Stretnutie 7: Konektivita pobočkových sietí

Branch Office Challenges

- Common requirements that a branch network design needs to address include connectivity, security, availability, voice, and application optimization.
- The challenges when addressing these requirements include:
  - Bandwidth and network requirements
  - Consolidated data centers
  - Mobility
  - Disparate networks
  - Management costs

Dizajn pobočiek – „*Thin Branch*“

- „*Thin branch*” je aktuálny trend v dizajne pobočiek
  - Vďaka konsolidácii centier a novým zariadeniam pre pobočky
- Služby kedysi poskytované na viac serveroch, teraz môžu vykonávať nové modely Cisco ISR zariadení:
  - Voice
  - Application firewall
  - Intrusion prevention
  - Virtual private network
  - WAN optimization
  - Wireless
  - WAN backup
- Pritom prístup nemá vplyv na koncových používateľov

Výhody ISR

- ISRs reduce costs by deploying a single, resilient system for fast, secure delivery of multiple mission-critical business services, including:
  - Data
  - Voice
  - Security
  - Wireless

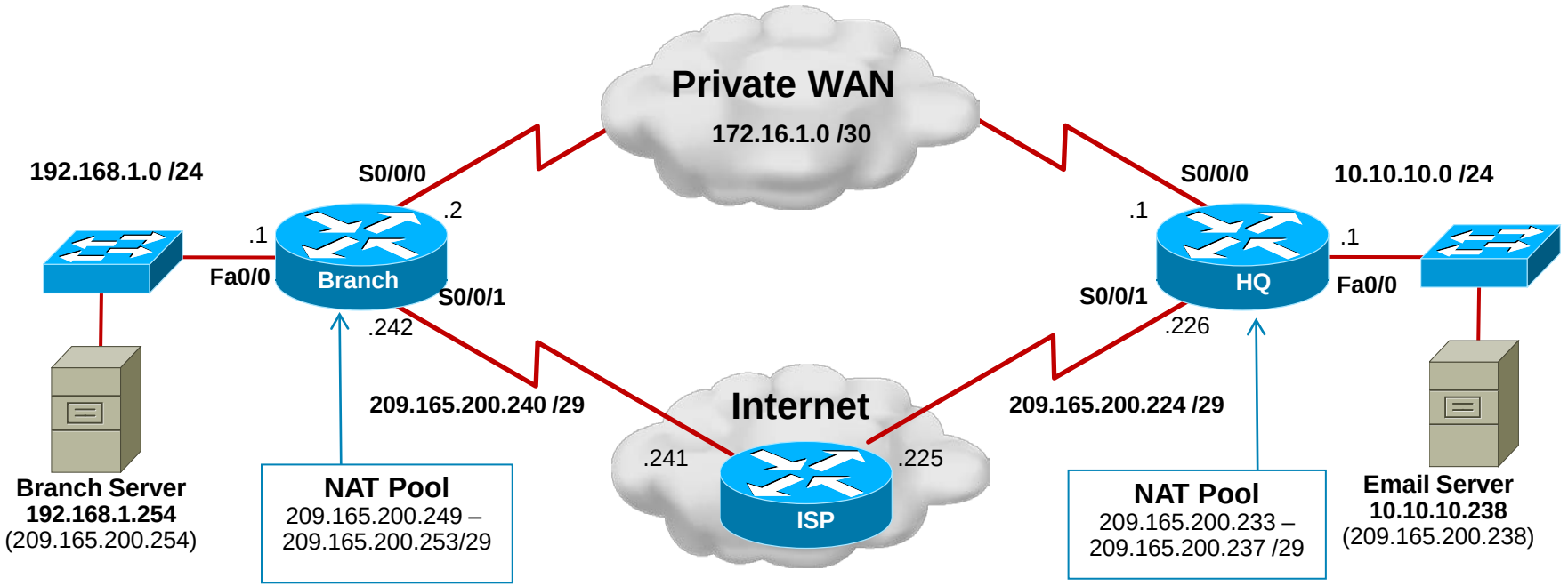
Cisco 2800 Series Integrated Services Routers

Implementačný plán

1. Vyrieš a umiestni broadband konektivitu
2. Konfiguruj statické smerovanie
   - Floating static routes (backup route)
3. Verifikuj a zdokumentuj činnosť ďalších služieb
   - NAT/PAT (Dynamic and static), DHCP, ACL, HSRP (if exists redundacy)
4. Implementuj a vylaď činnosť IPsec VPN
5. Konfiguruj GRE tunely

- **Note:**
  - The implementation in this chapter is not exhaustive and other solutions could also be applied.
  - The following is to serve as a guide and as just one possible solution to routing to a branch site.

