Łukasz Buczyński

Routing i koncentracja VPN wielu oddziałów oraz centralny UTM

Kim jestem ?

Administrator z wieloletnim doświadczeniem, obecnie zarządzam infrastrukturą w dużym przedsiębiorstwie, czasem poprowadzę jakieś szkolenie. W sieciach specjalizuje się w zagadnieniach takich jak: routing, zabezpieczenia brzegu sieci oraz VPN na urządzeniach Mikrotik i nie tylko. Poza sieciami zajmuje się administracją systemami Windows oraz Linux, nastawionymi na wysoką dostępność i odporność na awarię a więc klastry, NLB itp. Po godzinach, jeśli tylko zostaje trochę czasu pasjonat elektroniki oraz IoT.

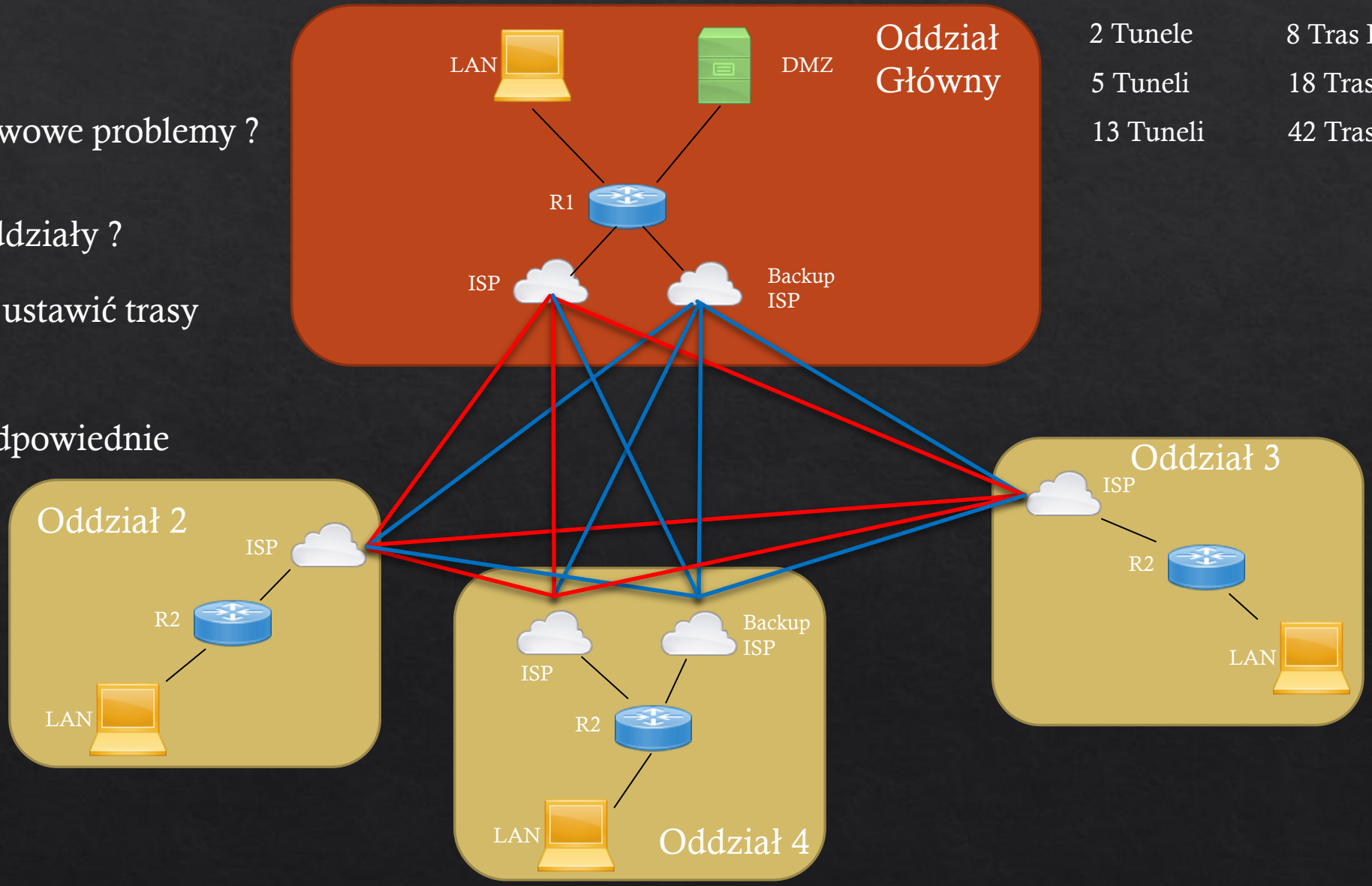
Kontakt: buczynsl@gmail.com

- MTCNA, MTCRE, MTCWE, MTCSWE
- MCP, MCDST, MCSA, MCSE
- ZCS, K-ADMIN-S, EITCA/IS

Stare Dobre Czasy

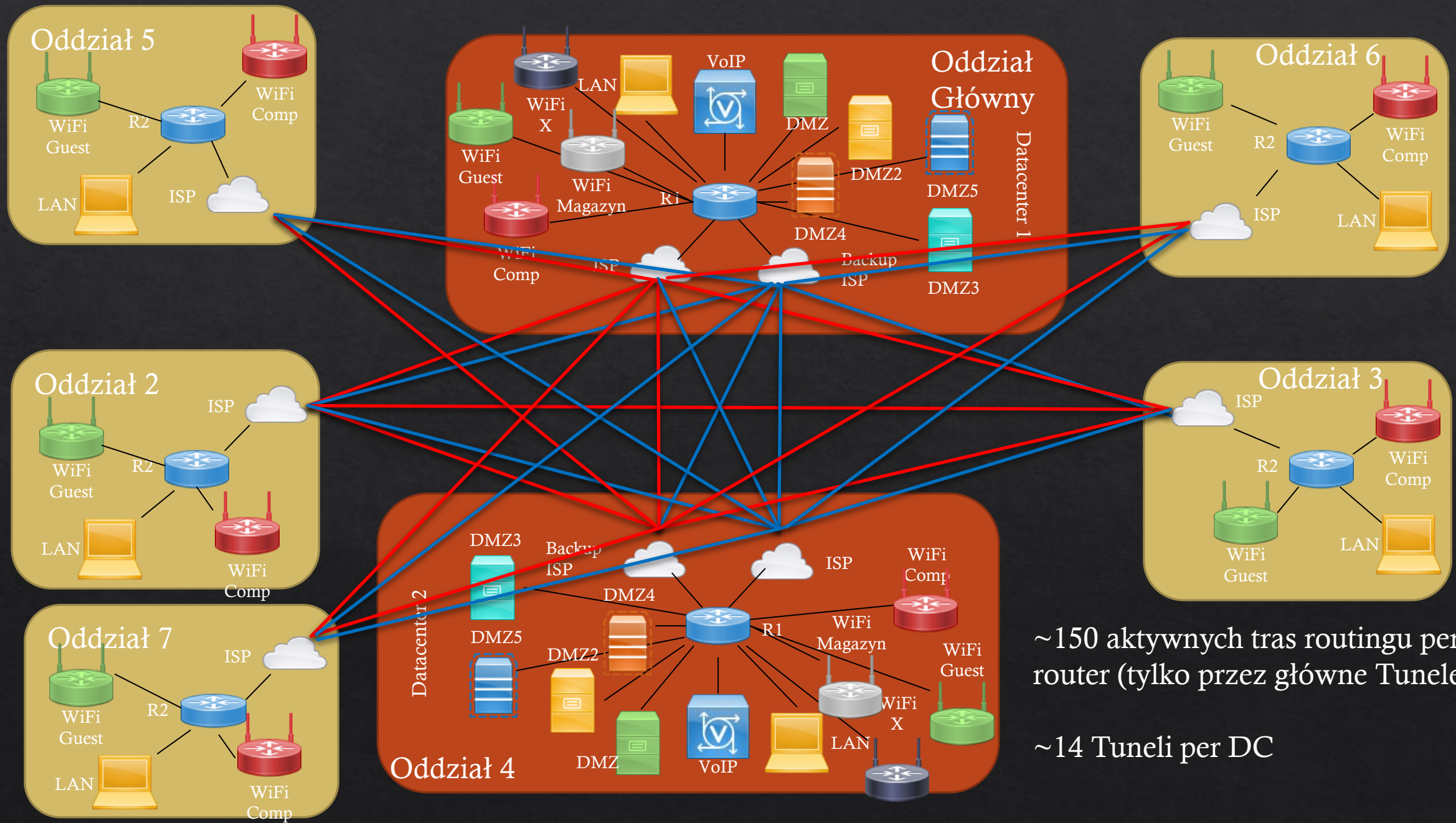
Jakie mamy podstawowe problemy ?

