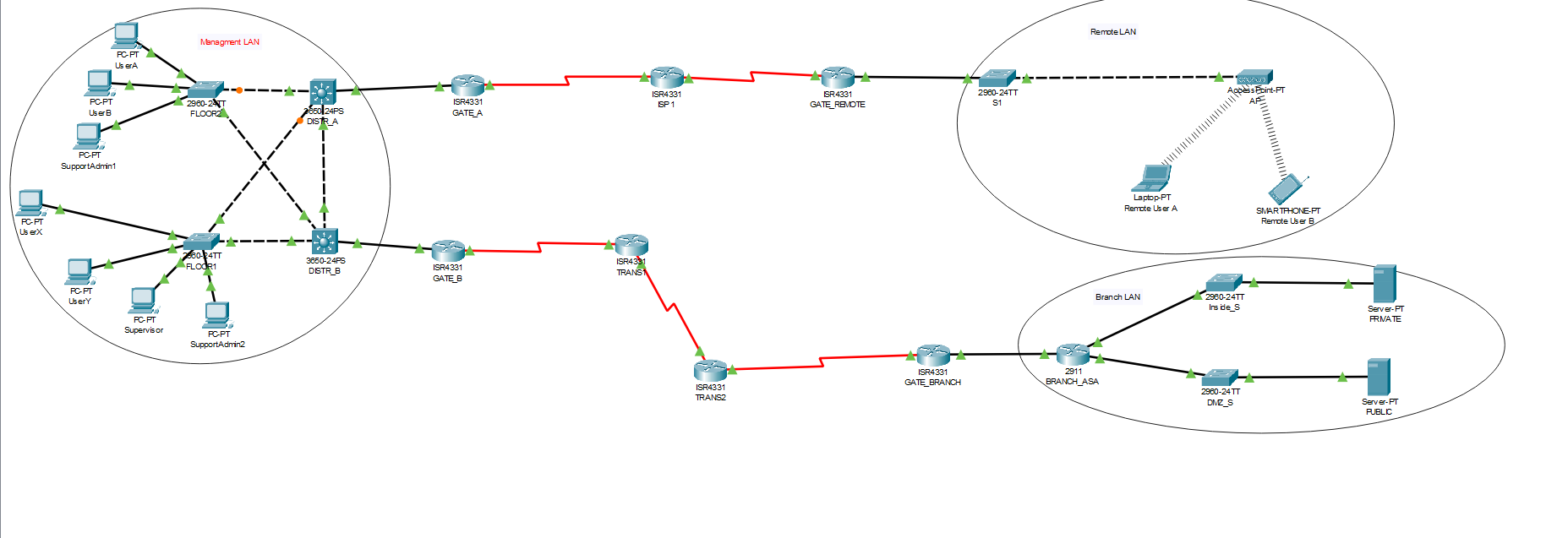
Zaawansowane techniki bezpieczeństwa sieci teleinformatycznych Projekt

Michał Lidwa 4ID14A

Topologia finalna



Zastosowane Adresacje sieci LAN

Managment LAN

VLAN99Admins – 192.170.99.0/25

VLAN101Users - 192.168.101.0/24

VLAN102Users - 192.168.102.0/24

Remote LAN

Remote LAN – 192.168.1.0/24

BRANCH LAN

DMZ ZONE – 209.170.17.0/24

INSIDE ZONE - 209.170.16.0/24

Zastosowane Adresacje sieci WAN

GATE\_A – ISP 1 81.26.4.0/30

ISP 1 - GATE\_REMOTE 81.26.4.4/30

GATE\_B – TRANS1 81.26.4.8/30

TRANS1 -TRANS2 209.165.200.0 /24

TRANS 2 – GATE\_BRANCH 81.50.200.0/24

GATE\_BRANCH – BRANCH\_ASA 209.170.250.224/29

Ogółny opis topologii

W topologii dla routerów GATE\_A i GATE\_B zastosowano HFRP, implementację FHRP (brama redundantna) dla każdego vlan.

