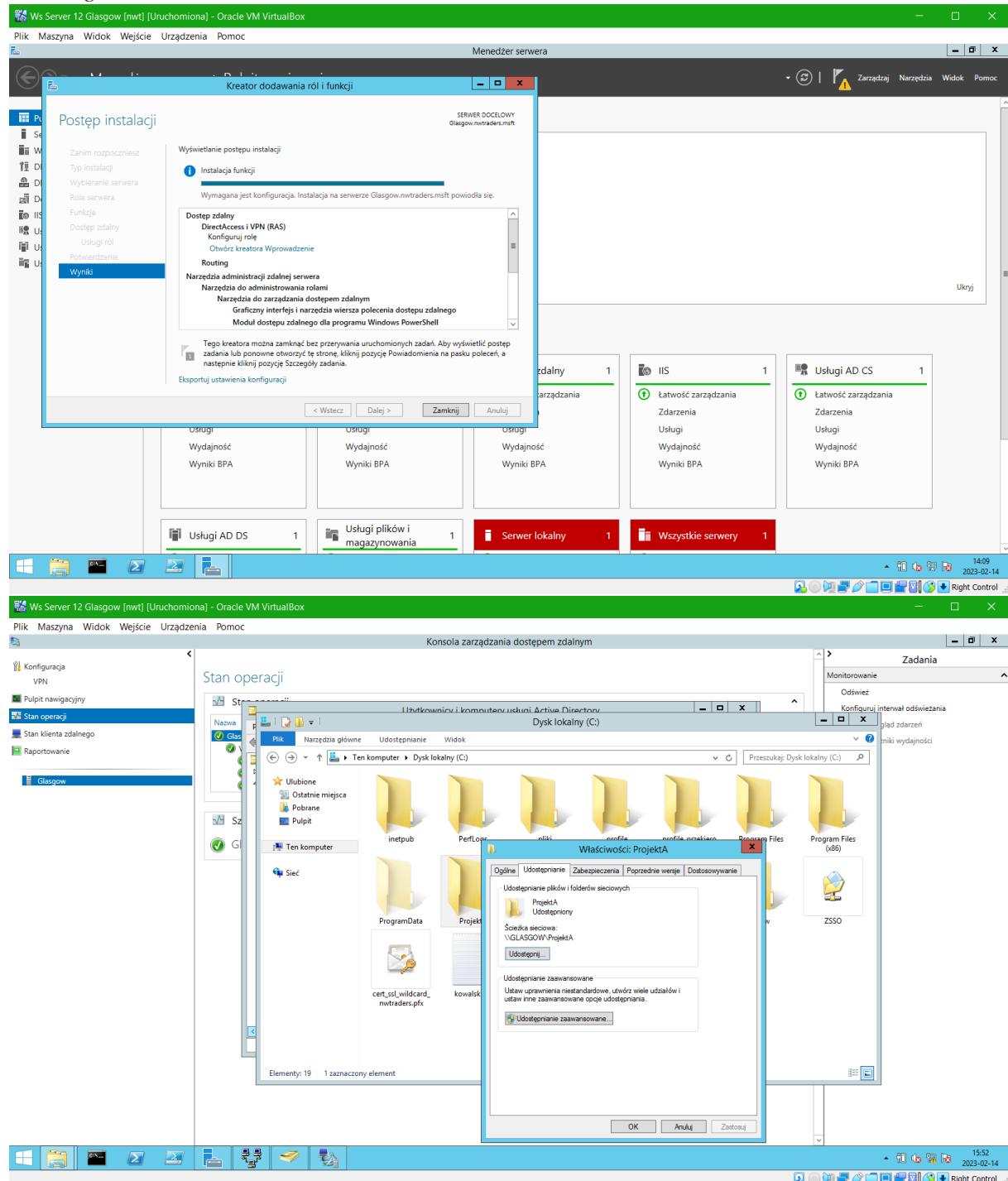
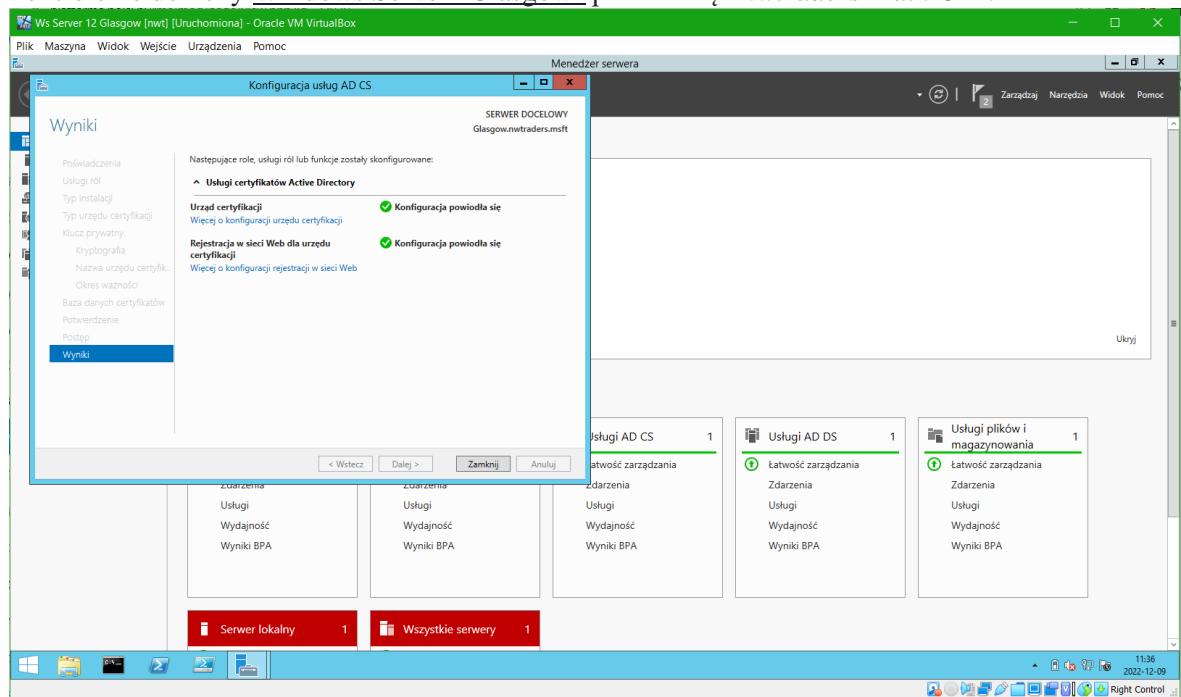


Laboratorium realizowane na zajęciach (Moduł 6) – Kryptograficzne metody ochrony informacji

Udostępnić w systemie Windows Server "Glasgow" udział sieciowy o nazwie "wspolny" dostępny dla wszystkich pracowników oraz zainstalować rolę dostępu zdalnego i aktywować w niej usługę "Routing LAN".



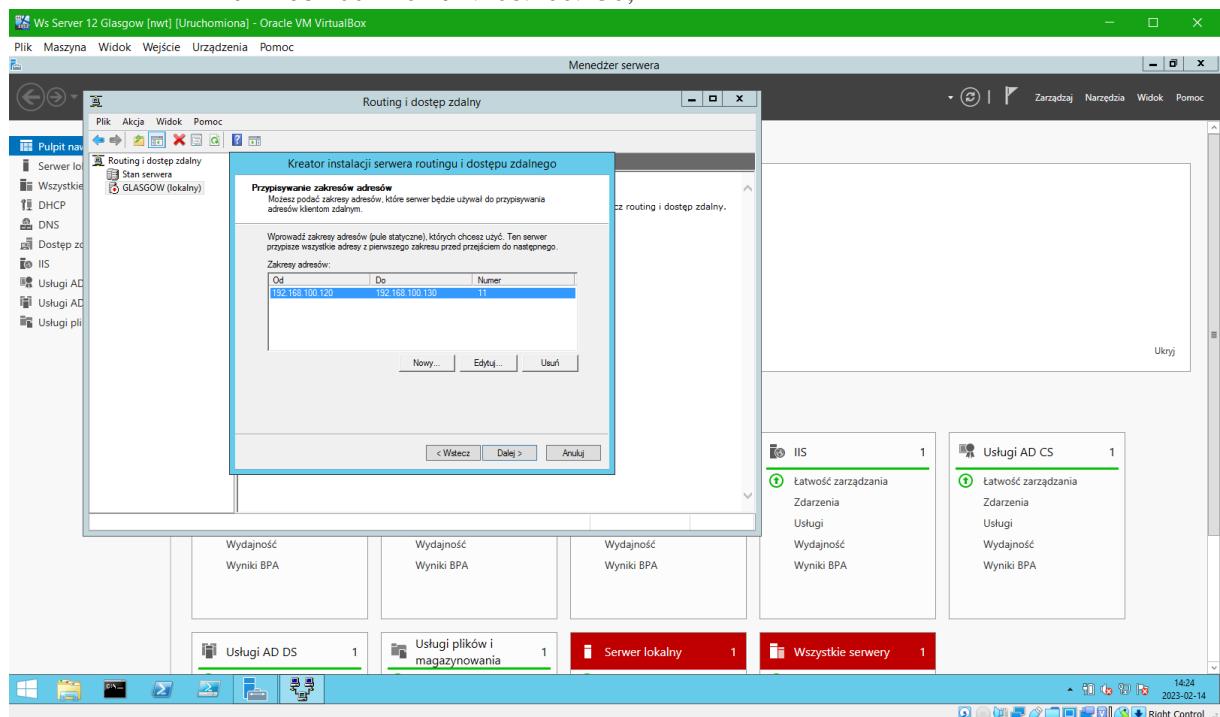
Wdrożyć lokalną infrastrukturę klucza publicznego zintegrowaną z usługą Active Directory, na kontrolerze domeny Windows Server "Glasgow" pod nazwą "Nwtraders Main CA".



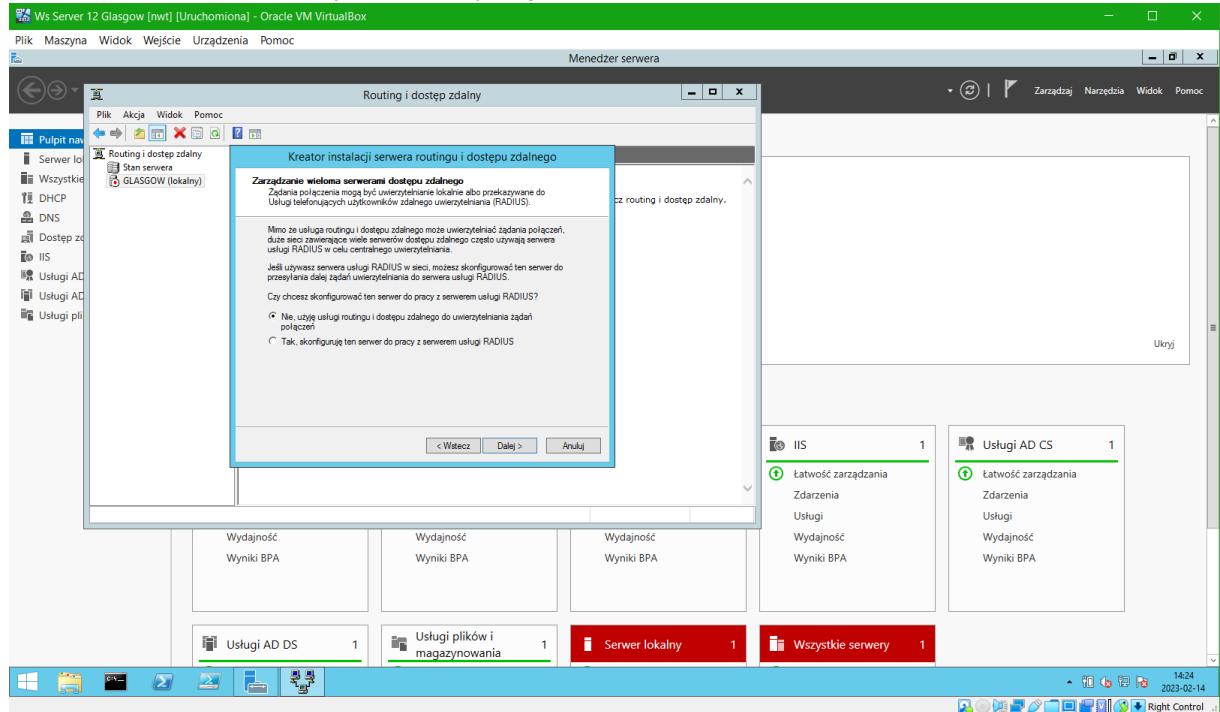
Zadanie 1

Zainstalować server VPN w systemie Windows Server "Glasgow":

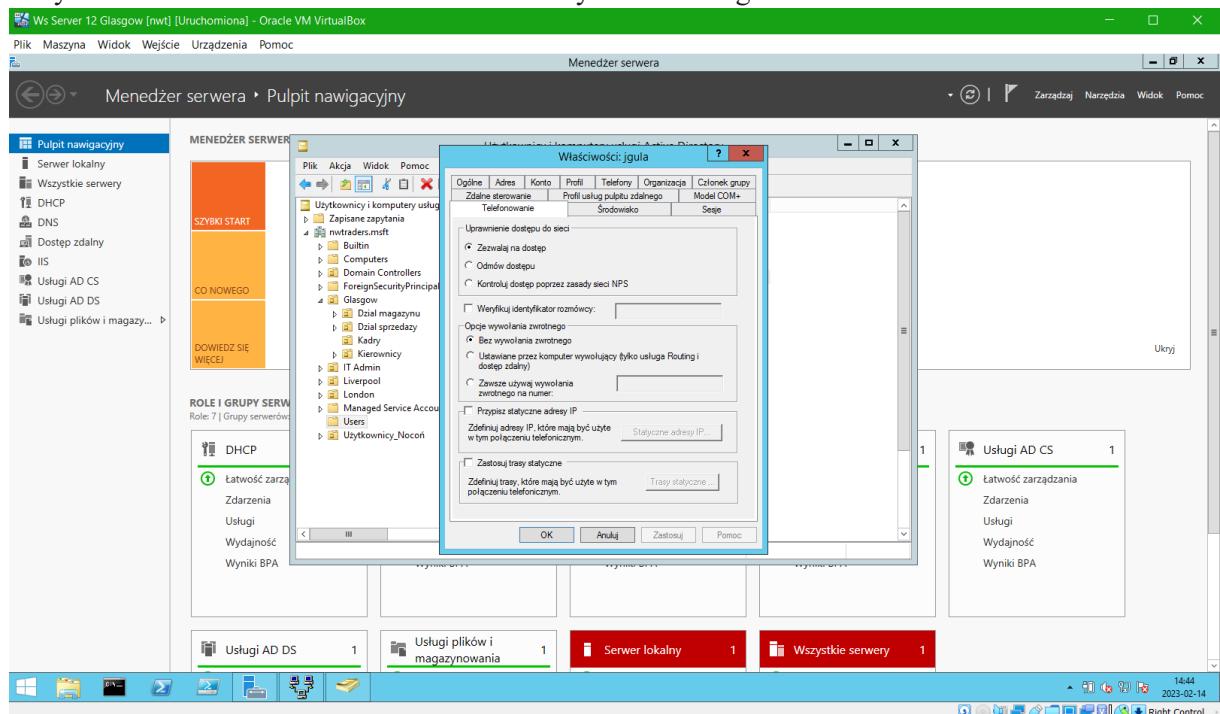
- klientom łączącym się poprzez VPN adresy IP przydzielać ma sam serwer VPN z określonego zakresu adresów: 192.168.100.120-192.168.100.130;



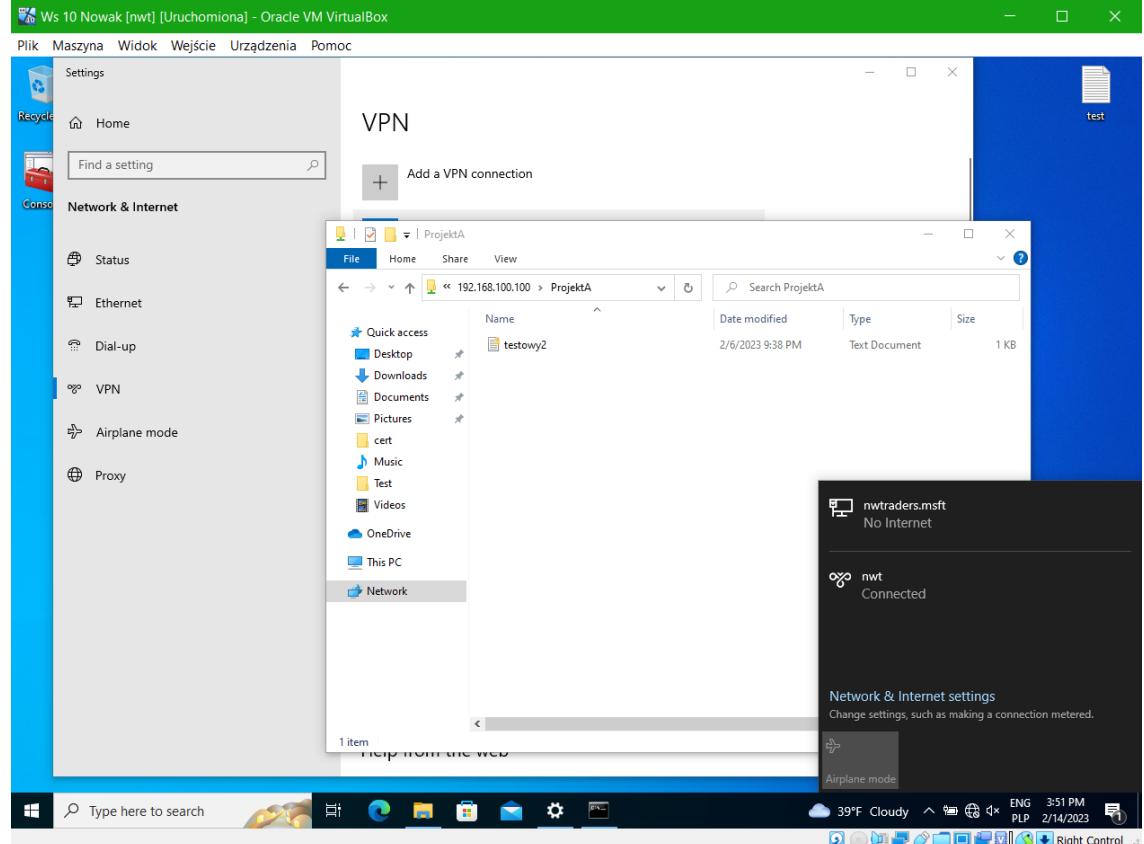
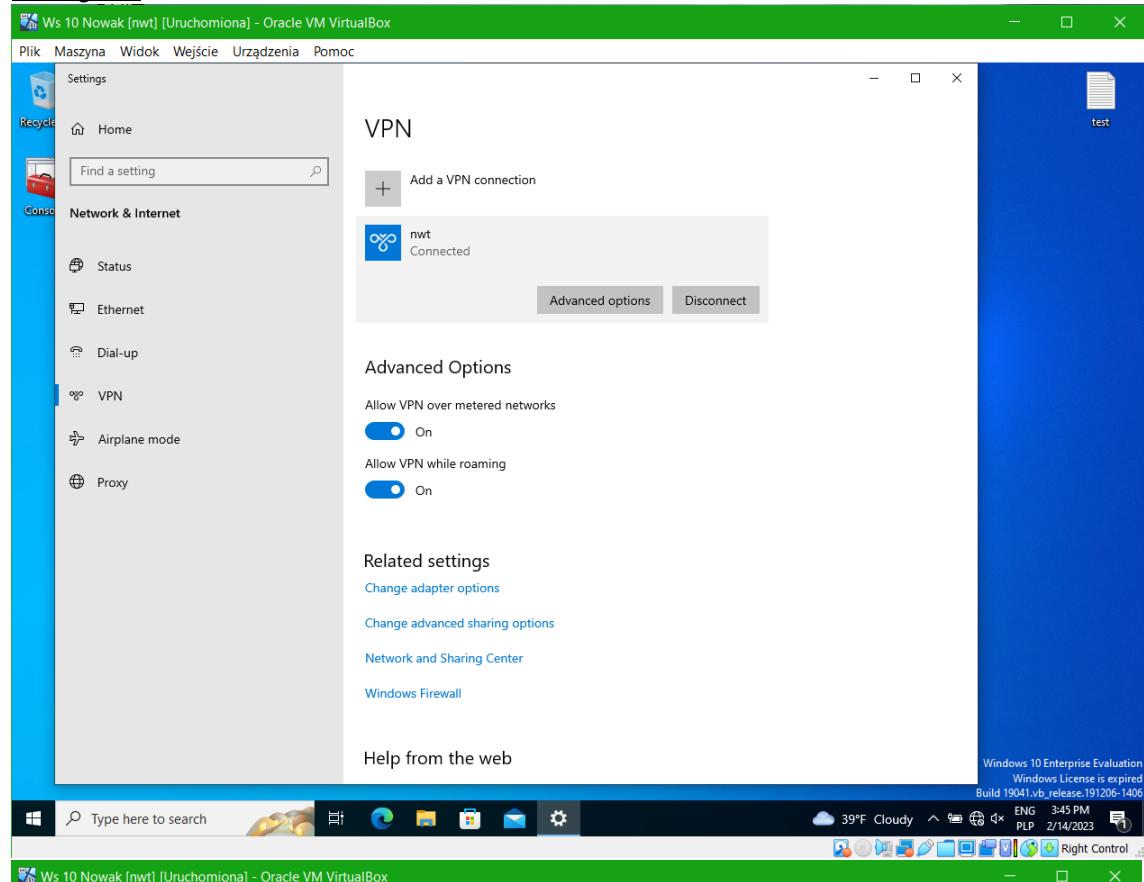
- serwer VPN nie będzie używać autentykacji RADIUS.