Príklad pobočkovej siete



Tunelovanie

Čo je to tunelovanie?

- 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

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

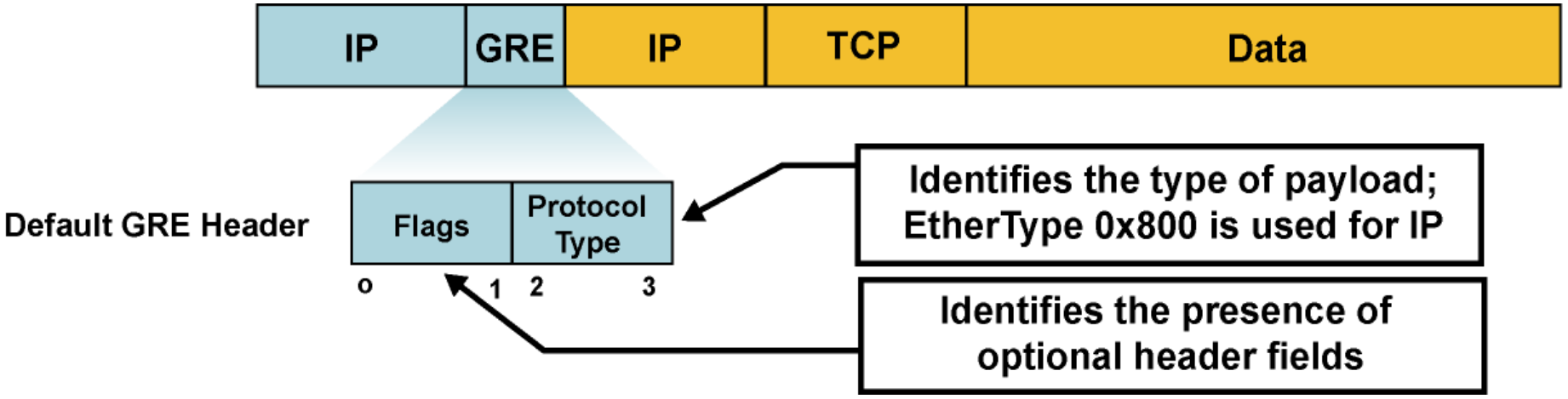
Tunelovacie protokoly

- 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

Generic Routing Encapsulation – GRE

- GRE je pomocný tunelovací protokol na 3. vrstve
  - Podporuje rôzne typy tunelovaných paketov
  - Vytvára virtuálny point-to-point prepoj medzi dvojicou smerovačov
  - Vkladá sa do IP paketov
  - Umožňuje prenášať aj multicastový traffic (NBMA povaha)
- Autorom protokolu je spoločnosť Cisco, no protokol je otvorený a dokumentovaný v RFC 2784

GRE hlavička



- GRE je bezstavový, bez riadenia toku dát
- GRE neposkytuje zabezpečenie
  - žiadna dôvernosť, autentifikácia alebo kontrola integrity
- Overhead GRE tunelov je 24B
  - 20B na novú IP hlavičku a 4B na GRE hlavičku

GRE hlavička – príznaky

- GRE príznaky sú uložené v prvých dvoch bajtoch:
  - Checksum Present (bit 0): Indikuje prítomnosť voliteľnej GRE hlavičky s kontrolnou sumou
  - Key Present (bit 2): Indikuje prítomnosť voliteľnej GRE hlavičky s tzv. kľúčom
  - Sequence Number Present (bit 3): Indikuje prítomnosť voliteľnej GRE hlavičky so sekvenčným číslom
  - Version Number (bits 13–15): Číslo verzie. Verzia 0 zodpovedá základnej GRE implementácii. PPTP protokol používa verziu 1.
  - Protocol Type: Typ prenášaného protokolu. Spravidla sa tu nachádza identická hodnota ako v poli EtherType v rámci Ethernet.