VLAN99Admins adres wirtualny 192.170.99.3

VLAN101Users adres wirtualny 192.168.101.3

VLAN102Users adres wirtualny 192.168.101.2

Dodatkowo by vlany komunkowały się z jednego routera i drugiego w zaleznosci gdzie idzie pakiet zastosowane został tunel GRE dla każdego vlan, czyli w sumie 3 tunele miedzy GATE\_A i GATE\_B routerami.

Dla VLAN99Admins zastosowano tunel o adresacji 172.170.99.0/24

Dla VLAN101Users zastosowano tunel o adresacji 172.16.101.0/24

Dla VLAN102Users zastosowano tunel o adresacji 172.16.102.0/24

Routing jaki zastosowany został następująco w sieci WAN:

GATE\_A – ISP 1 BGP

ISP 1 - GATE\_REMOTE OSPF

Dodatkowo w routerze GATE\_REMOTE zastosowano na wyjście routing statyczny domyślny na potrzeby implementacji NAT

GATE\_B – TRANS1 BGP

TRANS1 -TRANS2 OSPF

TRANS 2 – GATE\_BRANCH OSPF

GATE\_BRANCH – BRANCH\_ASA OSPF

W sieci MAIN SITE wdrożono bezpieczeństwo portów, ochronę DTP i STP w switchach FLOOR1 i FLOOR2. Zastosowano port security dla portów fastethernet na makimum 2 oraz w trybie naruszenia restrict. Zastosowano tez spanning-tree w strybie Bpduguard. W sieci MAIN SITE VLAN zwykłych użytkowników nie mają między sobą dostępu, ale każda ma dostęp do sieci VLAN administratora i do zewnętrznego Internetu.

W sieci Remote zastosowano NAT oraz ochrone WiFI WPA2 oraz DHCP z ochroną spoofowaniem.

Do logowania SSH zastosowano dwa konta o nazwie SupportAdmin1 i SupportAdmin2. Oraz stworzono 2 widoki o tych samych nazwach co konta. Logowanie do SSH jest dopuszczalne tylko dla VLAN99Admins poprzez ACL

Pomiędzy Remote LAN a vlanem administratorów w MAIN SITE zastosowano VPN tunel IPsec.

W Branch LAN zastosowano zapora sieciową ze trzema strefami IN,OUT,DMZ.

Adresacja tych stref.