Aktywować J. Guli działu Kadr możliwość korzystania z usługi VPN.

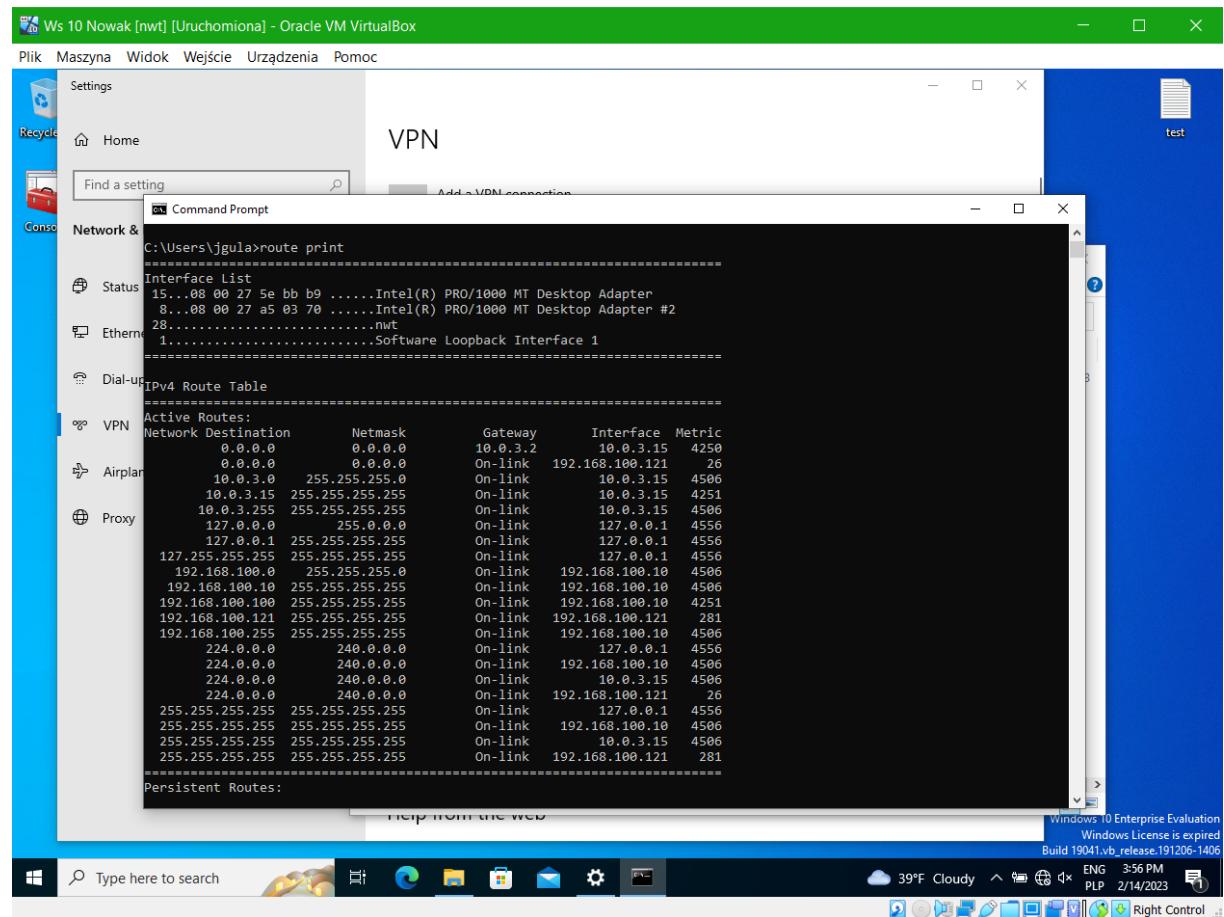


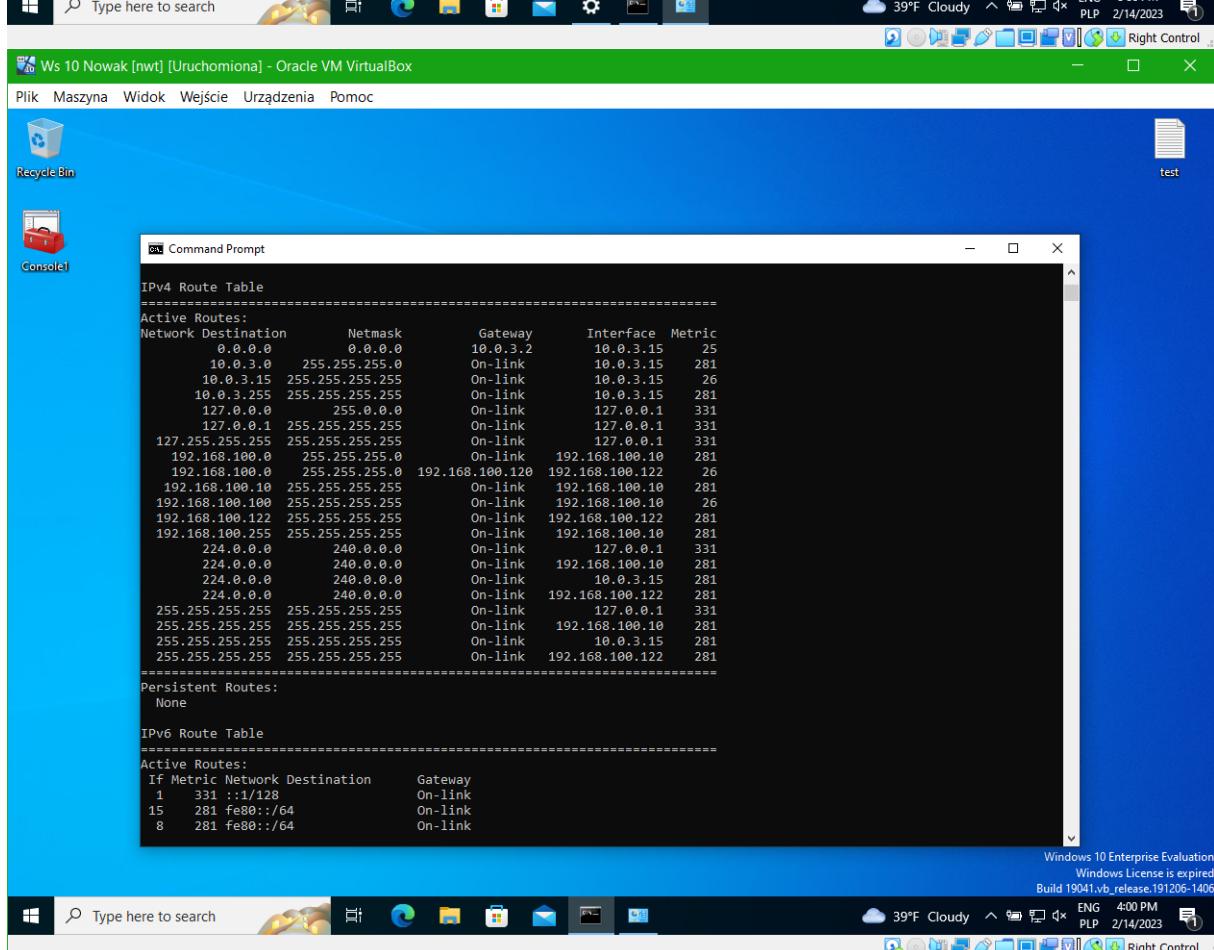
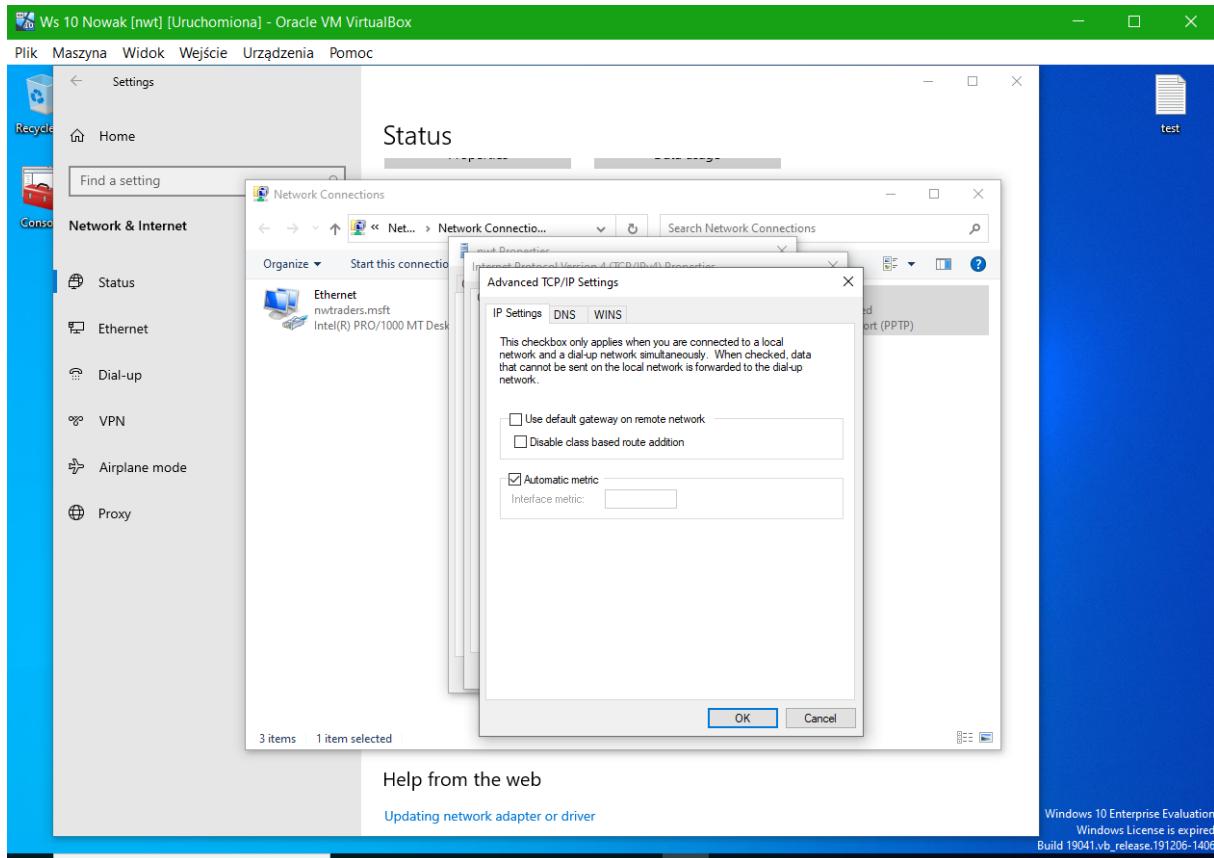
Skonfigurować w laptopie J. Guli z systemem Windows "Nowak" połączenie VPN do zainstalowanego serwera VPN i zweryfikować jego prawidłowe działanie próbując uzyskać poprzez serwer VPN dostęp do udziału sieciowego //192.168.100.100/wspolny w systemie Windows Server "Glasgow".



Zadanie 2

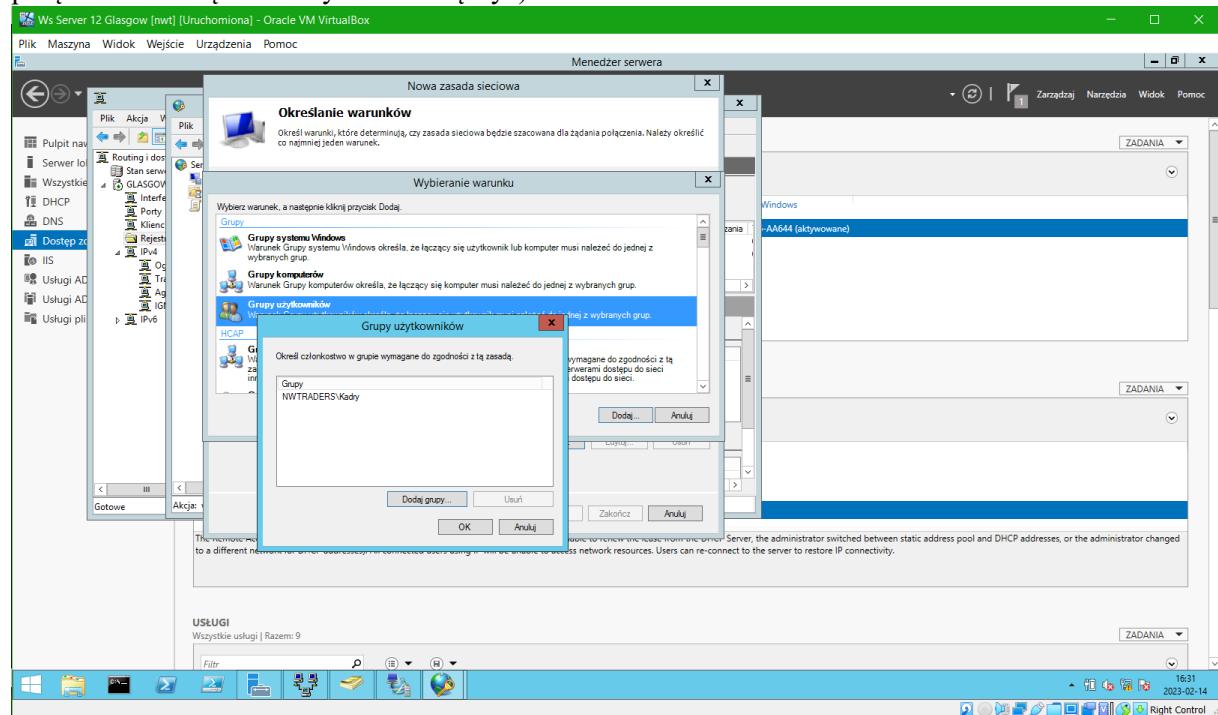
Usunięcie w kliencie VPN na laptopie J. Guli korzystania z bramy w sieci zdalnej firmy przez tegoż klienta VPN.

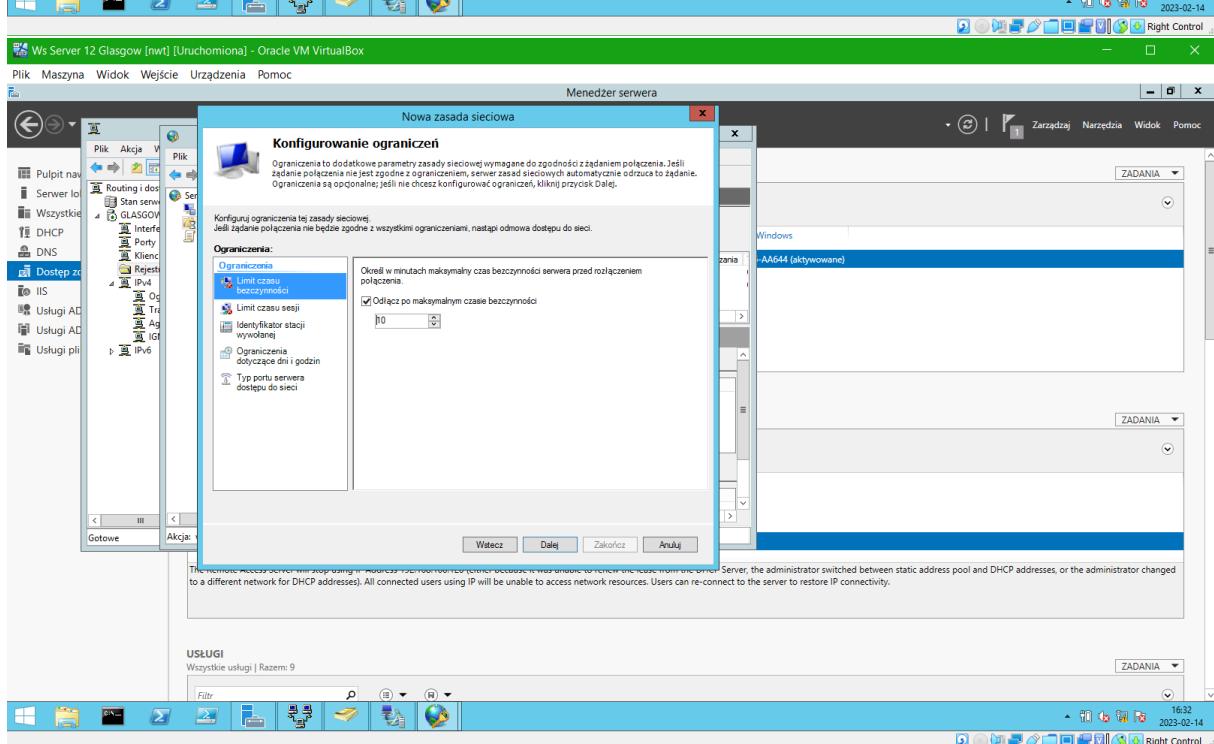
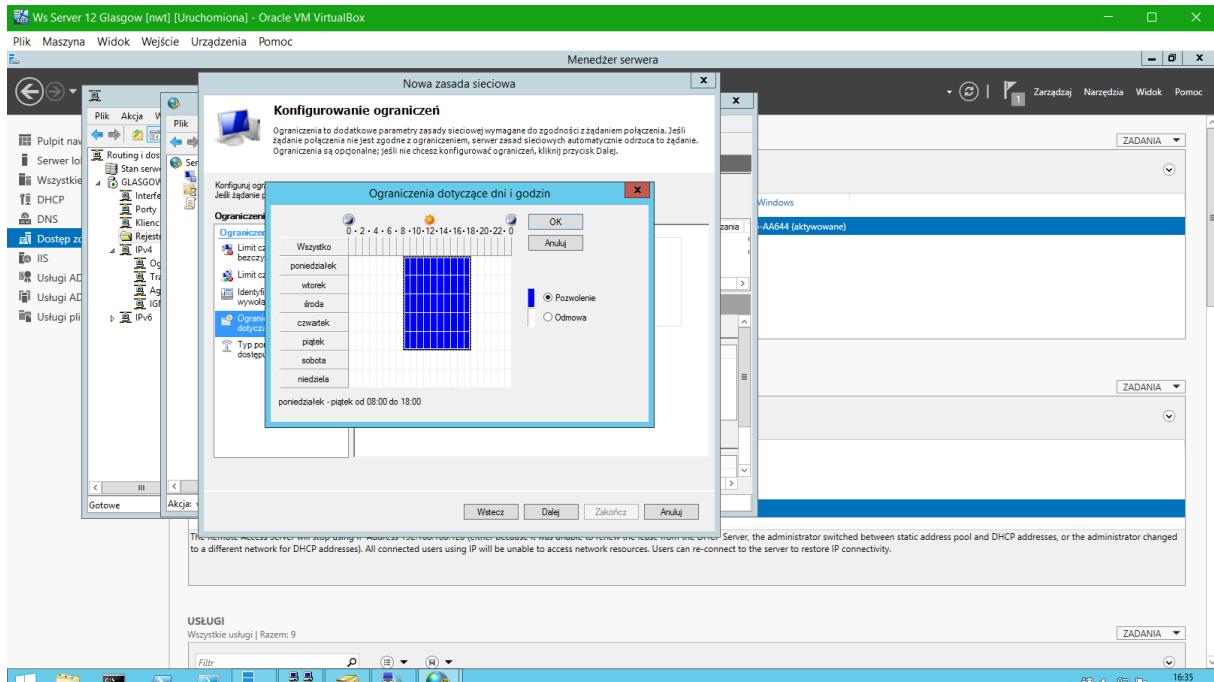




