



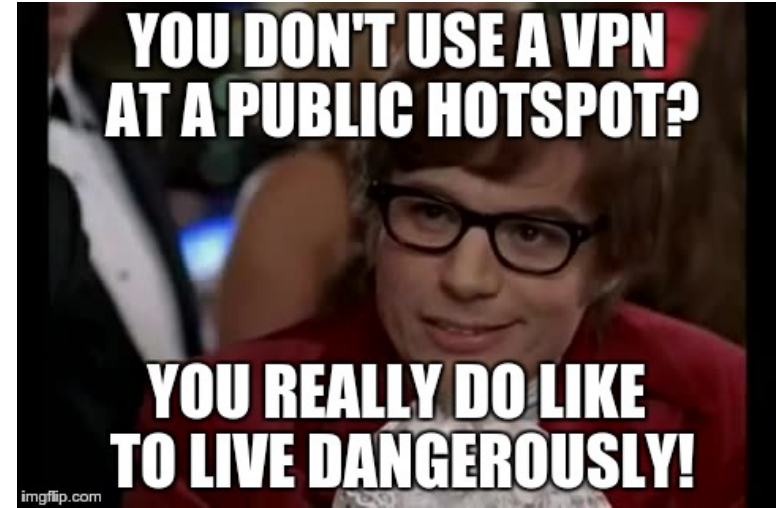
VIRTUAL PRIVATE NETWORKS (VPN)

CUPRINS

- ❑ Motivare
- ❑ Ce este un VPN
- ❑ Funcțiile VPN
- ❑ Tunelare
- ❑ Tipuri de VPN-uri
- ❑ Site-to-Site vs Remote-access
- ❑ VPN GRE
- ❑ Configurare GRE
- ❑ Depanare GRE
- ❑ Anexe

MOTIVARE

Este necesară utilizarea
unei soluții de tip VPN?



Ce este un VPN?

- Un VPN este o rețea privată punct la punct peste o rețea publică (ex: Internet)
- Un VPN nu garantează neapărat confidențialitatea traficului
- Pot fi folosite metode criptografice
- Un VPN devine un tunel prin care sunt transportate date criptate
- Poate asigura și autentificarea sursei datelor



Beneficiile rețelelor virtuale - VPN

- **Cost redus**

VPN-urile nu au nevoie de legături fizice dedicate și pot funcționa fără hardware specializat

- **Securitate crescută**

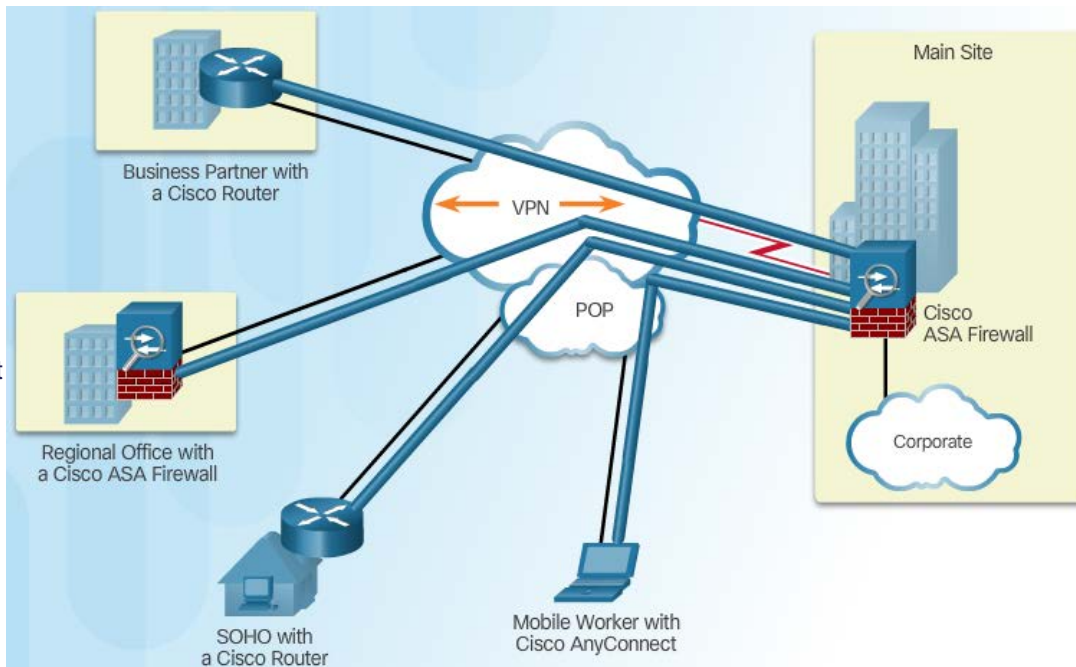
VPN-urile folosesc protocoale sigure de criptare și autentificare

