Politechnika Świętokrzyska Wydział Elektrotechniki, Automatyki i Informatyki
Katedra Informatyki Stosowanej

Bezpieczeństwo infrastruktury sieciowej - projekt

Temat: Sieć firmy księgowej

Wykonali:
Mateusz Borcuch,
Aleksander Wosztyl

➢ Opis wykreowanej infrastruktury

Infrastruktura sieciowa została zaprojektowana dla firmy księgowości. Sieć została podzielona na podsieci dla administratorów oraz dla pracowników firmy. Posiadamy też osobną sieć dla głównych serwerów oraz dla podsieci pracowniczych WIFI aby umożliwiać im połączenia bezprzewodowe. Wprowadzono zabezpieczenia sieciowe takie jak: autoryzacja dostępu do urządzeń sieciowych. Sieć pracowników administracyjnych ma możliwość połączenia się do sieci każdego z pracowników. Nikt z sieci pracowniczych nie ma dostępu do sieci administratorów. Wdrożenie zabezpieczeń sieciowych takich jak autoryzacja dostępu do urządzeń sieciowych, SSH, VPN, firewall oraz listy ACL, jest niezbędne do zapewnienia bezpieczeństwa sieci. W przypadku naszego projektu zastosowano autoryzację dostępu do urządzeń sieciowych za pomocą protokołu AAA, SSH do bezpiecznej zdalnej administracji, VPN do bezpiecznego połączenia między lokacjami, firewall do blokowania nieautoryzowanego ruchu sieciowego oraz listy ACL do zarządzania ruchem sieciowym.

➢ Zagrożenia infrastruktury sieciowej

- Ataki brute force na SSH:

Zagrożenie: Hakerzy mogą próbować złamać hasła do systemu SSH za pomocą ataków typu "brute force".

- Ataki zero-day:

Zagrożenie: wykorzystują luki w oprogramowaniu, które są nieznane producentowi lub dostawcy oprogramowania.

- Ataki na warstwę fizyczną:

Zagrożenie: polegają na uszkodzeniu lub zniszczeniu infrastruktury sieciowej.

- Ataki DDoS:

Zagrożenie: Ataki DDoS mogą powodować niedostępność usług w sieci.

- Nieaktualne oprogramowanie:

Zagrożenie: Nieaktualne oprogramowanie może zawierać znane podatności, które mogą być wykorzystane przez atakujących.

- Ataki na AAA (Authentication, Authorization, Accounting):

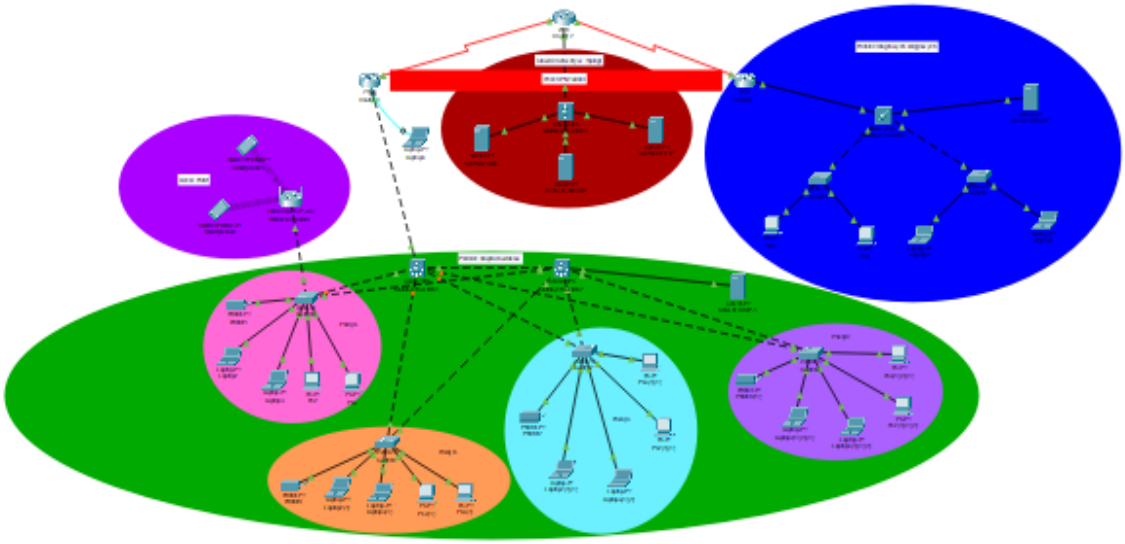
Zagrożenie: Ataki na system uwierzytelniania, autoryzacji lub rachunkowości mogą umożliwić nieuprawniony dostęp.

Ważne jest ciągłe monitorowanie sieci, analiza logów oraz dostosowywanie zabezpieczeń w miarę pojawiania się nowych zagrożeń.