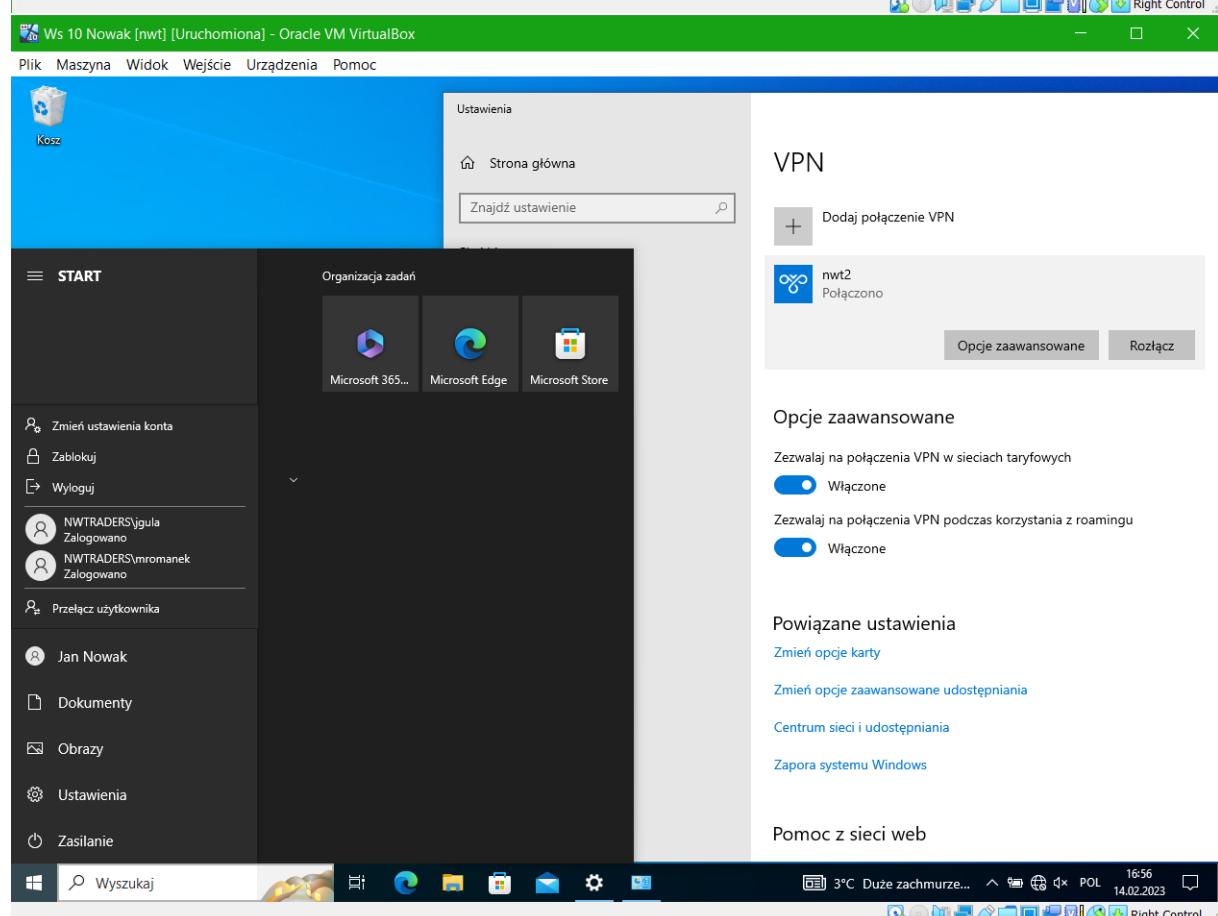
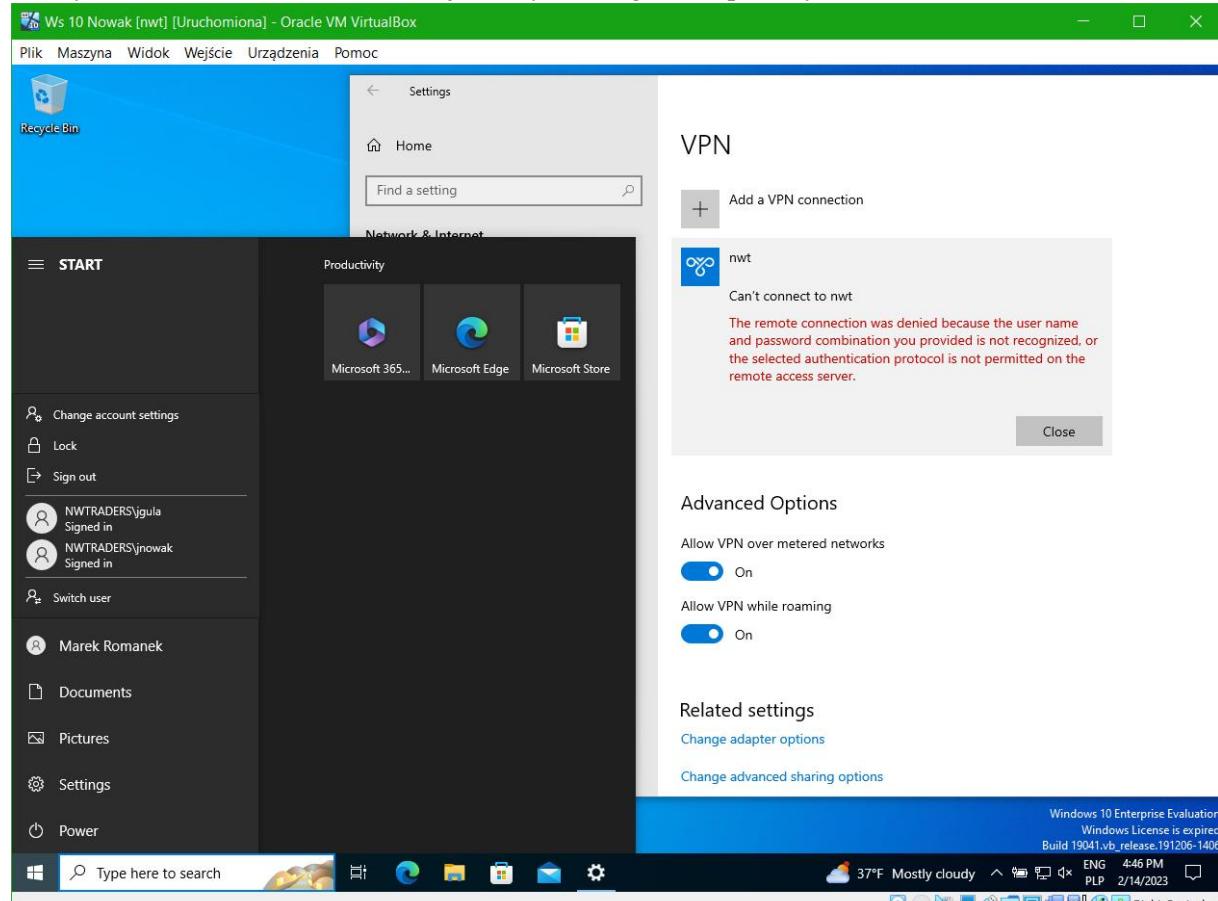
Zadanie 3

Utworzyć nową zasadę dostępu zdalnego o nazwie "kadry" obowiązującą tylko użytkowników należących do grupy zabezpieczeń o nazwie "kadry" i obejmującą ograniczenia: połączenie z serwerem VPN możliwe tylko w godzinach od 8:00 do 18:00 w dni powszednie (jeżeli połączenie VPN będzie bezzczynne (nie będzie żadnej transmisji danych poprzez to połączenie) przez 10 minut, to połączenie ma się automatycznie rozłączyć).



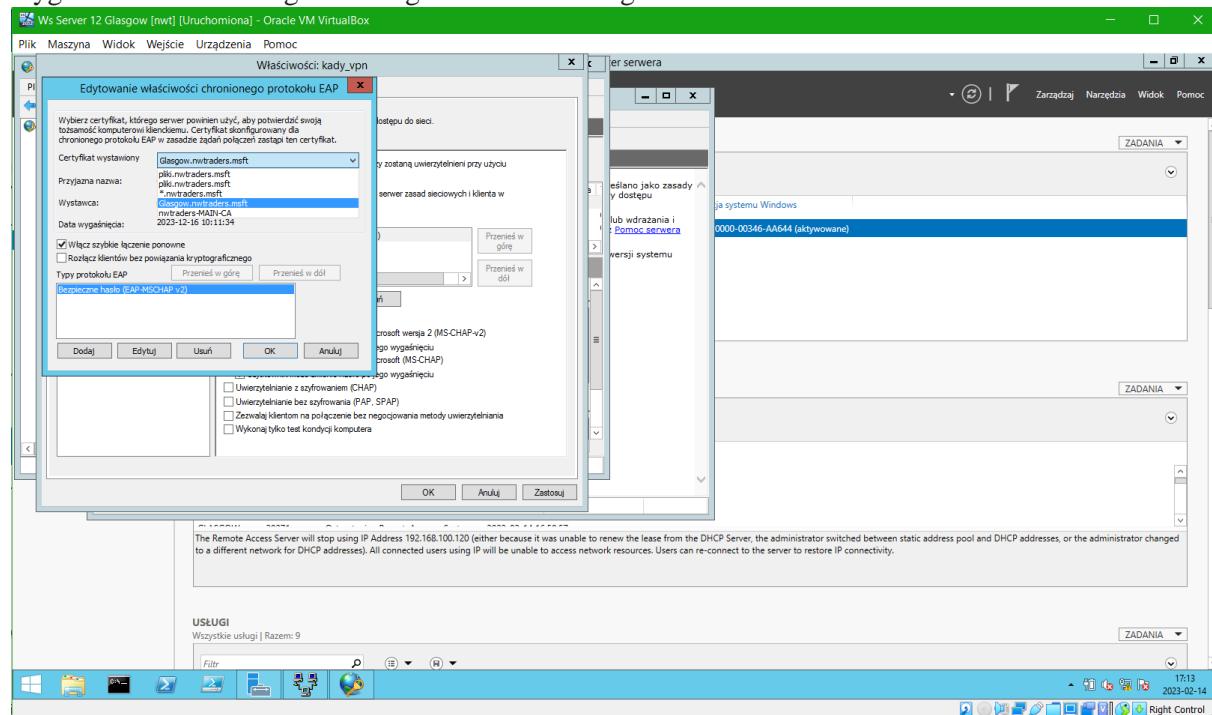


Zweryfikowanie działania utworzonej zasady zdalnego dostępu w systemie Windows "Nowak".

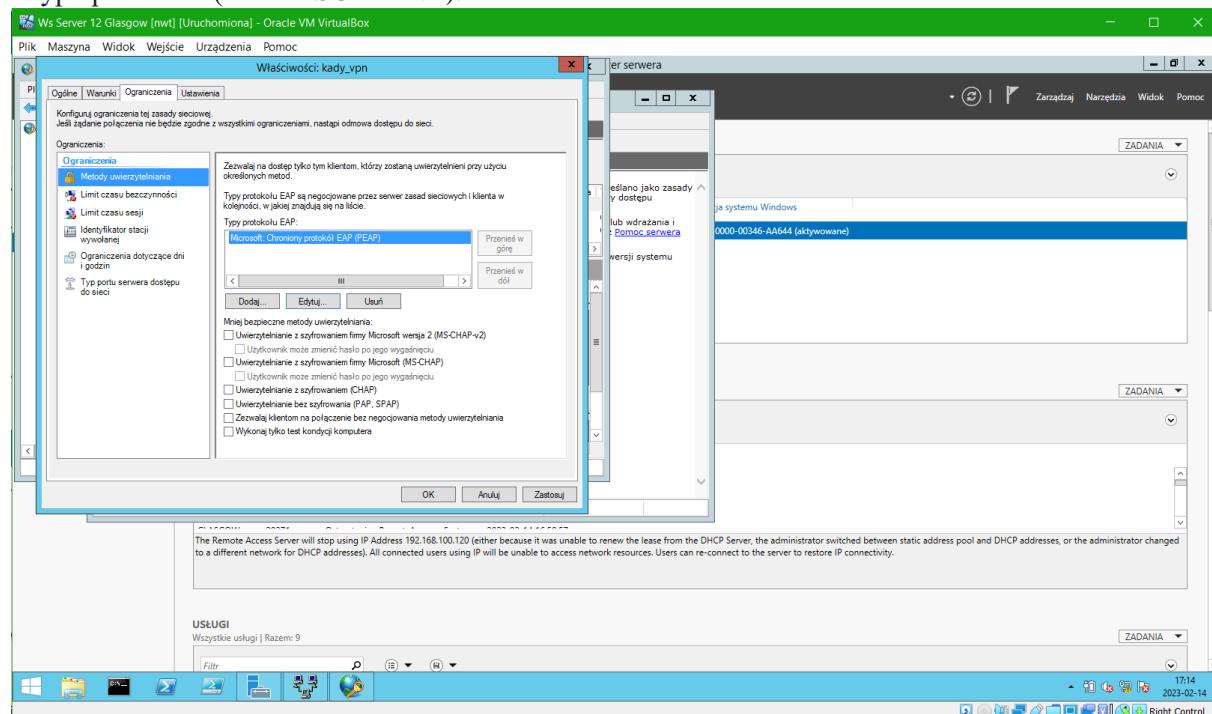


Zadanie 4

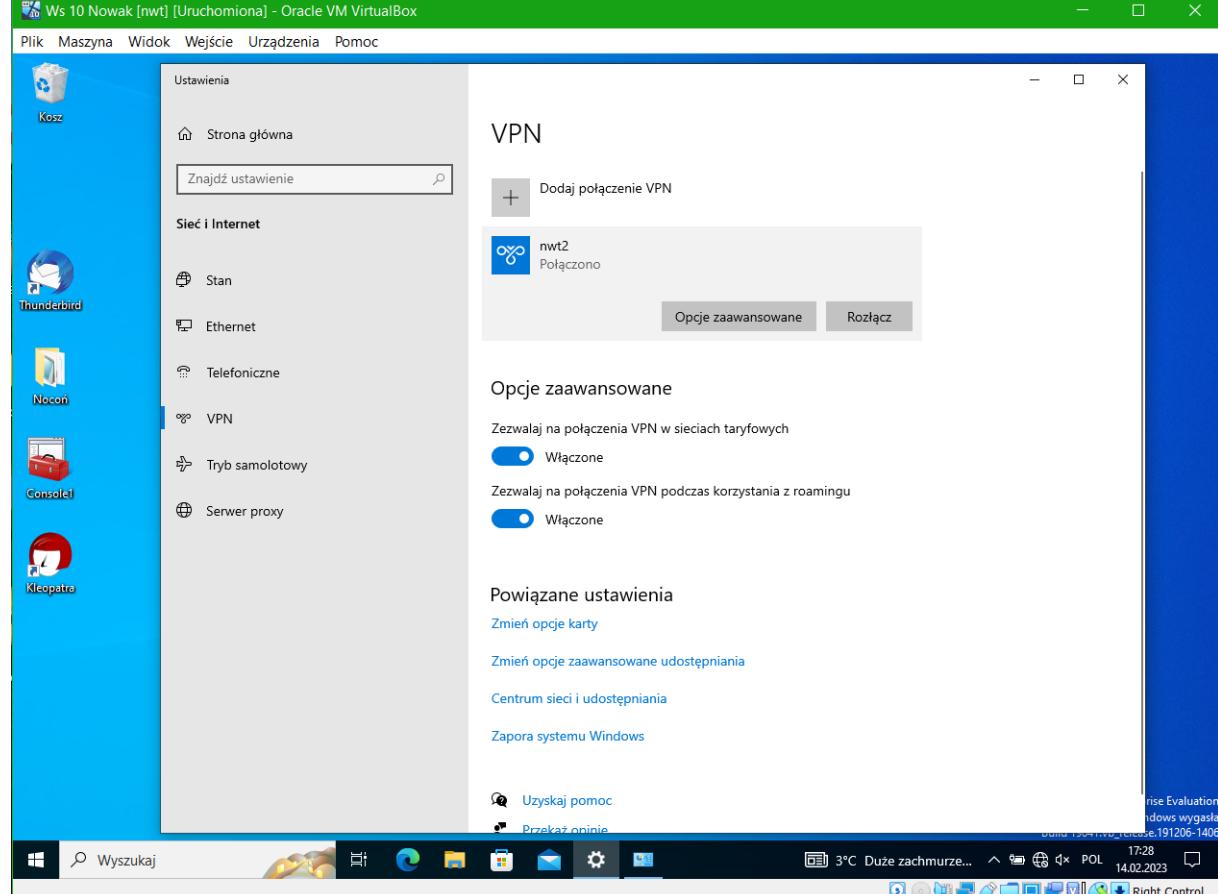
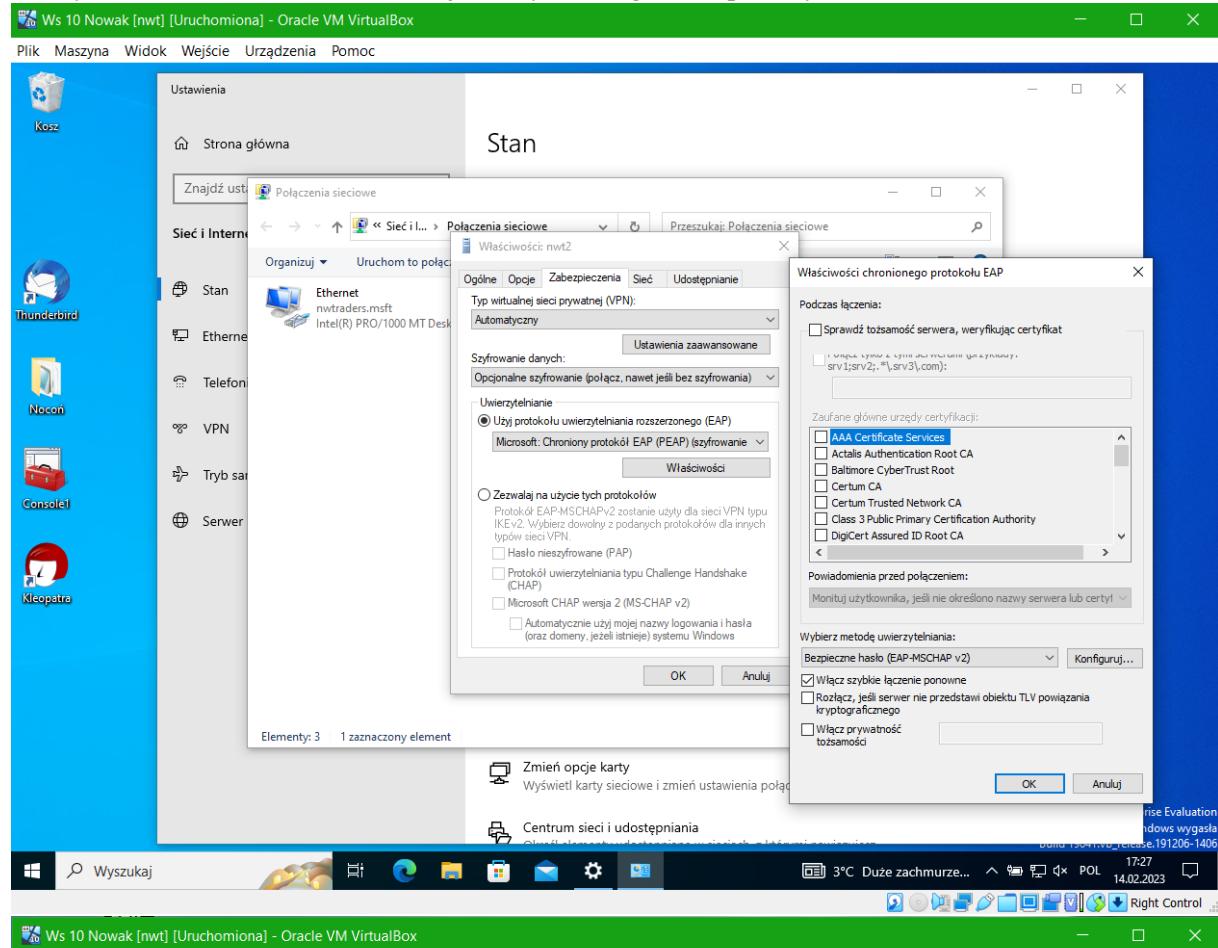
Sprawdzenie w systemie **Windows Server "Glasgow"**, czy serwer ma wygenerowany certyfikat "komputera" dla adresu domenowego wykorzystywanego do połączeń z usługą VPN, jeżeli nie ma, to wygenerowanie dla niego takowego o nazwie "Glasgow.nwtraders.msft".



