

# Sprawozdanie z modułu 6

## Przygotowanie do zadań

London: intnet (192.168.100.100/255.255.255.0), intnet2 (88.88.88.88/255.255.255.0)

Glasgow: intnet2 (88.88.88.89/255.255.255.0), intnet3 (172.16.0.1/255.255.255.0) - podpięty do domeny

Nowak: intnet2 (88.88.88.10/255.255.255.0) - nie podpięty do domeny

Przed rozpoczęciem zadań należy również udostępnić w systemie Windows Server "London" udział sieciowy o nazwie "wspolny" dostępny dla wszystkich pracowników, oraz zainstalować rolę dostępu zdalnego i aktywować w niej usługę "Remote Access".

Przed rozpoczęciem zadań należy również wdrożyć lokalną infrastrukturę klucza publicznego zintegrowaną z usługą Active Directory, na kontrolerze domeny Windows Server "London" pod nazwą "Nwtraders Main CA".

---

## Zadanie 1

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Pan Jacek Gula z działu Kadr chciałby pracować zdalnie z domu z udziałem sieciowym //192.168.100.100/wspolny udostępnionym w systemie Windows Server "London". Pan Jacek posiada w domu dostęp do Internetu. Bezpośredni dostęp do w/w udziału sieciowego z poza sieci firmy jest niemożliwy, gdyż udział ten jest widoczny tylko lokalnie, dla komputerów wew. sieci firmy.

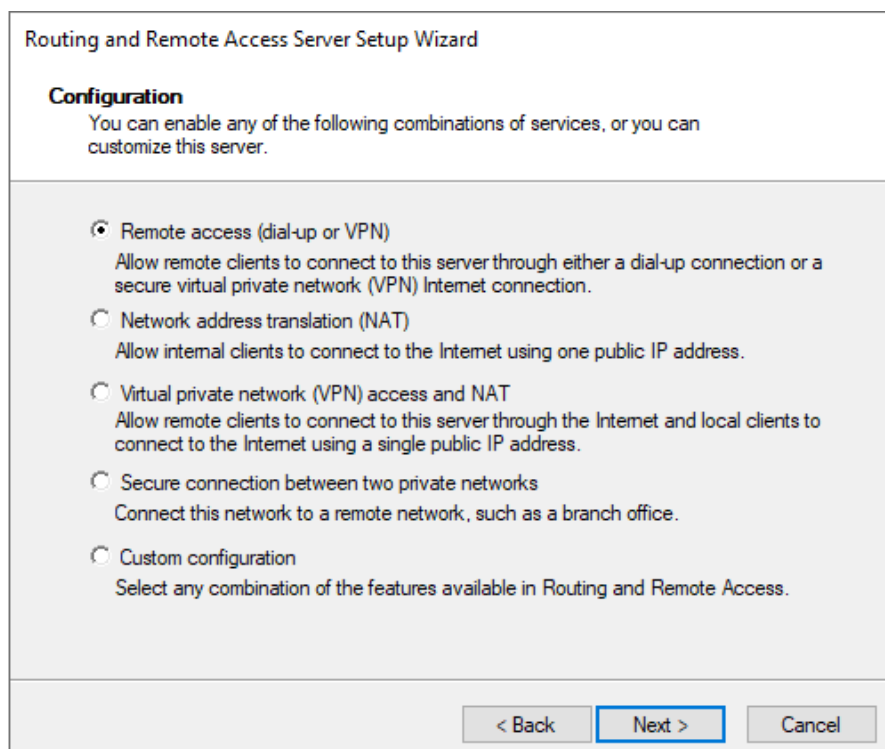
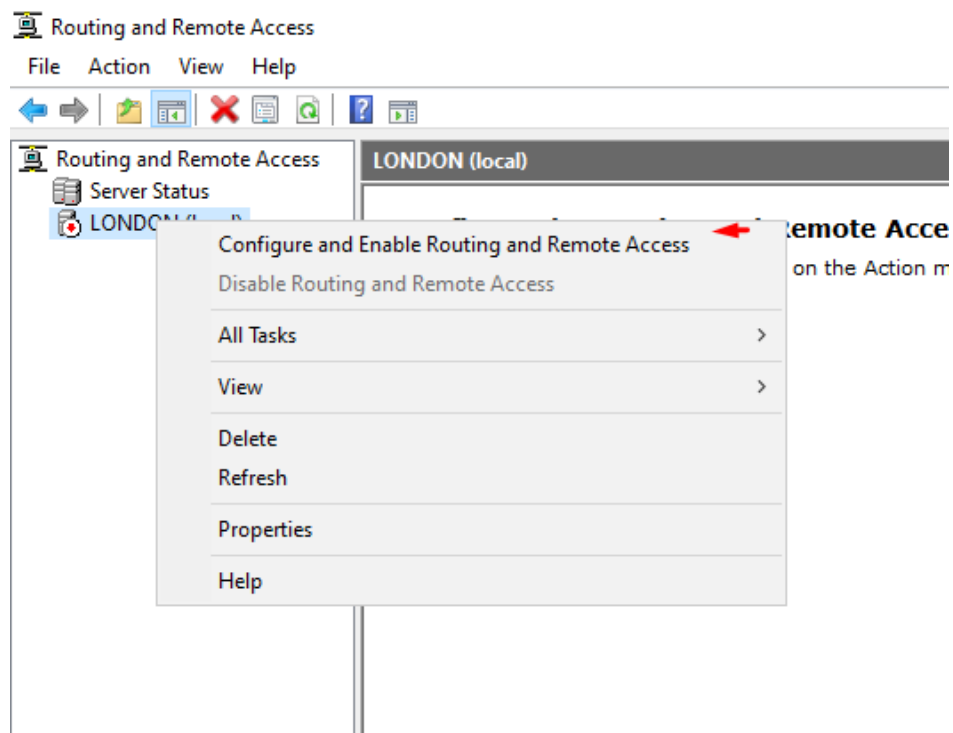
Przełożony Pana Jacka zgodził się na dostęp do tegoż udziału sieciowego spoza siedziby firmy, i poprosił administratora o skonfigurowanie obsługi połączeń VPN, aby takowy dostęp umożliwić.