1. Jak połączyć oddziały ?
2. Jak optymalnie ustawić trasy komunikacji?
3. Jak zapewnić odpowiednie reguły dostępu?



2 Tunele	8 Tras Routingu
5 Tuneli	18 Tras Routingu
13 Tuneli	42 Tras Routingu

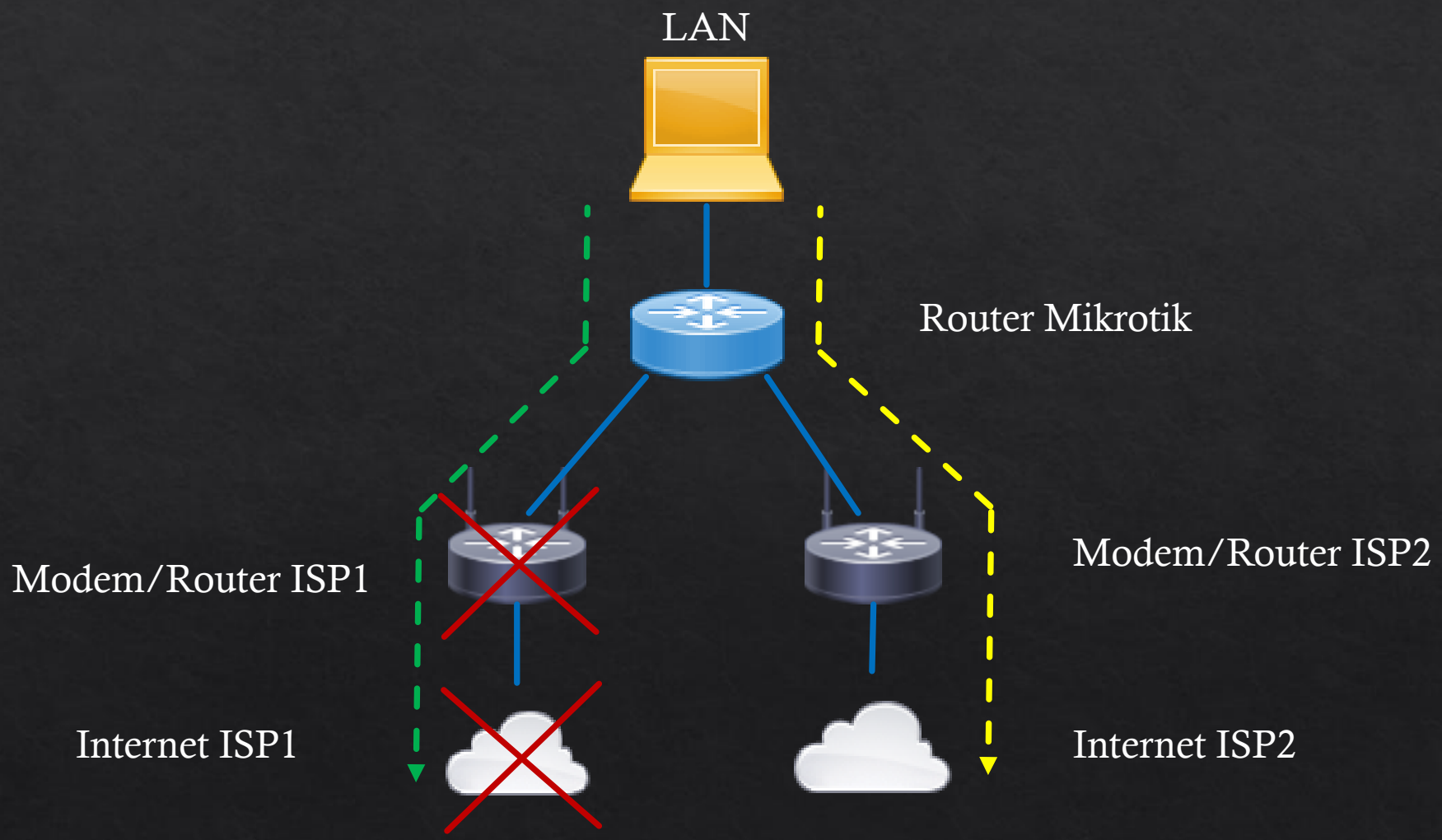
Co mamy obecnie



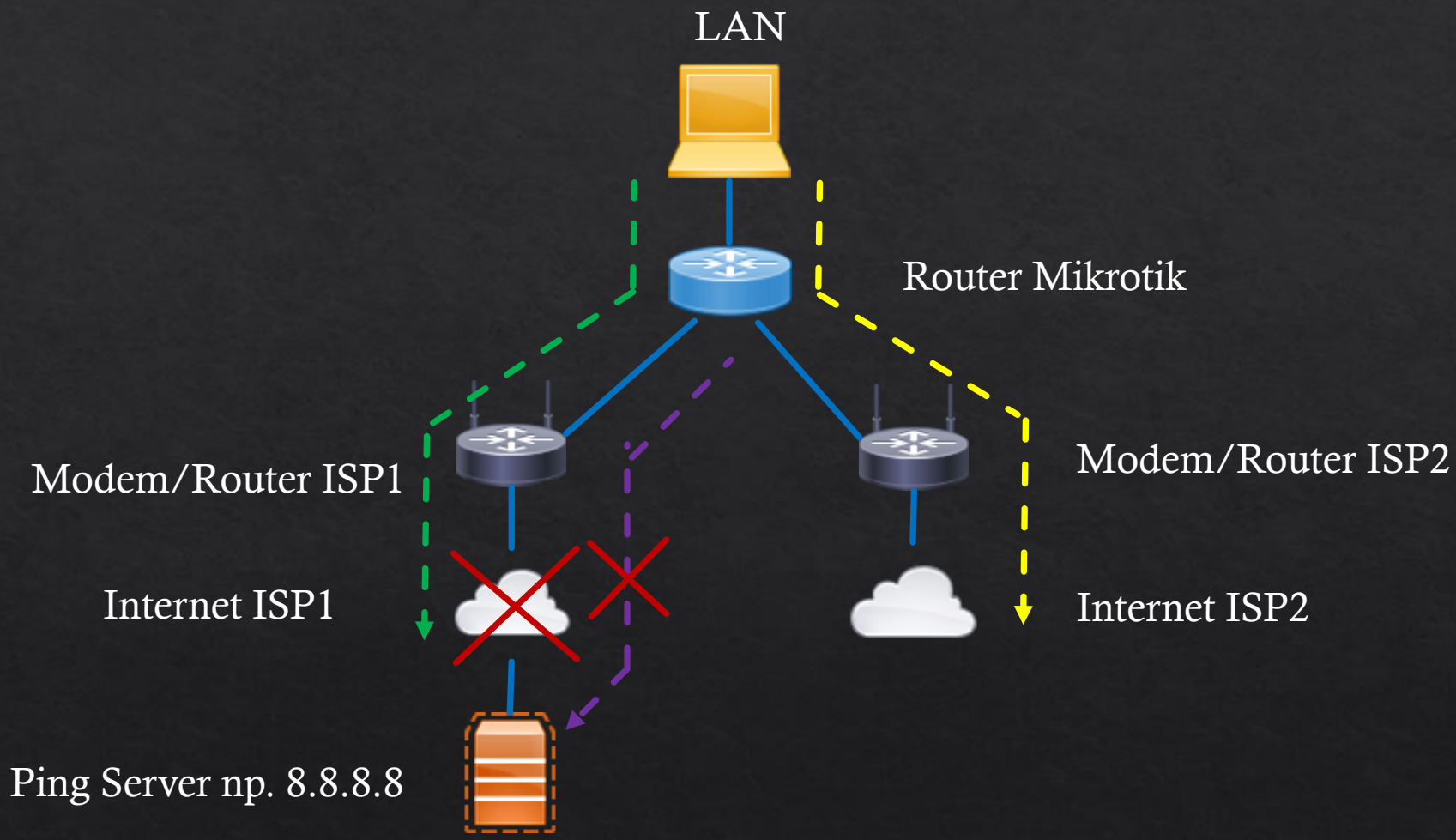
~150 aktywnych tras routingu per-router (tylko przez główne Tunele)

~14 Tuneli per DC

Multi WAN (Active/Backup)