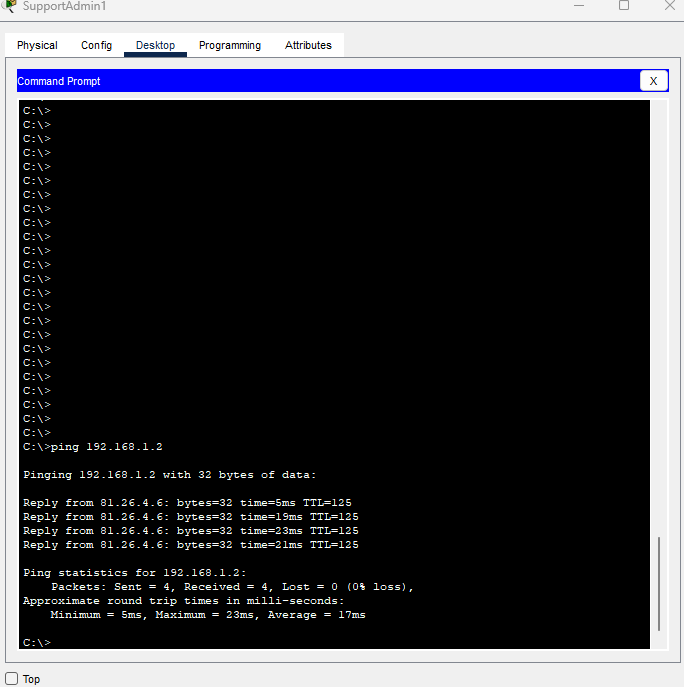
DMZ ZONE – 209.170.17.0/24

INSIDE ZONE - 209.170.16.0/24

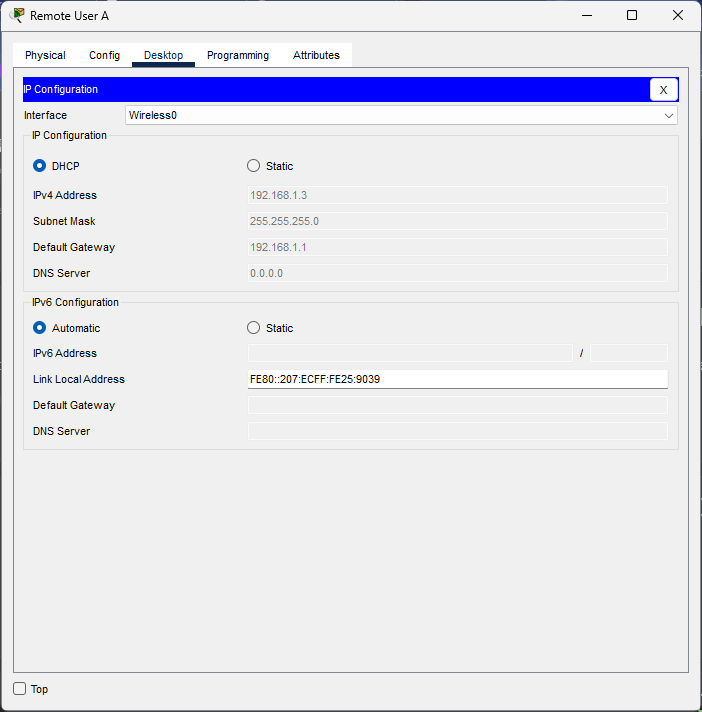
Do użytkowników i widoków wszystkich zastosowano hasło cisco12345 oraz hasło do trybu exec routerów tez hasło cisco12345

