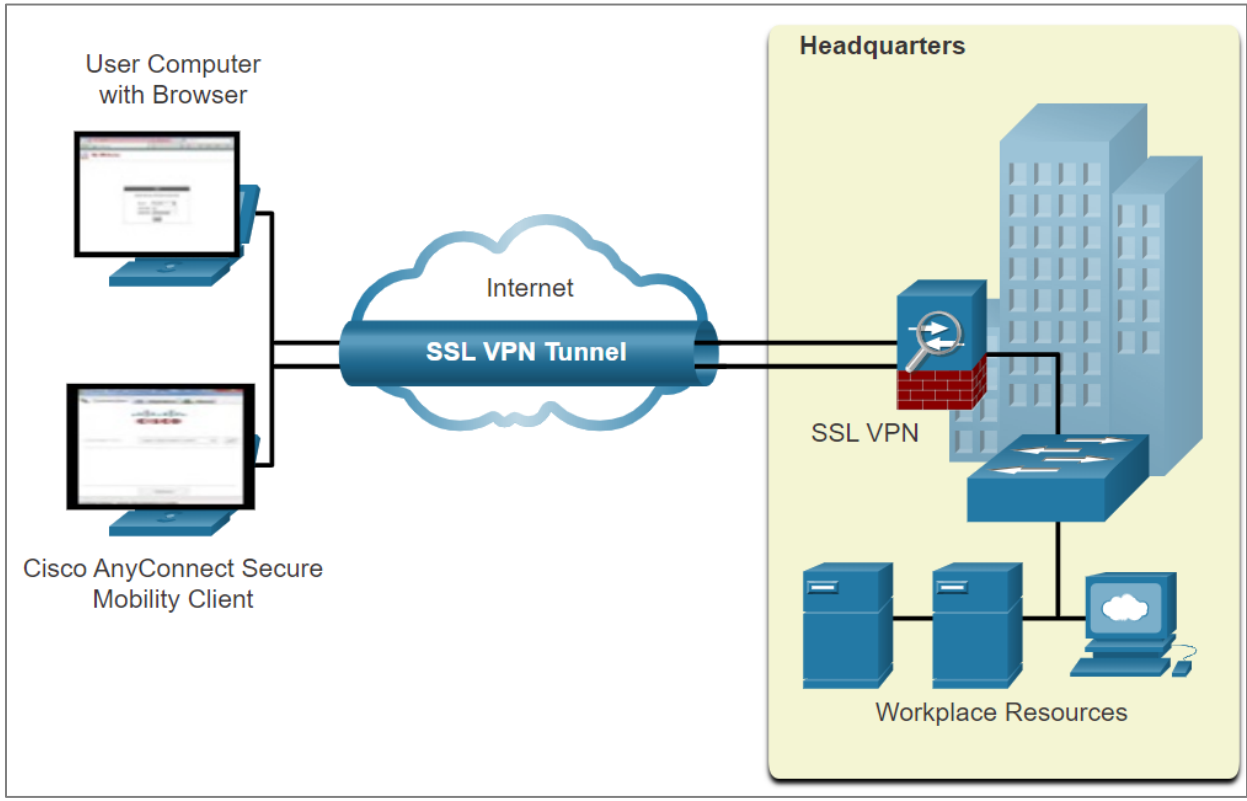


Typy a možnosti riešenia VPN – bližší pohľad

Remote-Access VPN

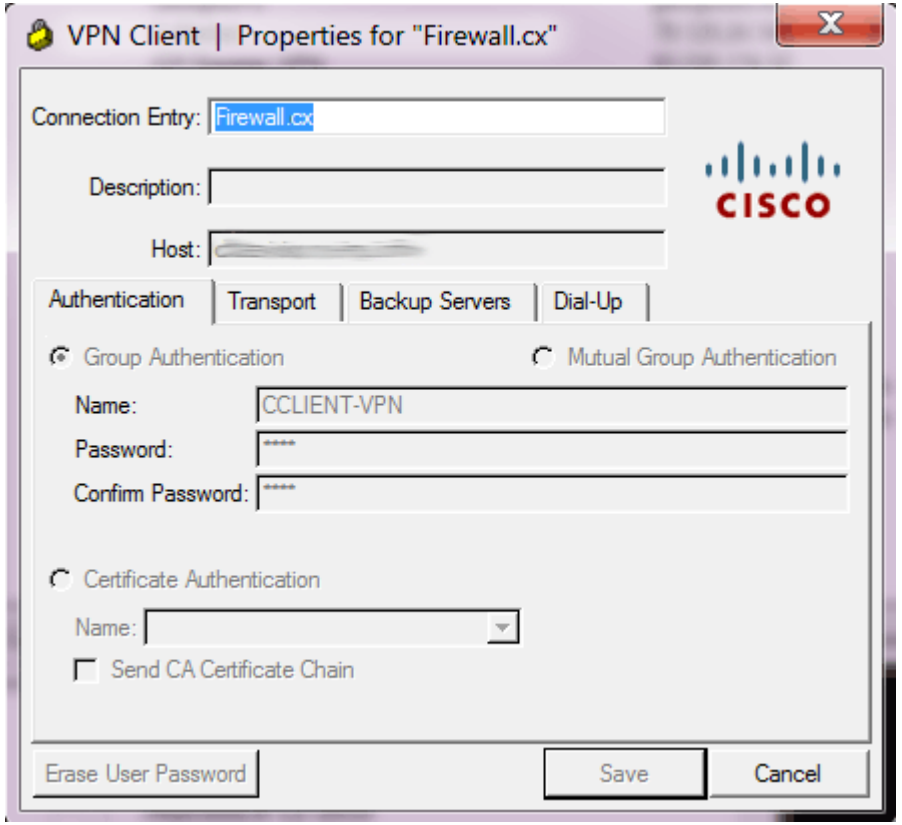
Remote-Access VPN

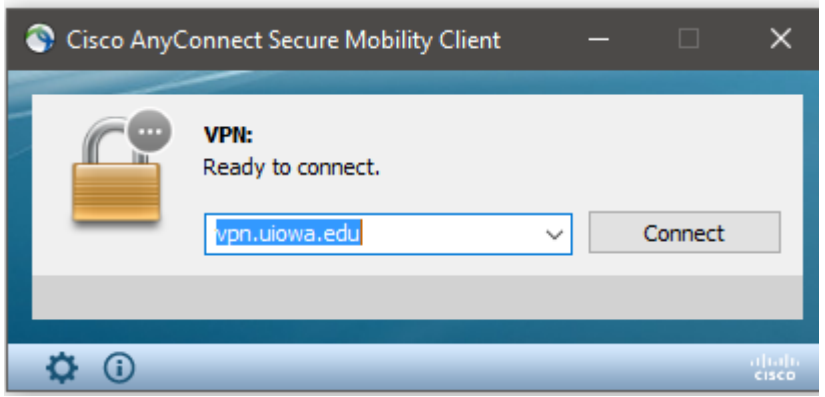
- Primárne určená pre mobilných pracovníkov / homeworkerov / partnerov spoločnosti
  - Používateľ sa pripája zo svojho NB/mobilu/tabletu do siete zamestnávateľa
  - Vytvára tunel zo svojho zariadenia na nakonfigurovanú VPN bránu
    - Spustením IPsec aplikácie
  - VPN ponúka prístup k špecifickým službám 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 – IPsec VPN**
    - Na koncovom zariadení je požadovaný nainštalovaný a nakonfigurovaný IPsec softvér (IPSec klient)
      - Cisco IPSec client (staršia verzia), Cisco AnyConnect Secure Mobility Client (aktuálny sw.), vstavaný IPSec vo Win 10 (KIS) (L2TP over IPsec)
    - 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 nahor
  - **Client-less VPN – SSL VPN**
    - Bez potreby inštalovať klienta => SSL VPN (TLS – Transport Layer Security)
    - Využíva PKI infraštruktúru kľúčov a certifikátov
    - V súčasnosti populárne, avšak vhodné len pre niektoré služby od L4 nahor
      - Primárne prístupné cez Web prehliadač



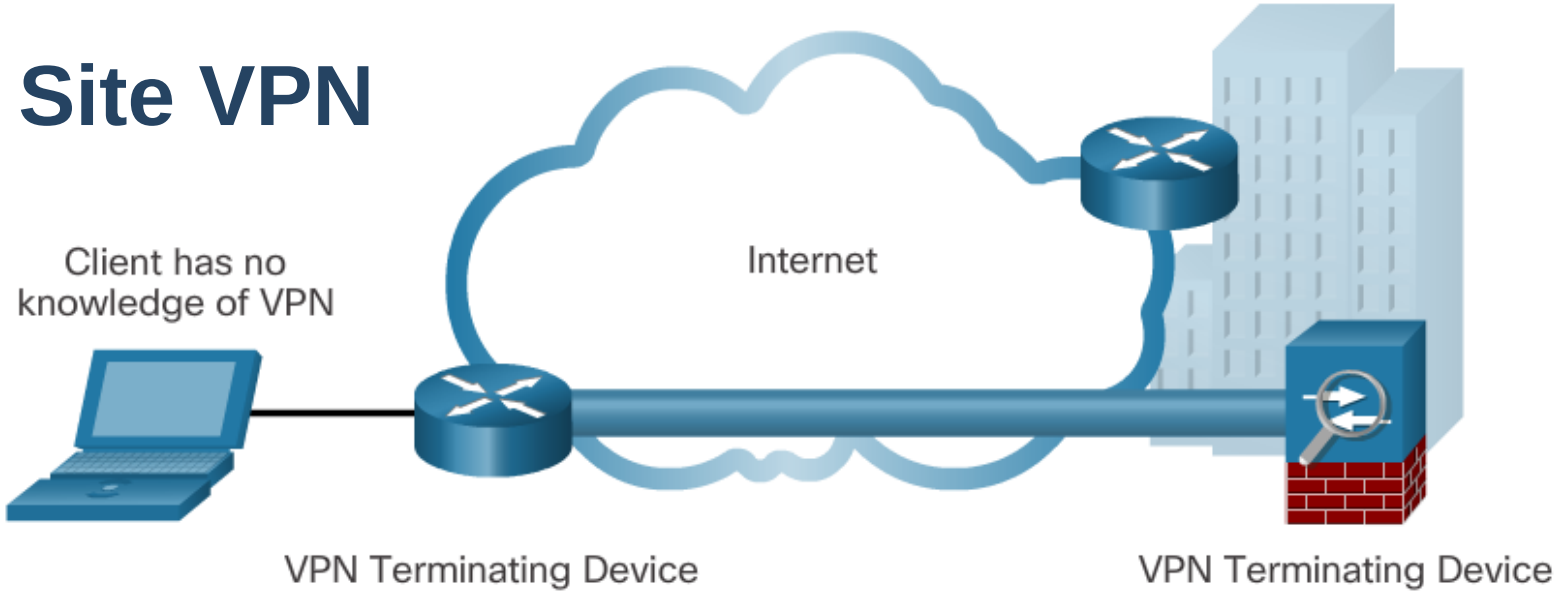


Porovnanie IPsec vs. SSL VPN

Vlastnosť	IPSec	SSL
Podpora aplikácii	**Rozsiahla** – podpora všetkých aplikácií od L3 nahor	**Limitovaná** – podpora len pre web aplikácie a zdieľanie súborov
Úroveň autentifikácie	**Vysoká** – dvojcestná autentifikácia s heslami či certifikátmi	**Stredne vysoká** – jedno a dvojcestná autentifikácia
Úroveň šifrovania	**Vysoká** – veľkosť kľúča od 56 do 256 bitov, mnoho typov algoritmov	**Stredne až vysoká** – veľkosť kľúča od 40 do 256 bitov, menej typov algoritmov
Zložitosť pripojenie	**Stredná** – lebo vyžaduje inštaláciu a konfiguráciu klienta	**Nízka** – stačí web prehliadač
Možnosti pripojenia	**Obmedzená** – len zariadenie s klientom, podpora klientov pre rôzne OS býva obmedzená	**Rozsiahla** – môže používať hocijaké zariadenie s prehliadačom

Site – to – Site VPN

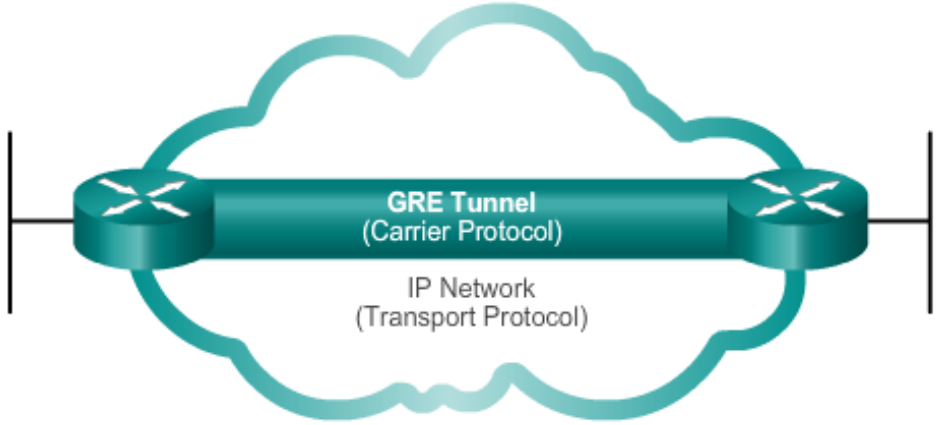
Site – to – Site VPN

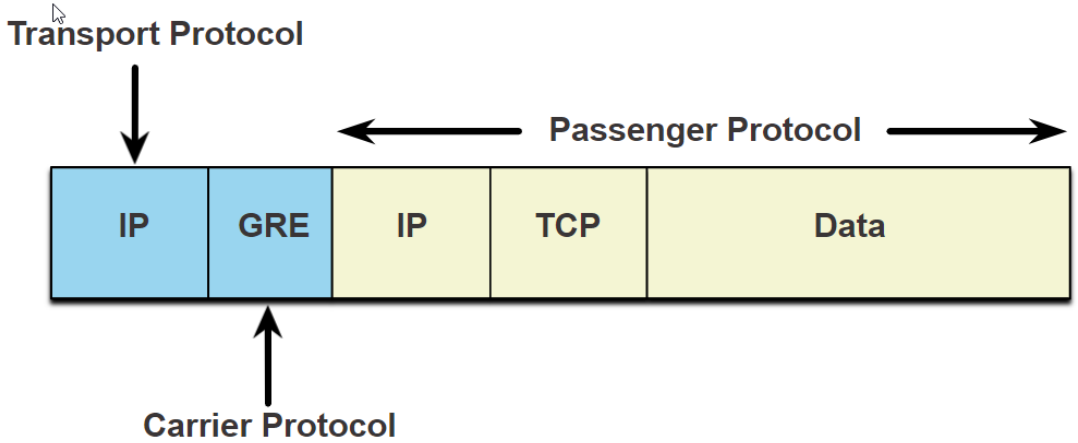


- Využíva koncept tunelovania medzi dvomi sieťovými zariadeniami
- Cisco riešenia Site–to–Site VPN
  - GRE
    - nešifrovaná, preto sa už neodporúča
  - IPSec – venjeme sa extra
    - šifrovaná VPN, problém so smerovaním
  - GRE over IPSec:
    - rieší problém so smerovaním, konfig. overhead
  - Cisco Dynamic Multipoint Virtual Private Network (DMVPN):
    - rieší overhead GREoverIPsec konfigurácie
  - IPsec Virtual Tunnel Interface (VTI)

