Bezpieczeństwo Sieci Komputerowych - laboratorium

Ćwiczenie 4: **Zapory ogniowe, filtrowanie ruchu**

Cel ćwiczenia: Opanowanie umiejętności konfiguracji zapory ogniowej dla małej sieci komputerowej udostępniającej usługi zewnętrzne.

Wprowadzenie

Cisco ASA jest zaporą ogniową dedykowaną dla niedużych sieci SOHO i oddziałów dużych sieci korporacyjnych. Urządzenie może być konfigurowane za pomocą CLI (przez port konsoli) lub przez interfejs www (wymaga zainstalowania aplikacji do zarządzania). ASA 5505 cechuje się następującymi parametrami:

- posiada 8 portów GI, które są portami warstwy 2 (!!!)
- umożliwia utworzenie 3 (w posiadanej licencji BASE) sieci wirtualnych w warstwie 3, porty fizyczne można przypisać do sieci VLAN.
- pracuje w oparciu o strefy bezpieczeństwa. Każdej sieci VLAN przypisuje się strefę, określoną liczbą z zakresu 0-100. Im wyższa liczba, tym 'bezpieczniejsza' strefa. Filtrowanie na podstawie stref umożliwia przesyłanie pakietów ze strefy 'bezpieczniejszej' do 'mniej bezpiecznej' i uniemożliwia przesyłanie pakietów w kierunku przeciwnym.
- umożliwia tworzenie list filtrowania ACL (podobnie jak routery Cisco). W przeciwieństwie do routerów (znanych z laboratorium 'Rozległe Sieci Komputerowe') w listach ACL używa się zwykłych (a nie 'dzikich'/wildcard) masek podsieci.
- umożliwia tworzenie tzw. 'obiektów' i 'grup obiektów' jako zbiorów adresów, sieci, portów, usług, itp. Dzięki temu np. wiele różnych podsieci IP można zgrupować w jednym obiekcie i obsługiwać jedną regułą filtrowania (nazwę obiektu/grupy a nie adres sieci podaje się w regule filtrowania).

Wymagane informacje

- Znajomość ogólnych zasad konfiguracji zapór ogniowych
- Wiedza na temat potrzeb i zasad budowy strefy DMZ
- Konfiguracja list ACL w Cisco IOS (Rozległe Sieci Komputerowe)
- Znajomość poleceń konfiguracyjnych ASA (*Dodatkowe informacje* i *Dodatek A*)
- Znajomość zasad budowy i konfiguracji sieci VPN

Dodatkowe informacje:

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/interface_start_5505.html
- http://slow7.pl/sieci-komputerowe/item/146-podstawowa-konfiguracja-cisco-asa
- https://issuu.com/gsgalezowski/docs/cisco_asa

Ćwiczenia do wykonania

- Jako zapora ogniowa skonfigurowane zostanie urządzenie Cisco ASA 5505. W ćwiczeniu wykorzystywane będą 2 komputery oraz własny laptop lub komputer na biurku prowadzącego (jako komputer w strefie zewnętrznej).
- Wykonując zadania proszę wszędzie gdzie to możliwe umieszczać **dane członków grupy** (nazwiska i numery indeksów) – w danych serwera i certyfikatach, nazwach tworzonych list ACL, plików, katalogów, kont użytkowników, treści plików, komunikatach, itp. Ich obecność na zrzutach ekranu w sprawozdaniu jest potwierdzeniem wykonania ćwiczeń.
- [ZE] oznacza konieczność umieszczenia odpowiedniego zrzutu ekranu w sprawozdaniu.
- Proszę nie ustawiać haseł ani nie zapisywać konfiguracji na ASA!