➢ Tabela adresacji

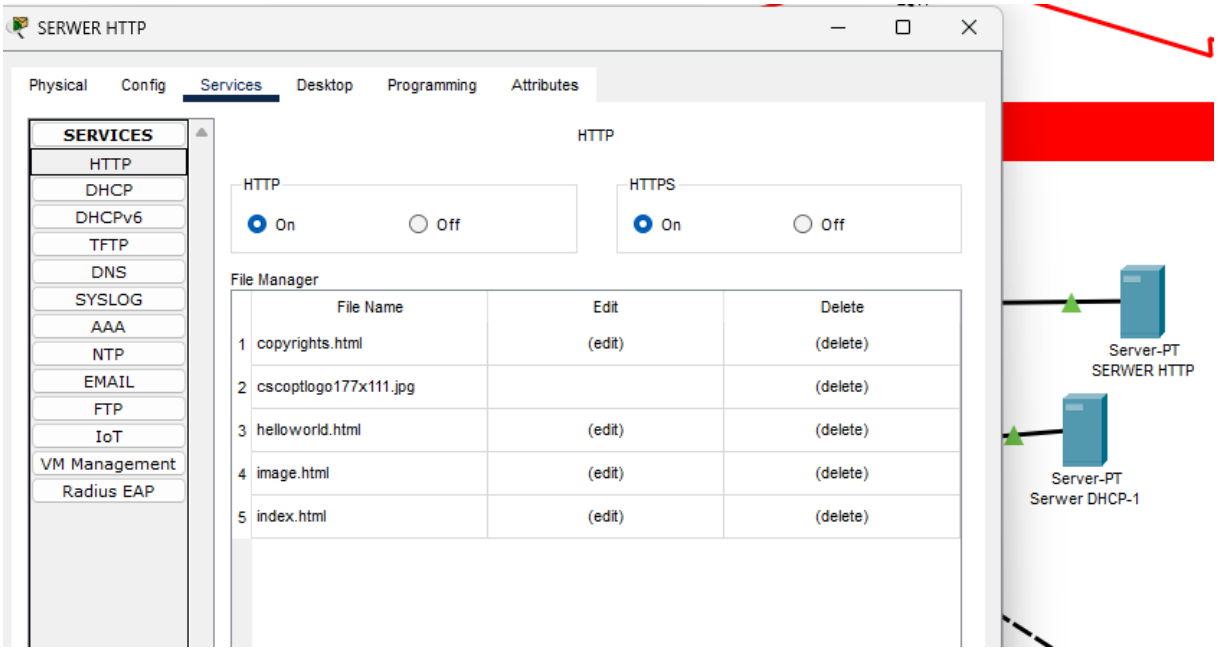
Device	Interface	IP ADDRESS	Default gateway	Maska
R1	Fe 0/0	192.168.4.1	-	255.255.255.0
R1	S 0/0/0	192.168.1.1	-	255.255.255.0
R2	Fe 0/0	192.168.5.1	-	255.255.255.0
R2	S 0/3/0	192.168.1.2	-	255.255.255.0
R2	S 0/3/1	192.168.2.1	-	255.255.255.0
R3	Fe 0/0	192.168.3.1	-	255.255.255.0
R3	S 0/2/0	192.168.2.2	-	255.255.255.0
SERWER-HTTP	Fe 0	192.168.5.2	192.168.5.1	255.255.255.0
SERWER DNS	Fe 0	192.168.5.3	192.168.5.1	255.255.255.0
SERWER DHCP-1	Fe 0	192.168.4.2	192.168.4.1	255.255.255.0
SERWER DHCP-2	Fe 0	192.168.3.2	192.168.3.1	255.255.255.0
SERWER SYSLOG	Fe 0	192.168.5.4	192.168.5.1	255.255.255.0

➢ Układ graficzny topologii sieci w Packet Tracer:

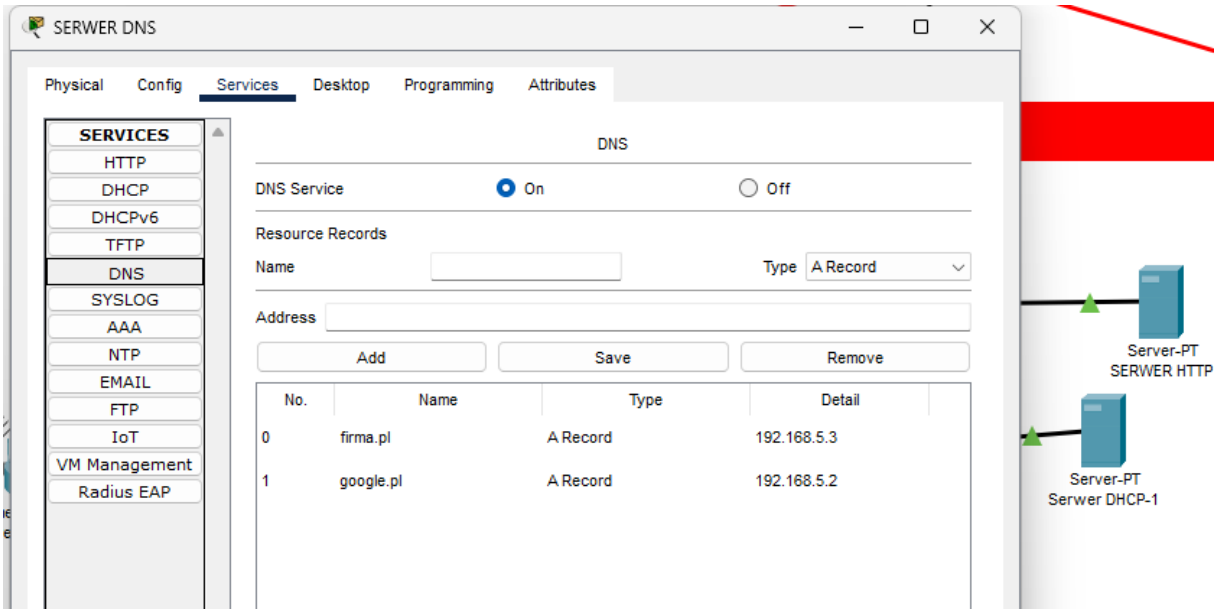


➢ Wykorzystane services

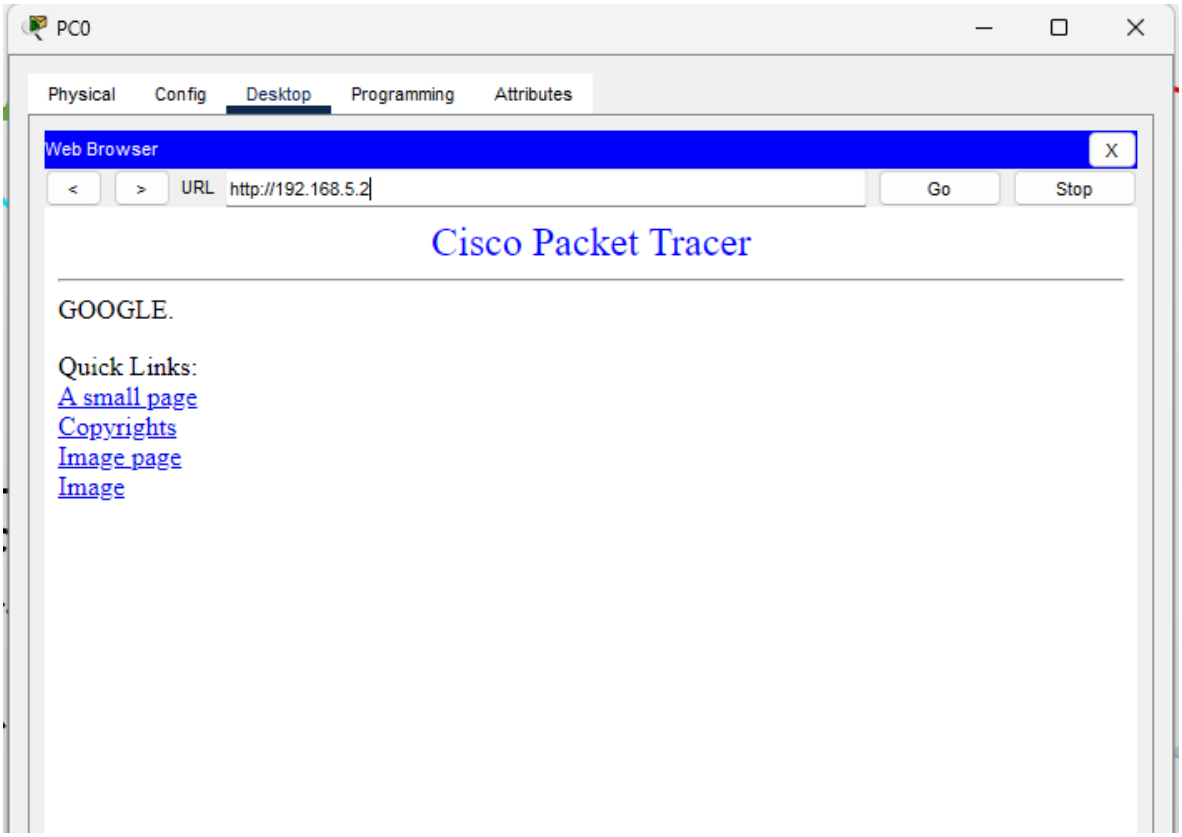