Generic Routing Encapsulation – GRE

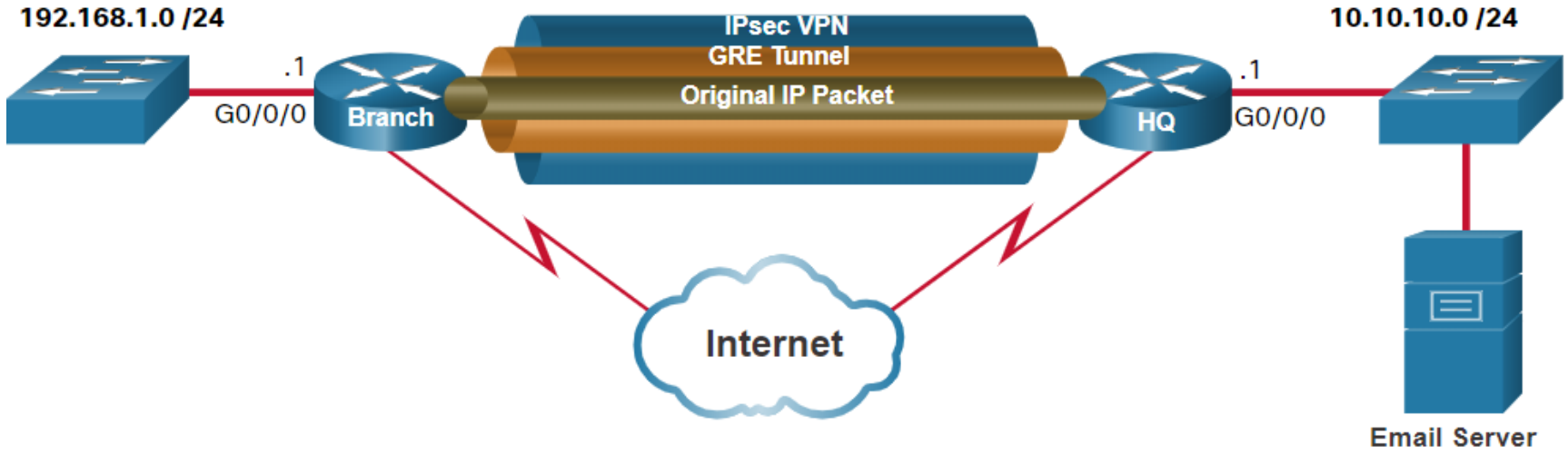
- GRE je pomocný tunelovací protokol na 3. vrstve
  - Podporuje rôzne typy tunelovaných paketov
    - Napr. IPv4, IPv6, IPX...
  - Vytvára virtuálny point-to-point prepoj medzi dvojicou smerovačov
  - Umožňuje prenášať aj multicastovú prevádzku
- GRE charakteristiky
  - je bezstavový, bez riadenia toku 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
    - Môže byť teda vložený do smerovacieho procesu





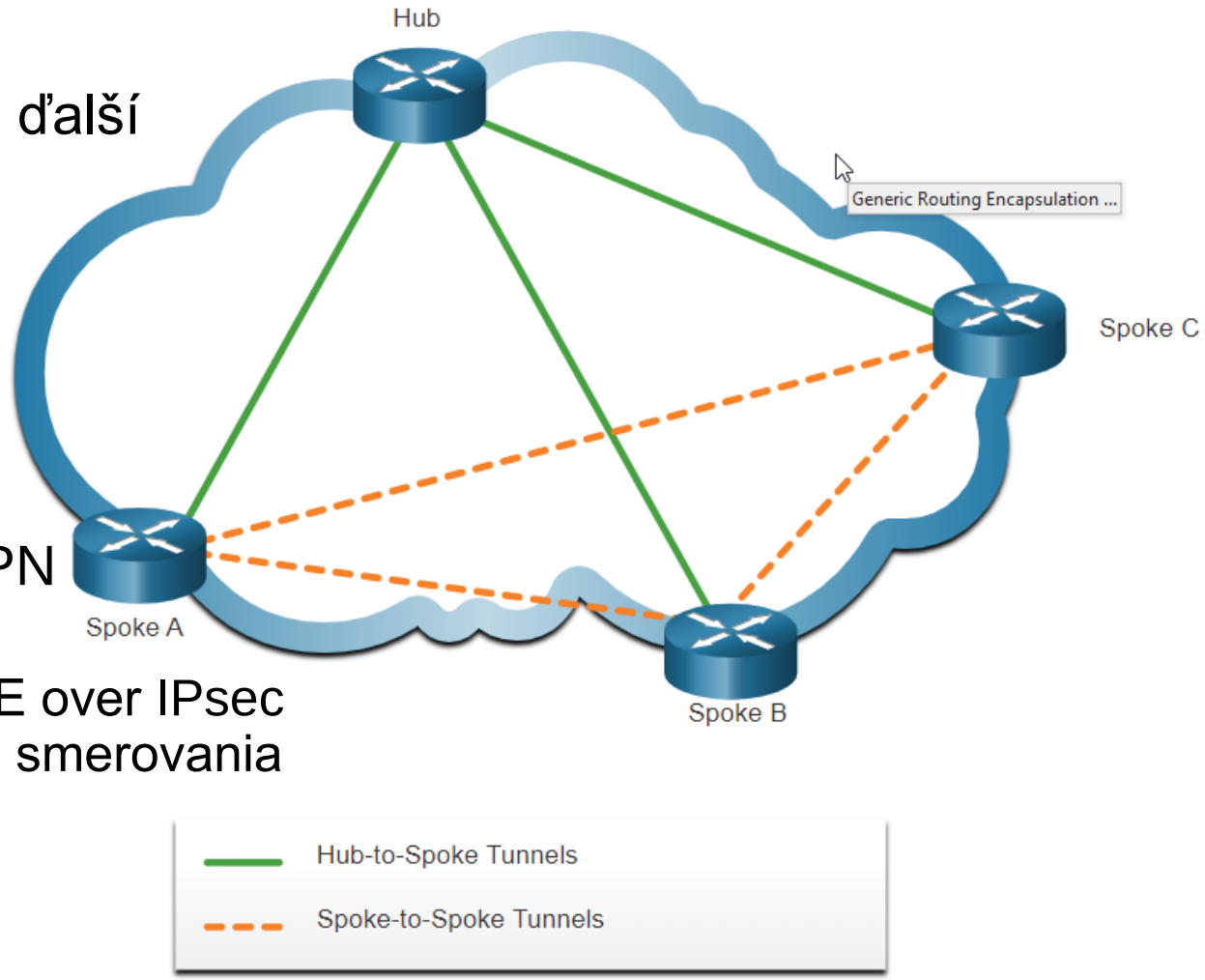
GRE over IPsec

- V realite 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



Dynamic Multipoint VPNs

- Avšak aj pri GRE over Ipsec sa objavuje ďalší problém
  - Konfigurácia GRE over IPsec
    - Vytvára Point-to-point tunely
    - Vytvárané manuálne a staticky
    - => zdĺhavé, vhodné len pre malý počet pobočiek
- Cisco riešenie => Dynamic Multipoint VPN (DMVPN)
  - Dynamické, zjednodušené vytváranie GRE over IPsec VPN pre riešenie problému veľa tunelov a smerovania
  - Škálovateľné riešenie pre veľa pobočiek
  - Dva odporúčané spôsoby nasadenia
    - Hub-to-Spoke tunnels
    - Spoke to Spoke tunnels

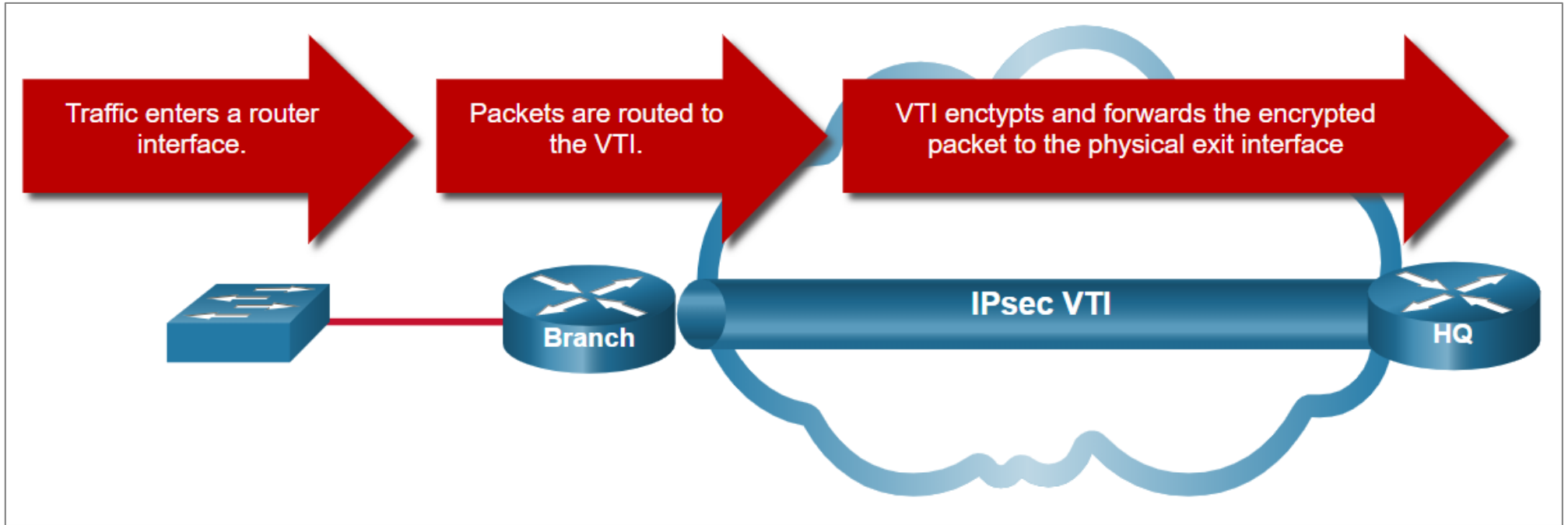


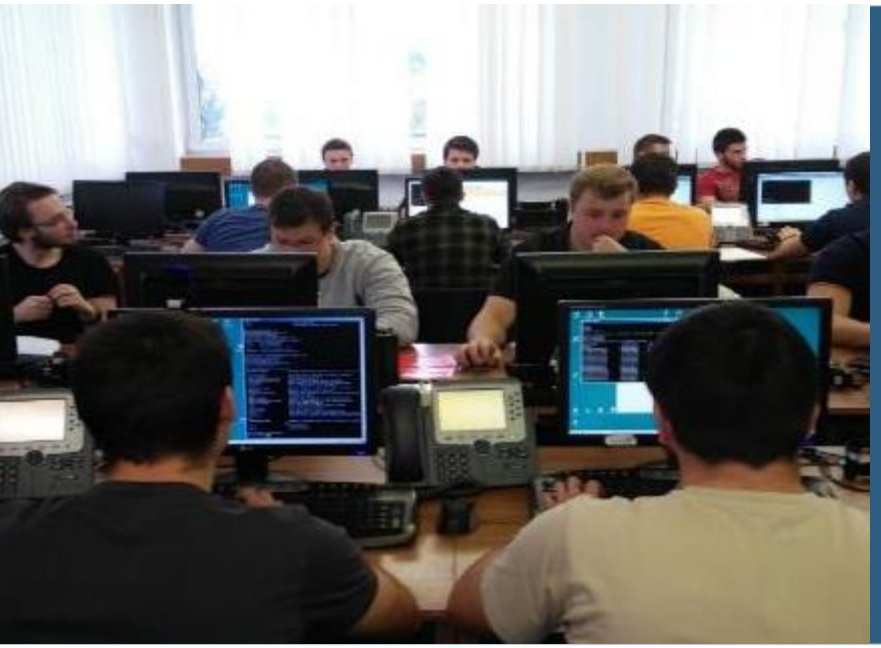
DMVPN využíva

- Tri technológie
  - Multipoint Generic Routing Encapsulation (mGRE) tunely
    - Viacbodové GRE tunely, aby som sa vyhol veľa rozhraniam p-t-p tunelov na danom smerovači (napr. hub)
  - Next Hop Resolution Protocol (NHRP)
    - Dynamické zisťovanie IP adries „next hop“ smerovačov pobočiek, kam chcem založiť tunnel
      - Mapovanie Privátnej IP siete pobočky na verejnú IP next hop-u
      - Klient / server arch
        - Klient: hlási svoje Ipčky, reistruje sa, a pýta sa na mapovanie
        - Server: drží si mapovania klientov
  - IP Security (IPsec)
    - Šifrovanie prevádzky

IPsec Virtual Tunnel Interface (VTI)

- Cisco vlastnosť:
  - IPsec VTI vytvára virtuálne rozhranie (niečo ako GRE rozhranie)
  - Prináša tak podporu unicast/multicast smerovania do Ipsec
    - Podpora činnosti smerovavích protokolov nad Ipsec VTI