- **Scalabilitate**

VPN-urile folosesc infrastructura existentă în Internet. Adăugarea de utilizatori și rețele este ușoară

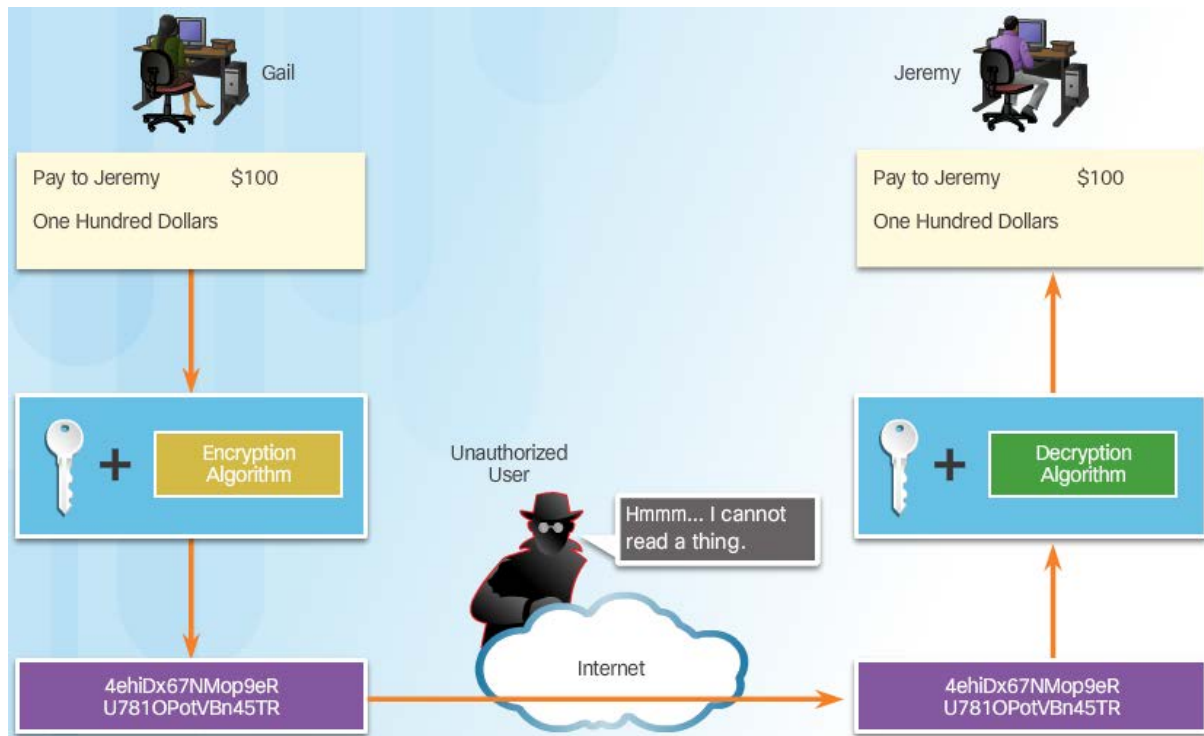
- **Compatibilitate**

VPN-urile pot traversa medii și rețele diferite



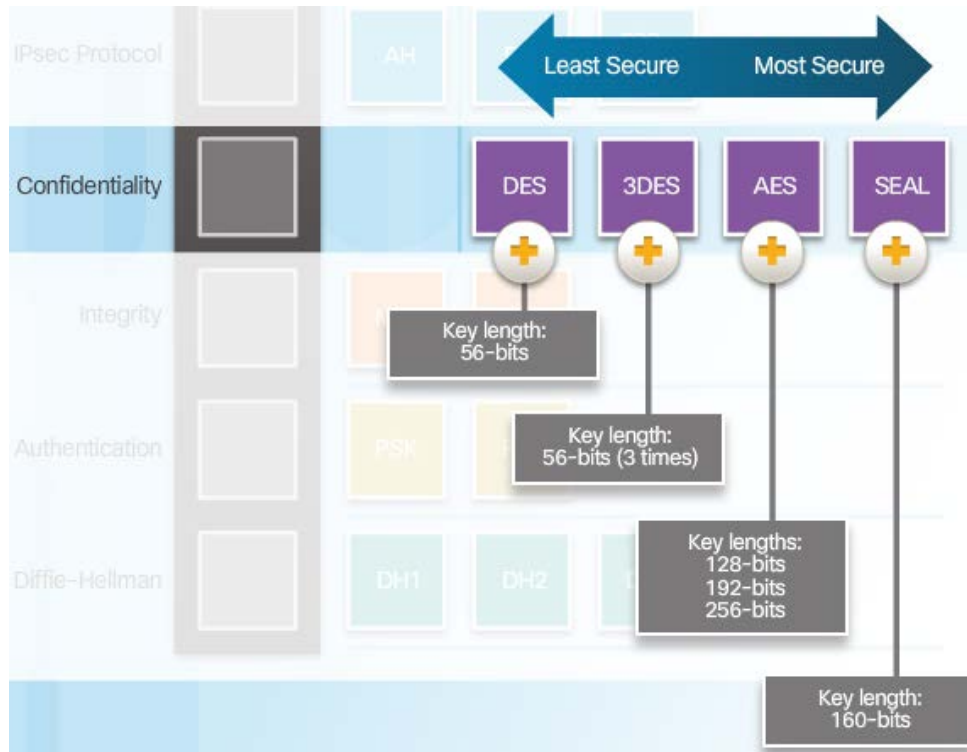