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 adresy odosielateľa a 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
  - Odporúča sa zvýšiť ho na realistickú hodnotu

Vytvorenie Tunnel rozhrania

```
Router(config)#
interface tunnel number
```

- Príkaz vytvorí virtuálne rozhranie tunela
- Keď je rozhranie vytvorené, vykoná sa konfigurácia jeho parametrov ako
  - IP adresa
  - Tunnel source
  - Tunnel destination
  - Tunnel mode (typ tunela)

Identifikácia zdroja GRE tunela

- Identita zdroja (počiatku) pre GRE tunel

```
Router(config-if)#
tunnel source {ip-address | ipv6-address | interface-type
  interface-number}
```

Parameter	Popis
ip-address	IP adresa, ktorá sa použije ako adresa odosielateľa (zdrojová adresa) pre pakety GRE tunela.
ipv6-address	IPv6 adresa, ktorá sa použije ako adresa odosielateľa (zdrojová adresa) pre pakety GRE tunela.
interface-type number	Typ a číslo rozhrania, ktoré sa použije ako zdrojové pre tunel (jeho IP).

Ukončenia GRE Tunela

- Identifikuje koniec tunela.

```
Router(config-if)#
tunnel destination {ip-address | ipv6-address | host-
  name}
```

Parameter	Description
ip-address	IP adresa, ktorá sa použije ako cieľová adresa pre pakety GRE tunela
ipv6-address	IPv6 adresa, ktorá sa použije ako cieľová adresa pre pakety GRE tunela
host-name	Meno cieľového hosta.

Nastavenie typu tunela

- Nastaví enkapsuláciu tunela

```
Router(config-if)#
tunnel mode {aurp | cayman | dvmrp | eon | gre ip | gre
 multipoint | gre ipv6 | ipip [decapsulate-any] | ipsec
 ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp}
```

- Voliteľný príkaz nakoľko default režim pre GRE tunely je **`tunnel mode gre ip`**

Príklad konfigurácie GRE tunela


```
hostname Bratislava
!
interface Serial0/0
 ip address 192.3.4.5 255.255.255.0
 no shut
!
interface Tunnel0
 bandwidth 1000
 tunnel source s0/0
 tunnel destination 223.1.2.3
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 10.0.0.1 255.255.255.0
!
router ospf 1
 network 10.0.0.1 0.0.0.0 area 0
```

```
hostname Kosice
!
interface Serial0/0
 ip address 223.1.2.3 255.255.255.0
 no shut
!
interface Tunnel7
 bandwidth 1000
 tunnel source s0/0
 tunnel destination 192.3.4.5
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 10.0.0.2 255.255.255.0
!
router ospf 1
 network 10.0.0.2 0.0.0.0 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