✓ SERWER HTTP

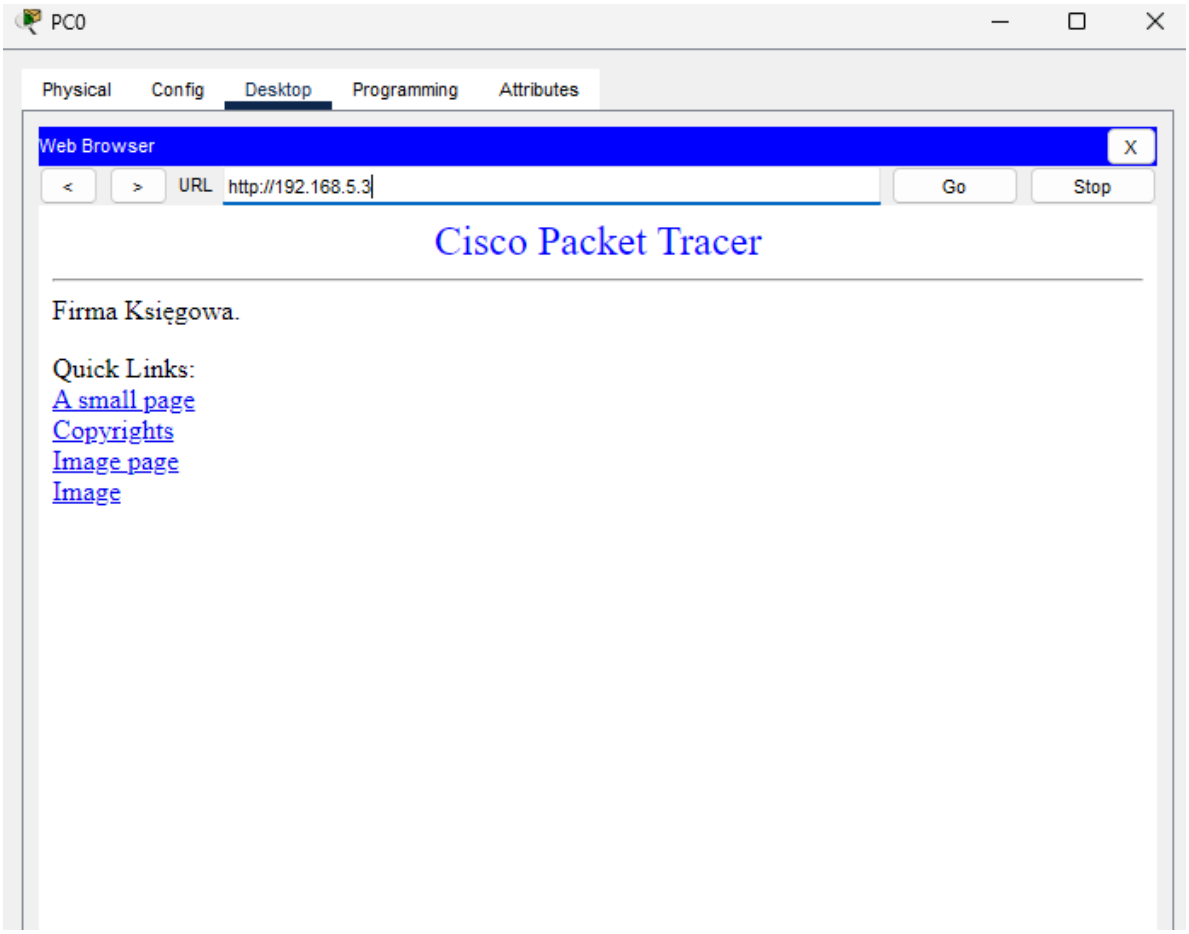


✓ SERWER DNS

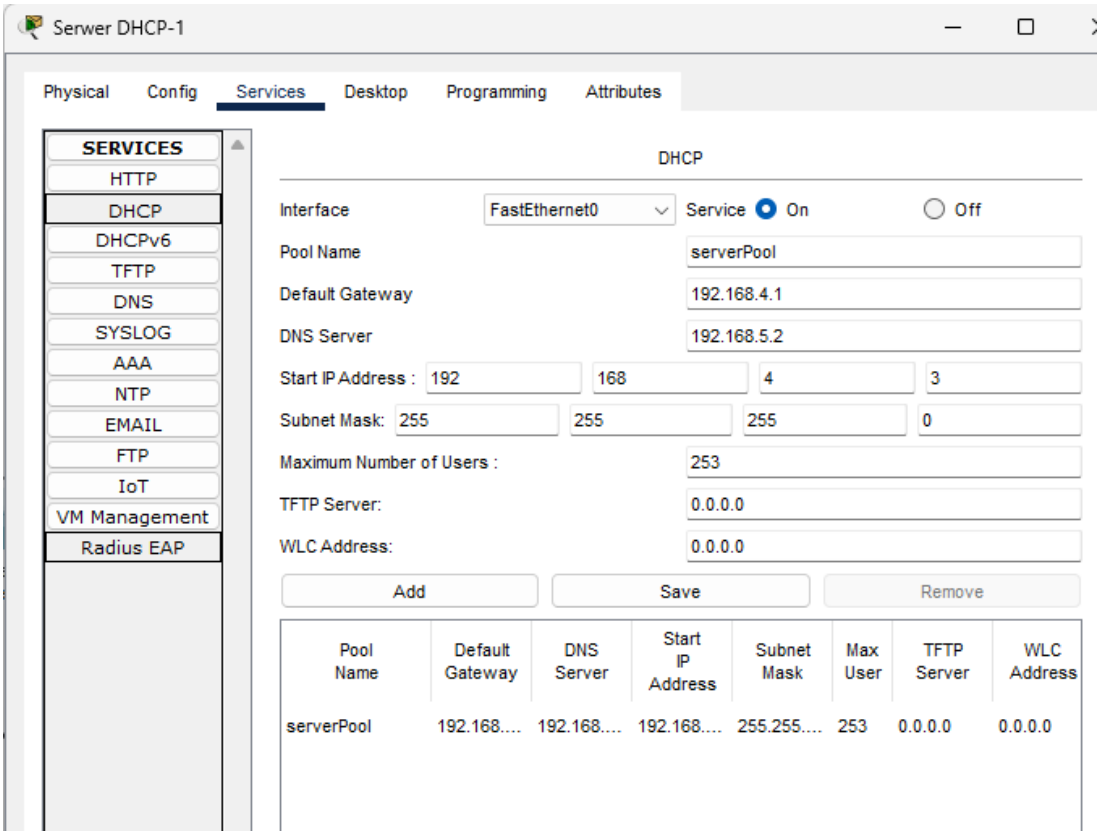