Funcțiile VPN: Confidențialitate

Asigurată cu ajutorul criptării:



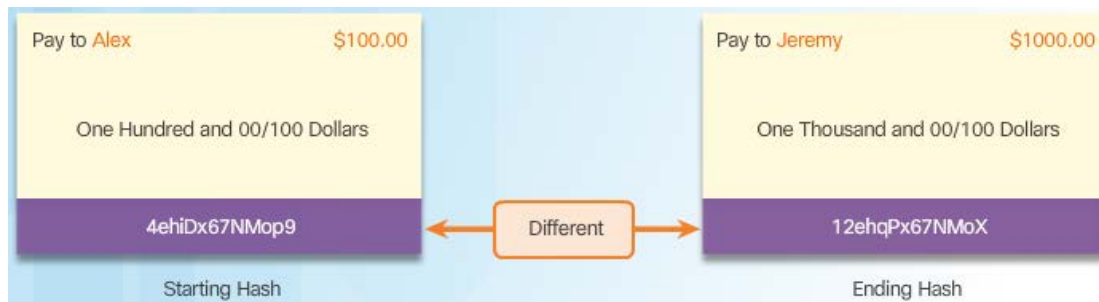
Funcțiile VPN: Confidențialitate

Criptosisteme utilizate:

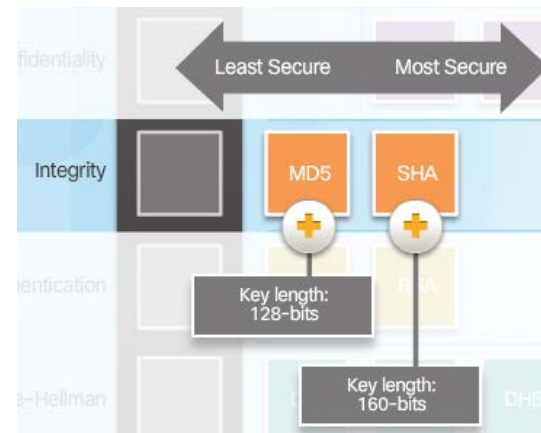


Funcțiile VPN: Integritate

Algoritmi utilizați:

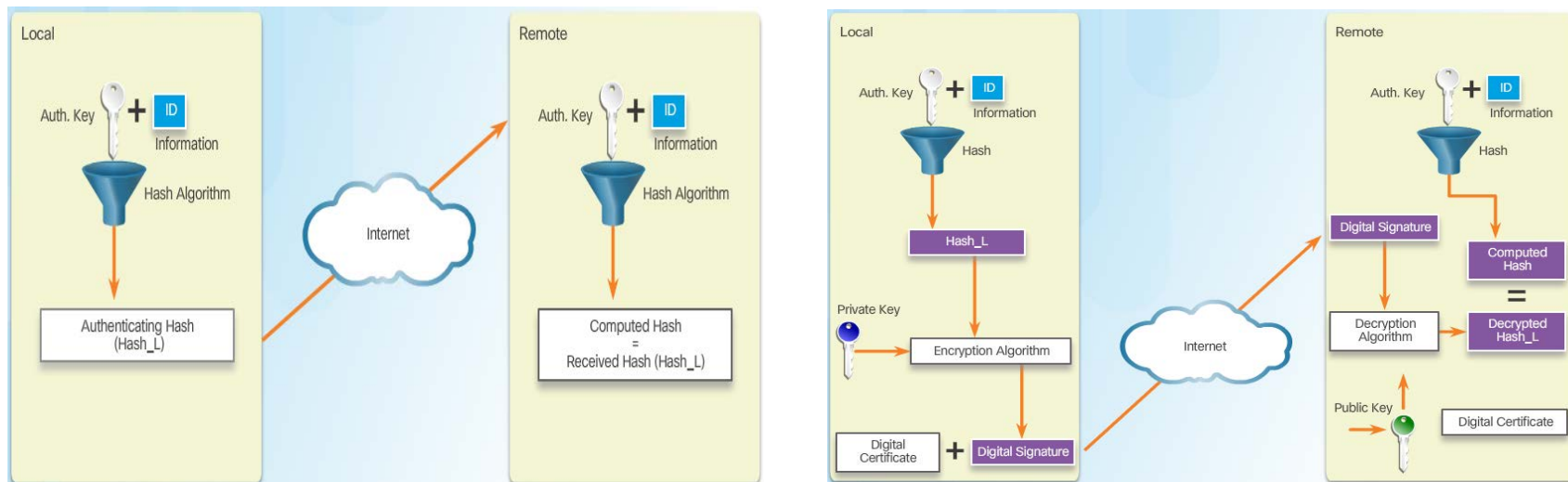
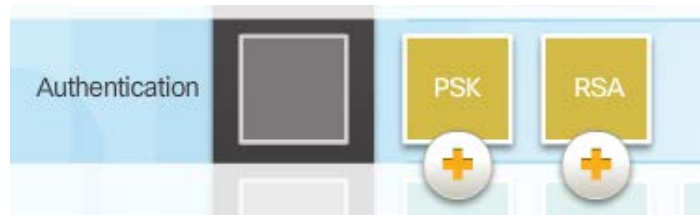


Securitatea algoritmilor



Funcțiile VPN: Autentificare

Algoritmi utilizați:



Tunelare: încapsulare

□ Orice tehnologie de VPN se bazează pe tunelare

Tunelarea presupune încapsularea cu încă un antet la nivelul la care se contruiește tunelul

Exemplu: tunelul *IP/IP*

- *Folosit când rețeaua sursă sau destinație nu este cunoscută în tabela de rutare a unui ruter intermediar*