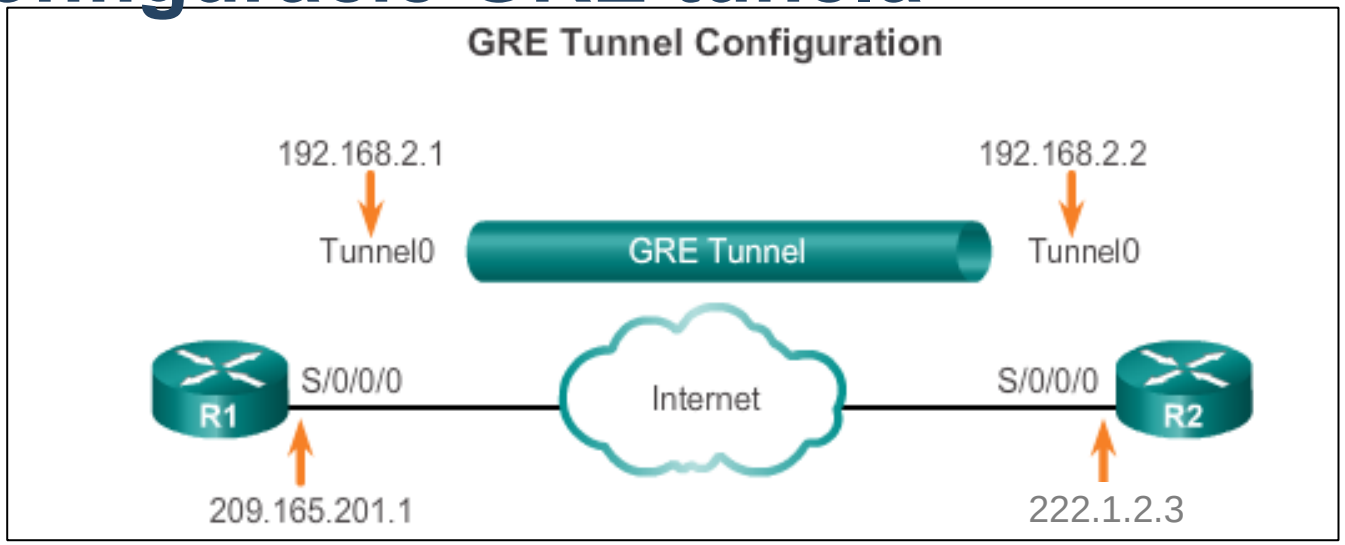
Jednoduchá konfigurácia GRE (**G**eneric Routing Encapsulation)

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

Overenie

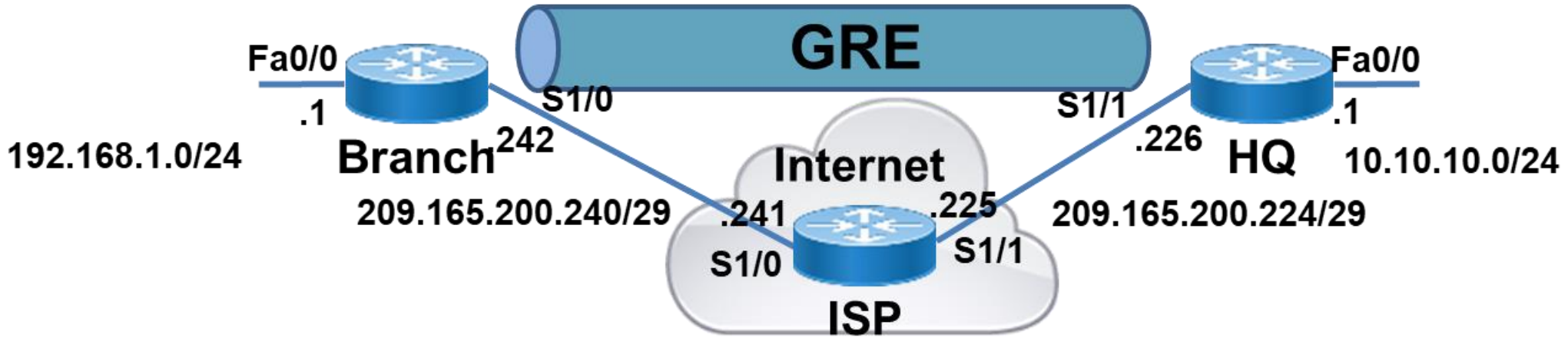
```
Pobocka# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 223.1.2.3
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 1000 (kbps)
  Tunnel receive bandwidth 1000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

<output omitted>
```

Konfig smerovačov - príprava

- Jednoduchá topo
- Na Pobocka a HQ
  - bude NAT
  - Bude static def. route
- Na ISP len IP adresy
- Potom konfig GRE
  - Adresa 172.16.1.0/24
  - Pobocka: .1, HQ: .2
- Routing OSPFv2

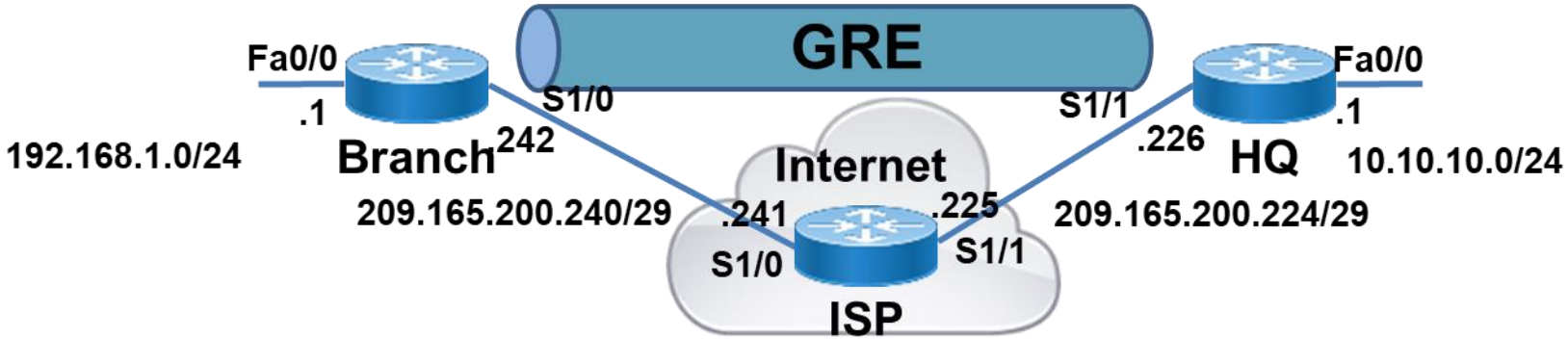
```
ena
conf t
hostname ISP
int s1/0
          ip add 209.165.200.241 255.255.255.248
          no shut
int s1/1
          ip add 209.165.200.225 255.255.255.248
          no shu
          exit
Line con 0
          logging synchronous
          end
Wr mem
```



Konfig smerovačov - príprava

```
! Pobocka
ena
conf t
hostname Pobocka
int fa 0/0
          ip add 192.168.1.1 255.255.255.0
          ip nat inside
          no keepalive
          no shut
int s1/0
          ip add 209.165.200.242 255.255.255.248
          ip nat outside
          no shu
          exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 int s 1/0 overload
ip route 0.0.0.0 0.0.0.0 s1/0
Line con 0
          logging synchronous
          end
wr mem
```

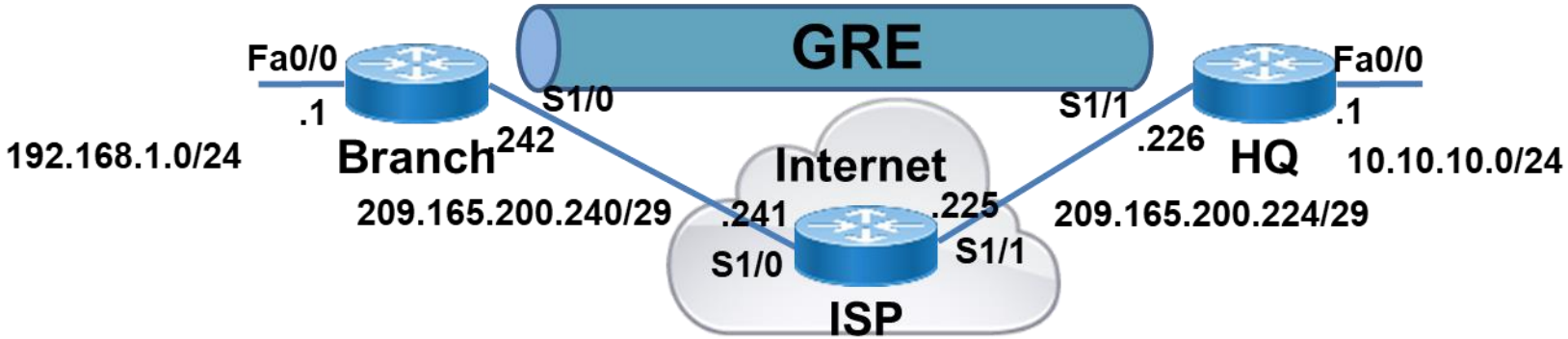
```
!HQ
ena
conf t
hostname HQ
int fa 0/0
          ip add 10.10.10.1 255.255.255.0
          ip nat inside
          no keepalive
          no shut
int s1/1
          ip add 209.165.200.226 255.255.255.248
          ip nat outside
          no shu
          exit
access-list 1 permit 10.10.10.0 0.0.0.255
ip nat inside source list 1 int s 1/1 overload
ip route 0.0.0.0 0.0.0.0 s1/1
Line con 0
          logging synchronous
          end
wr mem
```



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
```

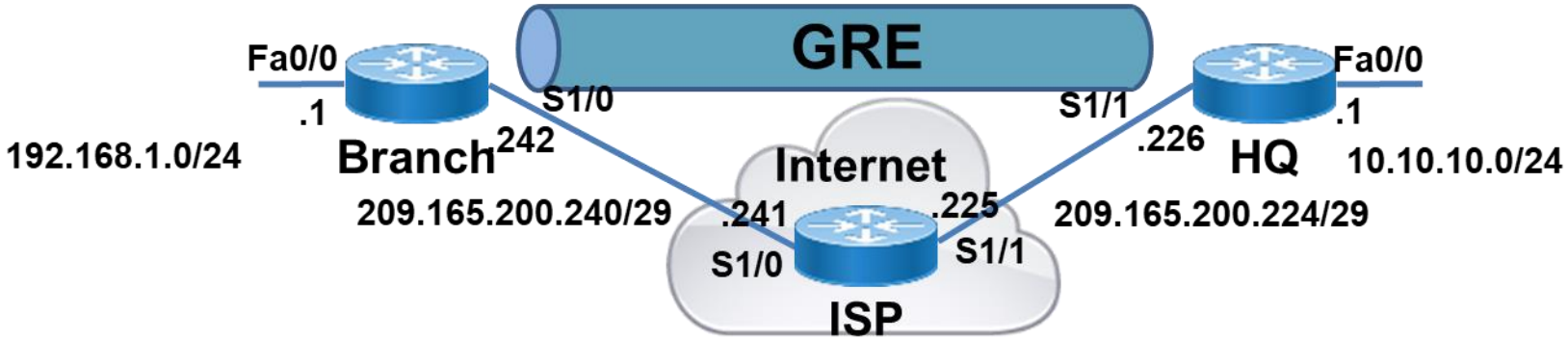


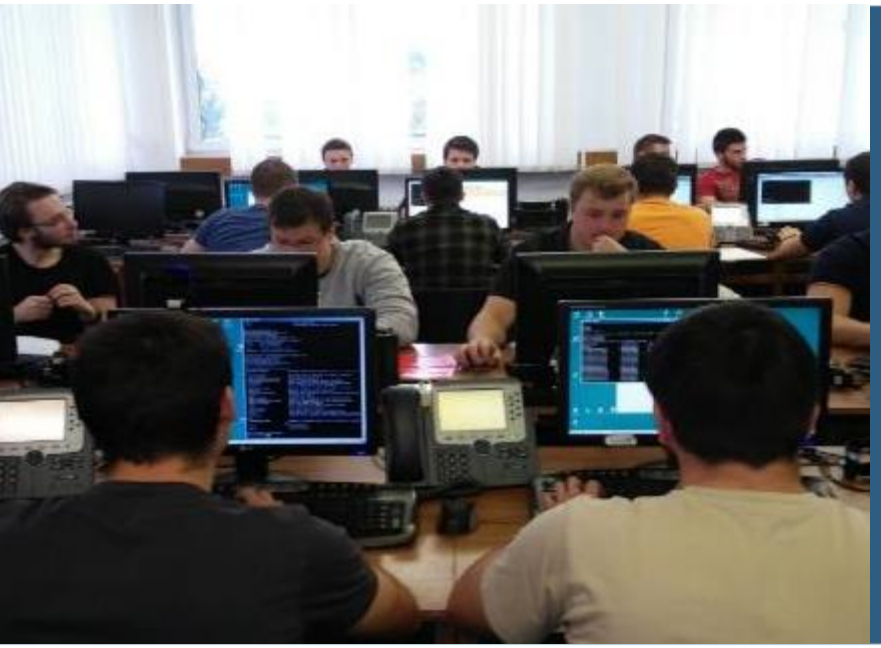
Overenie GRE

```
Ping
tracert
Sh int tunnel 0
Sh ip route
```

```
!HQ
HQ#ping 192.168.1.1 so fa 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/38/60 ms