Poprosił również, aby skonfigurować służbowego laptopa Pana Jacka na potrzeby połączeń VPN, i sprawdzić, czy dostęp zdalny do sieci z tego komputera jest możliwy.

Twoim zadaniem jest więc:

- zainstalować server VPN w systemie Windows Server "London", wg. poniższych wskazówek:
  - klientom łączącym się poprzez VPN adresy IP przydzielać ma sam serwer VPN z określonego zakresu adresów: 192.168.100.20-192.168.100.30,
  - serwer VPN nie będzie używać autentykacji RADIUS
- aktywować Panu Jackowi Guli działu Kadr możliwość korzystania z usługi VPN,
- skonfigurować w laptopie Pana Jacka 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 "London".



Tutaj trzeba wyjść i wejść, bo za pierwszym razem "VPN" jest wyszarzone (Bóg wie dlaczego).

## Routing and Remote Access Server Setup Wizard

### Remote Access

You can set up this server to receive both dial-up and VPN connections.

☒ VPN

A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

☐ Dial-up

A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

< Back

Next >

Cancel

## Routing and Remote Access Server Setup Wizard

### VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethernet	Intel(R) PRO/1000 MT ...	192.168.100.100
Ethernet 2	Intel(R) PRO/1000 MT ...	88.88.88.88

☒ Enable security on the selected interface by setting up static packet filters.

Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

< Back

Next >

Cancel

## Routing and Remote Access Server Setup Wizard

### IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

☐ Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly.  
If you do not use a DHCP server, this server will generate the addresses.

☒ From a specified range of addresses

< Back

Next >

Cancel

## Routing and Remote Access Server Setup Wizard

### Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number
192.168.100.20	192.168.100.30	11

New...

Edit...

Delete

< Back

Next >

Cancel

## Routing and Remote Access Server Setup Wizard

### Managing Multiple Remote Access Servers

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

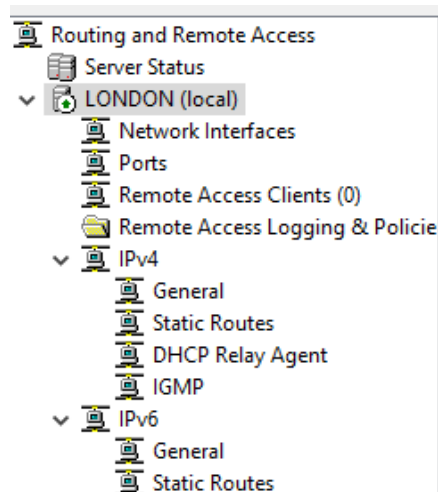
Do you want to set up this server to work with a RADIUS server?