Zmodyfikowanie zasady dostępu zdalnego o nazwie "kadry", zmieniając w ramach ograniczeń stosowaną metodę uwierzytelniania na "Chroniony protokół EAP (PEAP)", który z kolei ma korzystać z typu protokołu (EAP-MSCHAP v2).

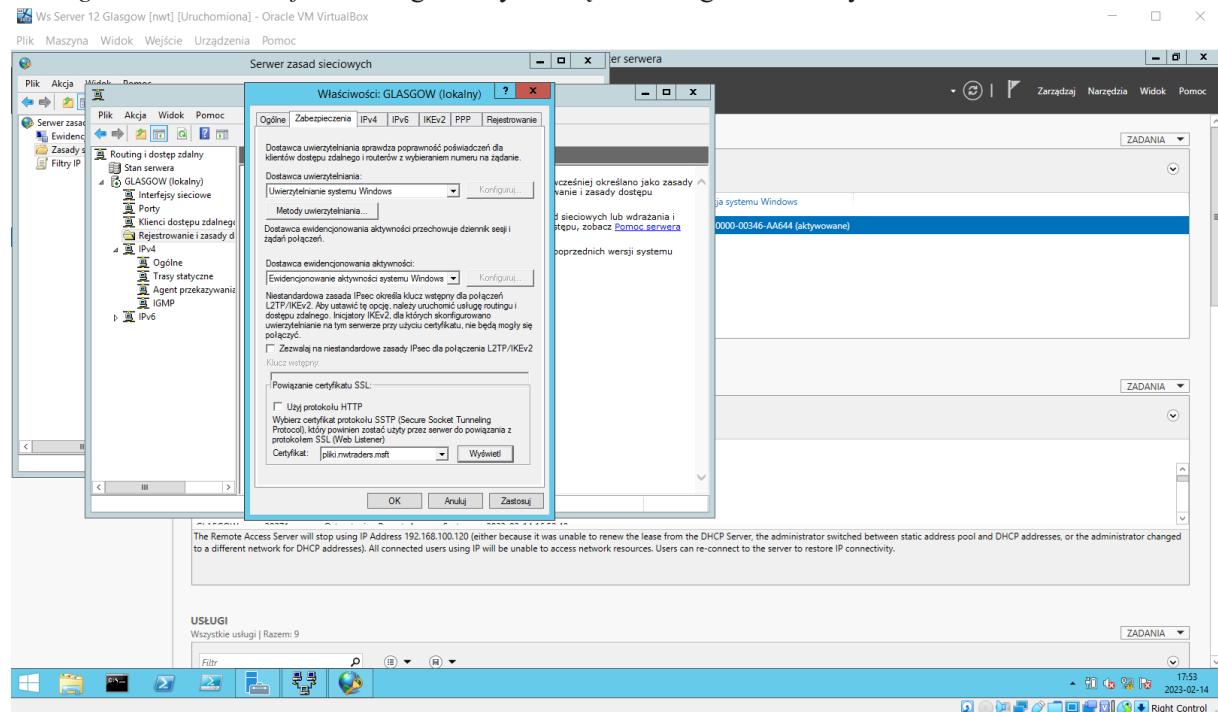


Zweryfikowanie działania utworzonej zasady zdalnego dostępu w systemie Windows.

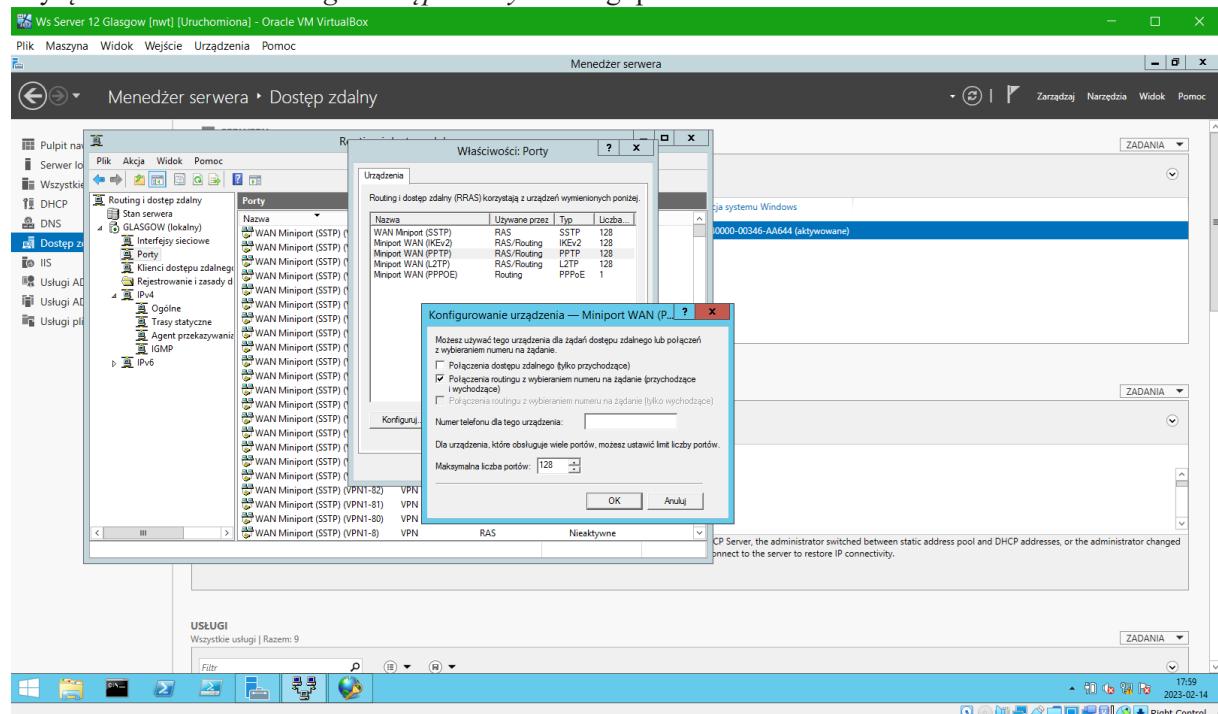


Zadanie 5

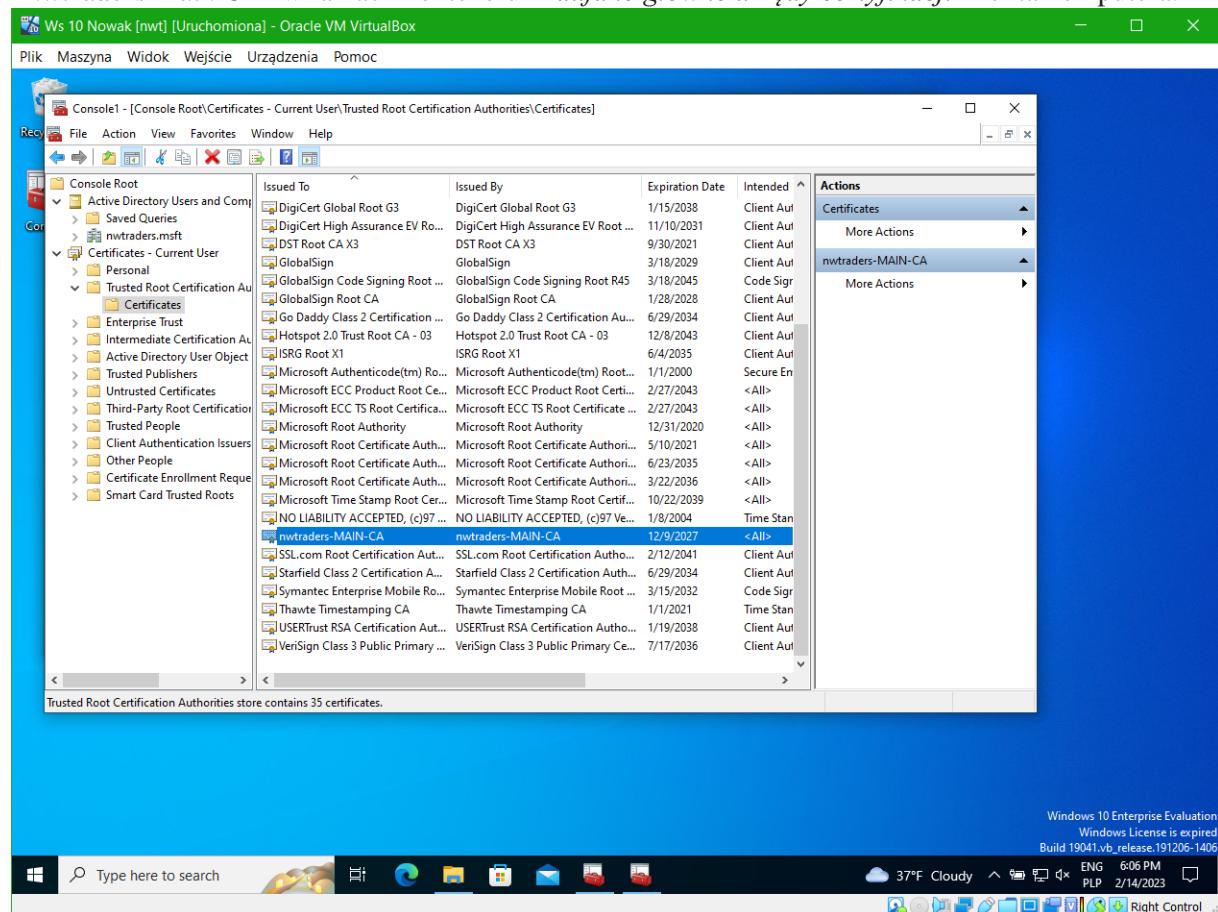
Powiązanie we właściwościach roli "Routing i dostęp zdalny" w ramach zabezpieczeń, certyfikatu SSL "Glasgow.nwtraders.msft" z którego korzystać będzie usługa VPN w trybie SSTP.



Wyłączenie w roli "Routing i dostęp zdalny" obsługi portów PPTP.

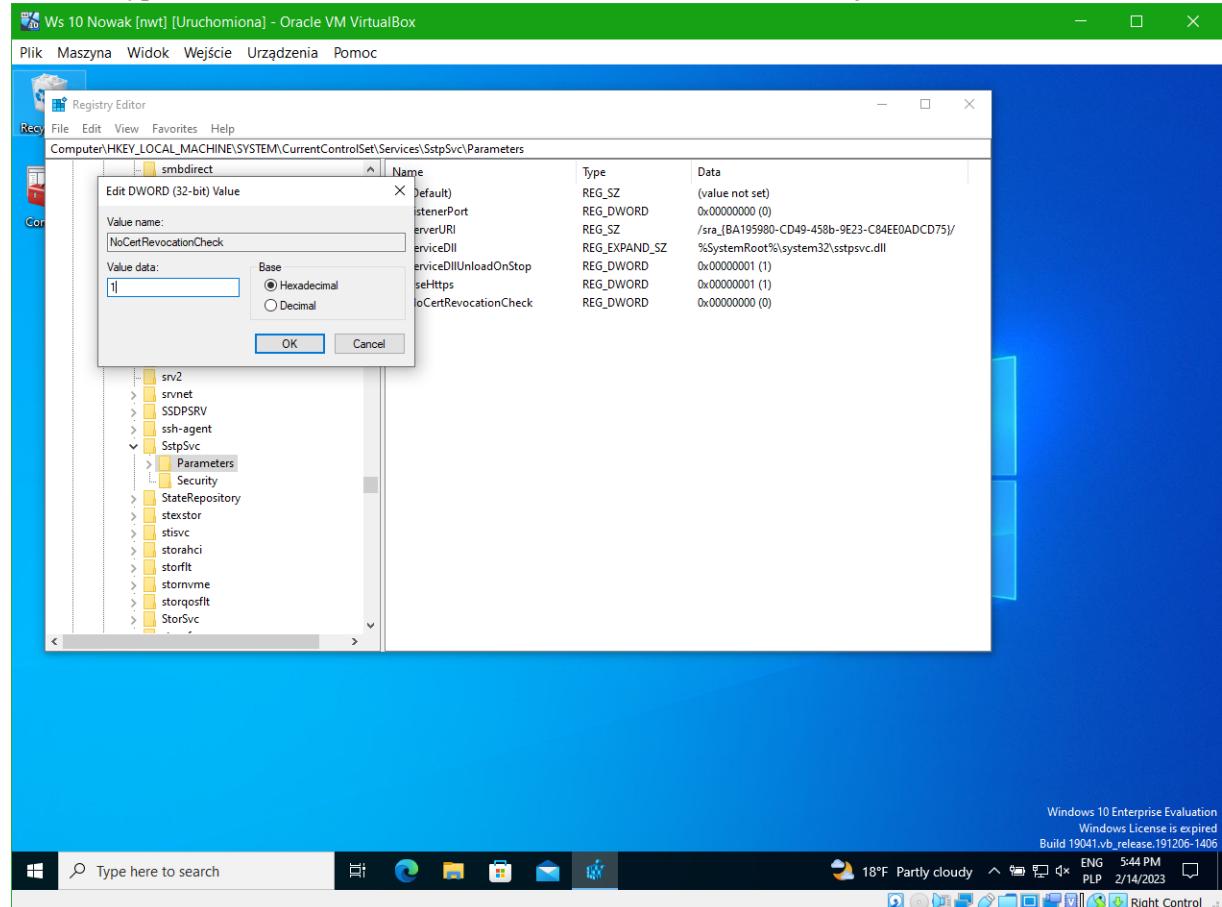


Zainstalowanie w systemie Windows "Nowak" certyfikatu głównego urzędu certyfikującego "*Nwtraders Main CA*" w ramach konteneru "*Zaufane główne urzędy certyfikacji*" konta komputera.



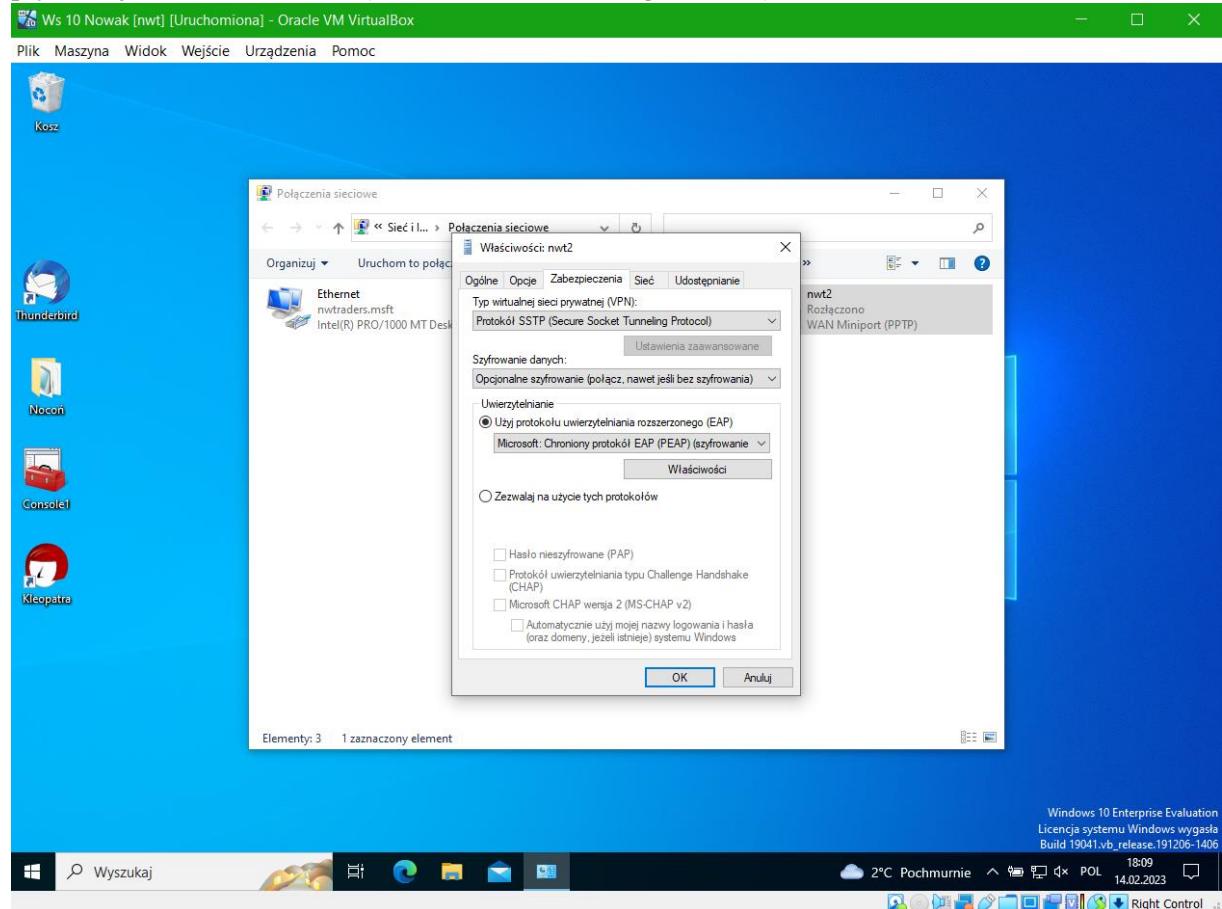
Utworzenie w systemie Windows "Nowak" w ramach klucza rejestru:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sstpsvc\parameters`

wartości typu DWORD32 o nazwie *NoCertRevocationCheck* ustawionej na 1.