Zostaną przedstawione zrzuty ekrany z działań niektórych rzeczy

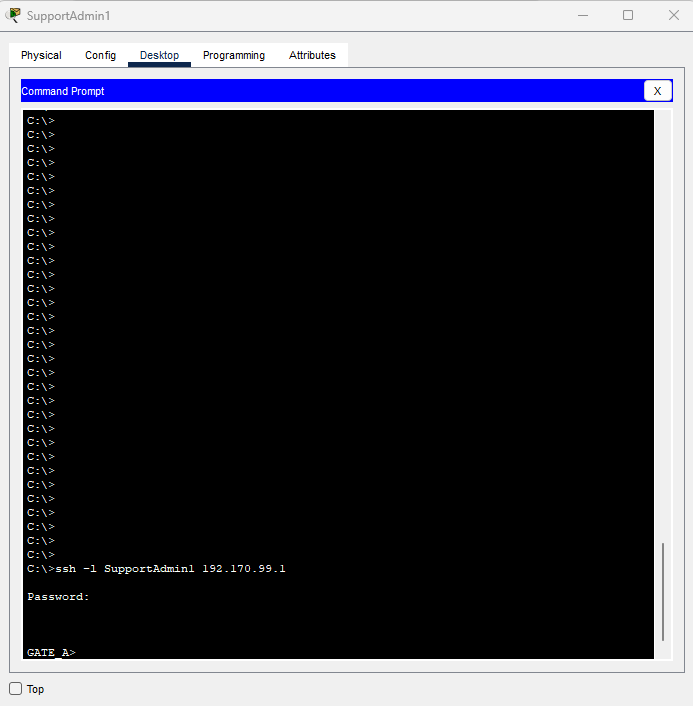
Działanie NAT, ping do sieci Remote



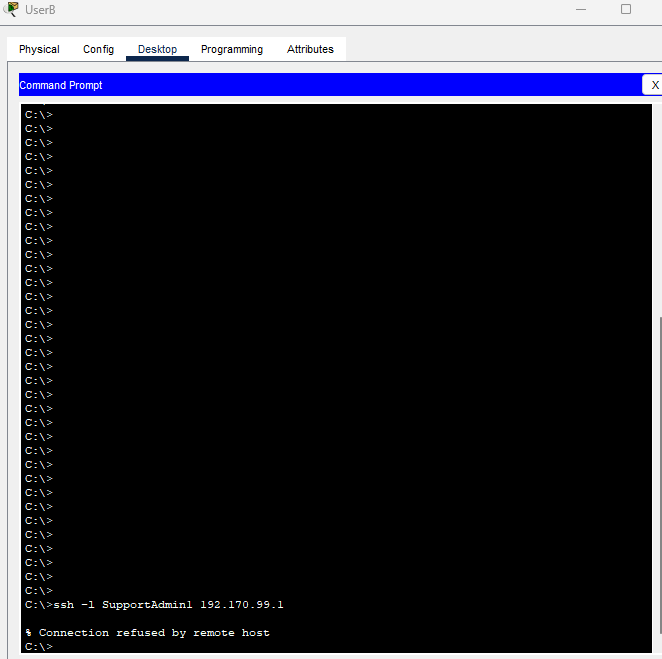
Działanie DHCP w sieci Remote



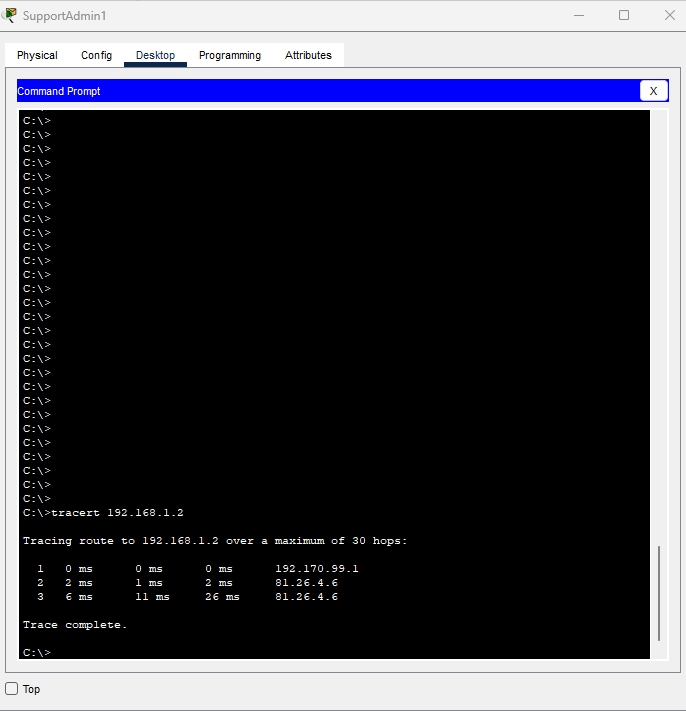
Możliwość logowania do routera GATE poprzez SSH dla VLAN99Admins



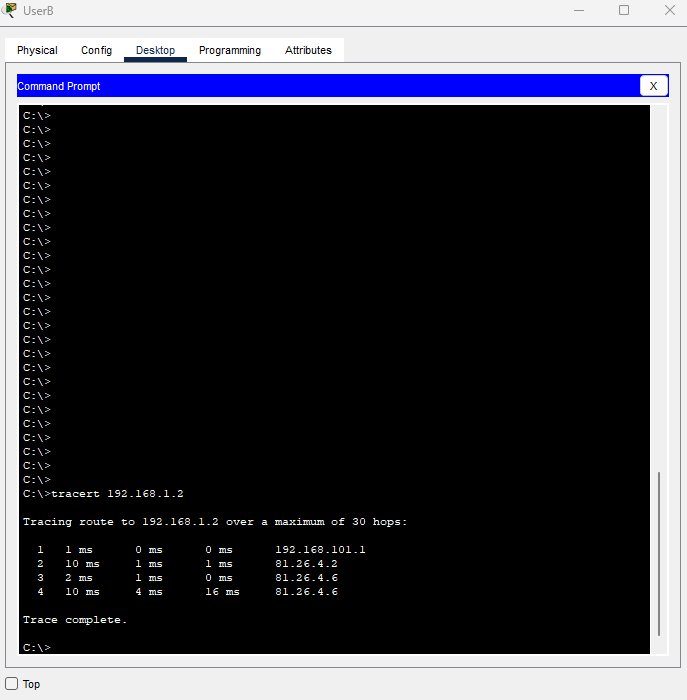
Możliwość błędnego logowania do routera GATE poprzez SSH dla VLAN101Users