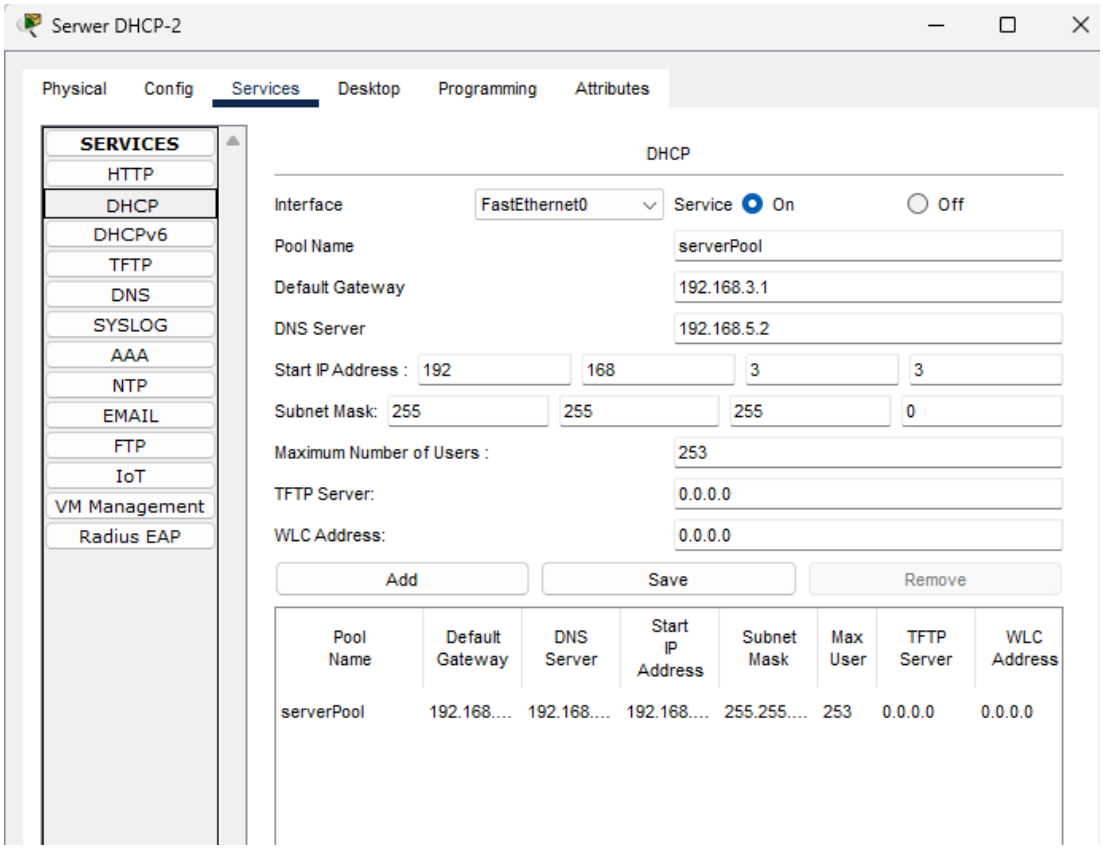
Przykłady przedstawiające prawidłowo skonfigurowane serwery.