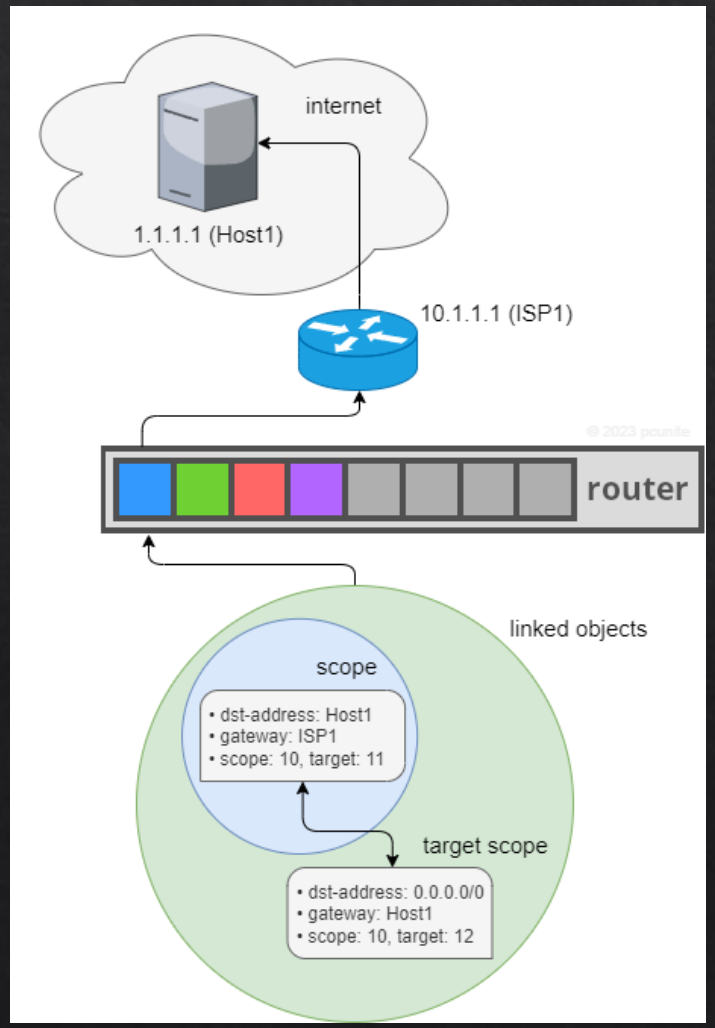
Recursive Routing/ Next hop Lookup



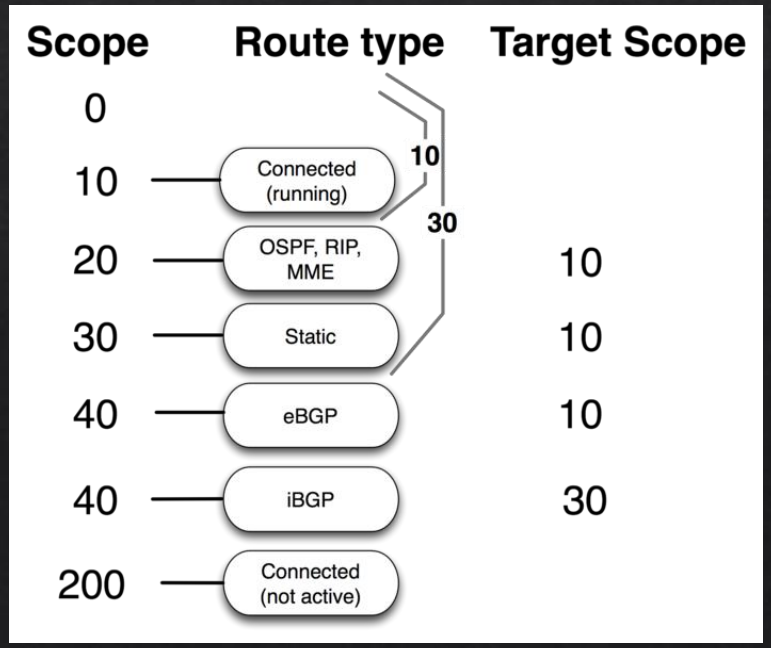
https://help.mikrotik.com/docs/display/ROS/IP+Routing#IPRouting-NexthopLookup

Scope, Target Scope, Gateway Ping

https://forum.mikrotik.com/viewtopic.php?t=192736&sid=30a1ce4962a1f12cac8a0345029adf8a