```
Branch# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.1/24
  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 192.3.4.5, 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 8000 (kbps)
  Tunnel receive bandwidth 8000 (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>
```

Rýchlokurz IPsec

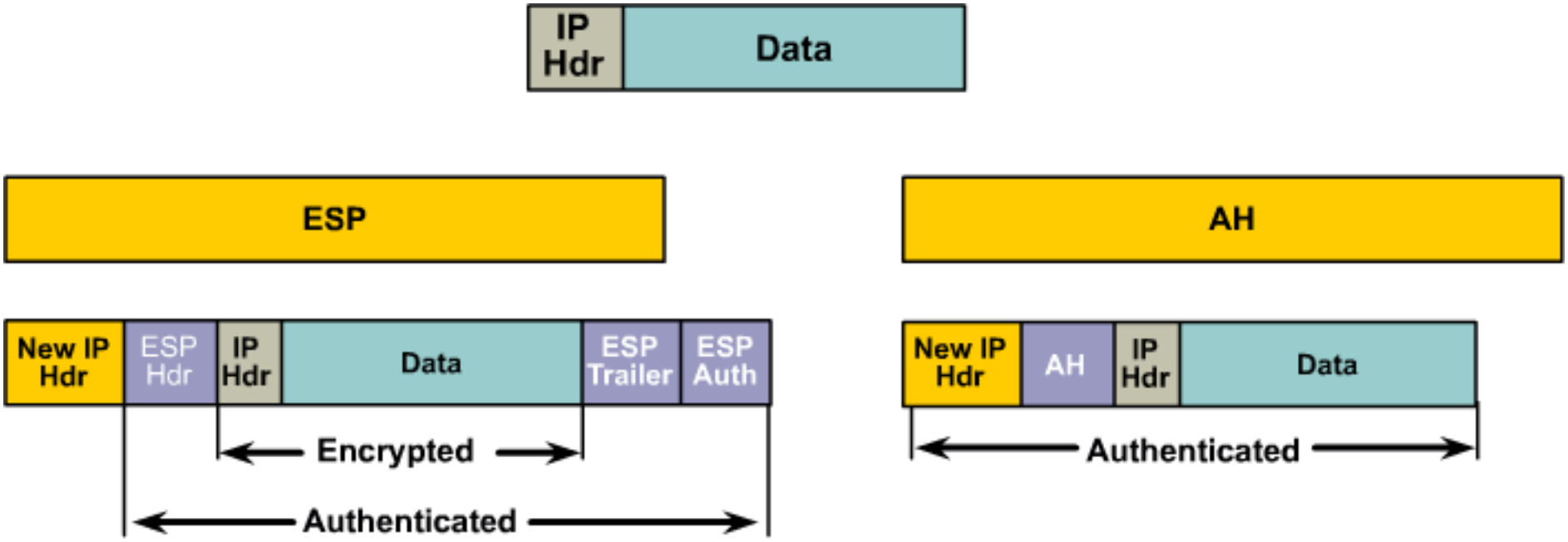
IP Security

- IPsec je séria IETF štandardov popisujúcich spôsob bezpečného prenosu IP paketov
- IPsec poskytuje
  - Utajenie údajov
  - Integritu dát
  - Autentifikáciu odosielateľa
  - Anti-replay (ochrana proti zopakovaniu paketu)
- IPsec používa tri hlavné podprotokoly
  - Internet Key Exchange (IKE) pre bezpečnú výmenu kľúčov a podporu NAT Traversal (UDP porty 500 a 4500)
  - Authentication Header (AH) pre autentifikáciu odosielateľa, zabezpečenie integrity a voliteľne anti-replay
  - Encapsulating Security Payload (ESP) pre utajenie obsahu, autentifikáciu, zabezpečenie integrity a voliteľne anti-replay

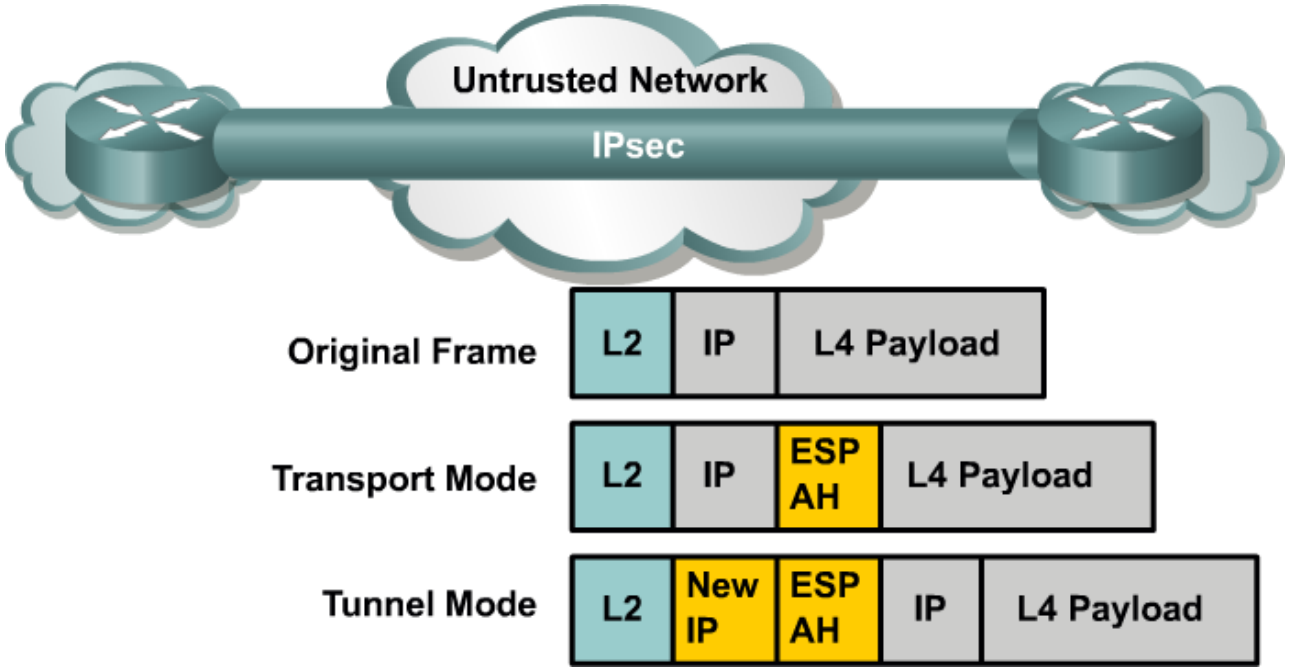
AH a ESP v IPsec

- AH chráni kompletný obsah paketu vrátane nemenných častí IP hlavičky
  - Nezabezpečuje však šifrovanie
  - Nemá rada NAT (prepisuje IP adresy v hlavičke)
- ESP chráni payload paketu šifrovaním
  - Nezabezpečuje hlavičku paketu
  - Autenticitu chráni dodatočne
- AH je v súčasnosti používaný zriedkavo, ESP veľmi často (firewally ASA AH vôbec nepodporujú)
- AH a ESP možno použiť súčasne

AH a ESP v IPsec



Režimy práce IPsec



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

Security Association v IPsec

- Security Association v IPsec je súhrn dohodnutých parametrov medzi IPsec susedmi
- SA obsahuje prevádzkové informácie
  - Akým spôsobom sa má overiť autenticita susedov
  - V akom režime má IPsec pracovať
  - Akým algoritmom a akým kľúčom sa majú dáta šifrovať
  - Akým algoritmom sa má overiť integrita prenášaných dát