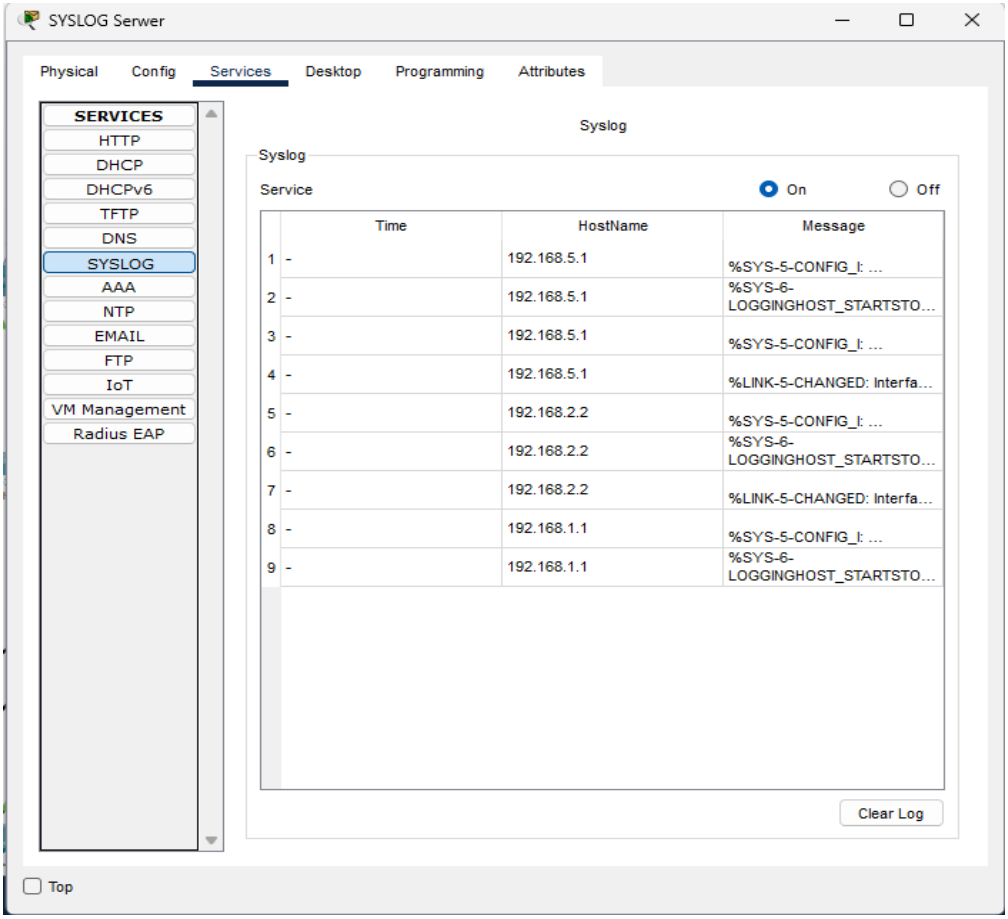
➢ KONFIGURACJA SERWERÓW DHCP



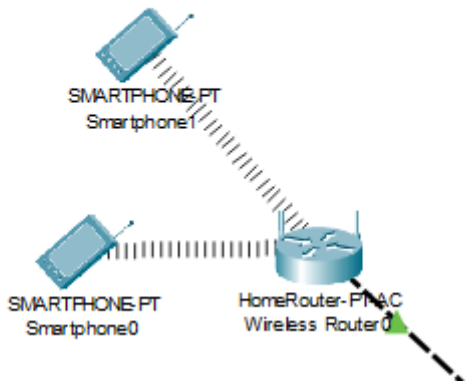


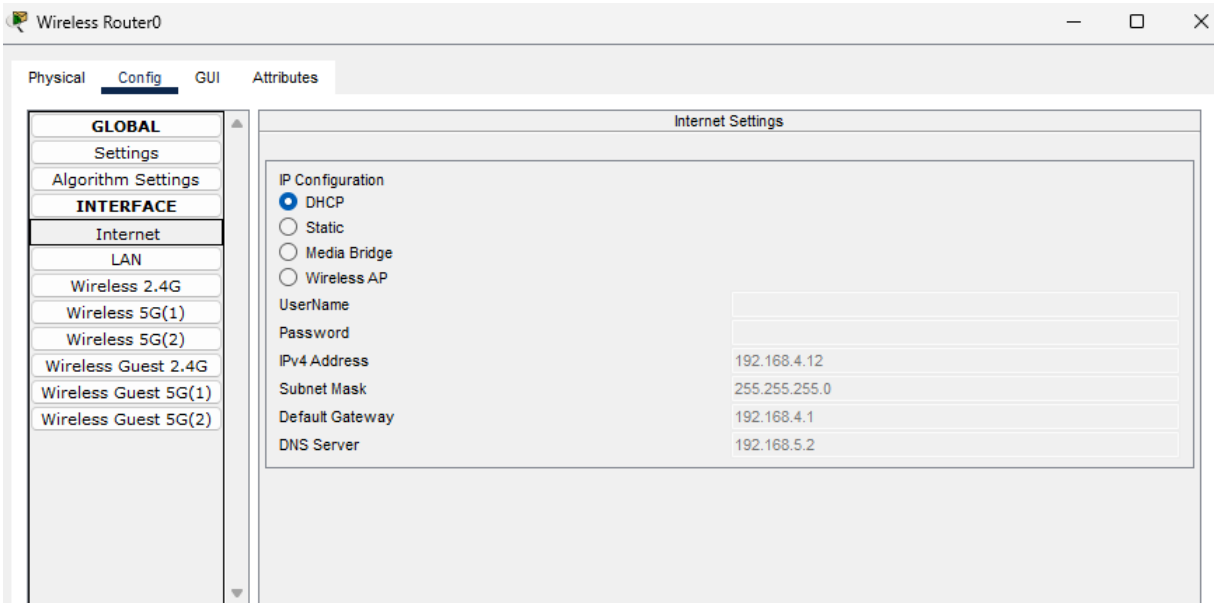
➢ SYSLOG serwer

Wykorzystanie protokołu komunikacyjnego który umożliwia urządzeniom przesyłanie informacji o zdarzeniach i działaniach sieci