HQ#tracer 192.168.1.1 so fa 0/0
Type escape sequence to abort.
Tracing the route to 192.168.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 28 msec 24 msec *
```



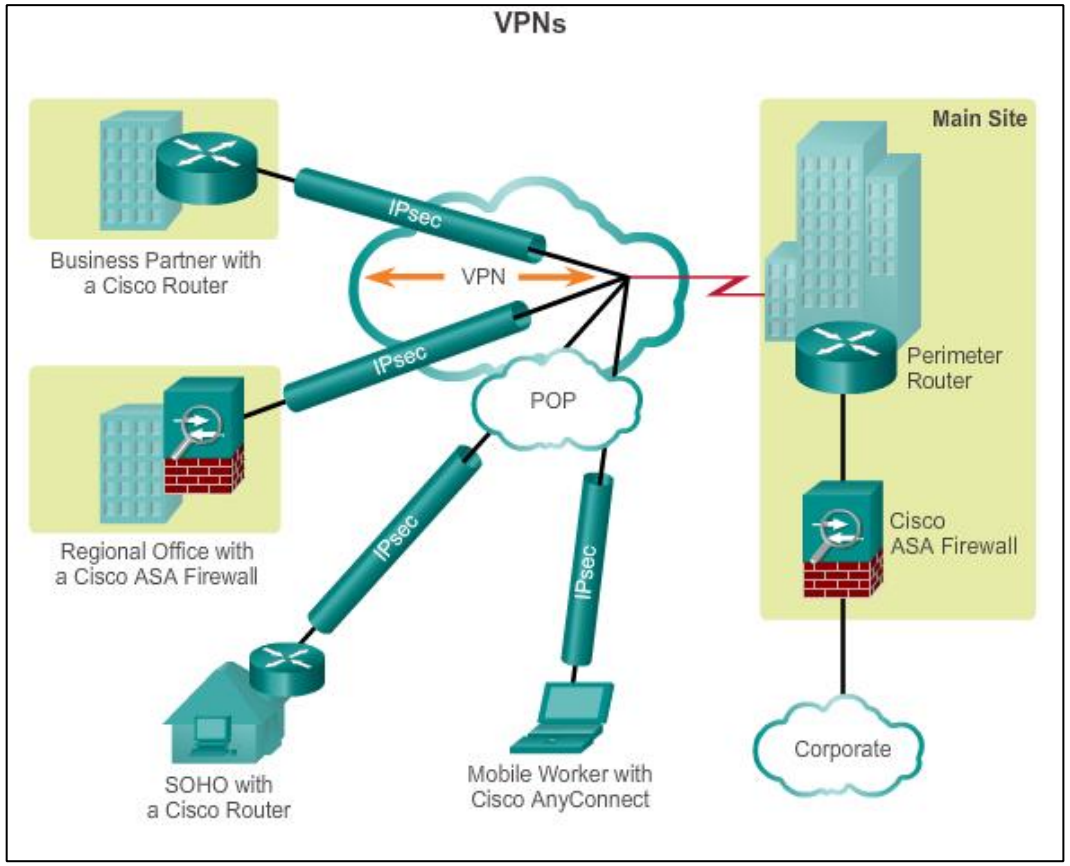


IPsec VPN Komponenty a činnosť

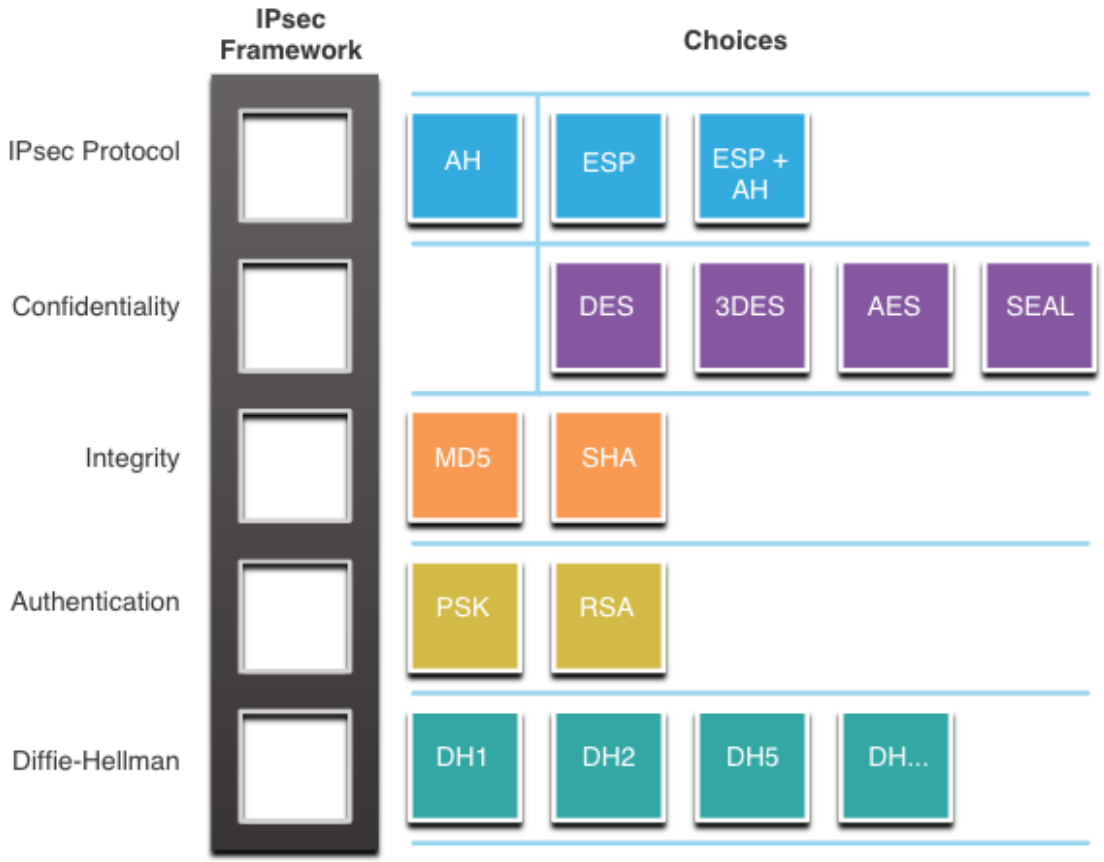
Úvod do IPsec

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



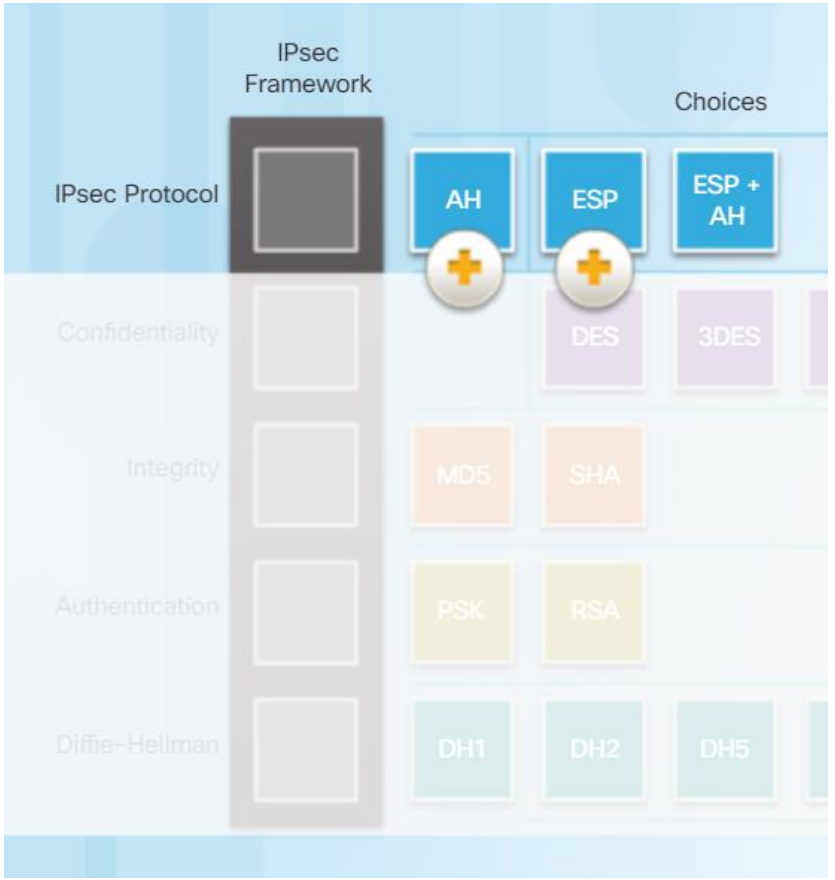
Sada použitých parametrov vytvára tzv. Security association (SA)

- 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 (**Authentication**)
    - 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

IPsec – protocol framework

IPsec Protokol Framework (cont.)

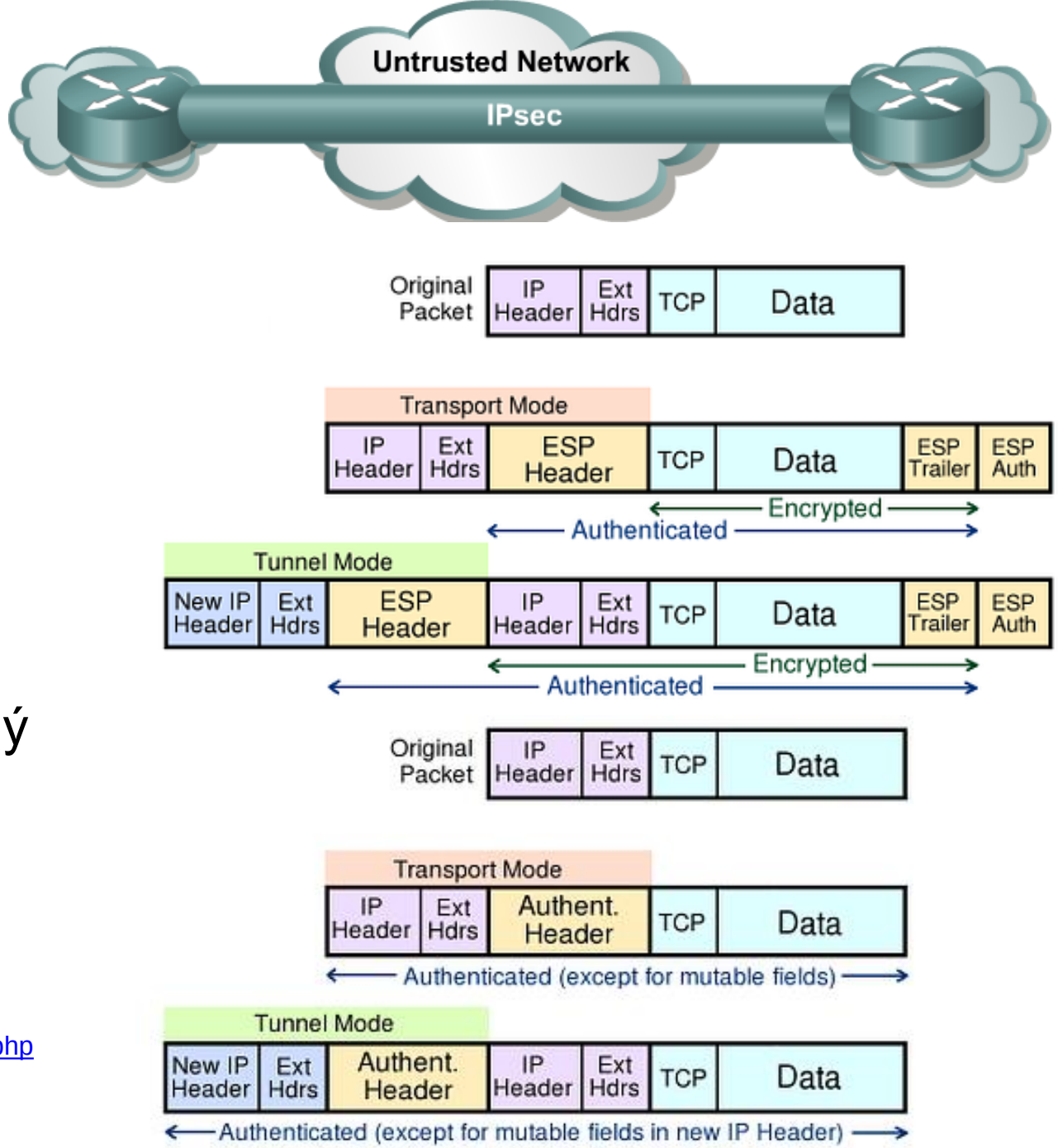
- Definuje spôsob činnosti Ipsec, sú dve základné:
  - Authentication header (AH)
    - Chráni kompletný obsah paketu vrátane nemenných častí IP hlavičky autentifikačnými mechanizmami
    - Nezabezpečuje však šifrovanie
    - Nemá rada NAT (prepisuje IP adresy v hlavičke)
  - Encapsulation Security Payload (ESP)
    - Chráni payload paketu šifrovaním
    - V transport režime nezabezpečuje hlavičku paketu
    - Autenticitu chráni dodatočne
- Pozn.
  - Použitie AS či ESP určuje aké ďalši 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

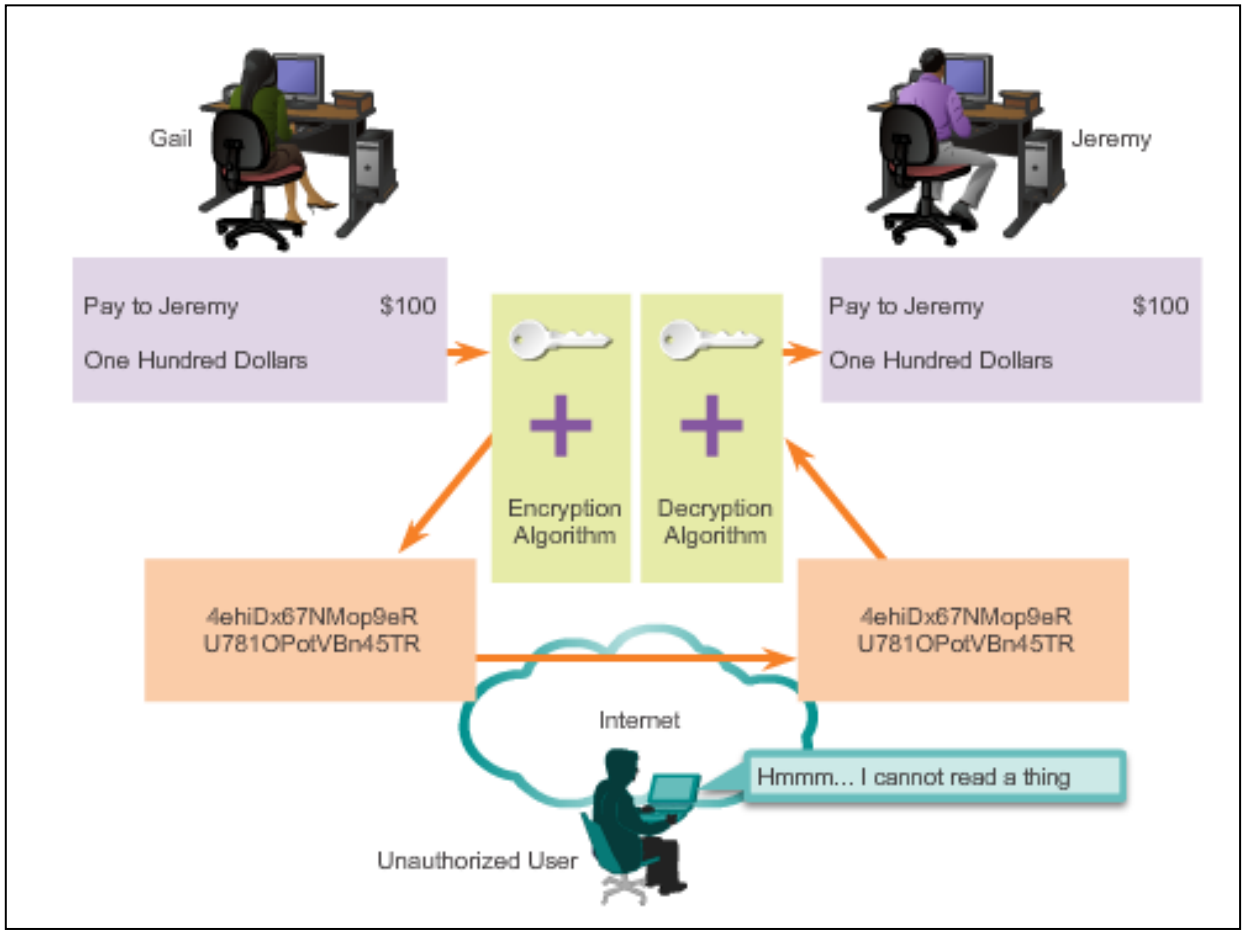
- Tunelový režim
  - Prikladá novú IP hlavičku a tuneluje pôvodný IP paket
  - Preferovaný
- Transportný režim
  - Ponecháva pôvodnú IP hlavičku
  - Na Cisco routeroch sa transportný režim využije len vtedy, ak je odosielateľom (autorom) paketu sám router

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



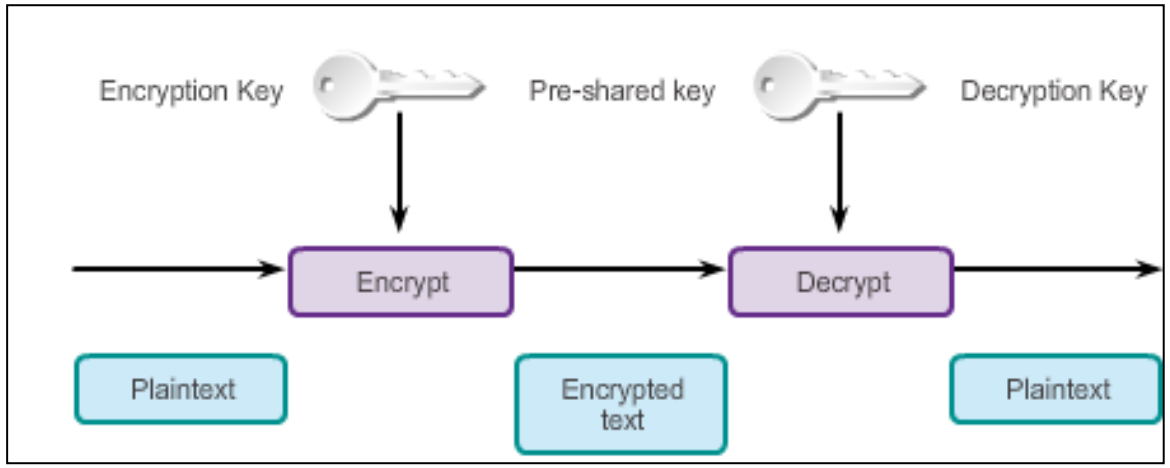
Utajenosť šifrovaním (Confidentiality with Encryption)

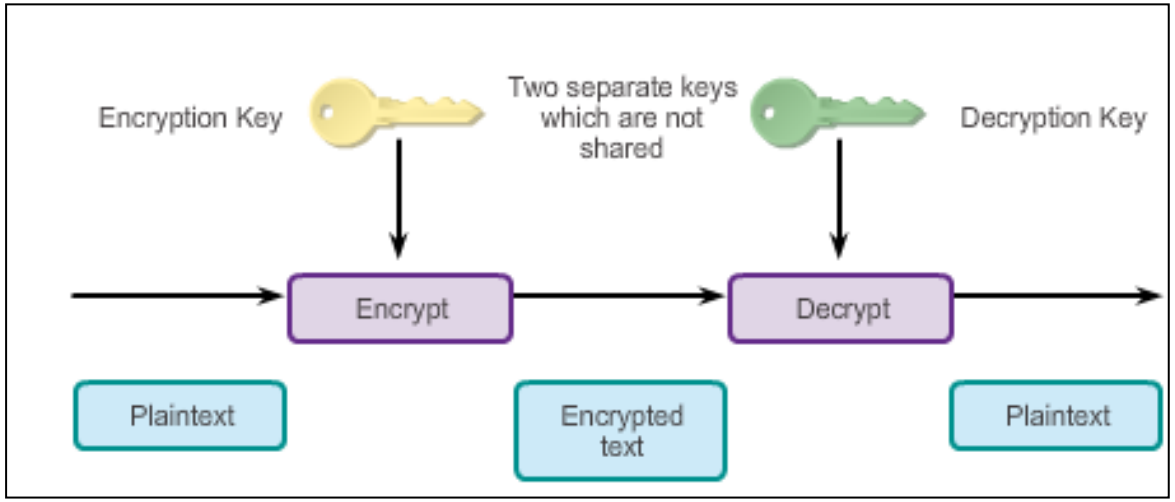
- Využíva techniky šifrovania
  - Konverzie pôvodnej správy do jej zameneného variantu
- Aby šifrovanie pracovalo správne
  - Musí odosielateľ aj príjemca poznať pravidlá použité na transformáciu pôvodnej správy do jej kódovanej podoby a späť.
- Pravidlá sú založené na algoritmoch a pridružených kľúčoch.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



Šifrovacie Algoritmy

