

Laboratorul 4 – VPN (Site-to-Site sau Remote Access)

Obiectiv: Stabilirea unei conexiuni securizate între locații

Teme:

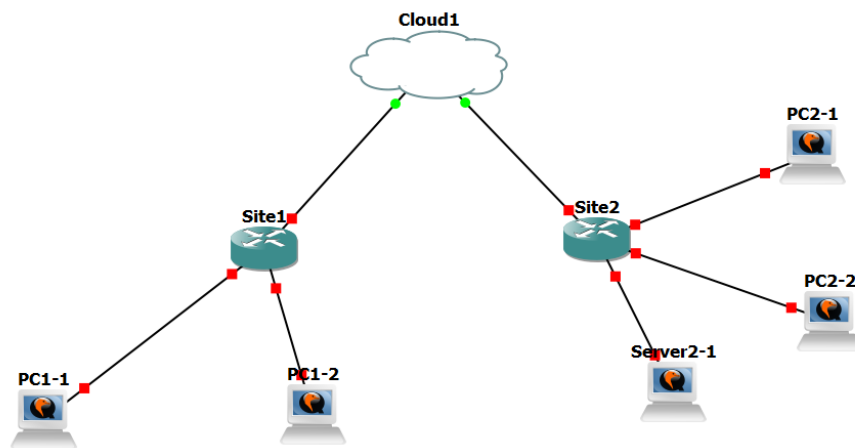
- VPN Wireguard site-to-site între două routere Mikrotik
- VPN L2TP/IPSec pentru acces remote
- Diagnosticare și depanare conexiune VPN

Dispozitive: 2 × Mikrotik CHR

Sustinere: Configurație VPN + test ping între rețelele locale

Topologie

Wireguard: 10.15.k.0/30
L2TP - Local Address: 172.25.k.1
LAN1 - 192.168.k.0/24
LAN2 - 192.168.k+1.0/24



Scop: stabilirea unei conexiuni criptate între routerele *Site1* și *Site2*, prin intermediul rețelei „Cloud1”.

Conexiunea va permite **acces doar către serverul din Site2** (nu către toate calculatoarele din LAN).

Se vor configura adresele WireGuard conform diagramei din topologie, unde **k** este numărul de ordine al studentului din listă.

Se va crea o regulă de firewall care să permită doar traficul din *Site1* către **Server2-1**.

VPN L2TP/IPSec pentru acces remote

- Routerul din **Site1** va funcționa ca **L2TP Server**.
- Routerul din **Site2** va fi clientul L2TP și va permite accesul utilizatorilor din LAN2 la rețeaua LAN1 prin tunel.
- Se vor configura parametrii L2TP/IPSec corespunzători (secret, user, IP pool).

- Se va testa conexiunea VPN de pe calculatoarele din Site2 (PC2-1, PC2-2).

Susținere laborator:

- Demonstrarea funcționării conexiunii VPN (WireGuard + L2TP/IPSec).
- Test *ping* între rețelele locale (LAN1 ↔ LAN2).
- Explicarea diferențelor dintre **Site-to-Site VPN** și **Remote Access VPN**.
- Fisier .rsc