  - Ako sa majú kľúče obmieňať
- O vytváranie a spravovanie SA medzi susedmi sa stará protokol ISAKMP (IKE)

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

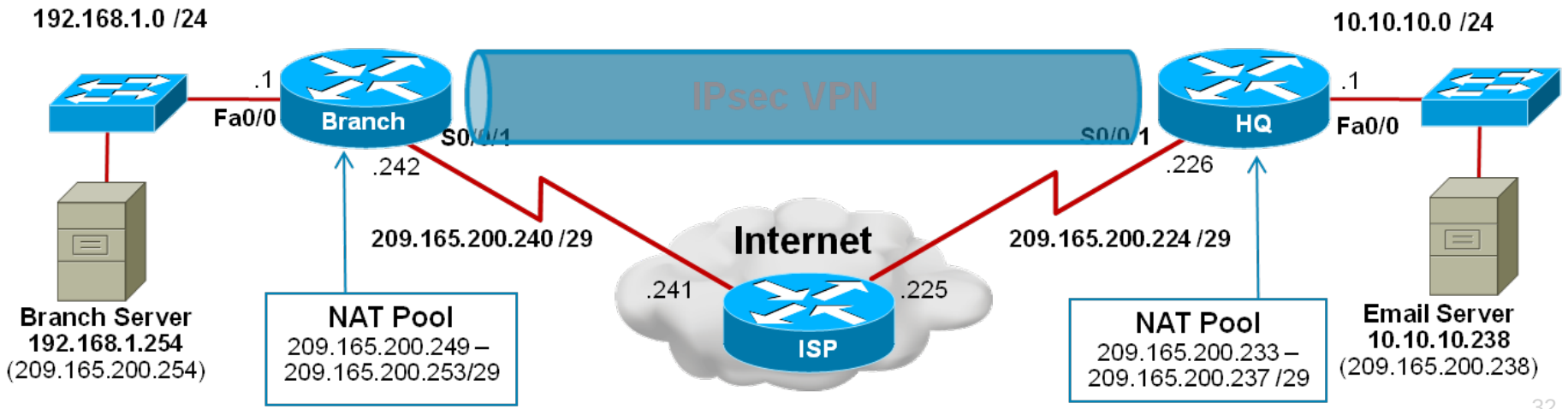
- IKE fáza 1 má tri kroky:
  - Dohodnutie ISAKMP politík
  - Výmenu kľúčov pomocou Diffie-Hellmanovho algoritmu
  - Overenie totožnosti susedov
- Dohodnutie ISAKMP politík
  - Aký šifrovací algoritmus? (confident.)
  - Aký hashovací algoritmus? (integr.)
  - Aká Diffie-Hellmanova grupa?
  - Aký spôsob overenia totožnosti? (auth.)
- Overenie totožnosti
  - Podľa spôsobu dohodnutého v prvom kroku
- IKE fáza 1 si vytvára zabezpečený kanál pre overenie totožnosti IPsec susedov a prípadne používateľov
  - Nedohaduje samotné vlastnosti pre činnosť IPsec
  - Tie sa dohodnú až vo fáze 2 pomocou tohto zabezpečeného kanála

Vytvorenie spojenia: IKE fáza 2

- IKE fáza 2 zodpovedá za dojednanie spôsobu použitia IPsec medzi susedmi
  - Aký protokol – AH, ESP, AH+ESP?
  - Aký režim – tunelový alebo transportný?
  - Aký šifrovací algoritmus?
  - Aký hashovací mechanizmus?
  - Aké šifrovacie kľúče?
  - Aká životnosť dohodnutých informácií?
- Prvé štyri vlastnosti sa nazývajú aj *transformačná sada*

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 kryptovaciu mapu a ACL, ktoré popisujú, čo sa má zabezpečiť pomocou IPsec a ako
  - Aplikovať kryptovaciu mapu na výstupné rozhranie
- Poznámka:
  - Internet je v príklade použitý len ako záložne spojenie pre private WAN



Vytvorenie ISAKMP politiky pre fázu 1

- Príklad vytvorenia ISAKMP politiky
- Šifrovanie: AES
  - Alternatívy: DES, 3DES
- Hash: MD5
  - Alternatíva: SHA
- Autentifikácia: zdieľaným heslom
  - Alternatívy: na báze RSA
- DH grupa: 2 (1024b)
  - Alternatívy: 1 (768b), 5 (1536b)
- Životnosť: 3600s
- Definované autentifikačné heslo cisco123 pre suseda **209.165.200.226**