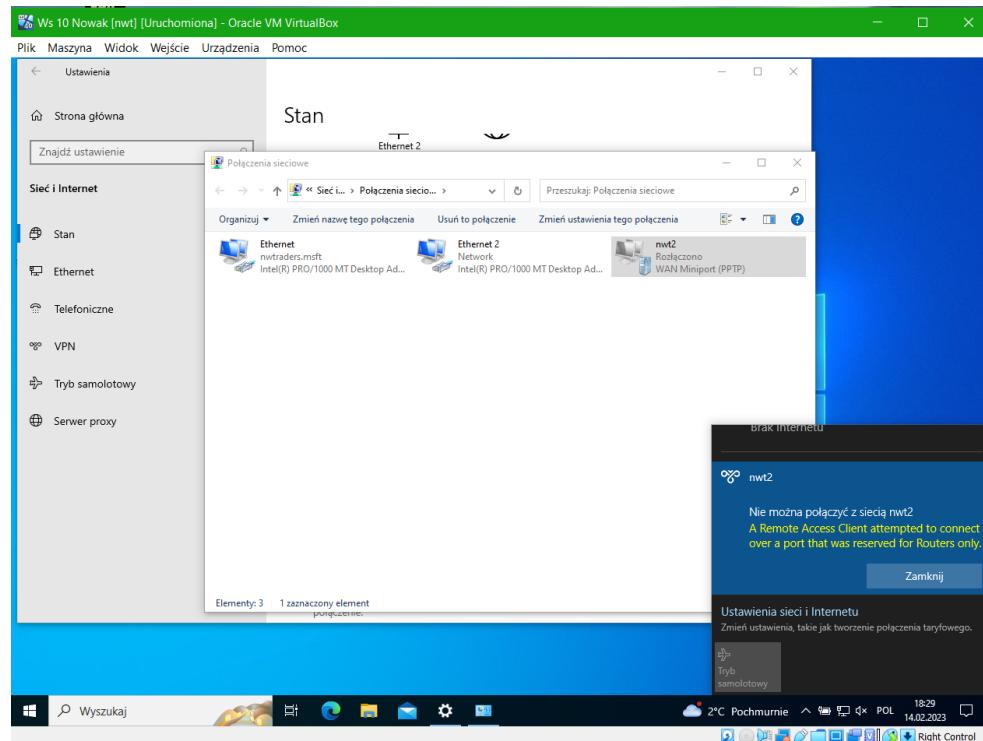
Zmiana w systemie Windows "Nowak" właściwości połączenia VPN do lokalnej sieci komputerowej *Nwtraders*, poprzez zmianę w zakładce "Zabezpieczenia" typu wirtualnej sieci

prywatnej na "Protokół SSTP (Secure Socket Tunelling Protocol)".



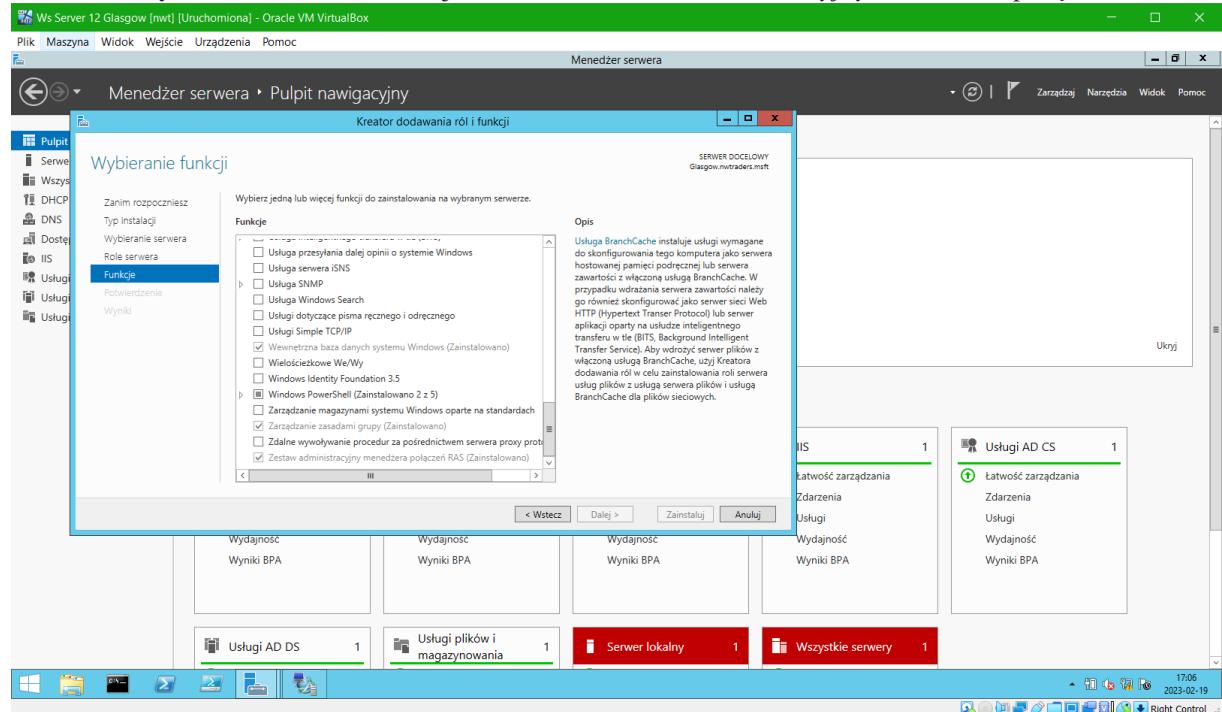
Zweryfikowanie działania połączenia VPN opartego na protokole PPTP oraz SSTP w systemie Windows "Nowak".

Po PPTP:

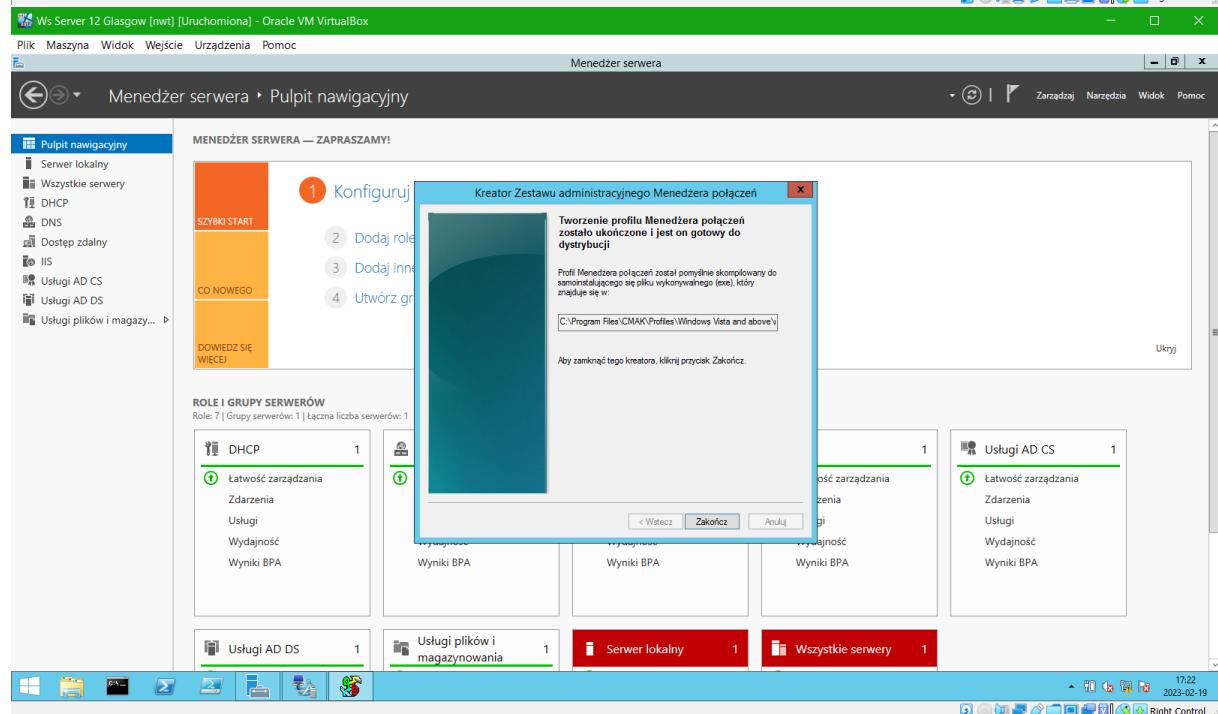
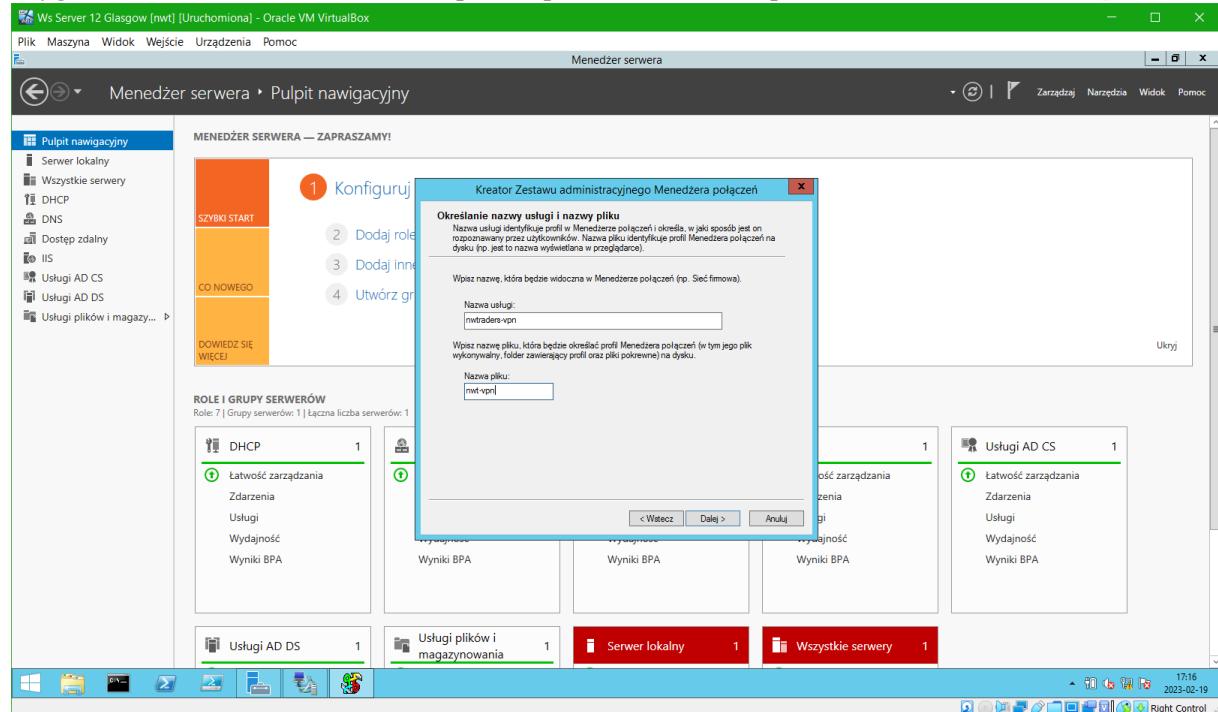


Zadanie 6

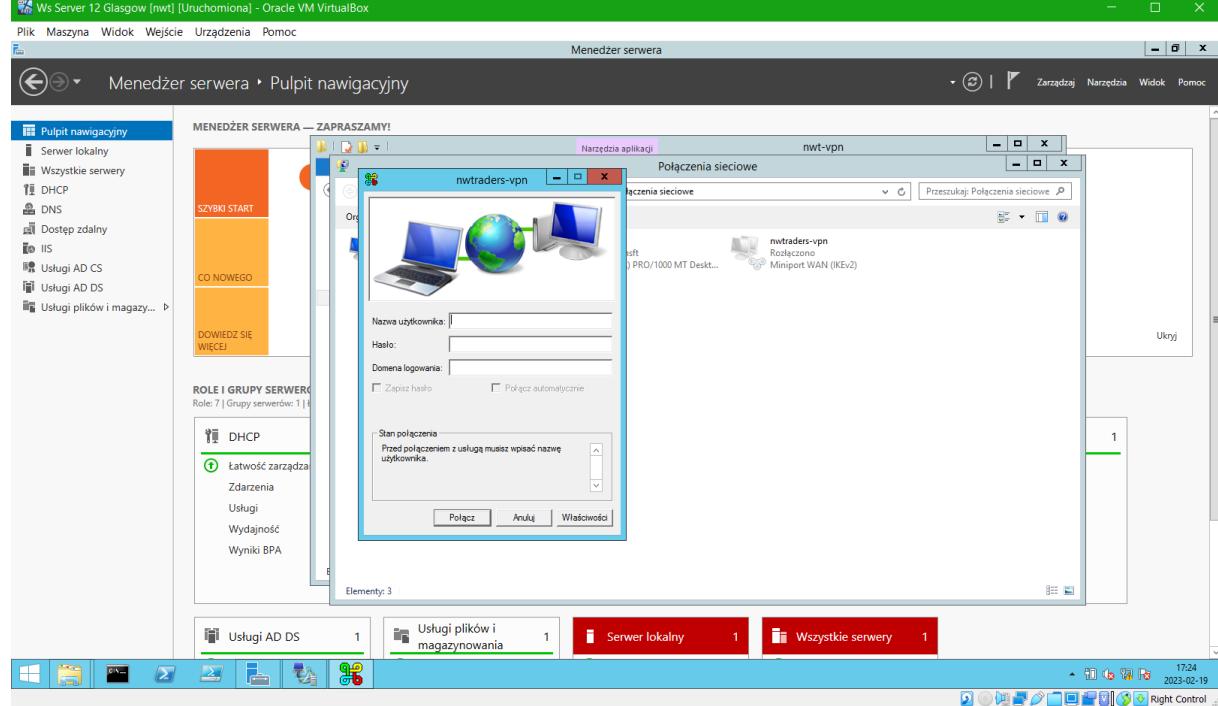
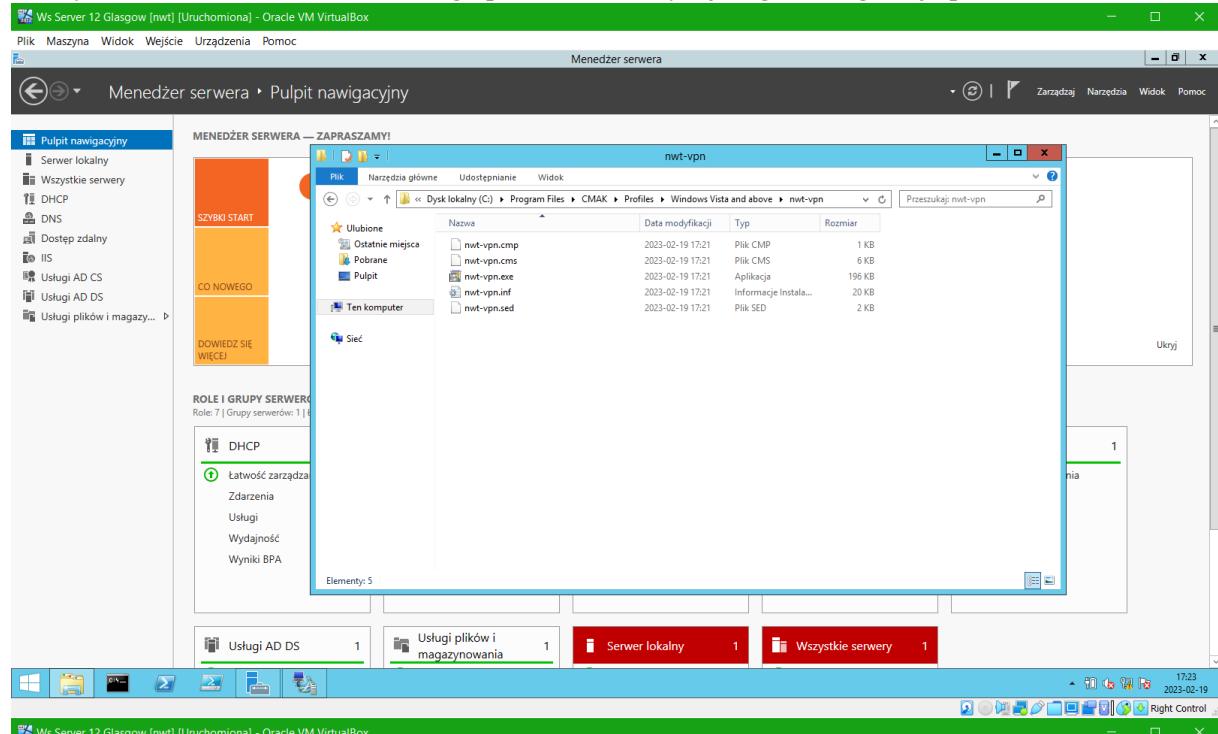
Dodanie w systemie Windows funkcji o nazwie "Zestaw administracyjny Menedżera połączeń".



Wygenerowanie w narzędziu CMAK profilu połączenia VPN w pliku o nazwie "nwtraders-vpn.exe".

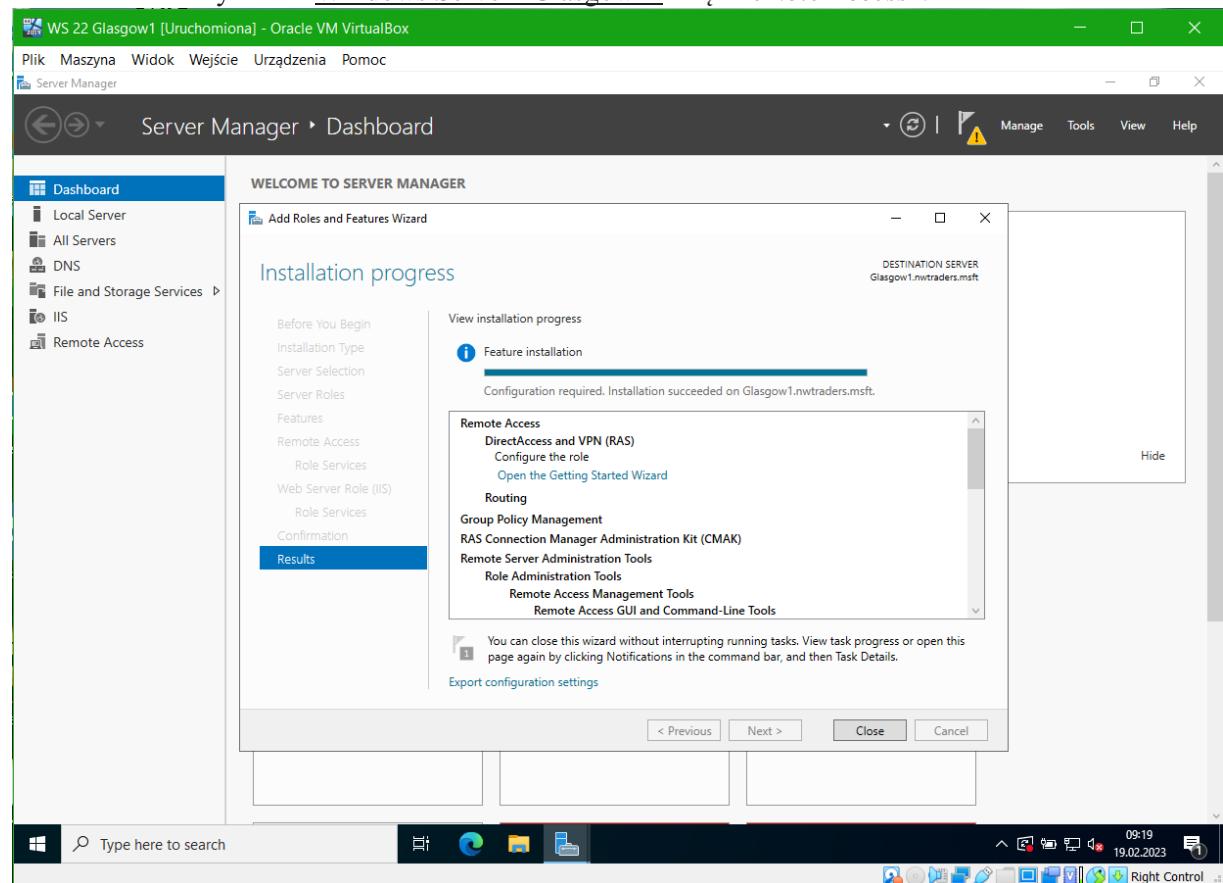


Zweryfikowanie działania utworzonego profilu automatyzującego konfigurację połączenia VPN.