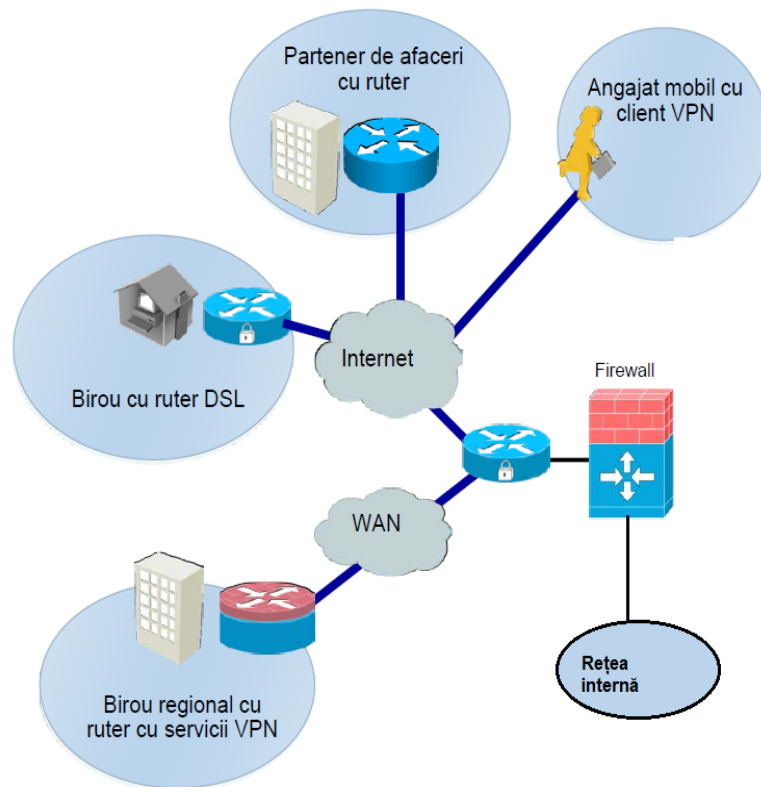


- *Antetul IP original nu este cunoscut rutelor intermediare!*

Clasificarea soluțiilor VPN

Virtual: Informația într-o rețea privată este transportată peste o rețea publică

Privat: Traficul poate fi criptat pentru a asigura confidențialitate

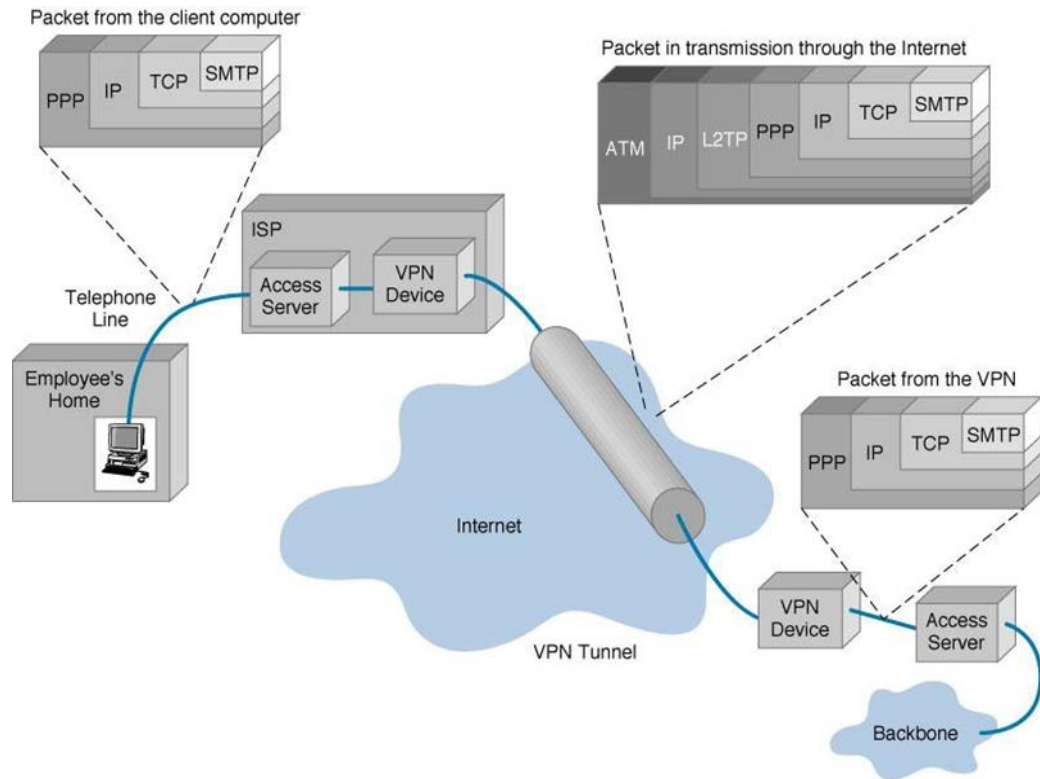


Clasificarea soluțiilor VPN

- Un VPN este un tunel care interconectează două puncte peste o rețea publică
- Pentru a transporta datele la destinație, un antet este adăugat la toate pachetele ce trec prin tunel (oferă toate beneficiile unui VPN)
- Antetul conține și informațiile de adresare ce permit pachetelor să ajungă la destinație
- VPN-urile pot fi implementate la nivelurile 2, 3 și 5
- Este prezentat un model de nivel 3