1. Połączyć się z ASA za pomocą konsoli. Wyświetlić i zapoznać się z bieżącą konfiguracją urządzenia (domyślnie brak hasła do trybu *enable* – należy nacisnąć *Enter*). Zwrócić uwagę na domyślne sieci VLAN, serwer DHCP i adresację IP. W sprawozdaniu odpowiedzieć na pytanie: do jakich VLAN są domyślnie przypisane fizyczne porty urządzenia ?
   Zmienić nazwę urządzenia podając w niej nazwiska członków grupy [ZE].
2. Zbudować sieć zgodnie z rys. 1, podłączając sieć w pracowni do odpowiedniego prekonfigurowanego portu zapory. W razie potrzeby skonfigurować na komputerach ‘ręcznie’ adres serwera DNS.

Rys. 1. Schemat połączeń w zadaniu 2.

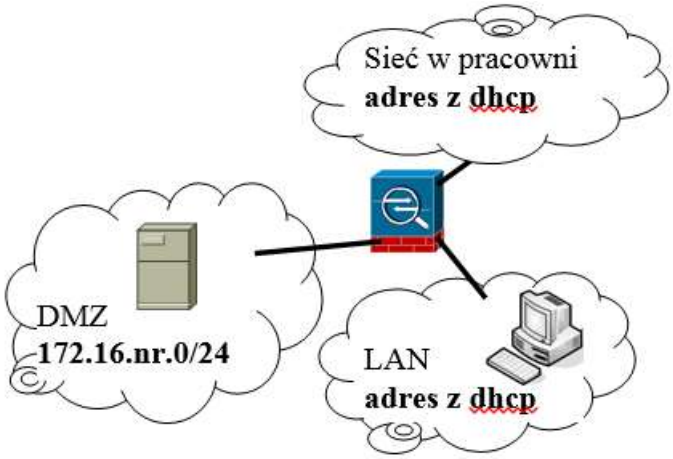
Czy z serwera LAN jest dostęp do następujących usług: serwerów WWW w Internecie, serwera DNS (program *nslookup* i tłumaczenia nazw w przeglądarce), serwerów w sieci pracowni (np. FTP), czy można 'pingować' i badać trasę (tracert) do poprzednio wymienionych serwerów i komputerów w pracowni ? Jeśli któreś z wymienionych nie działa proszę (w sprawozdaniu) wyjaśnić przyczynę.

Utworzyć 2 konta dla administratorów [ZE].

3. Skonfigurować na zaporze reguły [ZE]:
   - pozwalającą na powracające odpowiedzi ICMP, aby z komputerów można było 'pingować' i śledzić trasę do serwerów w Internecie (można dodać regułę acl lub akcje w obiekcie *policy-map*),
   - blokującą protokół ftp z sieci LAN,
   - blokującą sieci LAN dostęp do eportalu (156.17.70.219).

   Zweryfikować działanie reguł. Zgłosić prowadzącemu. Odpowiednie fragmenty pliku konfiguracji oraz wyniki komendy wyświetlającej reguły zamieścić w sprawozdaniu.
4. Podłączyć i skonfigurować urządzenia zgodnie z rys. 2:
   - Strefa DMZ ma zostać zbudowana na porcie 0/7, z poziomem bezpieczeństwa 50. Adresy przypisywane ręcznie. Translacja statyczna (1:1) na zaporze - o adres zewnętrzny poprosić prowadzącego [ZE].
   - Konfiguracja strefy LAN pozostaje jak w poprzednim zadaniu.
   - Usunąć z zapory reguły skonfigurowane w ćw. 3.
   - Na serwerze w DMZ uruchomić usługi: WWW, FTP, Telnet/SSH a także umożliwić odpowiadanie na ping (odpowiednio skonfigurować lub wyłączyć zaporę osobistą). Przetestować działanie usług (lokalnie - do 'samego siebie') .

- Podobnie uruchomić serwer ftp i umożliwić odpowiedzi na *ping* na komputerze w LAN.



Rys. 2. Schemat połączeń w zadaniu 4.