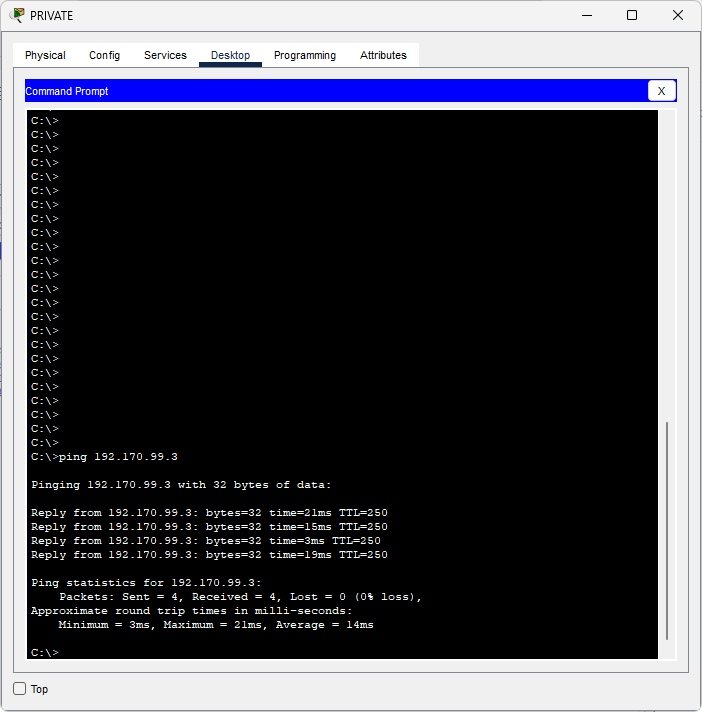
Działanie tunelu IPSec dla VLAN99Admins do sieci Remote



Działanie normalne trasy do sieci Remote od VLAN101Users



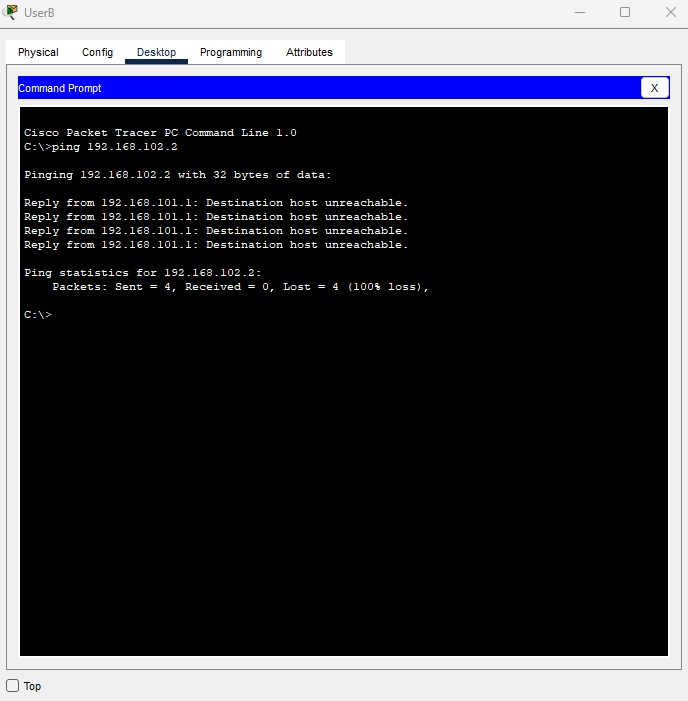
Komunikacja z sieci Branch ze strefy IN do OUTSIDE