VPN – nivel 3

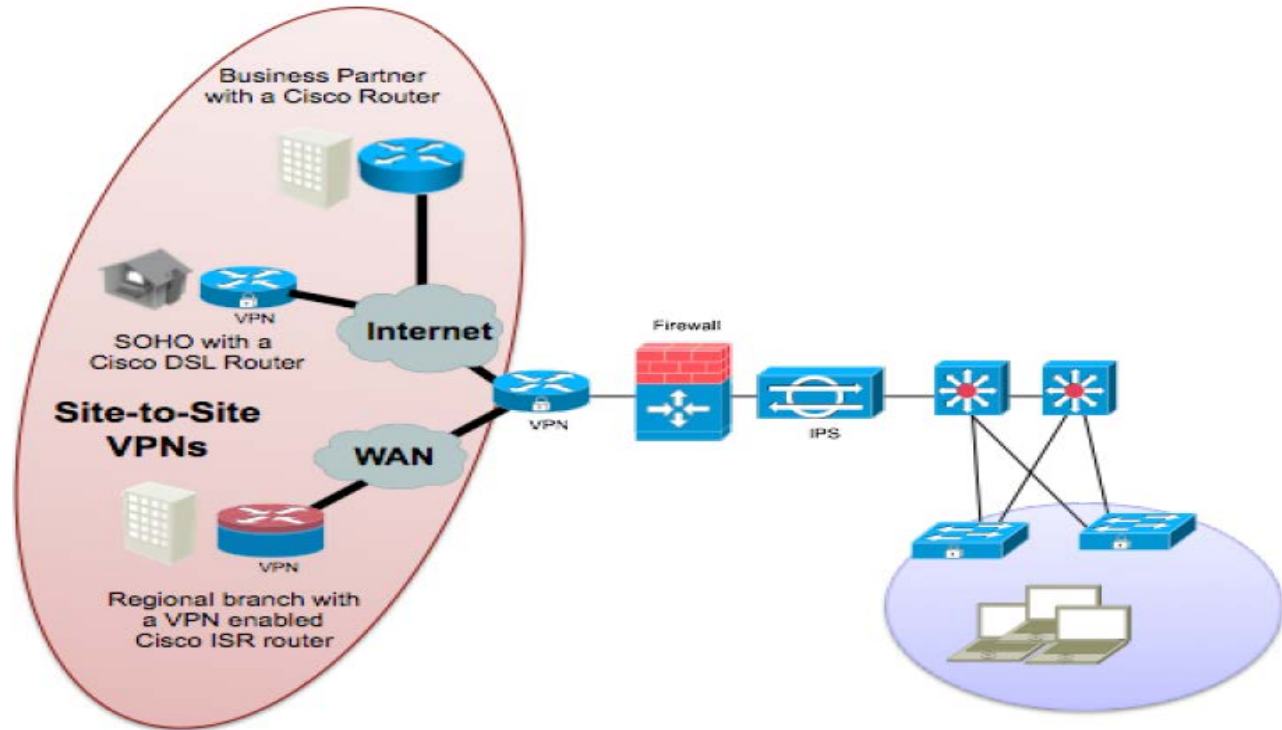
- Exemple: GRE, IPSec, MPLS
- Protecția datelor într-un VPN este oferită de framework-ul **IPsec**
- Dispozitive de criptare și servicii de VPN trebuie să existe la ambele capete ale VPN-ului
- Dispozitivele intermediare nu vor ști ce tip de trafic transportă



Topologii VPN

- Există două tipuri de topologii VPN:
- VPN - Remote-access
 - ✓ Utilizatorii remote trebuie să aibă conexiune la Internet
 - ✓ Parametrii VPN-ului sunt negociați dinamic
 - ✓ Utilizatorul stabilește tunelul VPN prin ISP
 - ✓ Tunelul este stabilit doar când este nevoie de el
- VPN-uri Site-to-site
 - ✓ Configurat între două dispozitive VPN
 - ✓ Mereu activ
 - ✓ Oferă interconectivitate între multiple rețele din ambele părți
 - ✓ Fiecare capăt de tunel joacă rolul unui gateway pentru rețelele sale