Jako komputer w '*Sieci pracowni*' zostanie użyty komputer na biurku prowadzącego (lub można podłączyć i użyć własny komputer).

5. Skonfigurować na zaporze regułę dostępu do serwera w DMZ [ZE]:
   - Umożliwić dostęp z zewnątrz (z '*Sieci w pracowni*') do strefy DMZ dla ping oraz jednej z do usług: WWW, FTP lub Telnet. Pozostałe usługi mają być blokowane. Regułę należy przypisać jako wejściową dla interfejsu zewnętrznego (od strony '*Sieci w pracowni'*).

   Zweryfikować działanie reguł. W sprawozdaniu zamieścić odpowiednie fragmenty pliku konfiguracji i wyniki komend wyświetlających reguły i statystyki ich użycia. Zgłosić prowadzącemu.
6. Skonfigurować na zaporze bramę VPN, umożliwiającą nawiązywanie połączeń z siecią LAN (VPN typu *client-to-side / remote-access*) – opis w dodatku B. Przetestować działanie z komputera w '*Sieci ćw. ASA*' - klient Cisco AnyConnect. Po nawiązaniu połączenia połączyć się z komputerem LAN za pomocą ping i ftp [ZE].
   Zgłosić prowadzącemu.

Sprawozdanie

Zamieścić zrzuty ekranu, fragmenty pliku konfiguracji zapory, komentarze i odpowiedzi na pytania, itp.

Ocena

Wyznaczona na podstawie zrealizowanych ćwiczeń oraz sprawozdania.

Dodatek A – komendy Cisco ASA

show int ip brief // wyświetlenie adresów IP (uwaga: inna składnia/kolejność opcji niż na routerach i przełącznikach)
show ip address
show switch vlan
show route
username Nowak secret Nowak12345
write erase // usunięcie konfiguracji startowej (odpowiednik *erase startup-config*)
nameif inside // nadawanie nazwy interfejsowi (w trybie konfiguracji interfejsu)

route outside 0.0.0.0 0.0.0.0 192.168.111.111 // zdefiniowanie trasy domyślnej (podany adres next-hop jest **przykładowy**)

konfiguracja strefy (vlan'u) DMZ:
ASA(config)#interface vlan 3
ASA(config-if)# ip address <adres> <maska>
ASA(config)# no forward interface vlan 1 (ze względu na ograniczenia licencji akademickiej typu *Base*, nie będzie możliwości dostępu z LAN do DMZ)
ASA(config)#nameif dmz
ASA(config)#security-level 35
ASA(config)#no shutdown
(następnie należy przypisać wybrane porty do utworzonego vlan'u)

konfiguracja NAT (dla serwera w strefie DMZ):
ASA(config)# object network STREFA_DMZ //ostatni parameter to nazwa obiektu
ASA(config-network-object)# host 172.16.1.5
ASA(config-network-object)# nat (inside,outside) static <adres_IP_zewnętrzny>
ASA(config-network-object)# end

show xlate // lista przekonwertowanych adresów

konfiguracja DHCP:
dhcpd address 192.168.1.5-192.168.1.100 inside // konfiguracja dhcp dla urządzeń w vlanie 'inside'
dhcpd enable inside // uruchomienie usługi (demona) dhcp

Włączenie zapory z badaniem stanów:

1. Utworzyć obiekt *class-map*. Obiekt definiuje kryterium dopasowania pakietów do reguł. *default-inspection-traffic* to reguła dopasowująca kilkanaście dobrze znanych portów (m.in. http, icmp, ftp…)
   ASA(config)# class-map INSPEKCJA
   ASA(config-cmap)#match default-inspection-traffic
2. Utworzyć obiekt *policy-map*. Obiekt przypisuje działanie poszczególnym kryteriom dopasowania. Opcja *inspect <usługa>* powoduje uruchomienie badania stanów dla *usługi* (np. http, icmp).
   ASA(config)#policy-map POLISA
   ASA(config-pmap)#class INSPEKCJA
   ASA(config-pmap-c)#inspect http
   ASA(config-pmap-c)#inspect icmp