```
crypto isakmp policy 1
  encryption aes
  hash md5
  authentication pre-share
  group 2
  lifetime 3600
  exit

crypto isakmp key 0 cisco123 address
  209.165.200.226
```

Vytvorenie transformačnej sady pre fázu 2 - detaily IPSec-u

- Transformačná sada stanovuje
  - Použitie AH alebo ESP
    - ESP
  - Šifrovací algoritmus a dĺžku kľúča
    - SHA
  - Hashovací algoritmus
    - HMAC
  - Tunelový alebo transportný režim

```
Branch(config)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
```

- Transformačné sady sú identifikované ľubovoľnými menami

```
crypto ipsec transform-set AH-ESP-3DES-SHA ah-sha-hmac esp-3des
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
```

Vytvorenie krypto mapy - špecifikácia VPN tunela

- Krypto mapa dáva do súvisu
  - IPsec suseda
  - ACL pre šifrovanú prevádzku medzi týmito susedmi
  - Použitú transformačnú sadu
  - Spôsob výmeny kľúčov medzi susedmi (ručne alebo ISAKMP)
  - Životnosť dohodnutých informácií, najmä kľúčov
- Krypto mapa musí obsahovať minimálne
  - Definovanie suseda
  - Odkaz na ACL
  - Odkaz na transformačnú sadu
- ACL definuje, aké pakety majú byť touto krypto mapou šifrované
  - Spravidla položky v tvare „z naších sietí do susedových sietí“
  - Vyhýbať sa položkám typu any!

Vytvorenie krypto mapy a aplikácia na rozhraní

- Príklad:
  - Blok 1: Minimálna konfigurácia, jediná transformačná sada

```
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)# crypto map HQ-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Branch(config-crypto-map)# set transform-set HQ-VPN
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 HQ-MAP
Branch(config-if)# ^Z
```

Kompletná konfigurácia Branch Router IPsec VPN

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 2
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.226
Branch(config)#
Branch(config)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
Branch(cfg-crypto-trans)# exit
Branch(config)#
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 HQ-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Branch(config-crypto-map)# set transform-set HQ-VPN
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 HQ-MAP
Branch(config-if)# ^Z
Branch#
```

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

IPsec: Záverečné poznámky

- Pre NAT-T musia byť na firewalloch otvorené porty
  - UDP/500
  - UDP/4500
- Vzhľadom na pomerne vysokú technickú náročnosť IPsec sa pre mobilných klientov odporúča nová technológia SSLVPN, ktorá má nižšie technické nároky

Overenie konfigurácie a činnosti IPsec

Command	Description
show crypto map	Displays the specifics contained in a crypto map configuration.
show crypto session	Displays the status information of the active crypto sessions.
show crypto ipsec sa	Displays the settings used by current SAs.
debug crypto ipsec	View real time IPsec events.
Clear crypto isakmp	
Clear crypto sa	

Príkaz show ip crypto ...

```
Branch# show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: HQ-MAP, 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: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0

<output omitted>
```

```
Branch# show crypto session
Crypto session current status

Interface: Serial0/0/1
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500
  IKE 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

Branch#
```

Príkaz show ip crypto ...