- ☒ No, use Routing and Remote Access to authenticate connection requests
- ☐ Yes, set up this server to work with a RADIUS server

< Back

Next >

Cancel



Jacek Gula Properties

Remote control Remote Desktop Services Profile COM+

General Address Account Profile Telephones Organization

Member Of Dial-in Environment Sessions

Network Access Permission

☒ Allow access

☐ Deny access

☐ Control access through NPS Network Policy

☐ Verify Caller-ID:

Callback Options

☒ No Callback

☐ Set by Caller (Routing and Remote Access Service only)

☐ Always Callback to:

☐ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

☐ Apply Static Routes

Define routes to enable for this Dial-in connection.

## Settings

Home

Find a setting

### Network & Internet

Status

Ethernet

Dial-up

VPN

Proxy

## VPN



Add a VPN connection



wioska Galów  
No Internet

### Advanced Options

Allow VPN over metered networks



On

Allow VPN while roaming



On

## Add a VPN connection

Connection name

wioska Galów

Server name or address

88.88.88.88

VPN type

Automatic

Type of sign-in info

User name and password

User name (optional)

jgula

Password (optional)

••••••••

☒ Remember my sign-in info

Save

Cancel



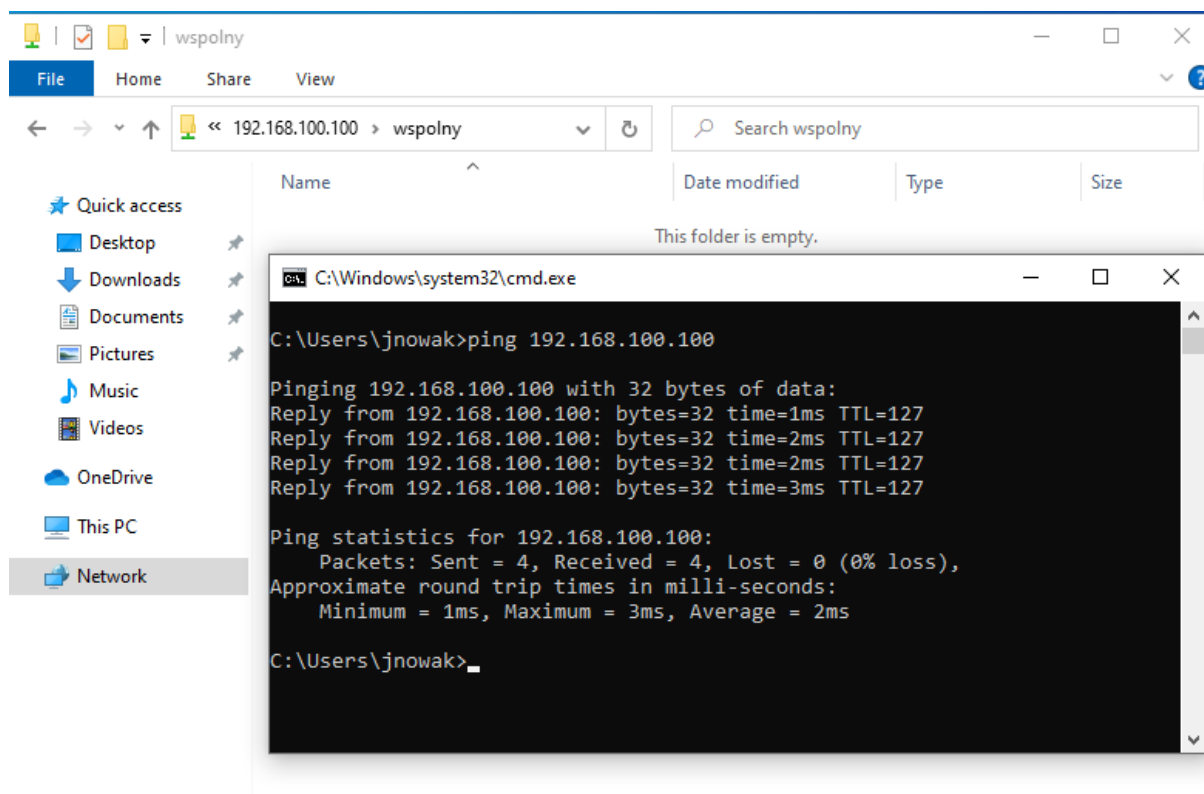
Network 3  
No Internet



wioska Galów  
Connected

Disconnect