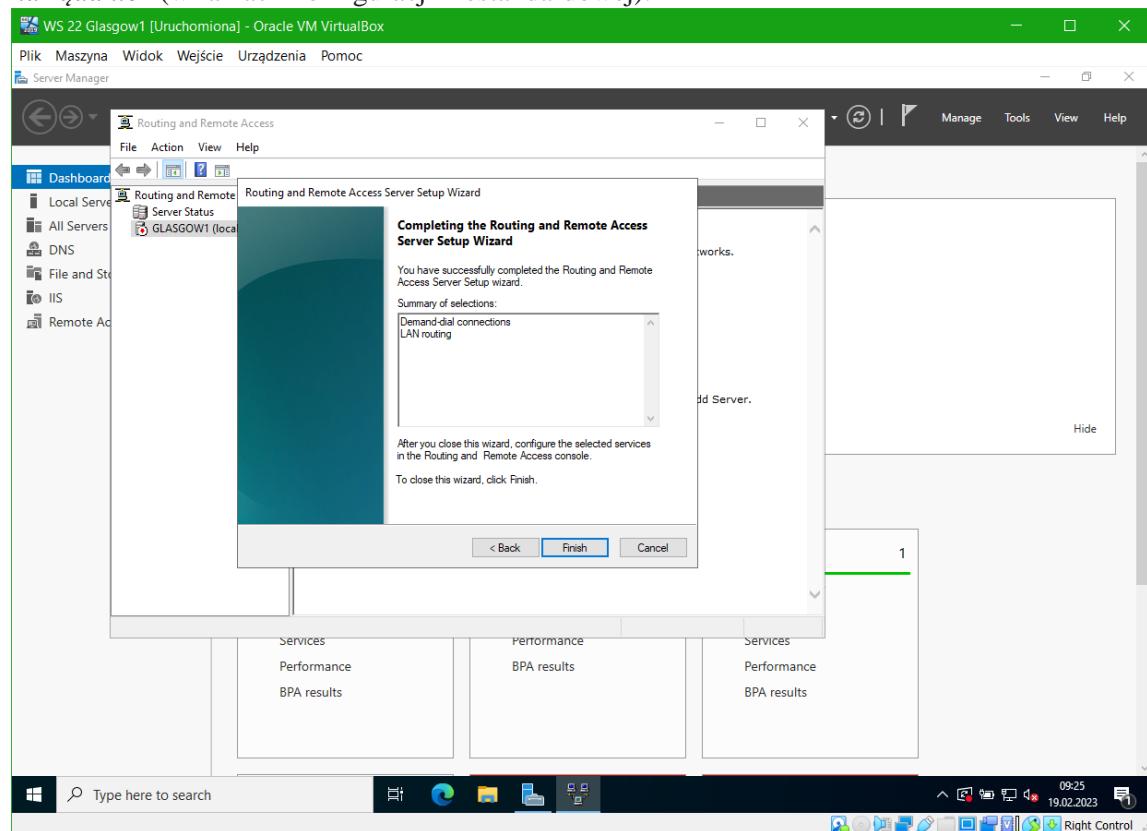


Zadanie 7

Zainstalować w systemie Windows Server "Glasgow1" rolę "Remote Access".

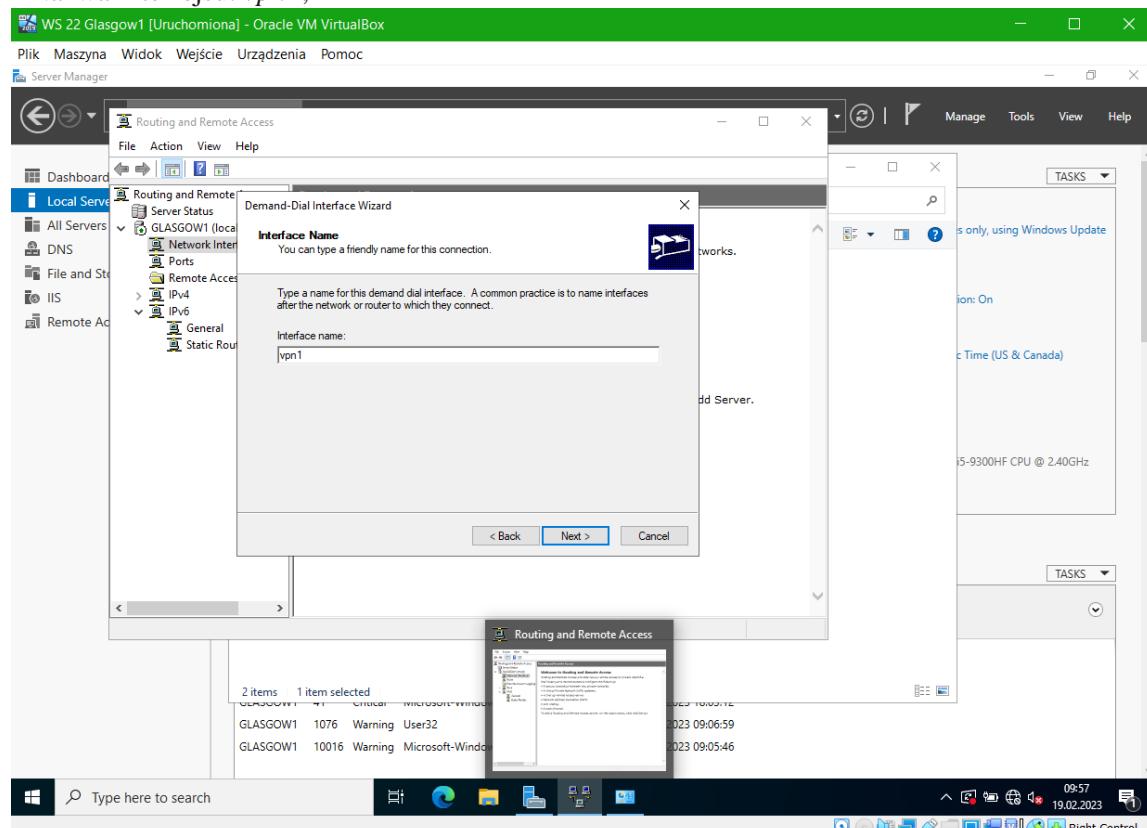


Włączyć w "Remote Access" usługę "Routing LAN" oraz usługę "Połączania z wybieraniem numeru na żądanie" (w ramach konfiguracji niestandardowej).

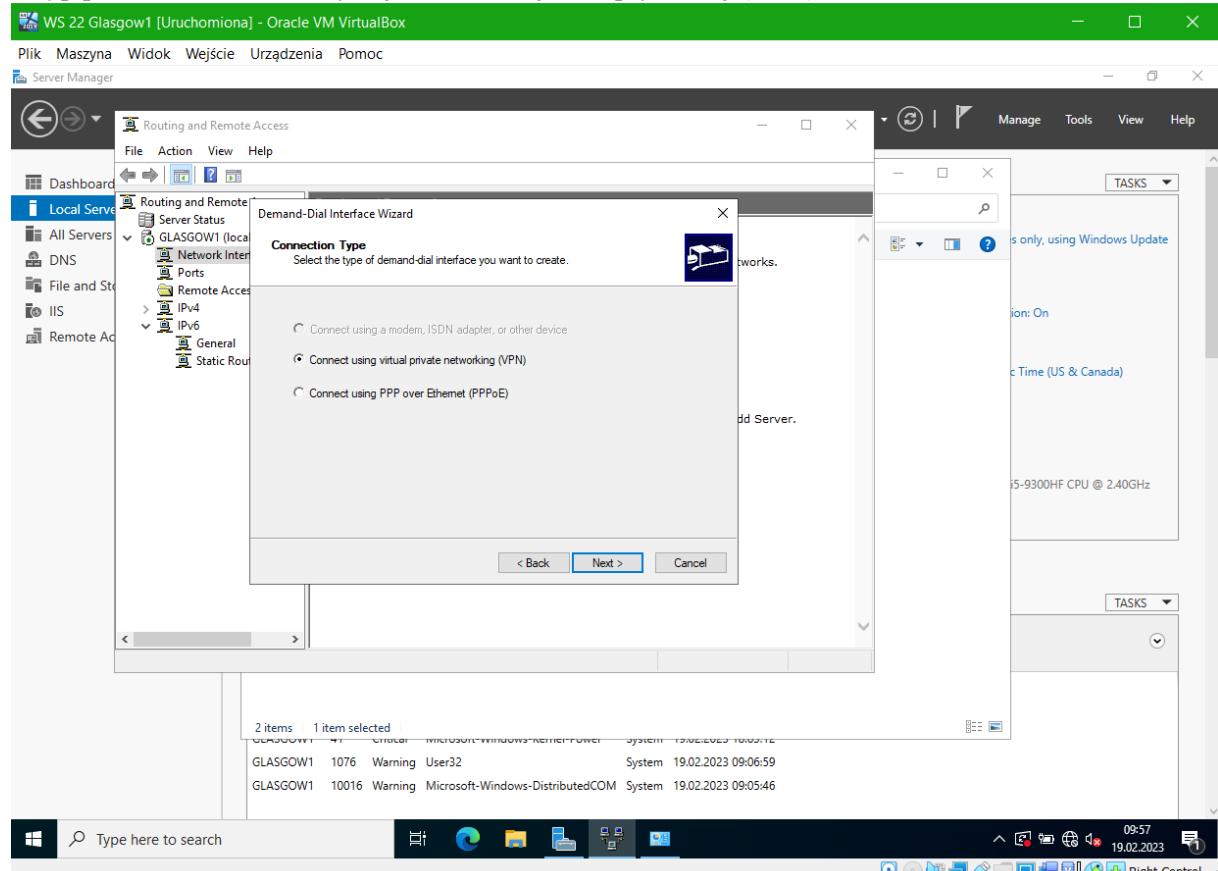


Skonfigurować w "Uslugie routingu i dostępu zdalnego" w ramach interfejsów sieciowych "Nowy interfejs wybierania numeru na żądanie":

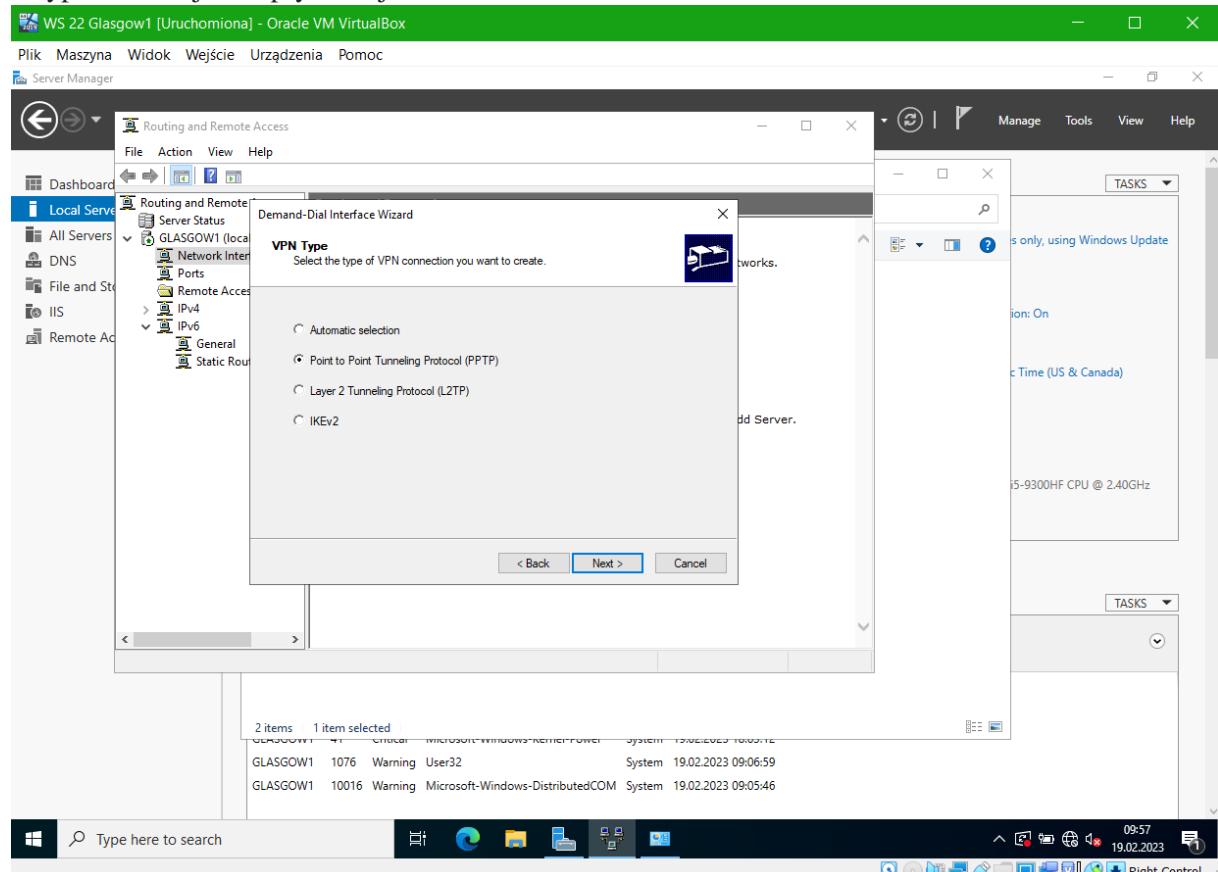
- Nazwa interfejsu: `vpn1`;



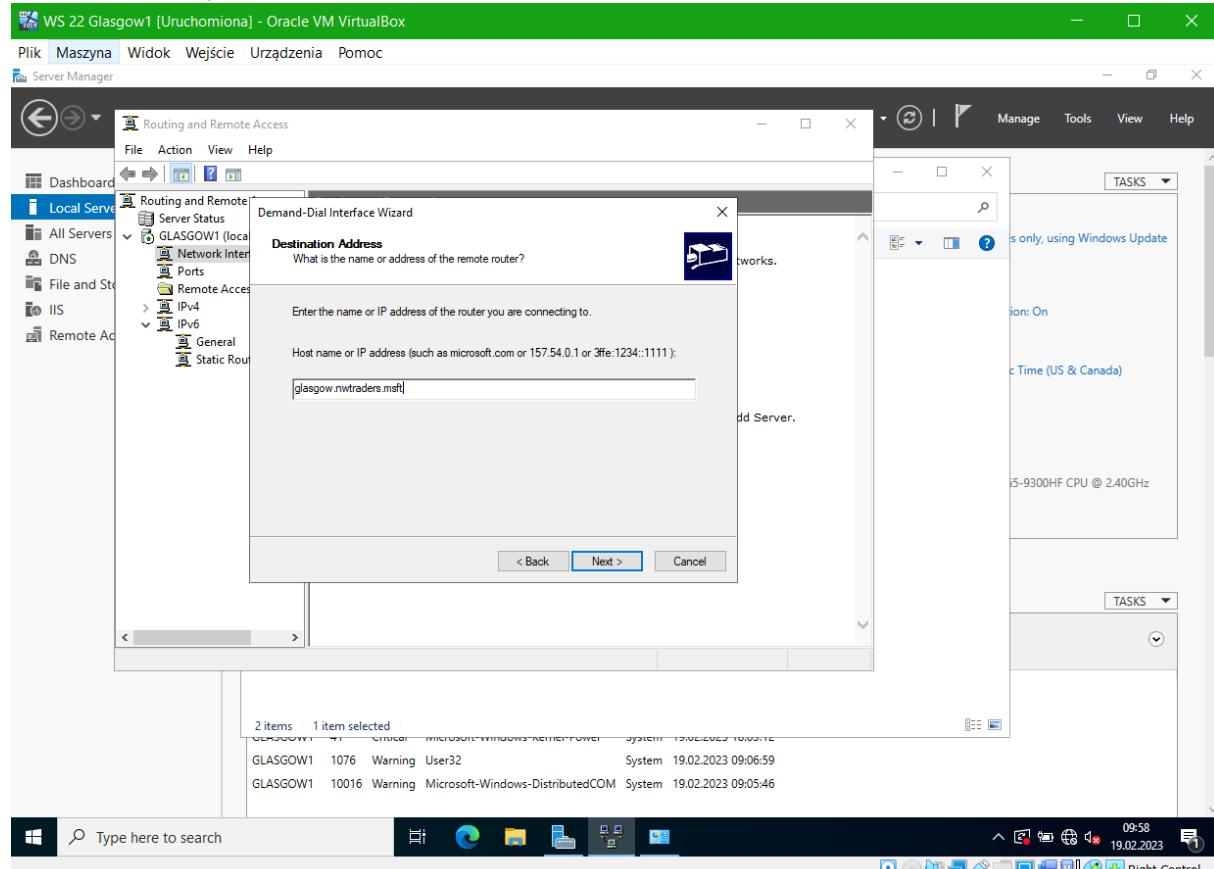
- Typ połączenia: Połącz używając wirtualnej sieci prywatnej (VPN);



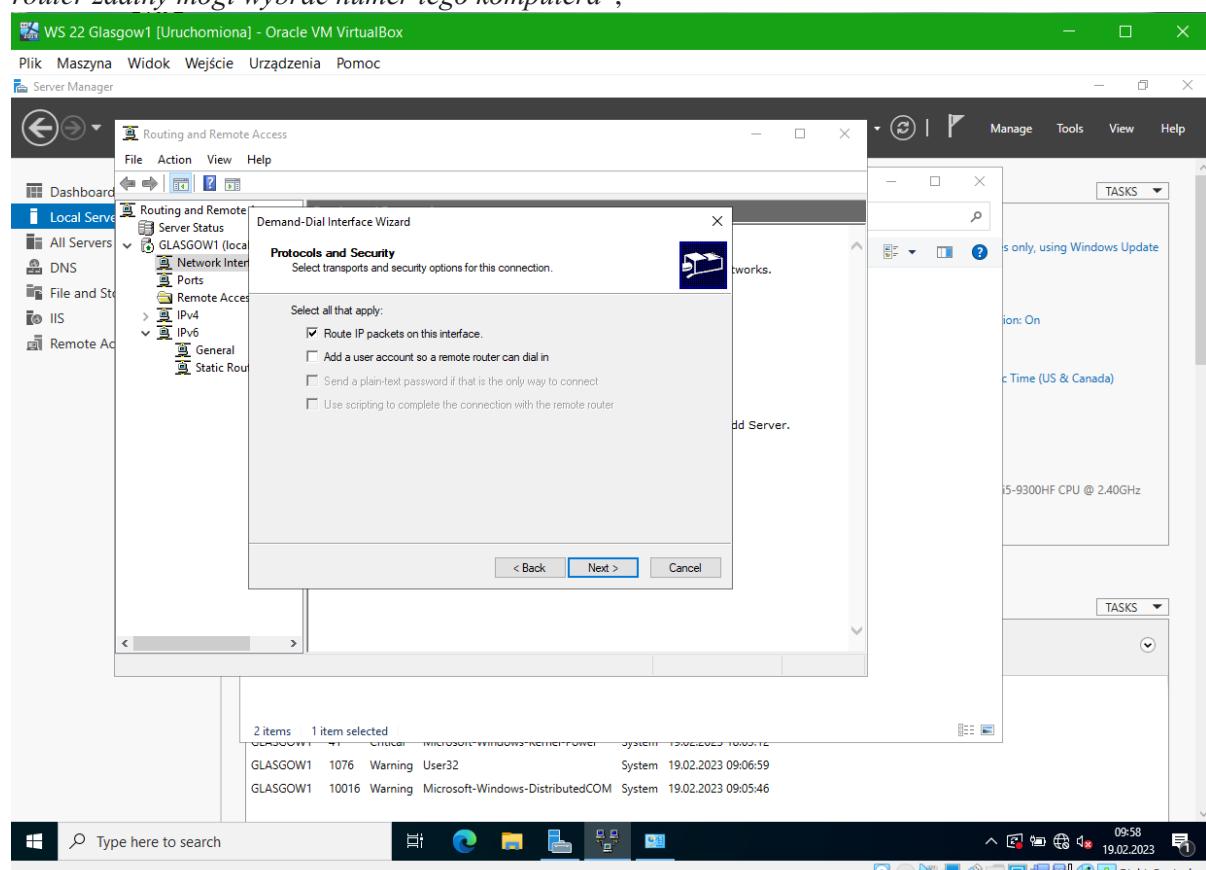
- Typ wirtualnej sieci prywatnej: PPTP;