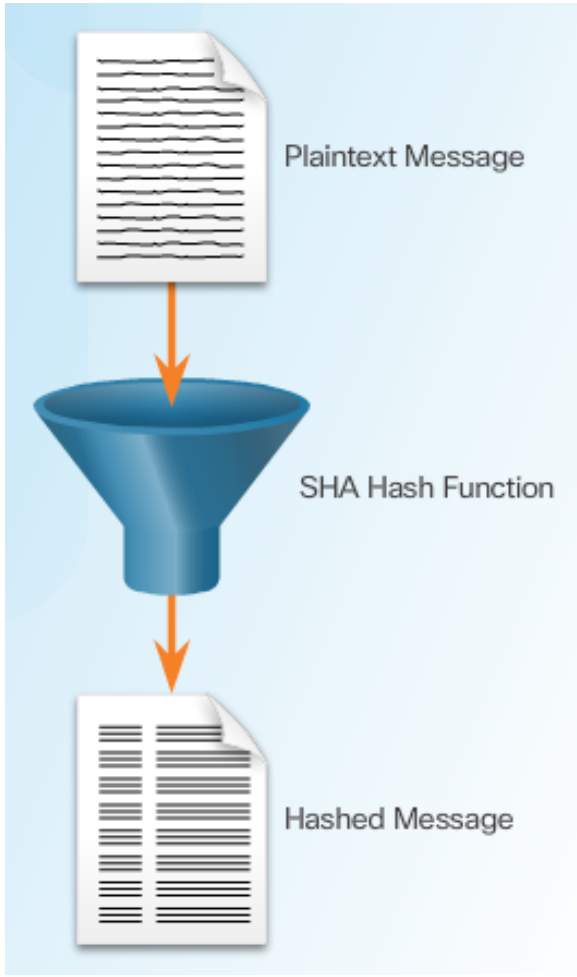
- Dva hlavné typy:
  - **Symetrické algoritmy**
    - **Rovnaký** kľúč pre šifrovanie aj dešifrovanie
    - DES, 3DES, AES, SEAL, RC šifry
    - Líšia sa rýchlosťou, silou kľúča (56-256b)
    - Nižšia bezpečnosť, veľká rýchlosť
  - **Asymetrické algoritmy**
    - Iný kľúč pre šifrovanie, iný pre dešifrovanie
    - 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

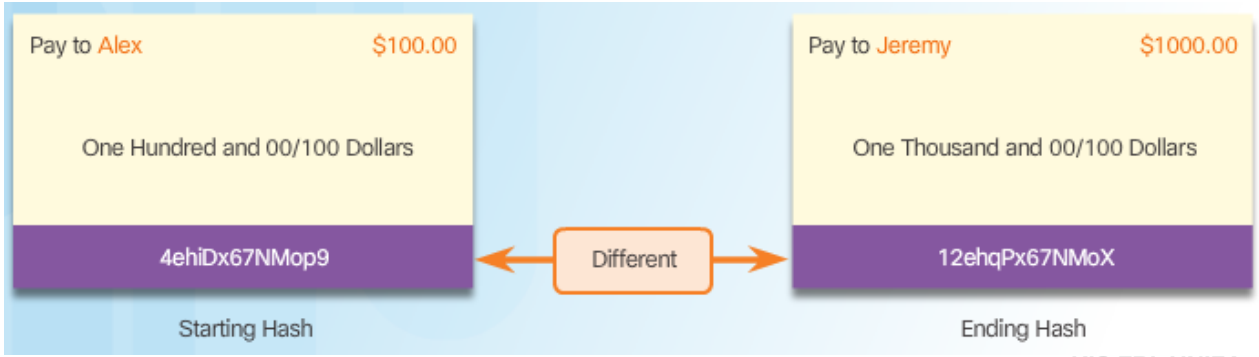




Dátová Integrita (Integrity)

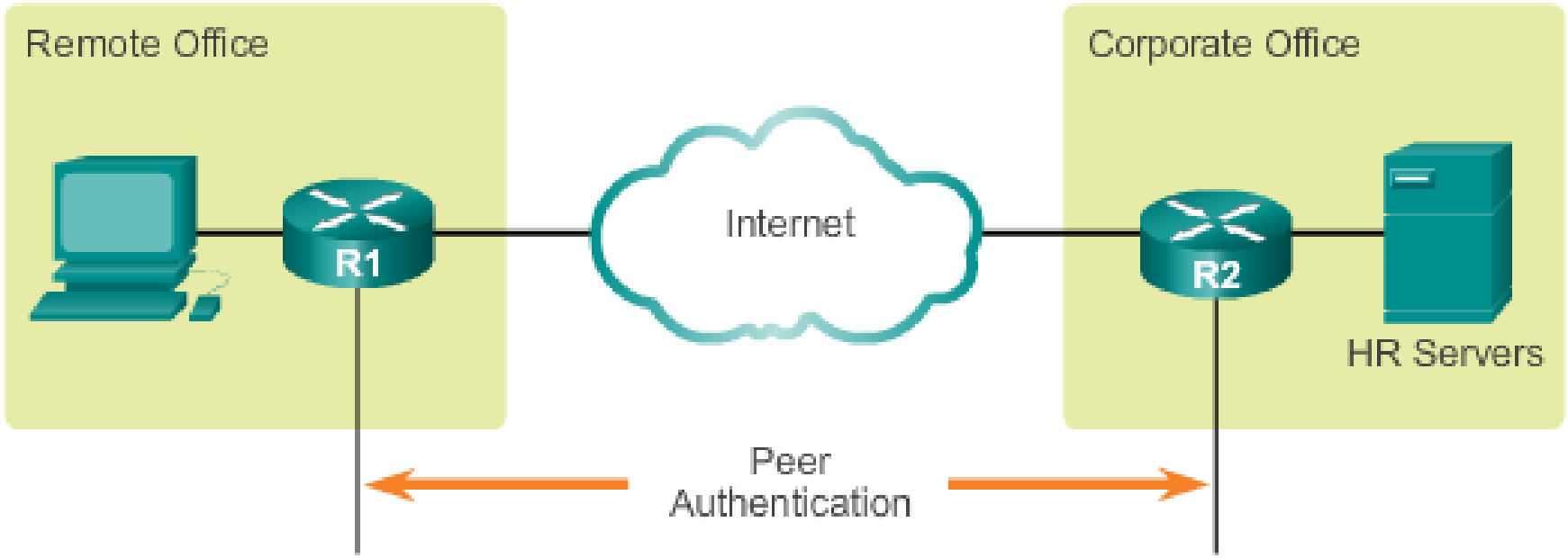
- Prostriedok na dosiahnutie, aby prijímateľ vedel, že so správou sa nemanipulovalo
  - Pôvodný odosielateľ
    - Generuje hash odosielanej správy
    - Ktorú pošle so samotnou správou.
  - Príjemca
    - Z prijatej správy vytvorí vlastný hash
    - Analyzuje správu a prijatý hash
    - Ak sú rovnaké, 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)





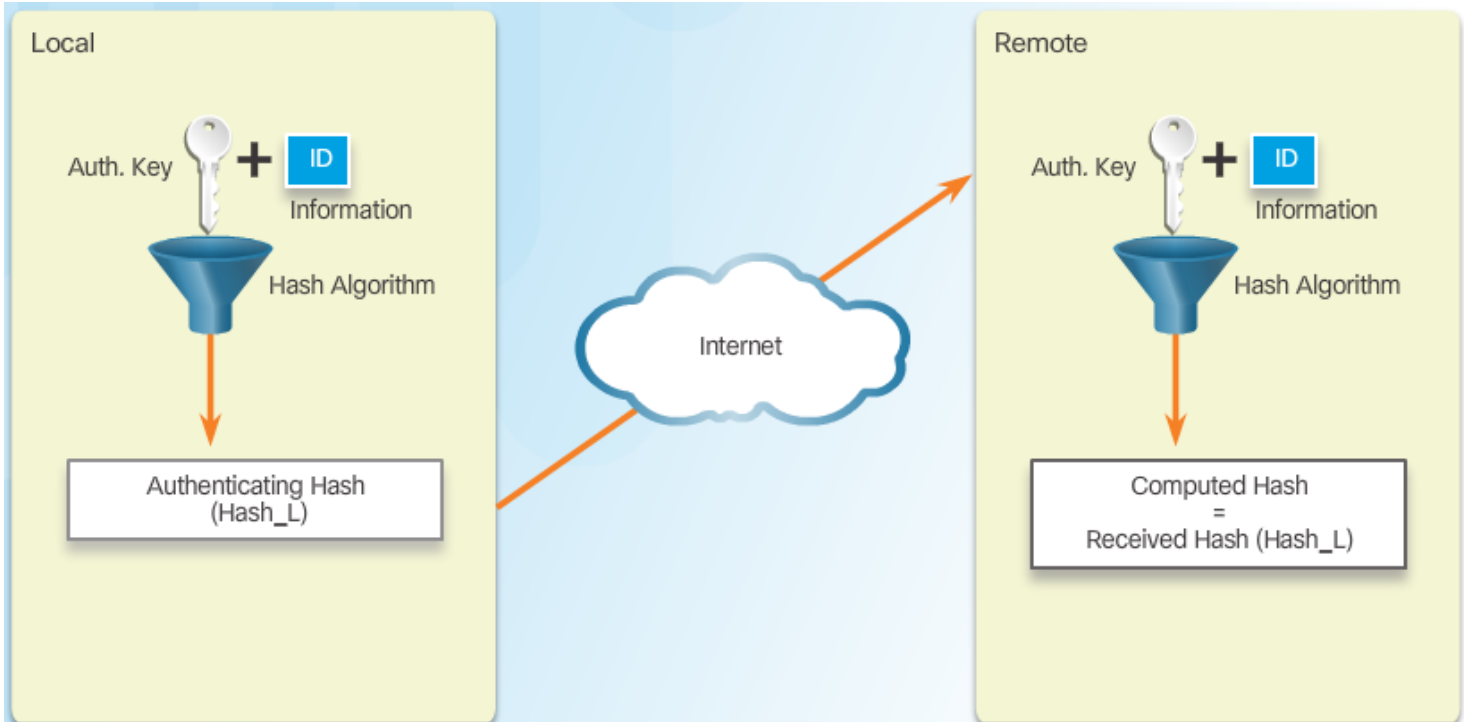
IPsec Autentifikácia (Authentication)

- 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)**



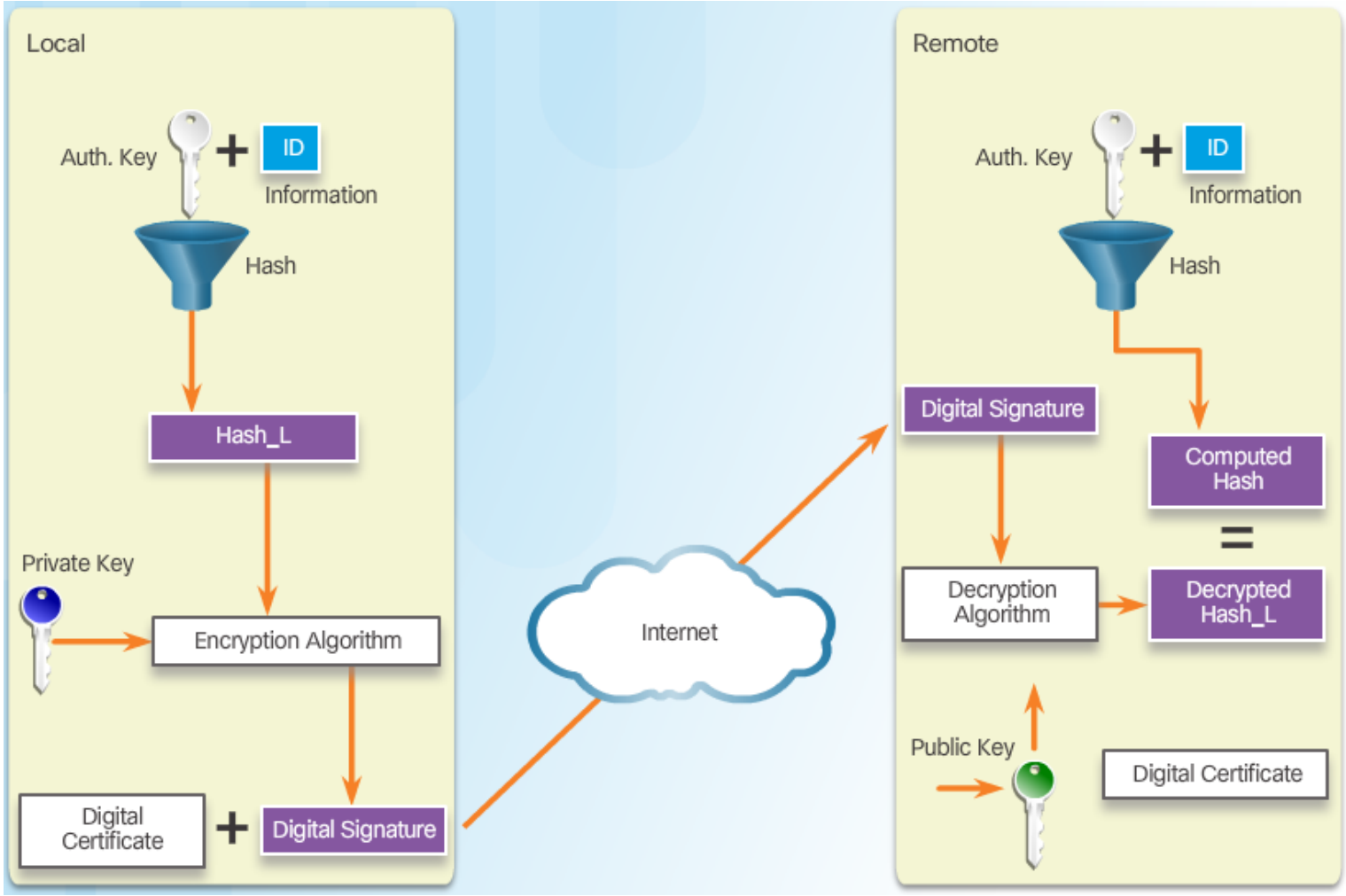
IPsec PSK autentifikácia

- **Pre-shared key (PSK) (zdieľaný kľúč)**
  - Kľúč sa zadáva na každom susedovi ručne adminom, jednoduchá manuálna konfigurácia
  - Používa symetrické šifrovanie => problém s prenosom kľúča
  - 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 prenos certifikátov používa digitálny podpis
  - Na šifrovanie používa asymetrické algoritmy



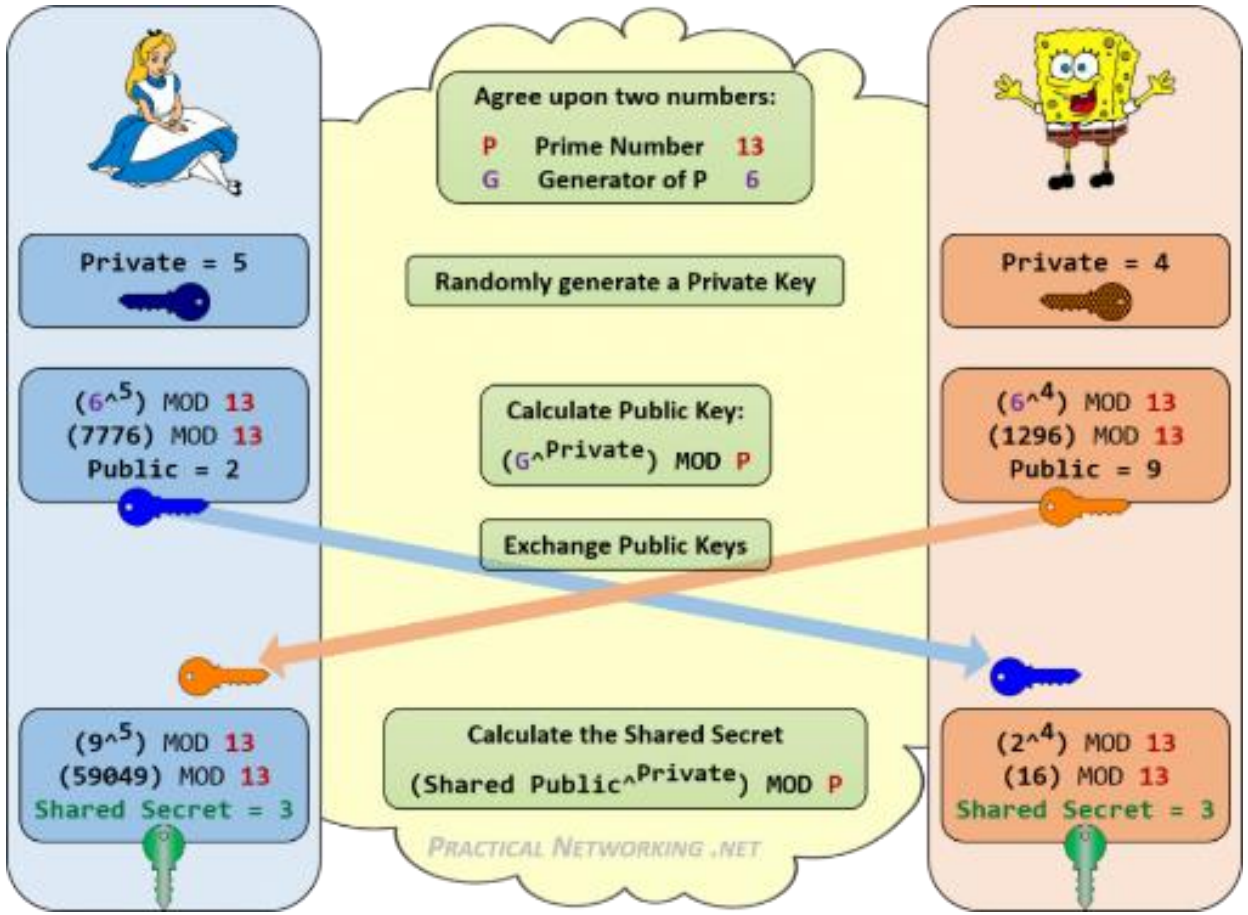
Výmena kľúčov cez Diffie-Hellman

- 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

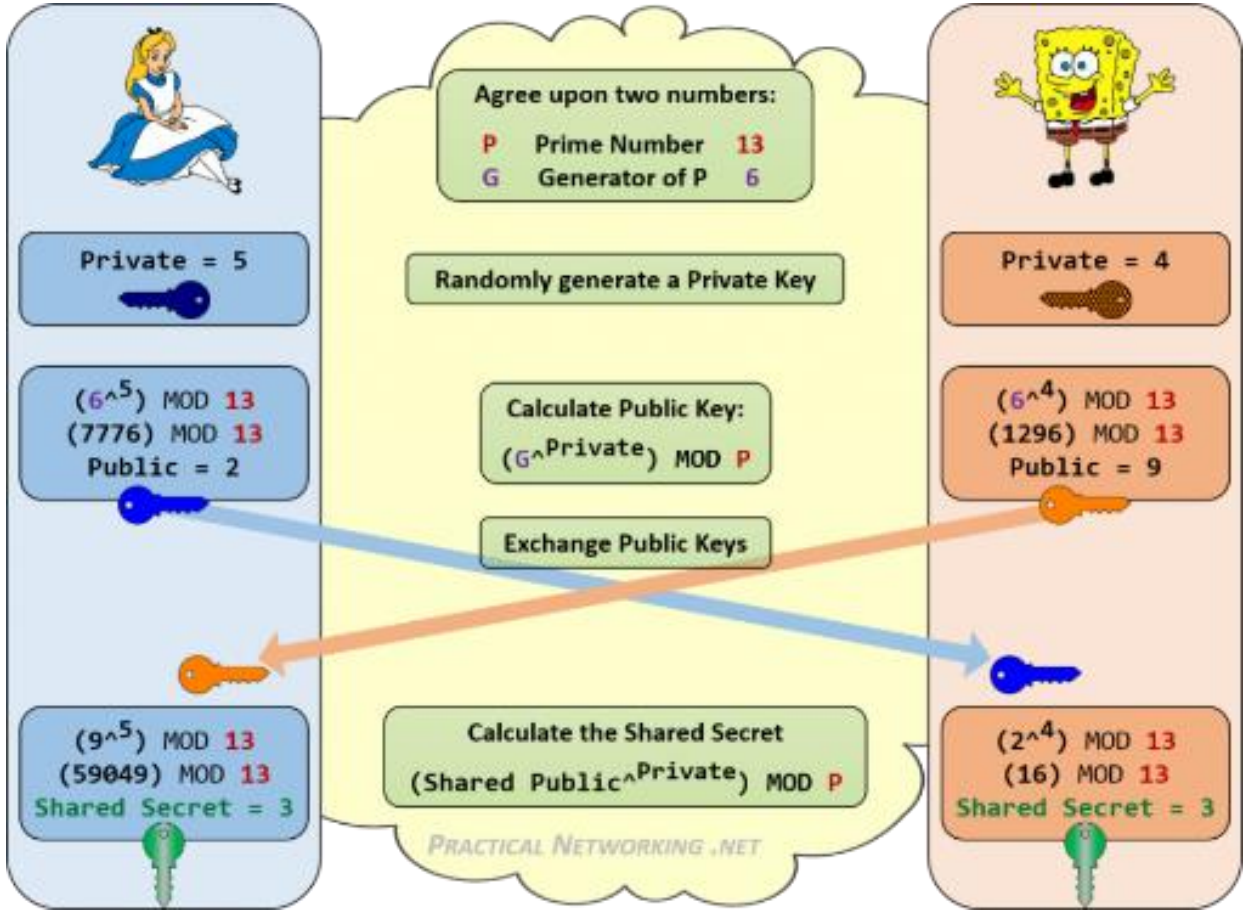
Diffie-Hellman Key Exchange

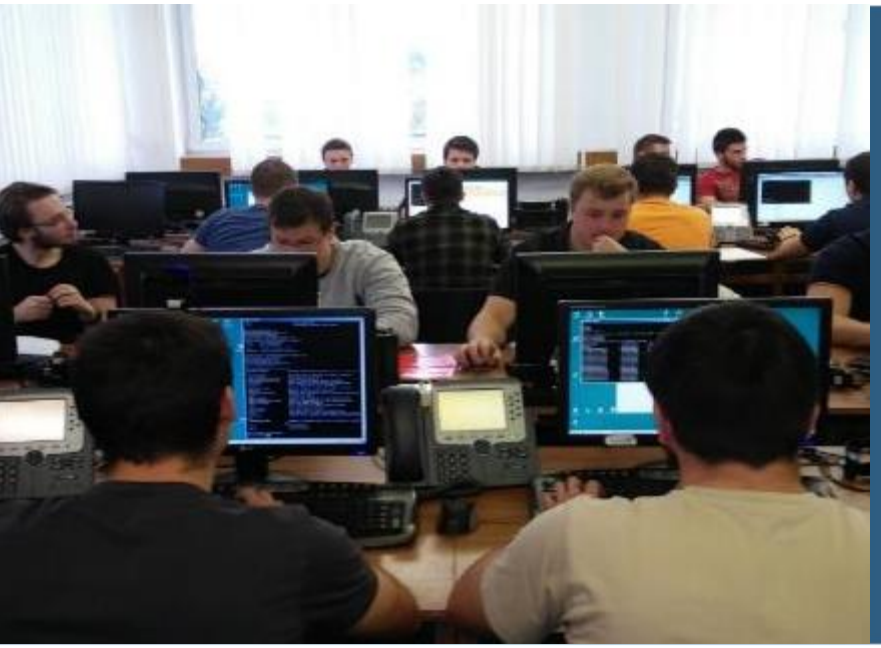
- Postup vo viac krokoch
  - 1) Obe strany sa najprv musia dohodnúť na dvoch číslach, ktoré si budú zdieľať
    - Čísla sa nemusia utajovať
    - P: prvočíslo, zvyčajne veľké
    - G: základ mocniny (mocnenec), zvyčajne malé
  - 2) Každá zo strán si lokálne vygeneruje náhodné privátne číslo PRIVATE
  - 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
    - 14, kľúč: 2048bitov
    - 15, kľúč: 3072bitov
    - 14, kľúč: 4096bitov