3. Dołączyć polisę do konkretnego interfejsu lub włączyć dla wszystkich (globalnie) za pomocą komendy *service-policy.*
   ASA(config)# service-policy POLISA global

Konfiguracja list ACL (jak na RSK):

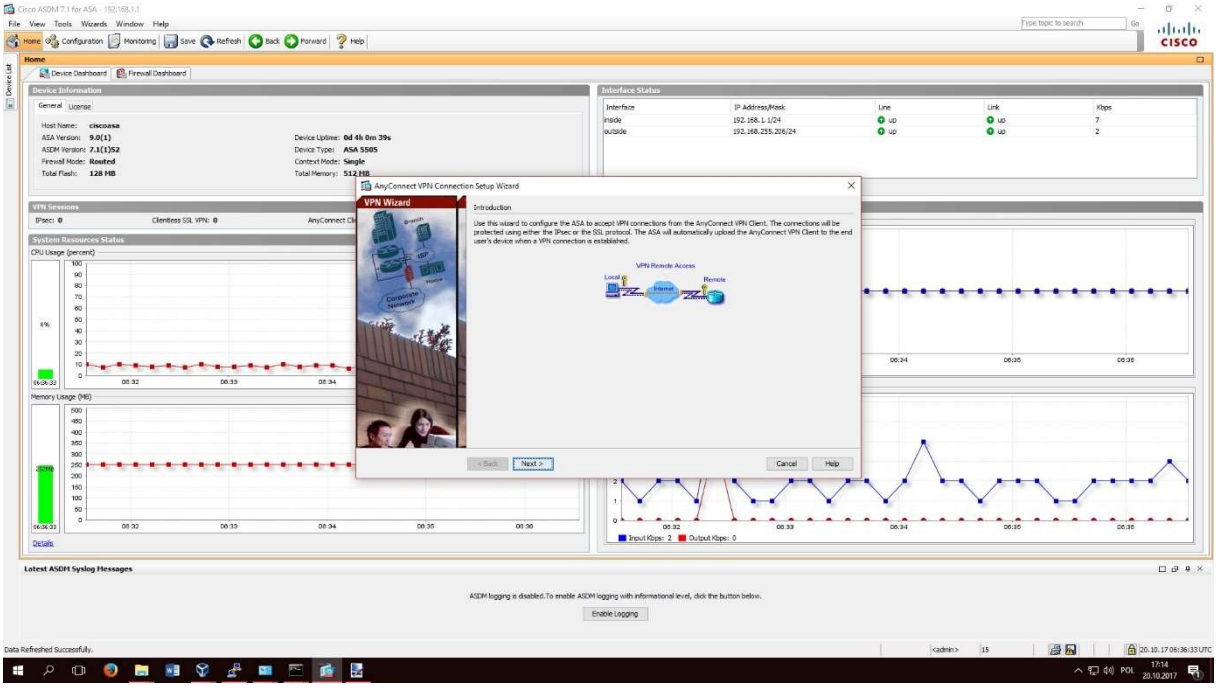
1. utworzyć listę ACL
   ASA(config)# access-list ZAKAZ_ICMP deny icmp any 172.16.49.0 255.255.0.0
2. Przypisać ją do interfejsu i kierunku (wejściowa lub wyjściowa), można wykorzystać nazwy interfejsów zdefiniowane komendą *nameif*.
   ASA(config)# access-group ZAKAZ_ICMP in interface outside