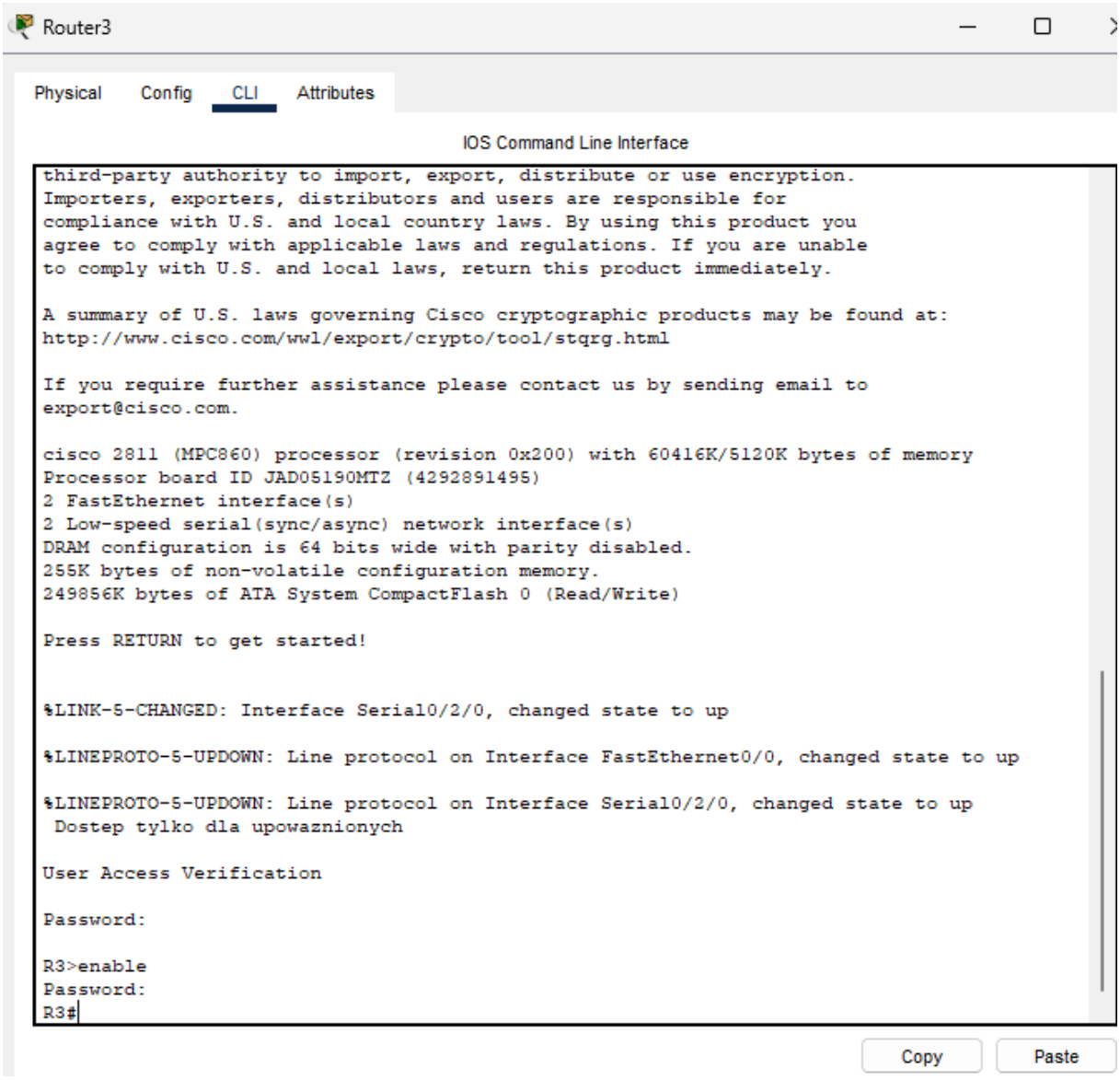


➢ Sieć bezprzewodowa: Wi-Fi





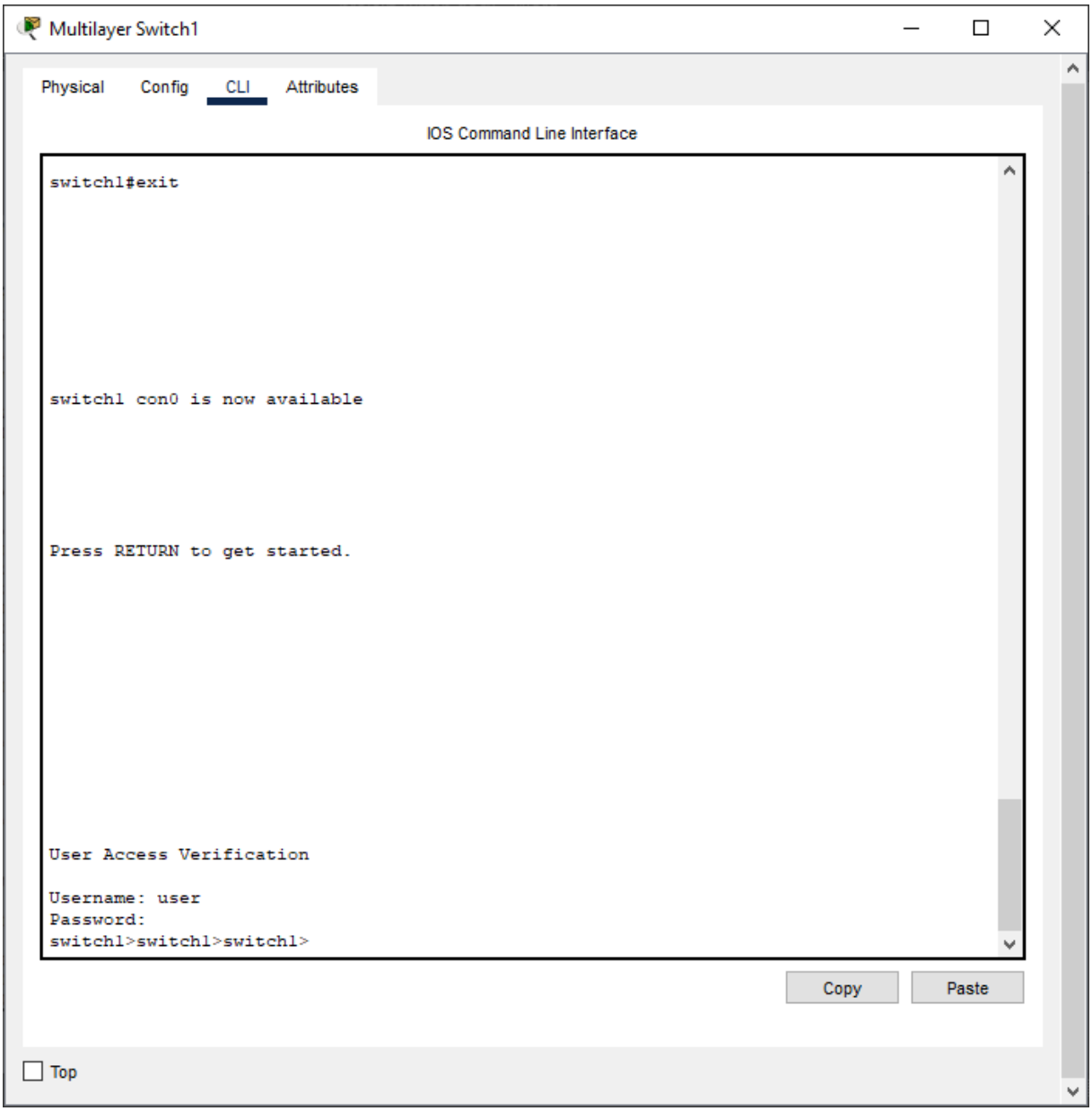
- **Zabezpieczenie urządzeń sieciowych - przykład**



➢ Listy ACL

Zastosowanie list ACL do zarządzania ruchem sieciowym. Kontrolowanie które pakiety mają być akceptowane na podstawie adresów IP

➢ Skonfigurowany poziom dostępowy AAA



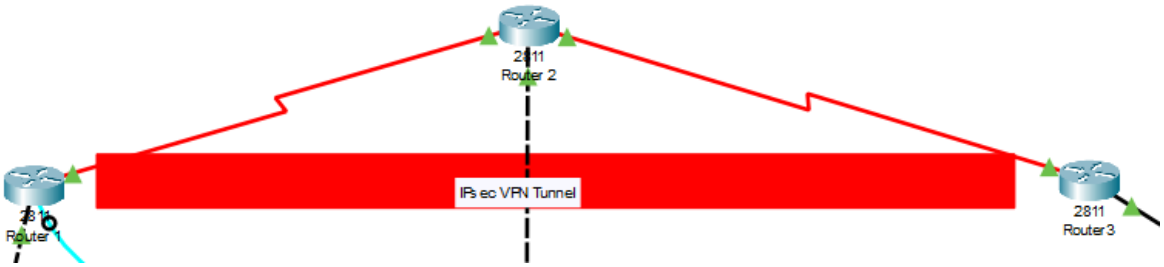
➢ Sposób łączenia się za pomocą SSH

Użyliśmy protokołu SSH do bezpiecznej zdalnej administracji w sposób zabezpieczony co potwierdza poniższy screen.

```
C:\>ssh -l cisco 192.168.3.1

Password:

 Dostep tylko dla upowaznionych

R3>
```

➢ VPN

Utworzyliśmy access list 120 pozwalający na bezpieczne połączenie między lokacjami dla IP 192.168.4.0 z maska 0.0.0.255 oraz dla IP 192.168.5.0 z maską 0.0.0.255




```
.nterface: Serial0/2/0
    Crypto map tag: VPN-MAP, local addr 192.168.2.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  remote  ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
  current_peer 192.168.1.1 port 500
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

    local crypto endpt.: 192.168.2.2, remote crypto endpt.:192.168.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/0
    current outbound spi: 0xDE427143(3728896323)

    inbound esp sas:
     spi: 0xF75A69D3(4149897683)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
       sa timing: remaining key lifetime (k/sec): (4525504/2810)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE
```

```
interface: Serial0/2/0
    Crypto map tag: VPN-MAP, local addr 192.168.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
   current_peer 192.168.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.2.2, remote crypto endpt.:192.168.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/0
     current outbound spi: 0xDE427143(3728896323)

     inbound esp sas:
      spi: 0xF75A69D3(4149897683)
 --More--
```

➢ Firewall

Zabezpieczenie Firewall'em sieci przed nieautoryzowanym ruchem sieciowym. Firewall blokuje kontakt do wewnątrz sieci 192.168.3.0

```
Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
 Dostep tylko dla upowaznionych

User Access Verification

Password:

R3>enable
Password:
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```