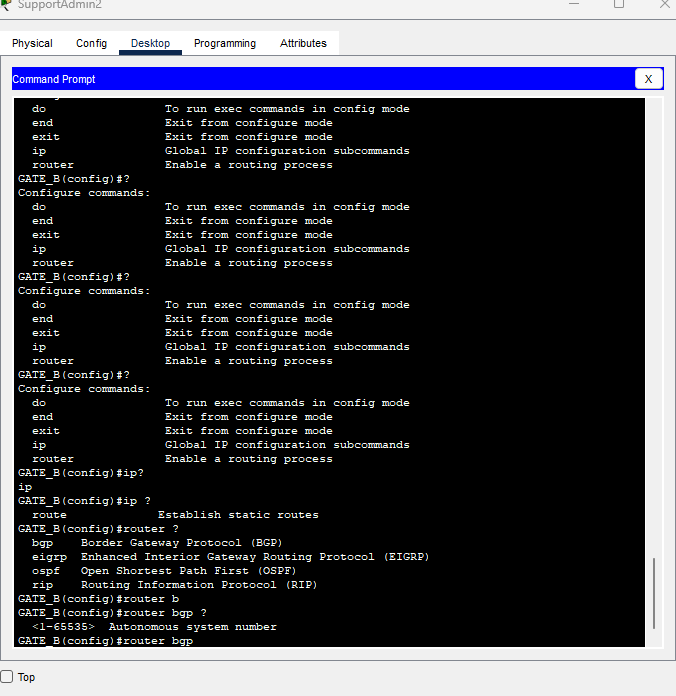
Działanie z sieci Managment do Branch do strefy DMZ z OUTSIDE poprzez przeglądanie strony postawionej w strefie DMZ przez serwer



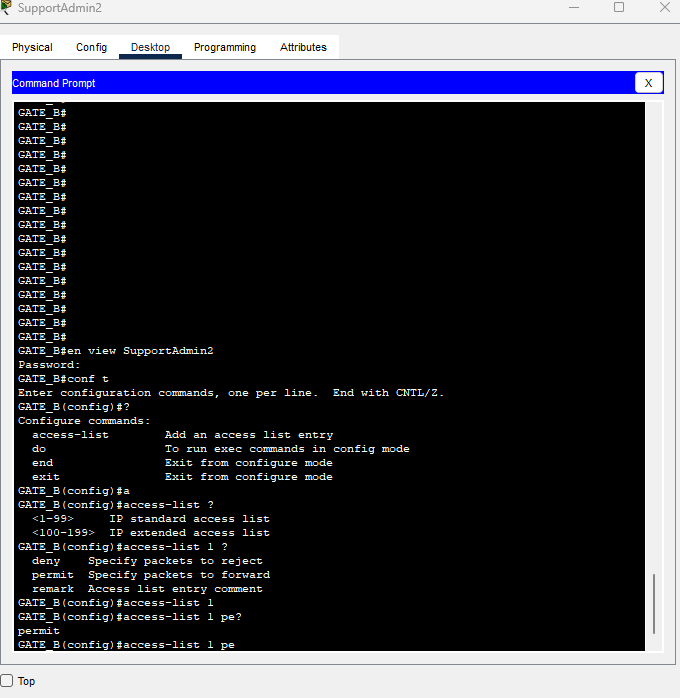
Działanie ACL by użytkownicy zwykli miedzy VLAN się nie komunikowali się. Tutaj z VLAN101Users do VLAN102Users