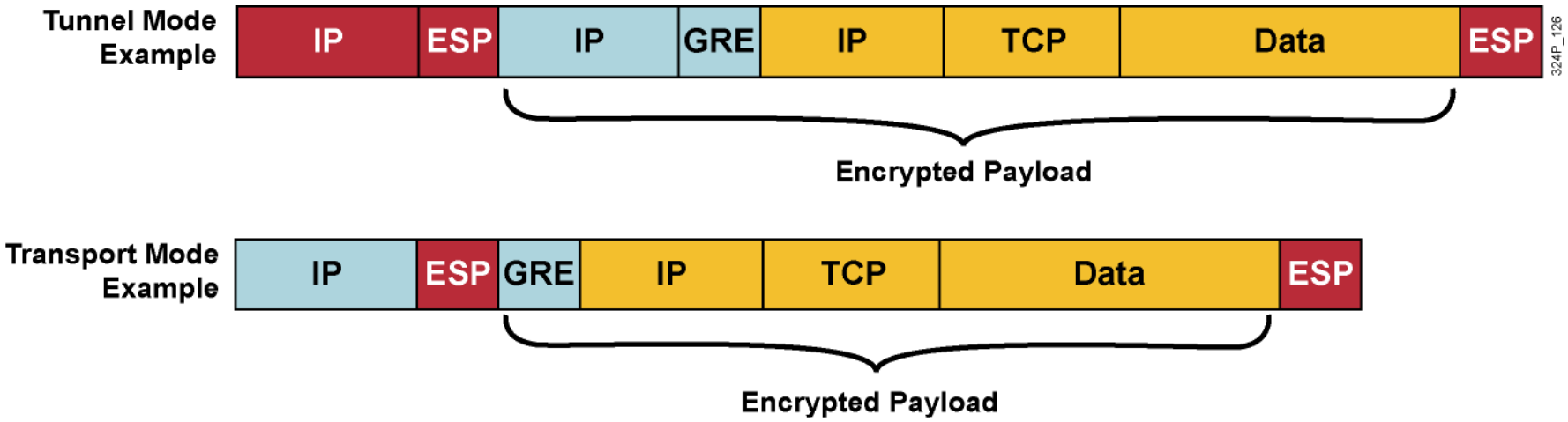
```
Branch# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Serial0/0/1
Uptime: 00:28:17
Session status: UP-ACTIVE
Peer: 209.165.200.226 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 209.165.200.226
     Desc: (none)
IKE SA: local 209.165.200.242/500 remote 209.165.200.226/500 Active
          Capabilities:(none) connid:1005 lifetime:23:31:42
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
     Inbound: #pkts dec'ed 4 drop 0 life (BPSKBPSec) 4444197/1902
     Outbound: #pkts enc'ed 4 drop 1 life (BPSKBPSec) 4444197/1902
```

Zabezpečené GRE tunely

IPsec + GRE?

- IPsec je skvelý pre bezpečný prenos dát, ale...
  - Podporuje iba IP protokol
  - Staršie IOSy nepodporujú IPsec+multicasty
  - Až donedávna jediným spôsobom konfigurácie IPsec bola kryptomapa na výstupnom rozhraní
    - Nebolo možné vytvoriť Tunnel interface, ktorý by reprezentoval vytvorený IPsec tunel
    - Nebolo možné nad týmto tunelom aktivovať smerovací protokol
- GRE je zasa skvelý tunelovací protokol, ibaže jeho bezpečnostné vlastnosti sú mizerné
- Riešenie: zabezpečiť GRE tunely pomocou IPsec

IPsec + GRE!