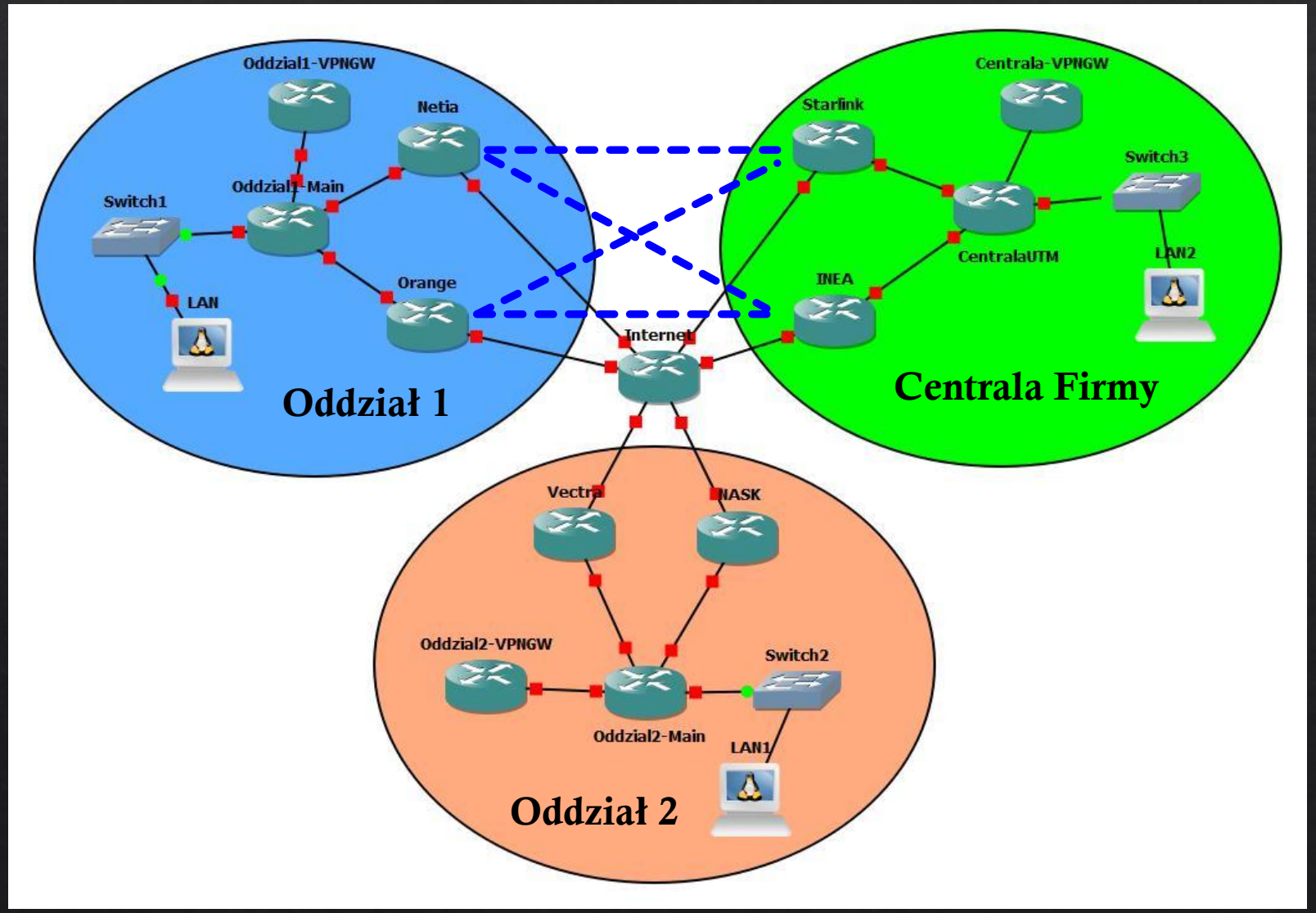


"Forum member **anav** has beautifully hacked this concept by always setting the default *Scope* to 10 and using the *Target Scope* parameter to change the relationship. "



https://help.mikrotik.com/docs/download/attachments/328084/scope_and_target_scope.png

Plan działania



- Recursive Routing
- Dodanie Bramy VPN
- Zestawienie bezpiecznych tuneli IPIP do centrali
- OSPF
- Wyjście do internetu przez centralę z zachowaniem multiwanów (oddziału i centrali) oraz wyjście lokalnym ISP w przypadku awarii centrali

Koniec!

Kontakt: buczynsl@gmail.com