Jednoduchá konfigurácia IPsec

Vytvorenie spojenia medzi IPsec susedmi

- Treba si uvedomiť
  - => šifrovanú IPsec VPN zakladáme cez nezabezpečený internet so vzdialenou „neznámou“ bránou
- VPN brány preto musia vyriešiť radu otázok:
  - Ako viem, že vzdialený sused je ten, ktorý má byť a nie je niekto cudzí či podstrčený?
    - Riešime autentifikáciou
  - Ako si vymeníme šifrovacie heslá pre šifrovanie dát cez nezabezpečený internet?
    - Zabezpečený kanál ešte nemáme
  - Aký symetrický algoritmus použiť na šifrovanie dát?
    - Aké heslo použiť na šifrovanie/dešifrovanie
  - Ktorá prevádzka bude šifrovaná a ktorá nebude?
  - Aký IPsec protokol a režim činnosti použijeme pre VPN ?
  - A mnoho ďalších ....

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.

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

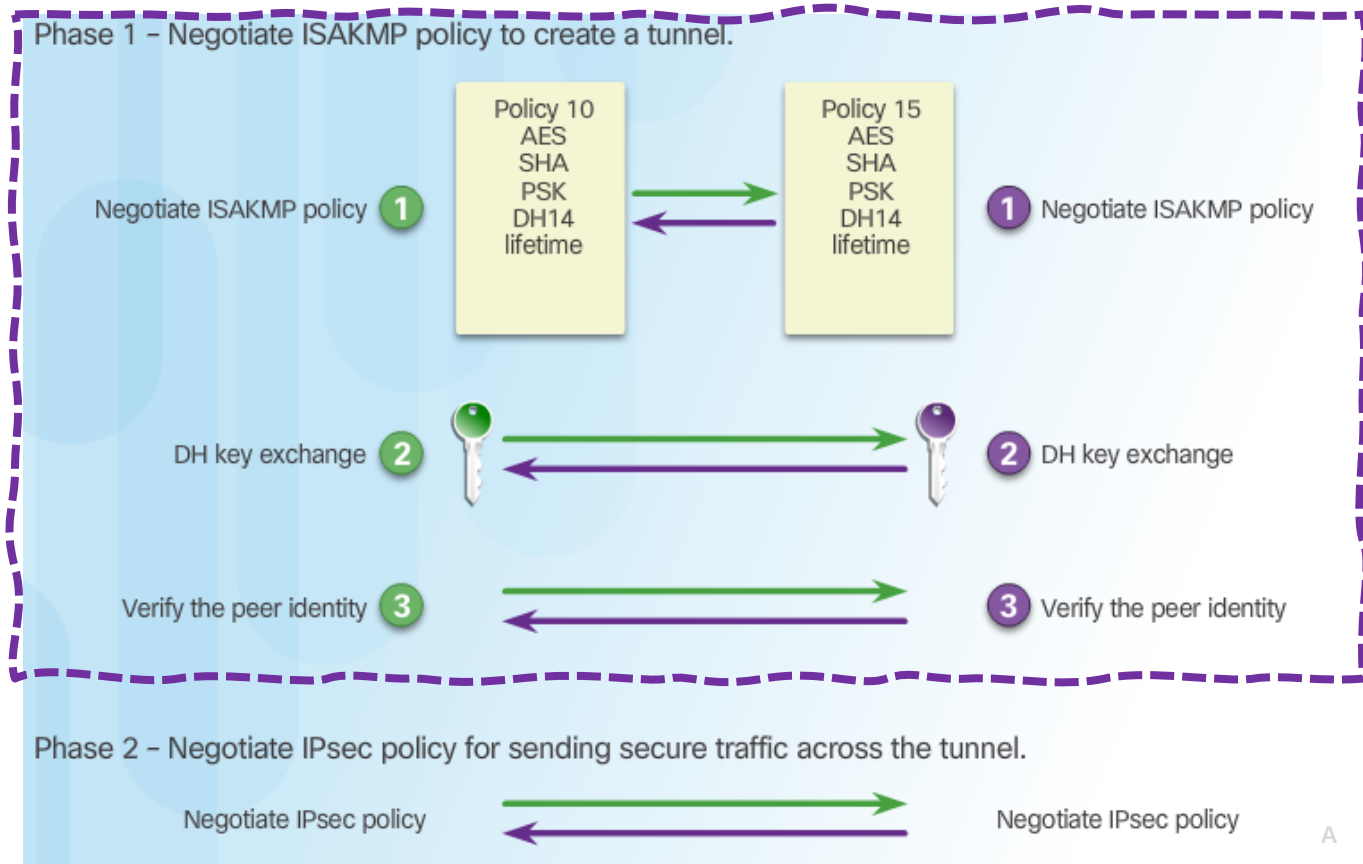
4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

Vytvorenie spojenia: IKE fáza 1 (IKE SA)

- IKE fáza 1 si vytvára zabezpečený kanál pre overenie totožnosti IPsec susedov a prípadne používateľov (zabezpečenie ISAKMP správ)
  - Nedohaduje samotné vlastnosti pre činnosť Ipsec tunela

- IKE fáza 1 má tri kroky:
  - Dohodnutie ISAKMP politík
  - Výmenu šifrov./hash kľúčov pomocou Diffie-Hellmanovho algoritmu
  - Overenie totožnosti susedov
- 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



Vytvorenie spojenia: IKE fáza 2

- IKE fáza 2 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 mechanizmus?

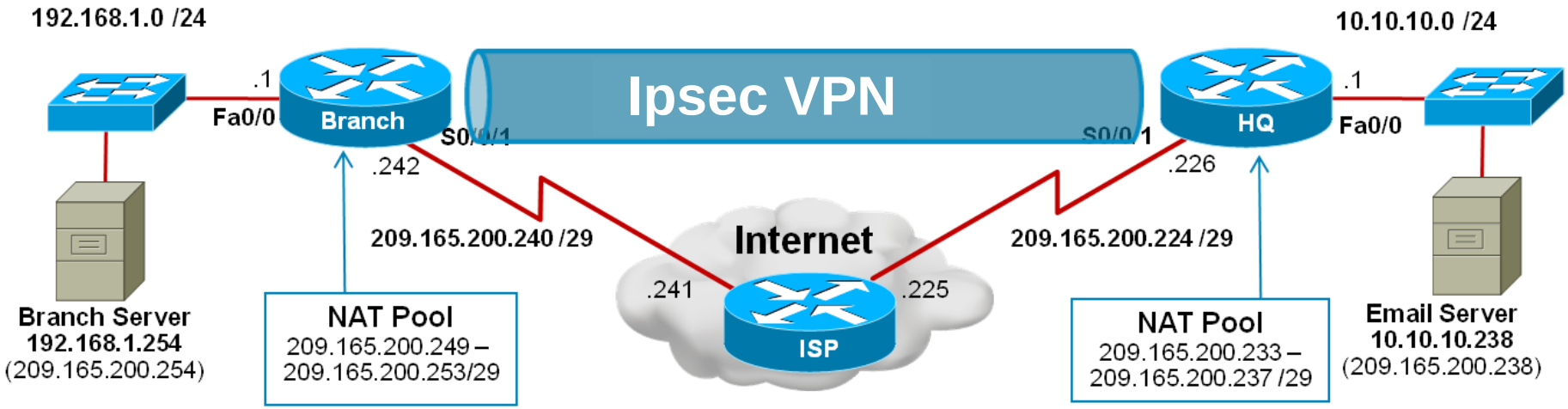
  transformačná sada
  - Aké šifrovacie kľúče?
  - Aká bude životnosť dohodnutých informácií?

Vytvorenie spojenia medzi IPsec susedmi

- Vytvorenie IPsec tunela sa nerobí vopred
- Vytvorenie tunela vždy spúšťa až príchod paketu prenášaného z jednej siete do cieľovej
- Pro příchode takéhoto paketu (identifikovaného ACL)
  - prebehnú obe fázy a vytvoria sa bezpečnostné asociácie spojenia
  - Ich použitie je viazané na dobu životnosti určenú konfiguráciou
  - Po dobe neaktivity a uplynutie lifetime je Ipsec ukončený
    - A vytvorený až pr

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#
```