VPN Site-to-site



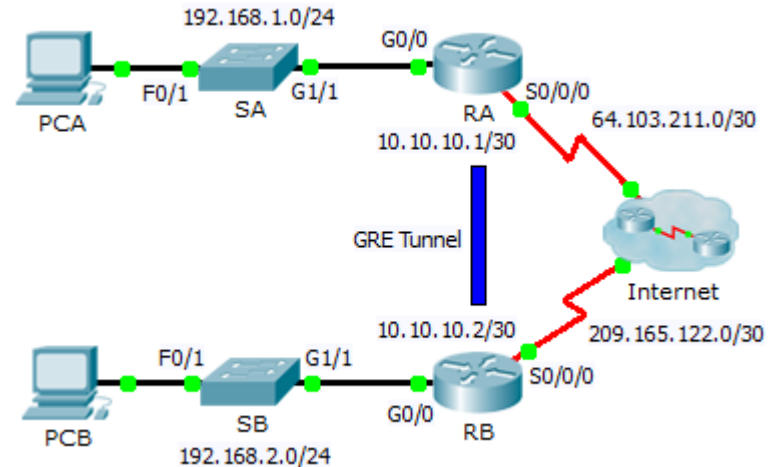
VPN GRE (încapsulare)

- GRE (Generic Routing Encapsulation)
 - ✓ Este un protocol de tunelare de nivel 3 OSI
 - ✓ Inițial dezvoltat de Cisco, acum standardizat
- Poate încapsula multiple tipuri de pachete într-un tunel IP
 - ✓ Adaugă un antet între antetul de nivel 3 al tunelului și payload
 - ✓ Acest antet identifică protocolul încapsulat
- Tunelurile GRE nu au stare: capetele nu rețin informații despre stare sau disponibilitatea celuilalt capăt
- Nu oferă mecanisme puternice de autentificare și confidențialitate



Configurare tunel GRE

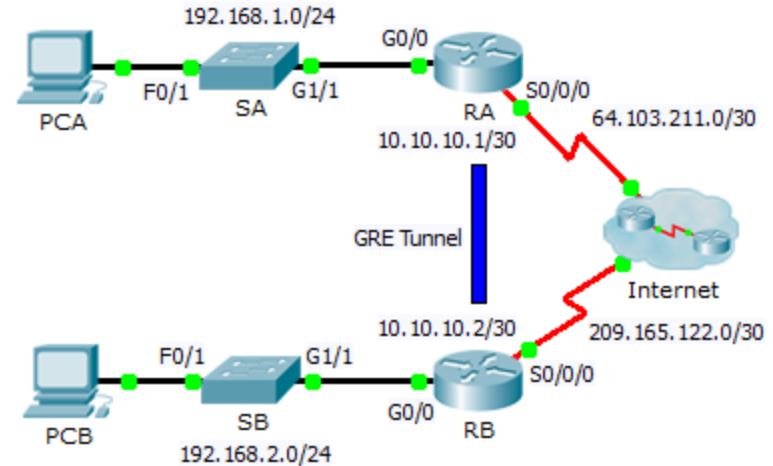
- Capetele tunelului sunt interfețe virtuale
- Tunelul este atașat unei interfețe fizice locale și se conectează la o interfață la distanță
- Tunelul trebuie să fie o rețea separată
- Precizarea modului de tunelare
- este opțională - *GRE este modul implicit* pentru orice tunel



Configurare tunel GRE

```
RA(config)# interface tunnel 0
RA(config-if)# ip address 10.10.10.1 255.255.255.252
RA(config-if)# tunnel source s0/0/0
RA(config-if)# tunnel destination 209.165.122.2
RA(config-if)# tunnel mode gre ip
RA(config-if)# no shutdown
```

```
RB(config)# interface tunnel 0
RB(config-if)# ip address 10.10.10.2 255.255.255.252
RB(config-if)# tunnel source s0/0/0
RB(config-if)# tunnel destination 64.103.211.2
RB(config-if)# tunnel mode gre ip
RB(config-if)# no shutdown
```



Depanarea GRE

- Un tunel GRE poate să nu funcționeze din mai multe motive.
- Verificați că:
 - ✓ Destinația tunelului este o adresă IP la care se poate ajunge (trebuie să fie prezentă în tabela de rutare)
 - ✓ Tunelul trebuie să aibă sursa și destinația valide
 - ✓ Traficul tunelului GRE să nu fie blocat de o altă regulă
 - ✓ Modul tunelului să fie același la ambele capete