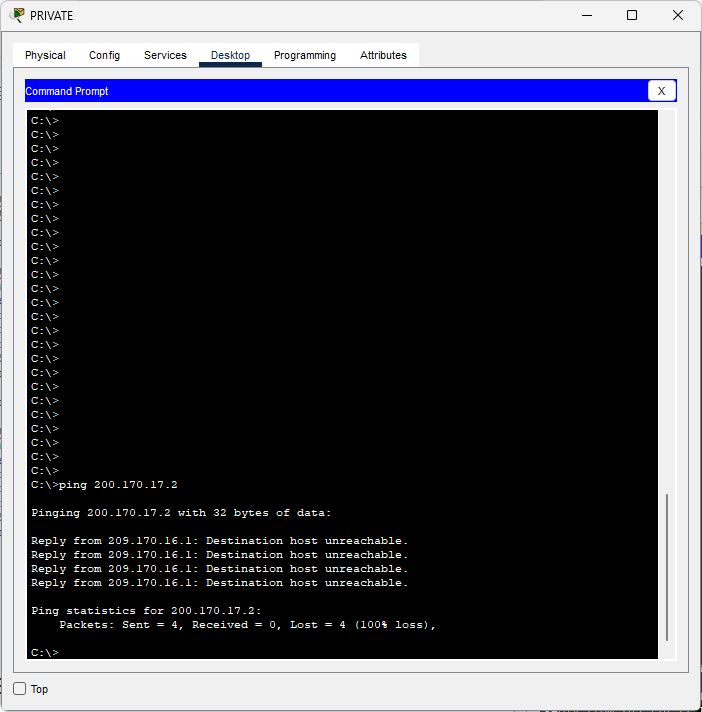
Widok dla SupportAdmin1

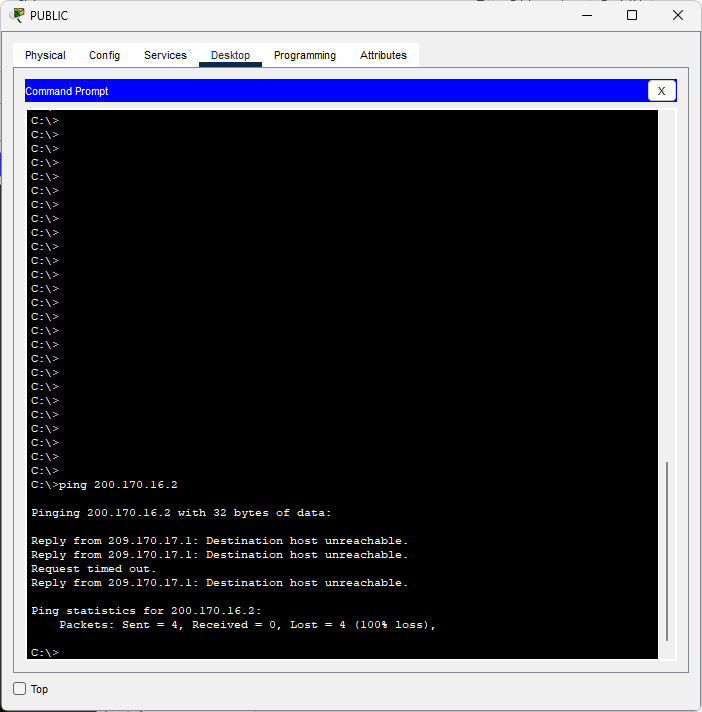


Widok dla SupportAdmin2

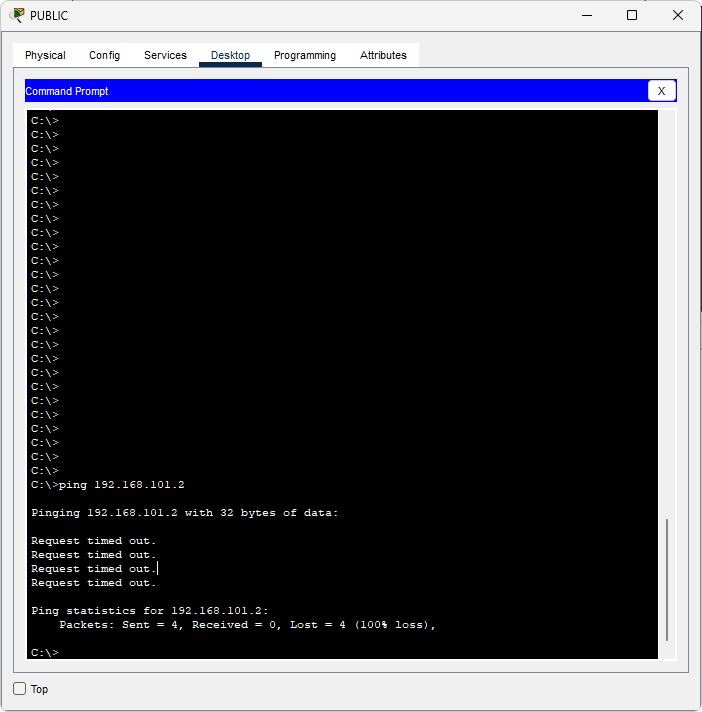


Brak komunikacji miedzy strefami DMZ a INSIDE





Brak komunikacji między Strefą DMZ a OUTSIDE



Brak komunikacji miedzy Strefą OUTSIDE a IN