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

❷ **IPsec trans. set**
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

Kompletná konfigurácia Pobocka Router IPsec VPN

```
Pobocka# conf t
Pobocka(config)# crypto isakmp policy 1
Pobocka(config-isakmp)# encryption aes 256
Pobocka(config-isakmp)# hash sha
Pobocka(config-isakmp)# authentication pre-share
Pobocka(config-isakmp)# group 24
Pobocka(config-isakmp)# exit
Pobocka(config)# crypto isakmp key cisco123 address 209.165.200.226
Pobocka(config)#
Pobocka(config)# crypto ipsec transform-set MOJA_TR_SADA esp-aes esp-sha-hmac esp-3des
Pobocka(cfg-crypto-trans)# exit
Pobocka(config)#
Pobocka(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Pobocka(config)#
Pobocka(config)#
Pobocka(config)# crypto map MOJA_MAPA 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Pobocka(config-crypto-map)# set transform-set MOJA_TR_SADA
Pobocka(config-crypto-map)# set peer 209.165.200.226
Pobocka(config-crypto-map)# match address 110
Pobocka(config-crypto-map)# exit
Pobocka(config)# int s0/0/1
Pobocka(config-if)# crypto map MOJA_MAPA
Pobocka(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

Overenie

- Zobrazí konfigurované ISAKMP politiky
  - **`Show crypto isakmp policy`**
- Zobraz PSK kľúč
  - **`sh crypto isakmp key`**
- Zobraz IKE phase 1 SA
  - Vidieť bude niečo až keď prebehne fáza **`1`**
  - **`Sh crypto isakmp sa`**
- Zobraz konfig a stav Sapre Ipsec
  - **`Sh crypto ipsec sa`**
- Zobraz crypto mapu
  - **`Show crypto map`**

  - **`Show crypto session`**

Overenie

```
Pobocka# sh crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #24 (2048 bit, 256 bit subgroup)
        lifetime:               86400 seconds, no volume limit
```

```
Pobocka# sh crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      209.165.200.226                           cisco123
```

```
Pobocka#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.200.226 209.165.200.242 QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Overenie

```
Pobocka#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local            Remote           I-VRF   Status Encr Hash   Auth DH Lifetime Cap.

1001  209.165.200.242 209.165.200.226          ACTIVE aes  sha    psk  24 23:54:29
       Engine-id:Conn-id =  SW:1

IPv6 Crypto ISAKMP SA
```

```
Pobocka#sh crypto session
Crypto session current status

Interface: Serial1/0
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500
  Session ID: 0
  IKEv1 SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
  IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 10.10.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

Overenie

```
Pobocka#sh crypto ipsec sa

interface: Serial1/0
    Crypto map tag: MOJA_MAPA, local addr 209.165.200.242

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(10.10.10.0/255.255.255.0/0/0)
   current_peer 209.165.200.226 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.200.242, remote crypto endpt.:
209.165.200.226
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb
Serial1/0
     current outbound spi: 0x3486AE69(881241705)
     PFS (Y/N): N, DH group: none
```

```
 inbound esp sas:
      spi: 0x96FAE6C7(2533025479)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto
map: MOJA_MAPA
        sa timing: remaining key lifetime (k/sec): (4270878/3185)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x3486AE69(881241705)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto
map: MOJA_MAPA
        sa timing: remaining key lifetime (k/sec): (4270877/3185)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
```

IPsec: Záverečné poznámky

- Ak tam máme na zariadení ACL musia byť pre Ipsec otvorené porty
  - ESP: UDP/50
  - ISAKMP: UDP/500

Konfig smerovačov - príprava

- Jednoduchá topo z predchádzajúceho príkladu
- Odstrániť tunnel int
  - `No int tu 0`
- Modifikuj NAT
  - Pobocka

```
No ip nat inside source list 1 int s 1/0 overload
Access-list 100 deny ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Access-list 100 permit ip 192.168.1.0 0.0.0.255 any
ip nat inside source list 100 int s 1/0 overload
```

  - HQ

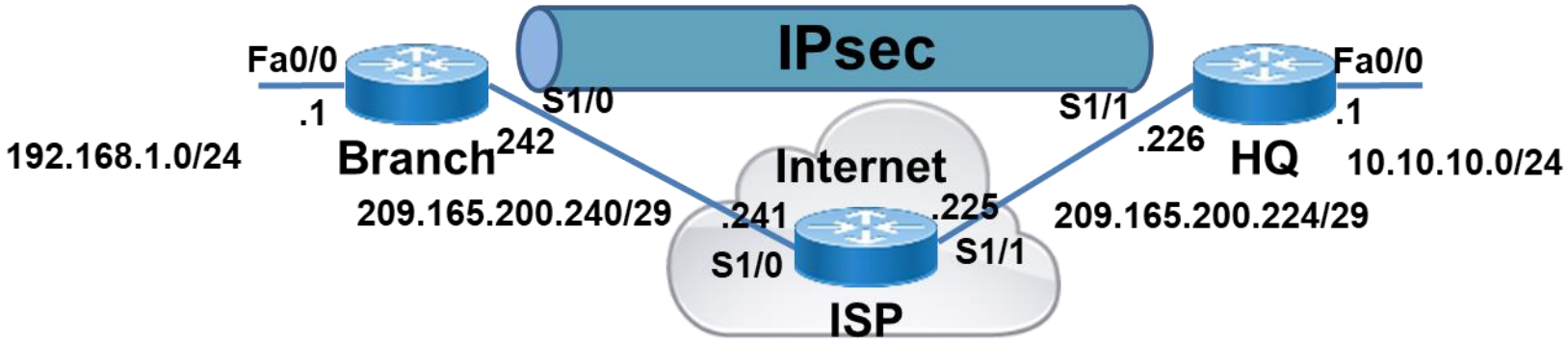
```
No ip nat inside source list 1 int s 1/1 overload
Access-list 100 deny ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
Access-list 100 permit ip 10.10.10.0 0.0.0.255 any
ip nat inside source list 100 int s 1/1 overload
```

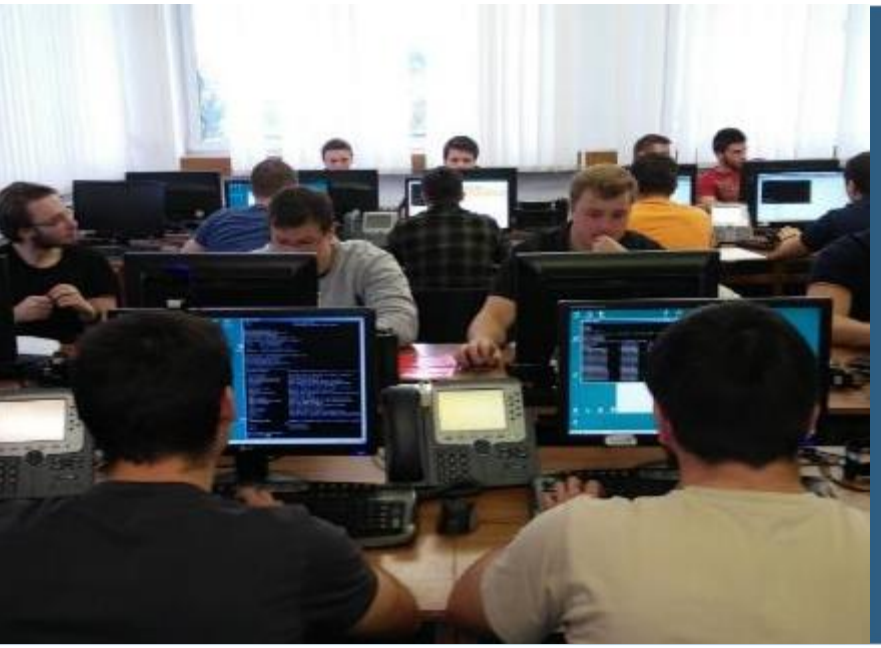
- Konfigurovať Ipsec na Pobocka a na HQ
- Pre overenie musí byť prevádzka z fa0/0 na fa0/0

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
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
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
```