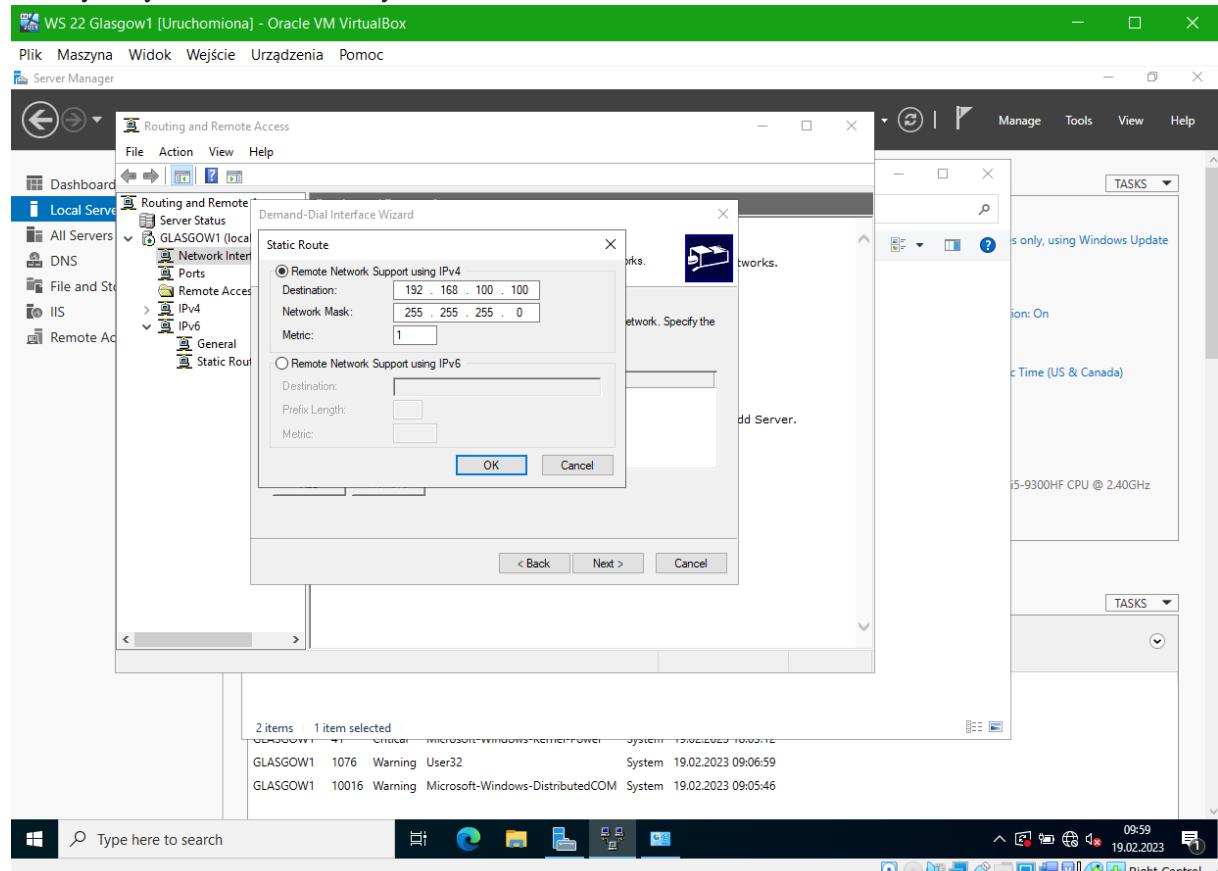
- Adres docelowy: *Glasgow.nwtraders.msft*;



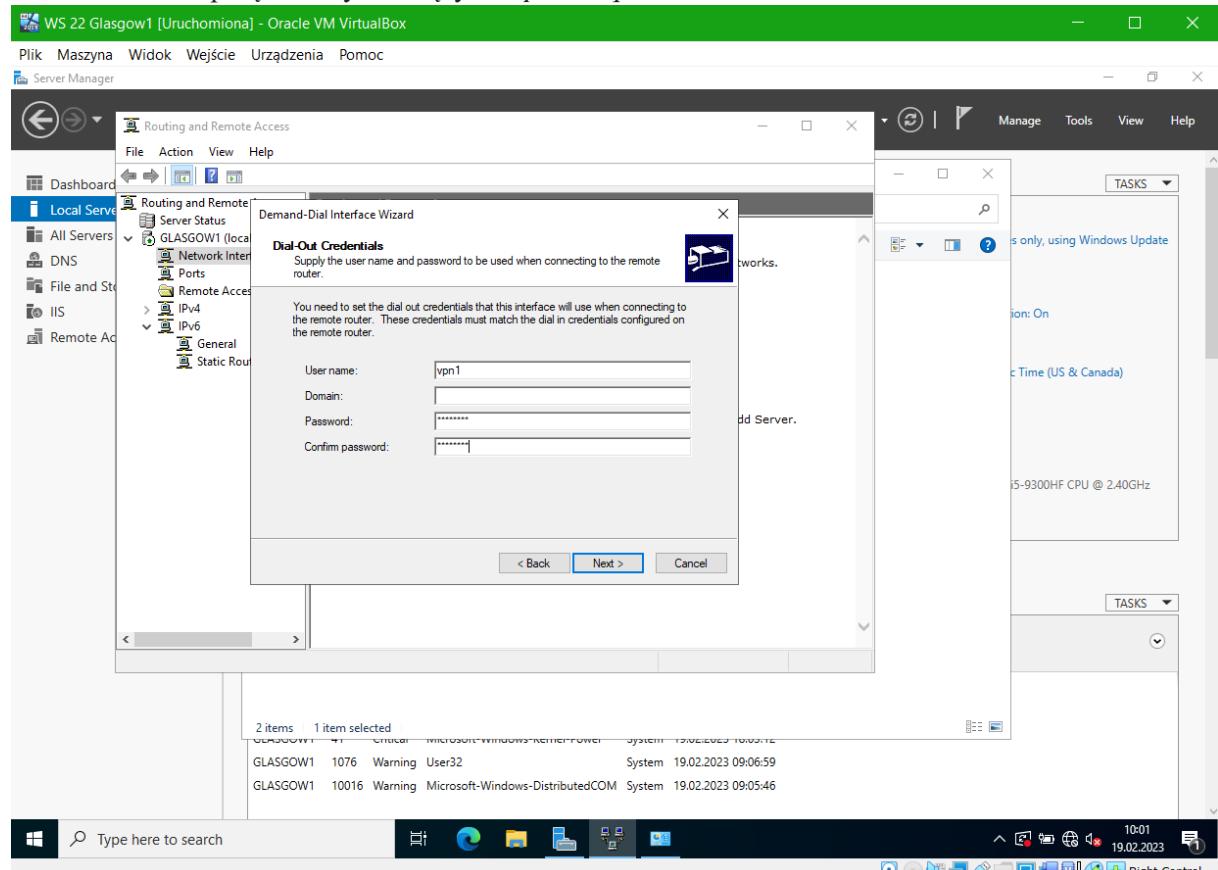
- Protokoły i zabezpieczenia: "Roześlij pakiety IP po interfejsie" oraz "Dodaj konto użytkownika, aby router zdalny mógł wybrać numer tego komputera";



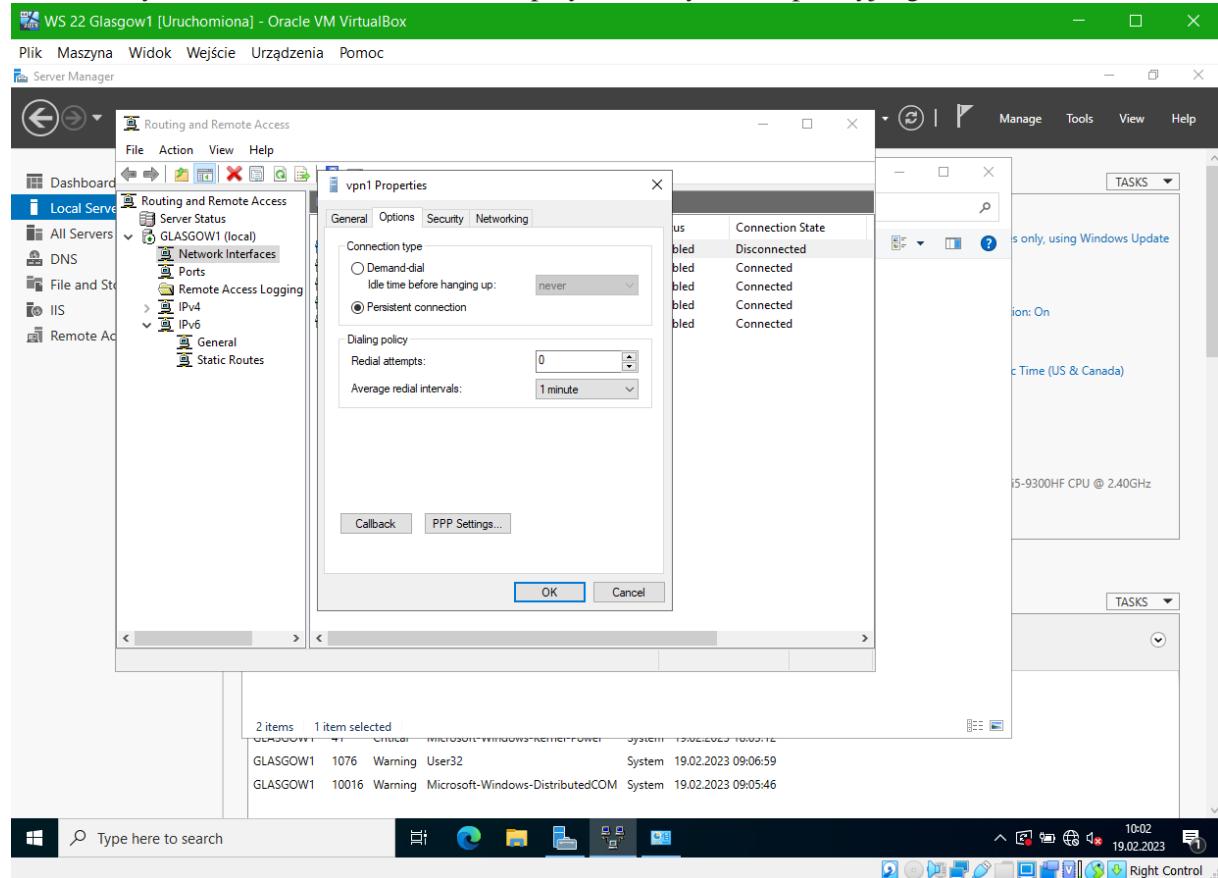
- Trasy statyczne do sieci zdalnych: 192.168.100.100/24;



- Poświadczenia połączeń wychodzących: vpn1/Zaq12wsx.

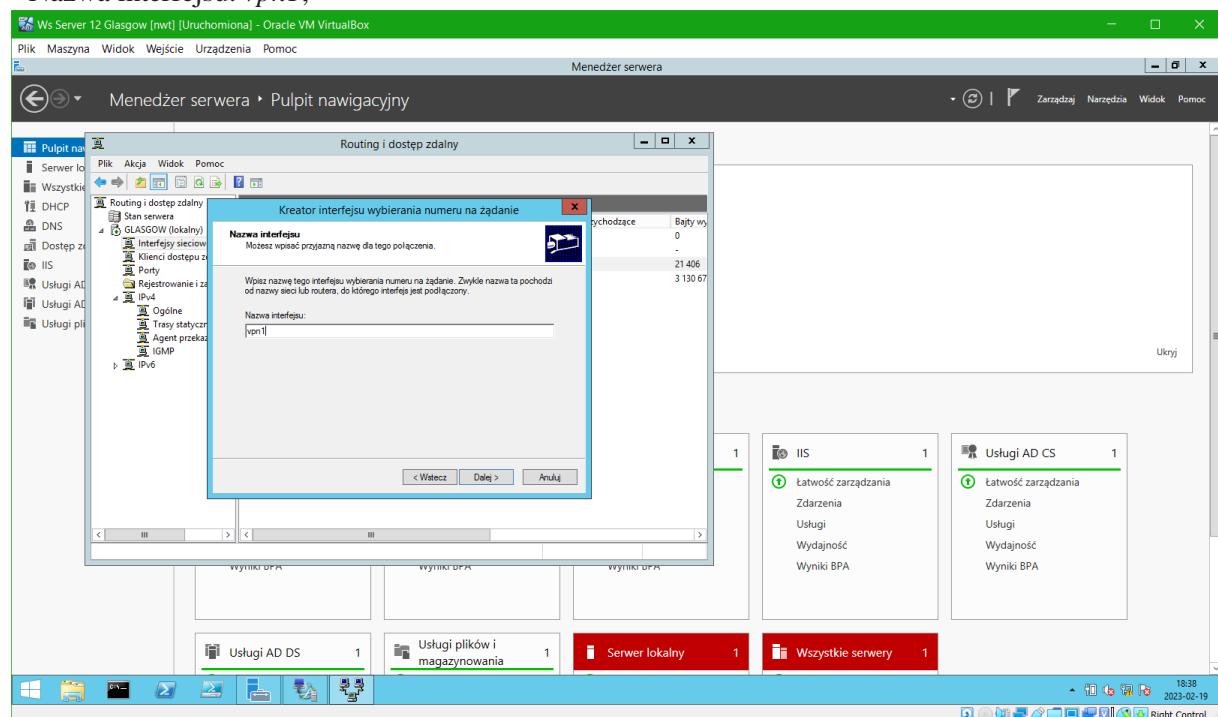


W ramach właściwości utworzonego interfejsu zaznaczyć opcję "Polaczanie trwałe", która pozwoli na automatyczne uruchamianie tunelu VPN przy starcie systemu operacyjnego.

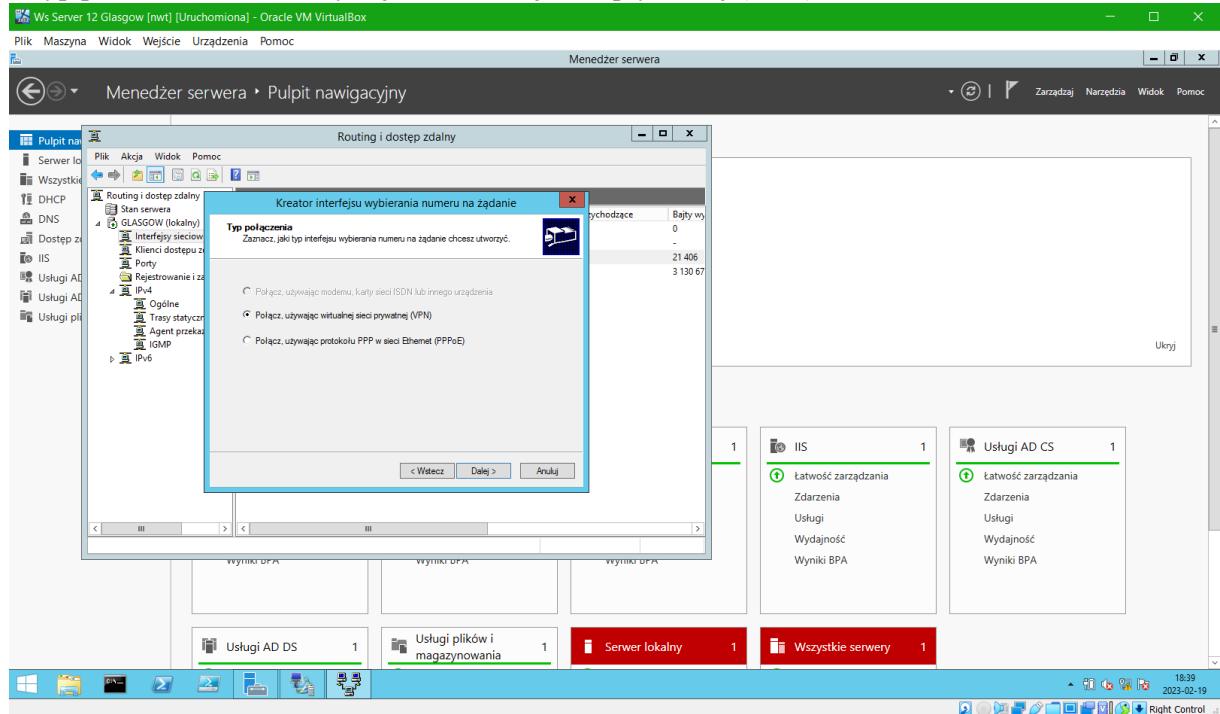


W systemie Windows Server "Glasgow" skonfigurować w "Uslugie routingu i dostępu zdalnego" w ramach interfejsów sieciowych "Nowy interfejs wybierania numeru na żądanie", konfigurując go zgodnie z poniższymi informacjami:

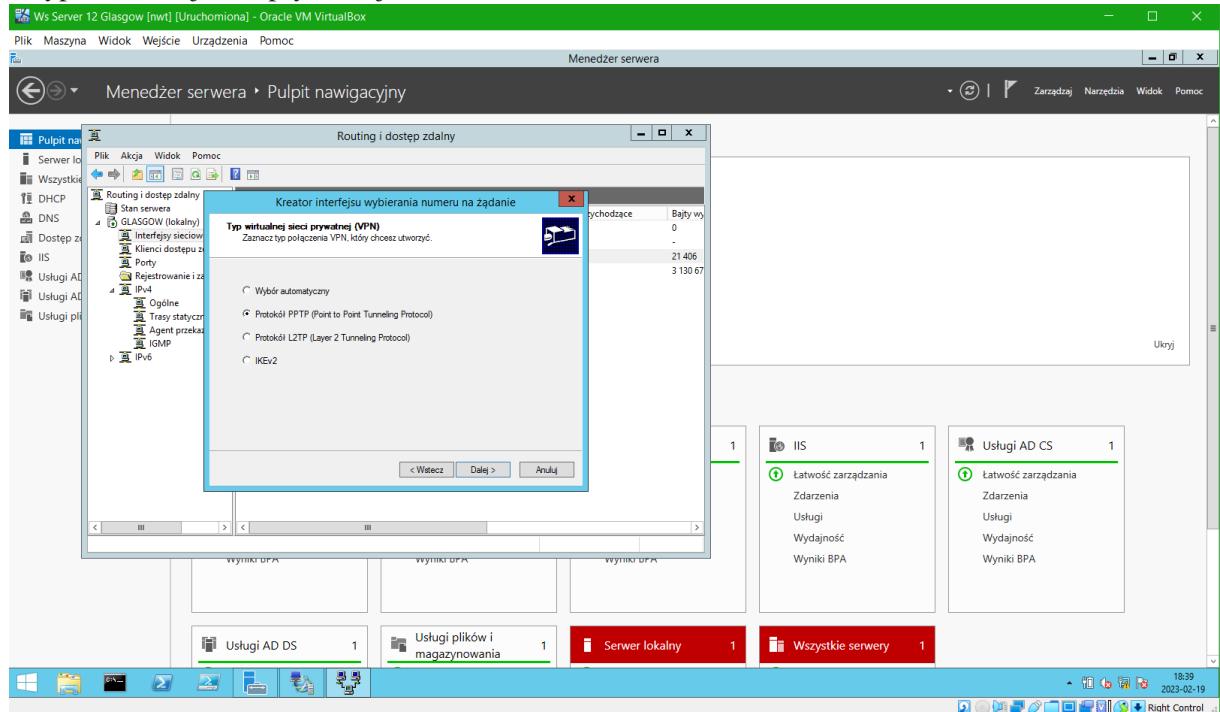
- Nazwa interfejsu: *vpn1*;