- GRE je možné využiť s IPsec v transportnom či tunelovom režime
  - Využitie transportného režimu môže v tomto prípade byť výhodné
  - Ušetrí sa 20B na jednej IP hlavičke na každom pakete
- Poradie enkapsulácie:
  - Prenášaný protokol → GRE → IPsec → IP

Konfigurácia IPsec+GRE

- Dva spôsoby
  - Pomocou kryptomapy (funguje na všetkých IOSoch)
  - Priamo na Tunnel rozhraní (na novších IOSoch) s využitím tzv. IPsec profilov bez kryptomapy
- Konfigurácia pomocou kryptomapy je taká istá ako pri obyčajnom 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**
  - IOSy staršie ako 12.2(13)T musia mať tú istú kryptomapu umiestnenú aj na rozhraní Tunnel, aj na výstupnom rozhraní (Doc ID 14125)
  - Všetky ostatné kroky konfigurácie IPsec sú tradičné

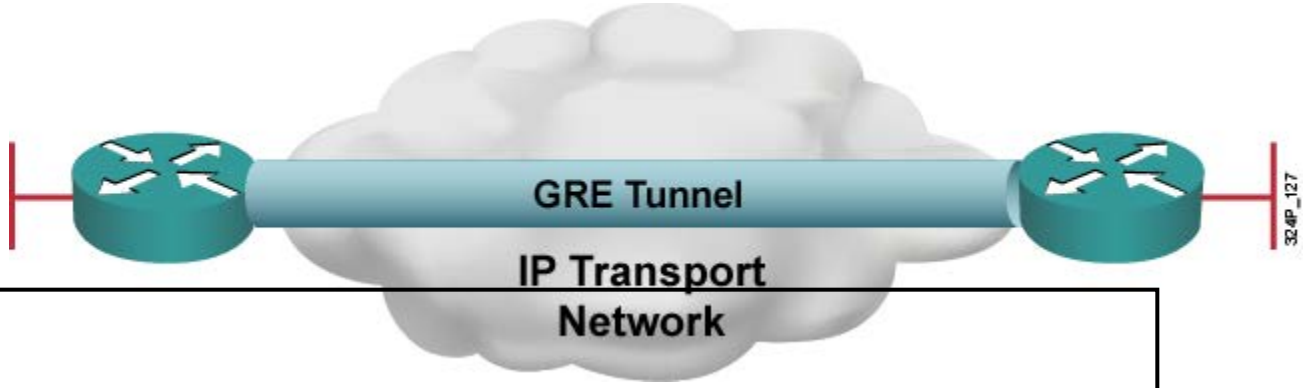
Príklad konfigurácie GRE+IPsec tunela


```
hostname Bratislava
!
crypto map Kryptuj 1 ipsec-isakmp
 match address 150
 set transform-set SilnaT
 set peer 223.1.2.3
!
interface Serial0/0
 ip address 192.3.4.5 255.255.255.0
 crypto map Kryptuj
!
interface Tunnel0
 tunnel source s0/0
 tunnel destination 223.1.2.3
 ip address 10.0.0.1 255.255.255.0
 crypto map Kryptuj ! Nie je potrebné v 12.2(13)T a novších IOSoch
!
access-list 150 permit gre host 192.3.4.5 host 223.1.2.3
```

Konfigurácia GRE+IPsec cez IPsec profily

- Novšie IOSy podporujú o niečo prehľadnejší spôsob
  - Tzv. IPsec profily
  - Príkaz **tunnel protection** na rozhraní Tunnel
- IPsec profil je zjednodušená forma kryptomapy
  - Nemá príkaz **`match address`** pre ACL
  - Nemá príkaz **`set peer`**
- Na rozhraní Tunnel existuje príkaz **`tunnel protection`**
  - Týmto príkazom sa tunel odvoláva na IPsec profil
- Pri tomto štýle konfigurácie zabezpečených GRE tunelov nie je potrebné vytvárať kryptomapu a ACL
  - Všetky ostatné potrebné IPsec kroky musia byť zachované (ISAKMP politiky, zdieľané heslá, transformačné sady)
  - Pozor – GRE Keepalives **nie sú podporované** s IPsec profilmi (Document ID 64565)

Príklad konfigurácie GRE+IPsec tunela




```
hostname Bratislava
!
crypto ipsec profile Kryptuj
 set transform-set SilnaT
!
interface Serial0/0
 ip address 192.3.4.5 255.255.255.0
!
interface Tunnel0
 tunnel source s0/0
 tunnel destination 223.1.2.3
 tunnel protection ipsec profile Kryptuj
 ip address 10.0.0.1 255.255.255.0
!
```


CISCO