Jednoduchá konfigurácia GRE over IPsec

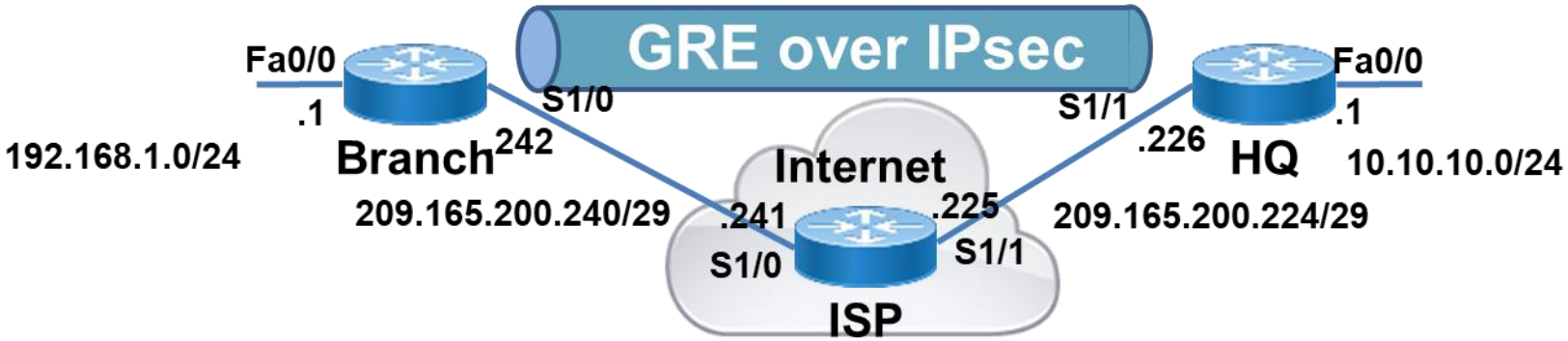
Jednoduchá konfigurácia GRE over IPsec

- 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
```

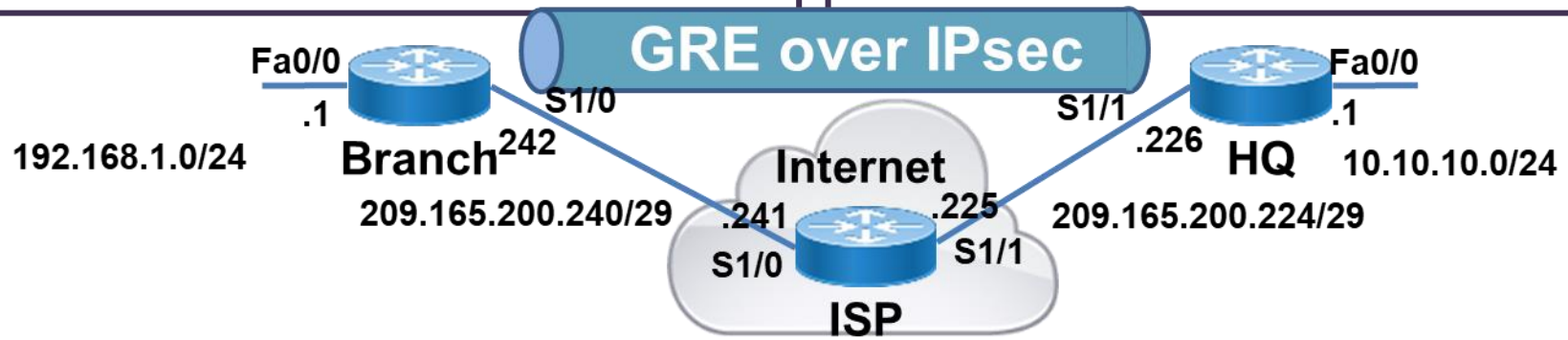
```
!HQ
ena
conf t
int tunnel 0
        tunnel source s 1/1
        tunnel destination 209.165.200.242
        tunnel mode gre ip
        ip add 172.16.1.2 255.255.255.0
router ospf 1
        network 10.10.10.0 0.0.0.255 area 0
        network 172.16.1.0 0.0.0.255 area 0
```



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
```



IPSec v PT

- Realizácia IPSec v P.T 7.3 pri použití 1841/19xx vyžaduje aktiváciu Security feature v IOS nasledovným postupom:
  - Zadaj show version a ak je security feature **disable**

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None
```

  - Zadaj príkaz v config mode

```
Router(config)#license boot module c1900 technology-package securityk9
```

  - a potom

```
ACCEPT? [yes/no]: yes
Router(config)# End
Router# Copy run startup
Router# reload
```

  - Po reštarte over, či je Security povolená

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

cisco Networking Academy

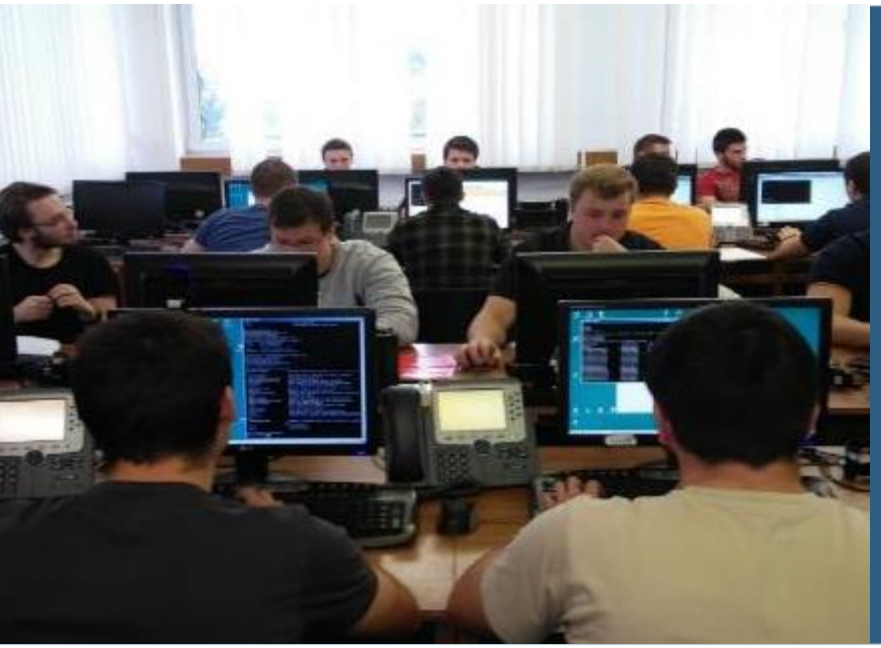
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť, nasledujú snímky len pre „sieťo-znalosti chtivých“ - CCNA 3 v7.0 nepokrýva

Ohodnoť našu CNA akadémiu na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

Vytvorené v rámci projektu KEGA 026TUKE-4/2021



Dynamic Multipoint VPN (DMVPN)

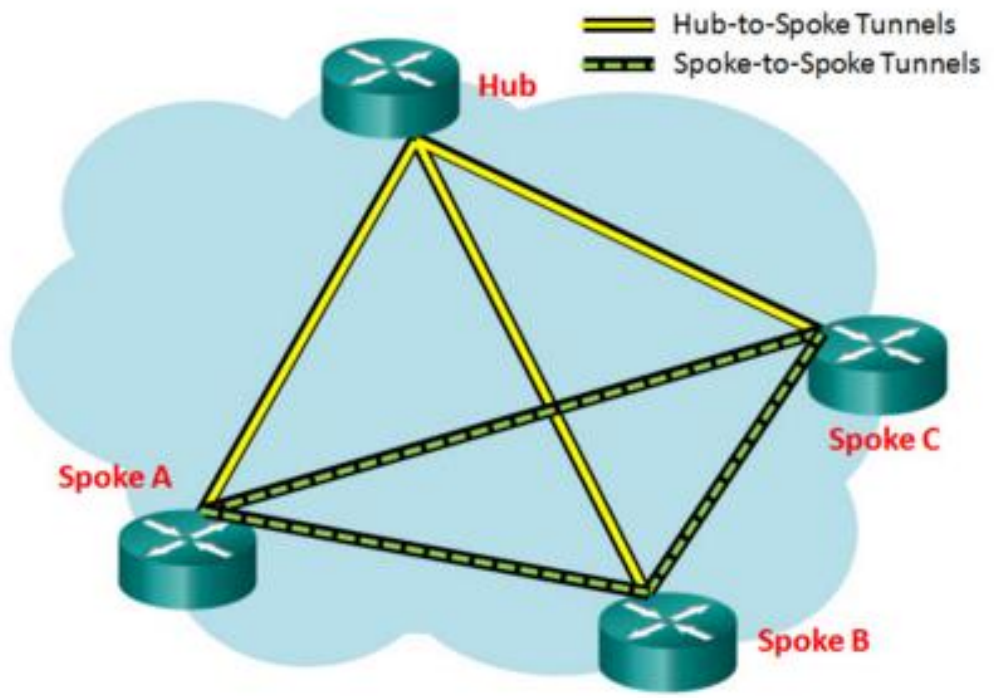
By MarMarc Khayat, CCIE #41288

Technical Manager, Cisco Networking Academy

- Trochu aktualizované

Why DMVPN?

- To have efficient spoke-to-spoke communication in a hub-and-spoke topology.
- Dynamic tunneling
  - No more static configuration of separated p-t-p tunnels is required
  - Spoke-spoke
  - Hub-spoke

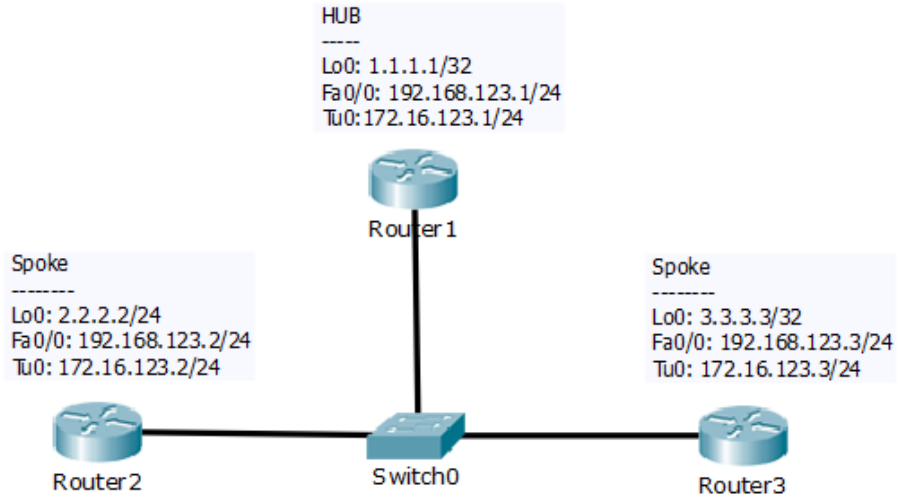


How are these tunnels built?

- Next Hop Resolution Protocol (NHRP)
- Multipoint Generic Routing Encapsulation (mGRE) tunnels
- IP Security (IPsec) encryption

Config Tasks

1. NHRP: set the hub as the server, allow multicast to flow to it.
2. mGRE tunnel config.
3. Enable IPSec encryption on the tunnels.



Príklad konfigurácie Hub and Spoke

```
!  Spoke config
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key MYKEY address 0.0.0.0
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
!
crypto ipsec profile MGRE
 set security-association lifetime seconds 86400
 set transform-set MYSET
!
interface Tunnel0
 ip address 172.16.123.1 255.255.255.0
 no ip split-horizon eigrp 10
 ip nhrp authentication CISCO
 ip nhrp map multicast dynamic
! Identifiy DMVPN net
! Have to be same on hub and spookes
 ip nhrp network-id 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile MGRE
! No explicit tunnel destination required
!
router eigrp 10
 network 1.0.0.0
 network 172.16.0.0
```

```
! Hub konfig
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key MYKEY address 0.0.0.0
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
!
crypto ipsec profile MGRE
 set security-association lifetime seconds 86400
 set transform-set MYSET
!
interface Tunnel0
 ip address 172.16.123.2 255.255.255.0
 ip nhrp authentication CISCO
 ip nhrp map multicast dynamic
! the HUB tunnel address
 ip nhrp nhs 172.16.123.1

! Map tunnel address of Hub to its real and globally
! reachable IP address
 ip nhrp map 172.16.123.1 192.168.123.1
 ip nhrp map multicast 192.168.123.1
 ip nhrp network-id 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile MGRE
!
router eigrp 10
 network 2.0.0.0
 network 172.16.0.0
```

Verification

```
Show dmvpn
! Not from the topology above
! Just an example

R1# show dmvpn
...

Tunnel0, Type:Hub, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
 1     172.16.25.2     192.168.0.2    UP 00:02:28 D
 1     172.16.35.2     192.168.0.3    UP 00:02:26 D
 1     172.16.45.2     192.168.0.4    UP 00:02:25 D
```

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

CISCO Networking Academy

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Vytvorené v rámci projektu KEGA 026TUKE-4/2021