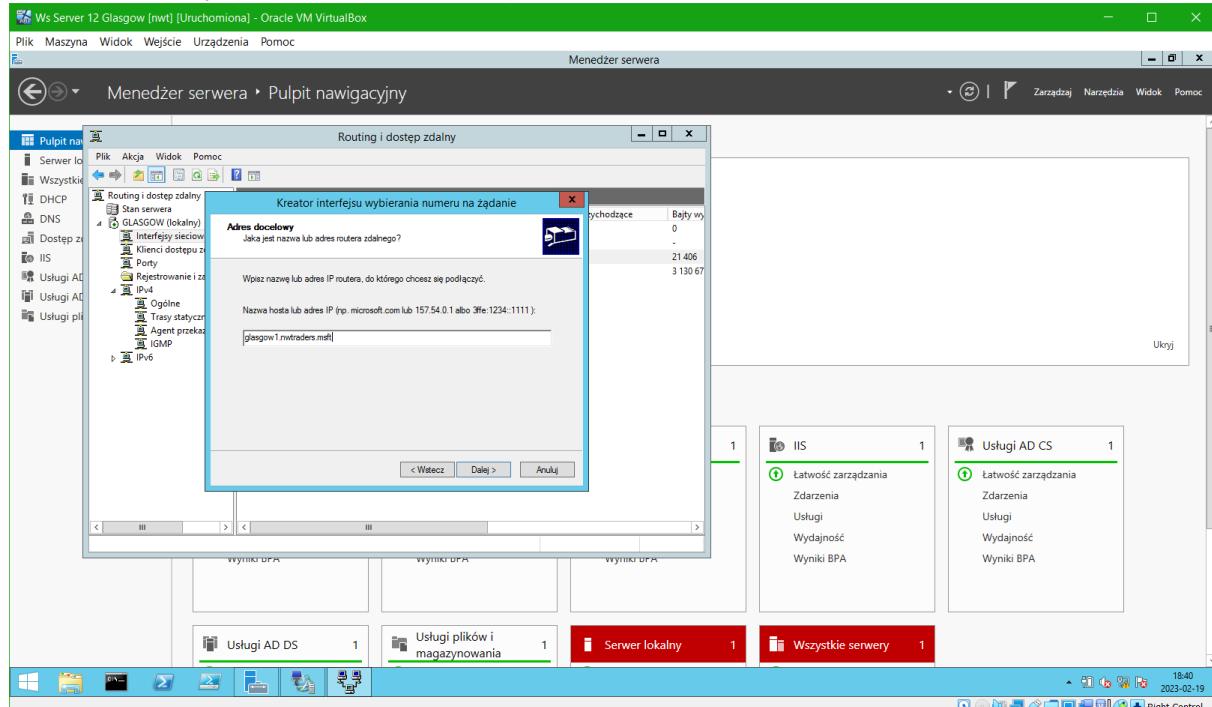
- Typ połączenia: Połącz używając wirtualnej sieci prywatnej (VPN);



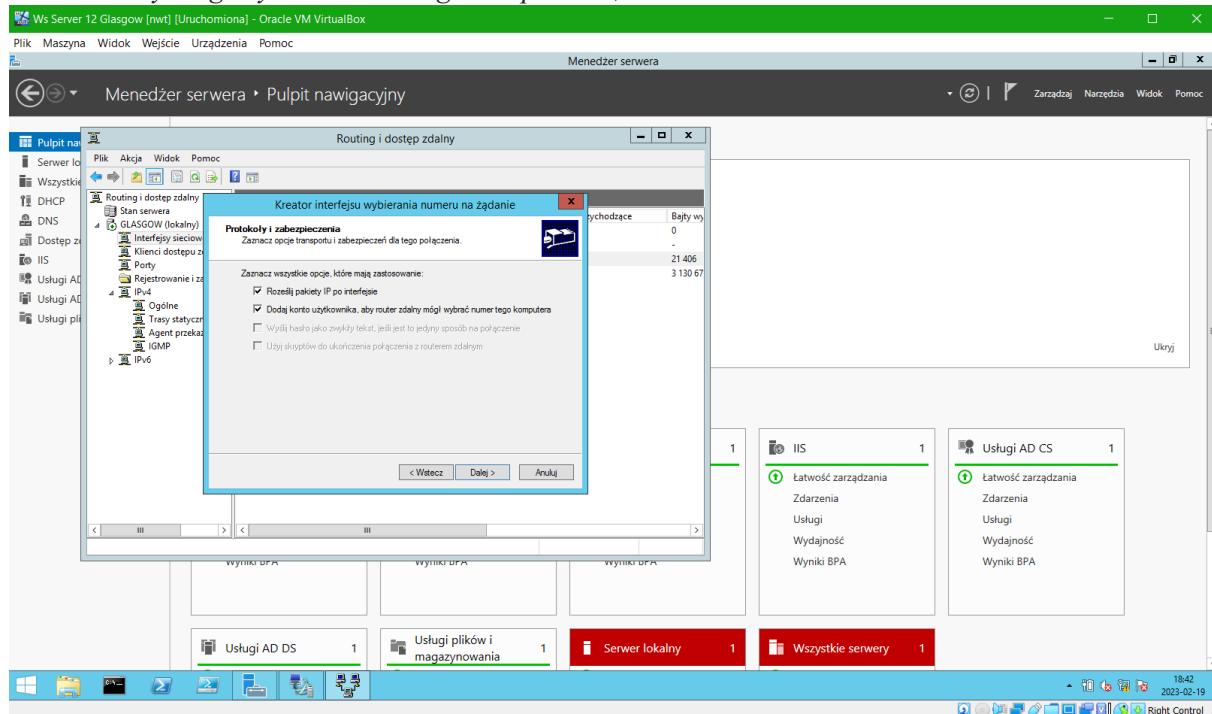
- Typ wirtualnej sieci prywatnej: PPTP;



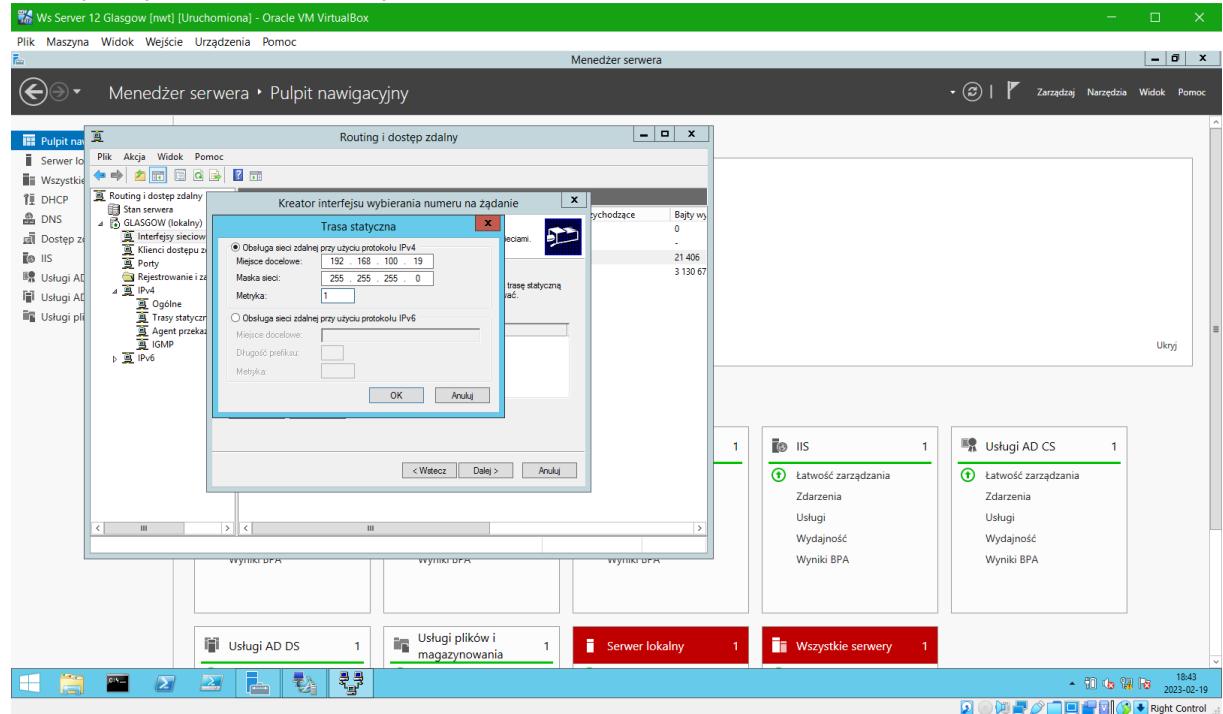
- Adres docelowy: *glasgow1.nwtraders.msft*;



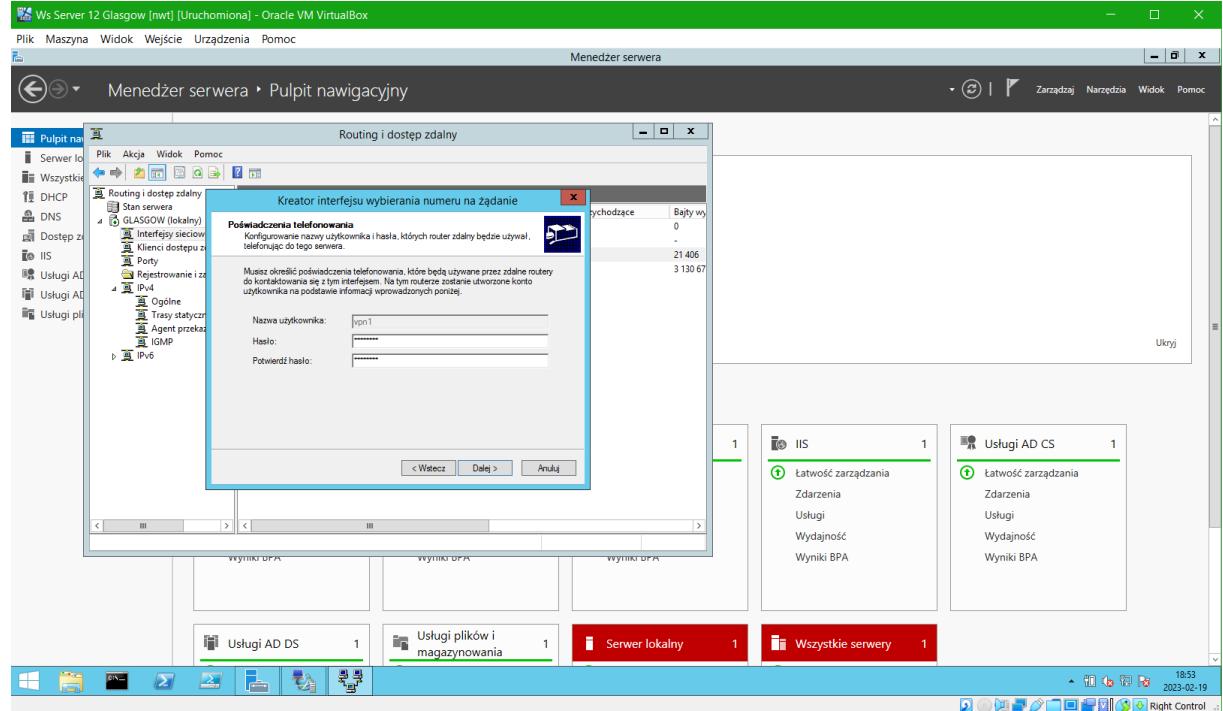
- Protokoły i zabezpieczenia: "Roześlij pakiety IP po interfejsie" oraz "Dodaj konto użytkownika, aby router zdalny mógł wybrać numer tego komputera";



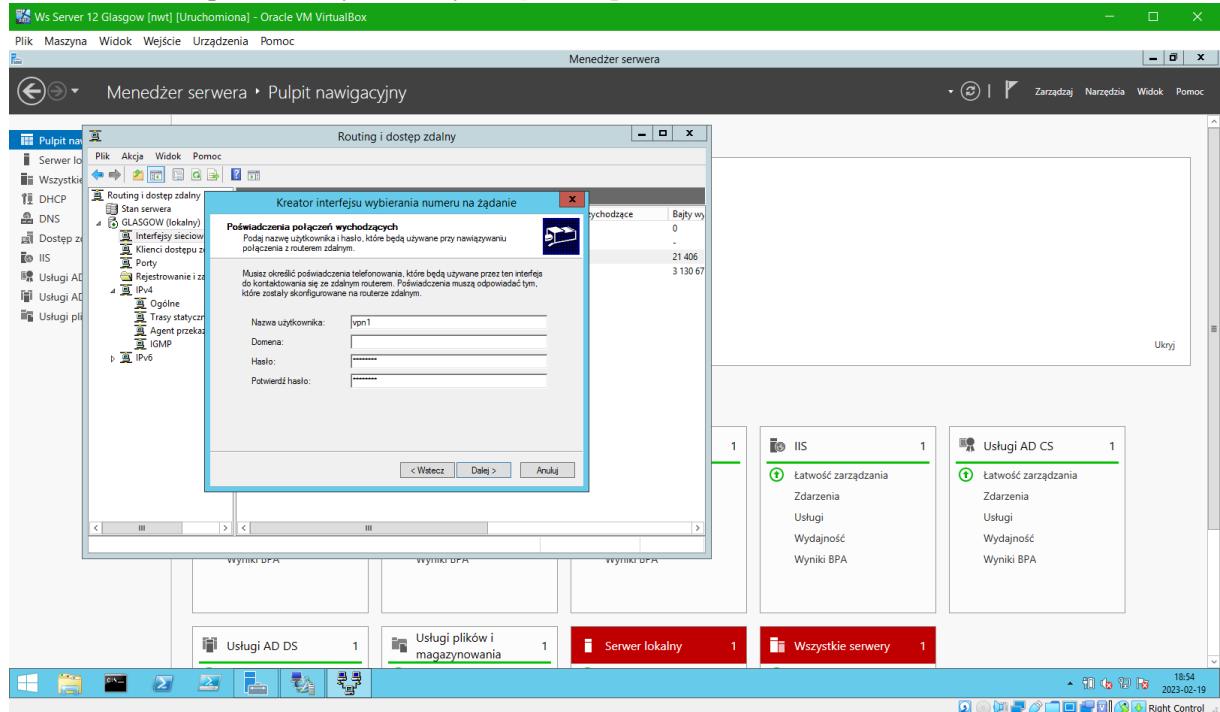
- Trasy statyczne do sieci zdalnych: 192.168.100.19/24;



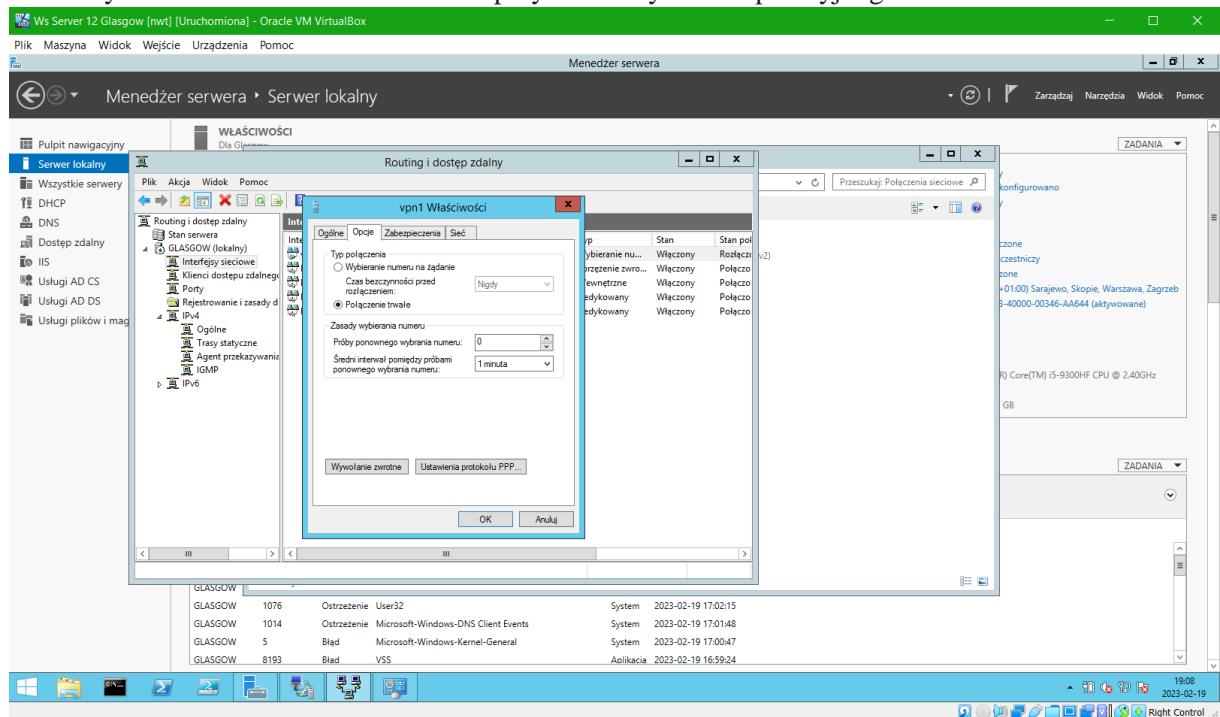
- Poświadczenia telefonowania: vpn1/Zaq12wsx;



- Poświadczenie połączeń wychodzących: *vpn1/Zaq12wsx*.



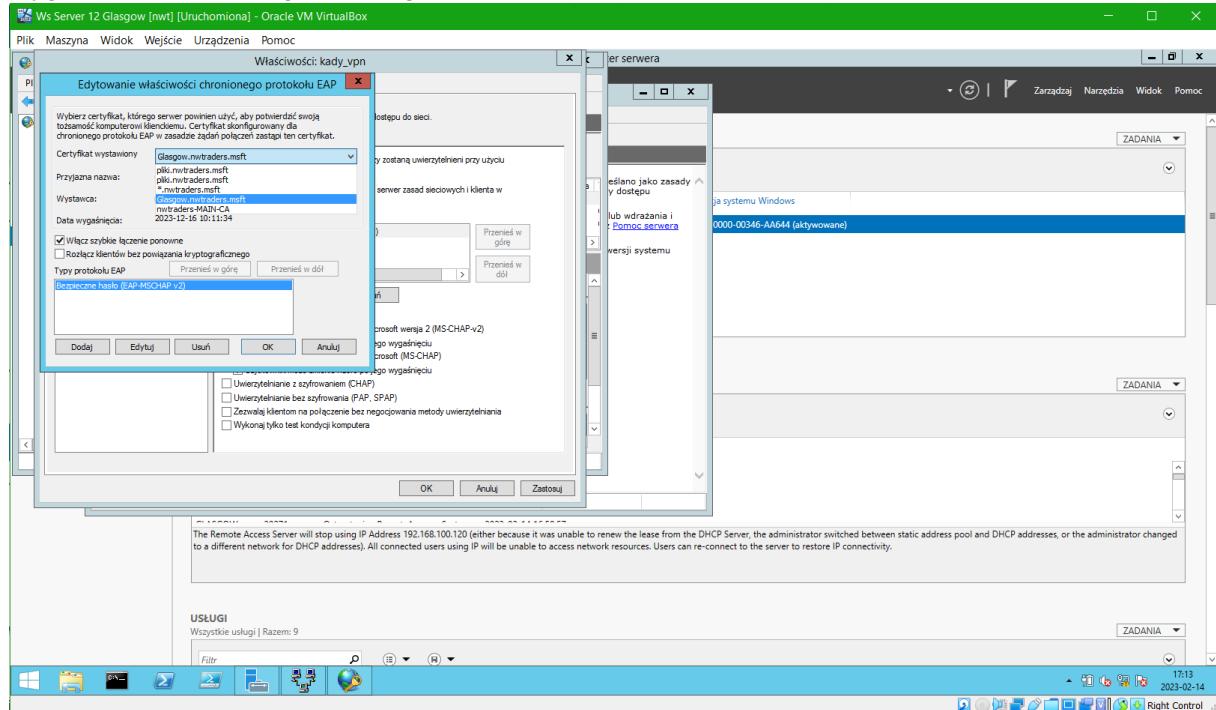
W ramach właściwości utworzonego interfejsu zaznaczyć opcję "*Połączenie trwale*", która pozwoli na automatyczne uruchamianie tunelu VPN przy starcie systemu operacyjnego.



Zadanie 8

Sprawdzenie w systemie Windows Server "Glasgow", czy serwer ma wygenerowany certyfikat "komputera" dla adresu domenowego wykorzystywanego do połączeń z usługą VPN, jeżeli nie ma, to

wygenerowanie dla niego takowego o nazwie "glasgow.nwtraders.msft".



W systemie Windows Server "Glasgow" oraz Windows Server "Glasgow1" zmiana we właściwościach interfejsu sieciowego o nazwie `vpn1`, w ramach zabezpieczeń, typu wirtualnej sieci prywatnej na "Protokół L2TP/IPsec" używającego certyfikatów do uwierzytelnienia.