Konfiguracja NAT dla serwera w strefie DMZ

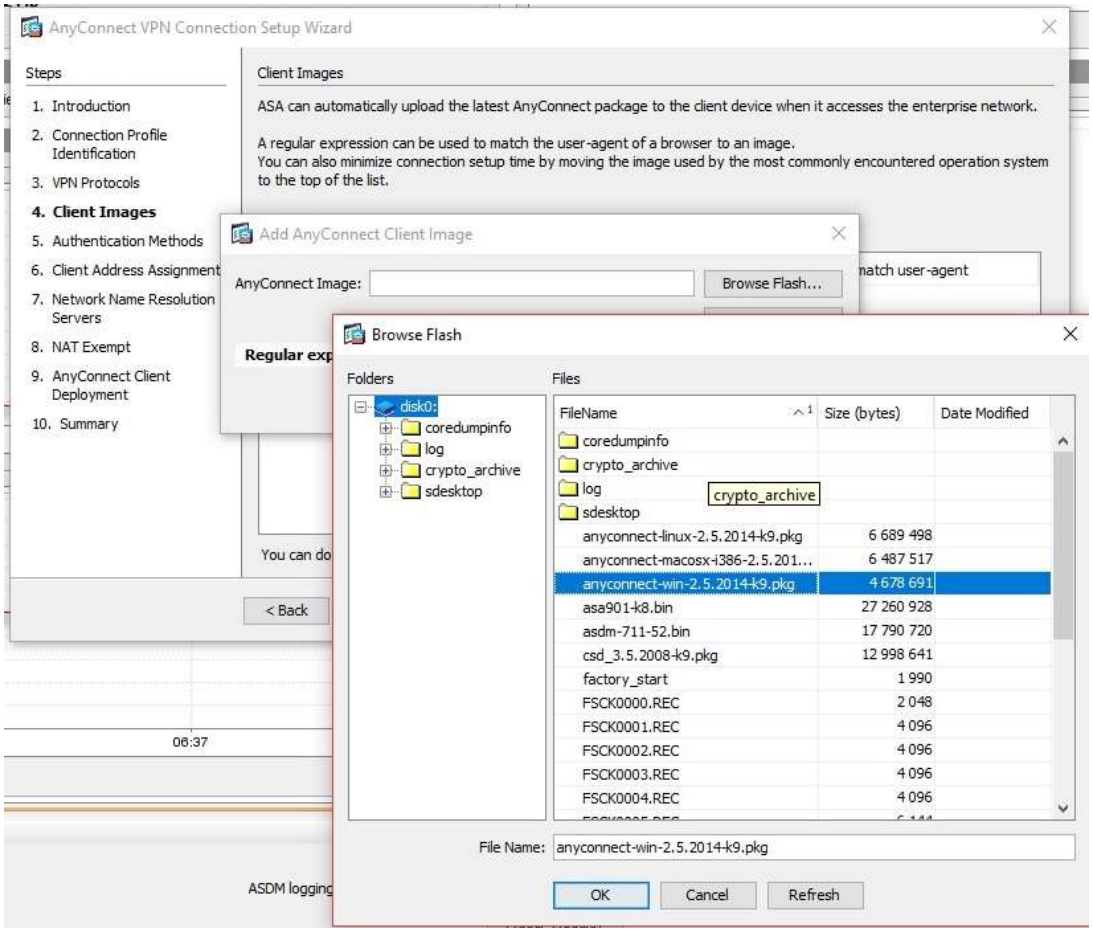
ASA(config)#object network strefa_dmz
ASA(config-network-object)# host <adres-ip-serwera-dmz>
ASA(config-network-object)# nat (dmz,outside) static <adres-zewnętrzny>

Dodatek B – konfiguracja AnyConnect VPN za pomocą Wizarda

- Zainstalować dm-launcher.msi – aplikację do zarządzania zaporą ASA przez interfejs graficzny. Połączyć się z zaporą i zalogować na uprzednio założone konto.
  Wybrać *Wizards > VPN Wizards > AnyConnect VPN Wizard*
  Next

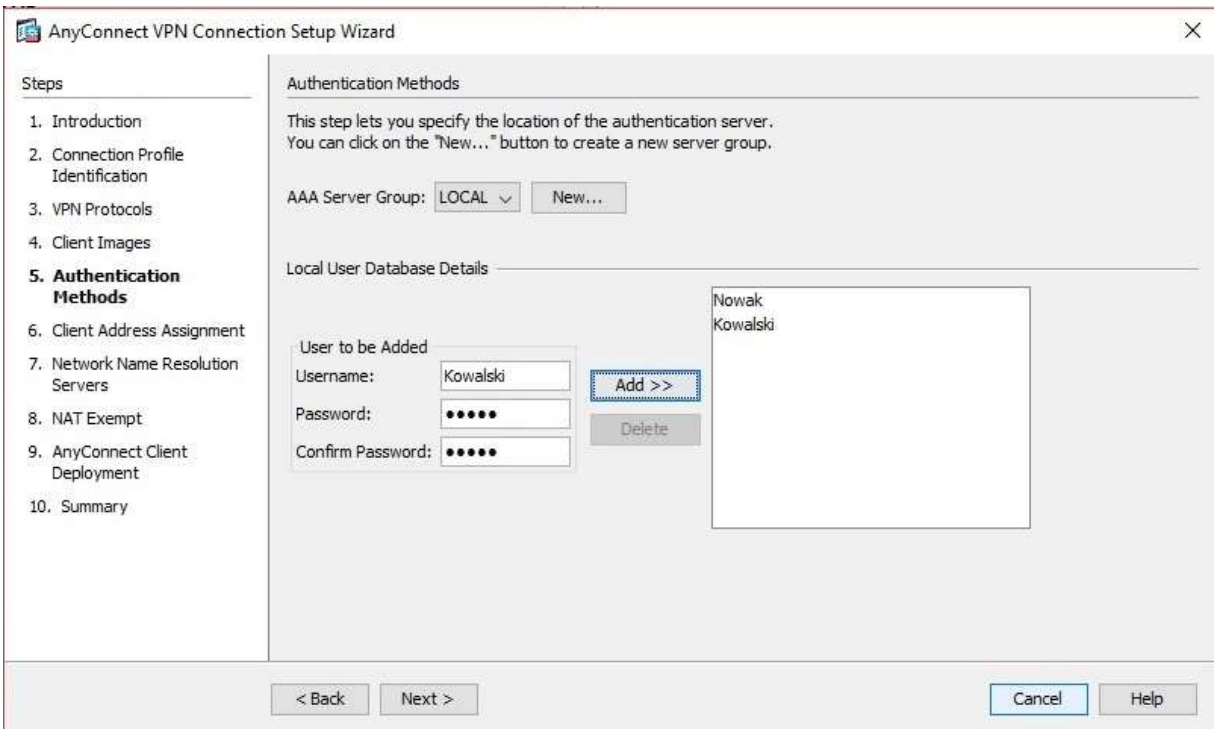


- Podać nazwę profilu, zaznaczyć ‘outside’ jako interfejs dostępowy VPN. *Next*
- Zaznaczyć SSL (lub odznaczyć IPSec), nie wybierać certyfikatu. *Next*
- Wybrać odpowiedni obraz serwera VPN dla klientów Windows
  (plik o nazwie ***anyconnect-win-2.5.2014-k9.pkg*** lub podobnej, znajdujący się w pamięci zapory)



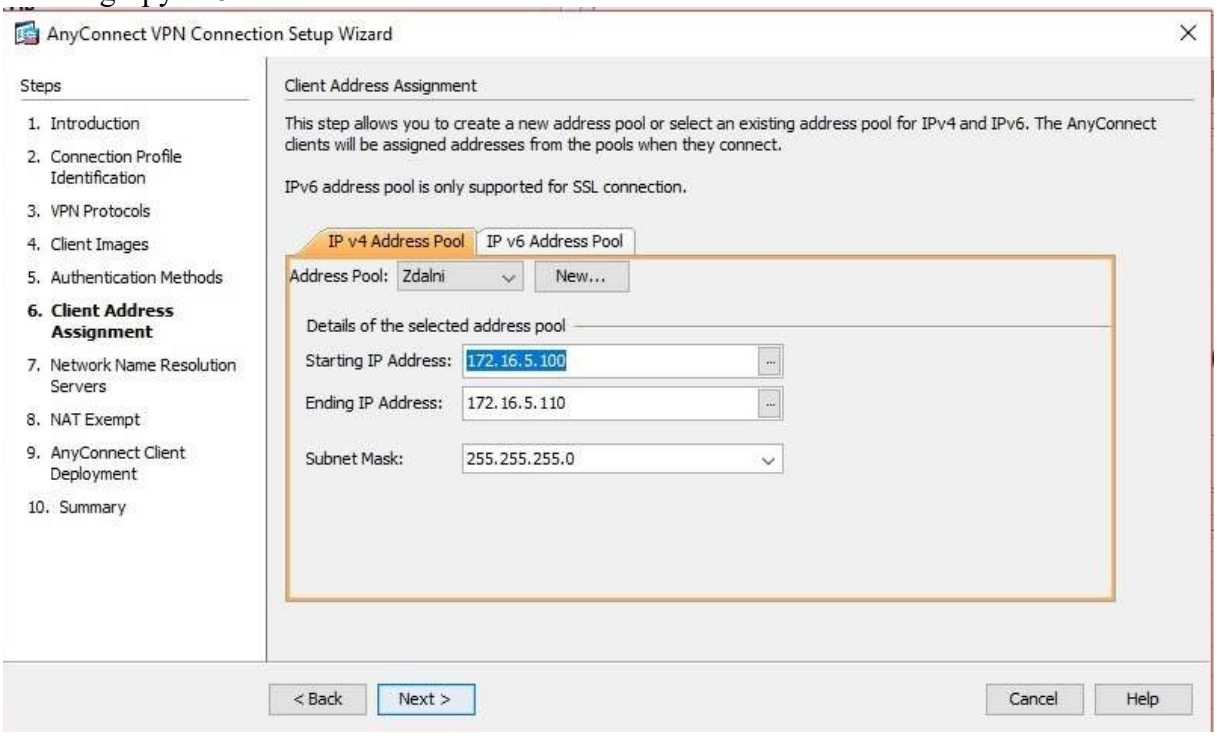
Next

- Upewnić się, że parametr ‘AAA Server Group’ na wartość ‘LOCAL’ – do uwierzytelniania zdalnych użytkowników ma zostać użyta lokalna baza danych. Utworzyć konta z hasłami dla dwóch zdalnych użytkowników.



Next

- Klientom zdalnym zostaną przypisane adresy IP z podsieci lokalnej. W kroku 6 należy określić, jakie adresy wolno im przydzielać (nie powinny być wykorzystywane w sieci lokalnej, np. być w puli serwera DHCP). Na rysunku poniżej przykład z pulą adresów grupy nr 5.



Next

- Podać dowolne dane w '*DNS Servers*' i „*Domain Name*' (w ćwiczeniu nie są wykorzystywane nazwy DNS). *Next*
- Zaznaczyć 'Exempt VPN traffic from network address translation'. Pozostawić domyślne wartości '*Inside Interface*' (***inside***) i '*Local Network'* (***any4***). *Next*
- *Next -> Finish*
- Uzyskiwania zdalnego dostępu:
    - z komputera prowadzącego – klient AnyConnect powinien być zainstalowany, podać adres i dane użytkownika (zatwierdzić wyjątek bezpieczeństwa).
    - z dowolnego komputera: połączyć się przeglądarką z 'zewnętrznym' portem routera, po zalogowaniu pobrać instalator klienta Any Connect. Zainstalować, połączyć się jak w poprzednim punkcie.