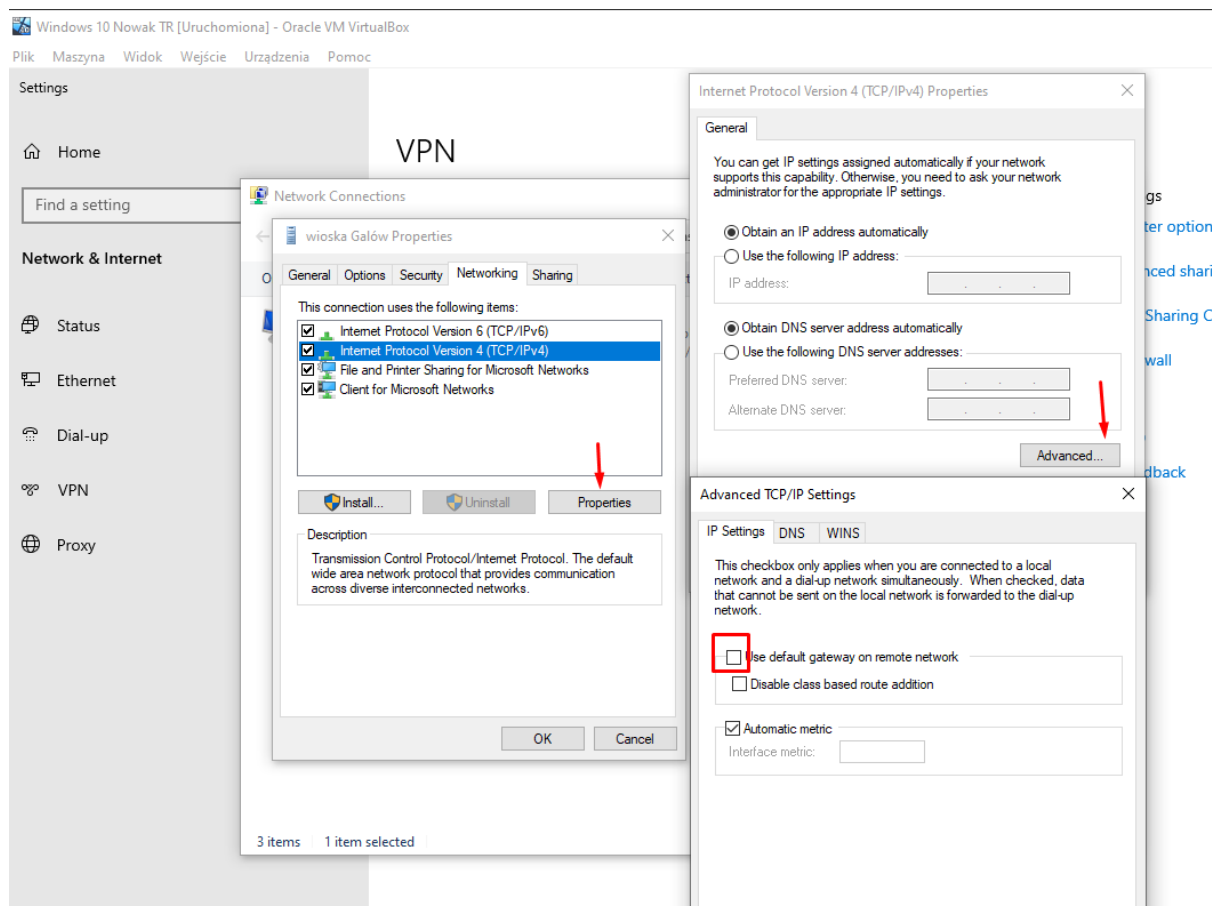


## Zadanie 2

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Pan Jacek Gula któremu zostało w jego laptopie służbowym skonfigurowane połączenie VPN narzeka, że po zrealizowaniu połączenia nie działa mu w sposób prawidłowy połączenie z siecią Internet (nie może otworzyć żadnej strony internetowej, klient poczty elektronicznej nie może się połączyć z serwerem poczty, itd.), przy czym dostęp do zasobów firmy (serwera plików, serwera terminalowego, itd.) może uzyskać w sposób prawidłowy.

Twoim zadaniem jest więc rozwiązanie powyższego problemu poprzez usunięcie w kliencie VPN na laptopie Pana Jacka Guli, korzystania z bramy w sieci zdalnej firmy przez tegoż klienta VPN.



Tablica routingu przed wyłączeniem:

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          On-link          192.168.100.28    26
88.88.88.0                  255.255.255.0    On-link          88.88.88.10      4506
88.88.88.10                 255.255.255.255  On-link          88.88.88.10      4506
88.88.88.88                 255.255.255.255  On-link          88.88.88.10      4251
88.88.88.255                255.255.255.255  On-link          88.88.88.10      4506
127.0.0.0                   255.0.0.0        On-link          127.0.0.1         4556
127.0.0.1                   255.255.255.255  On-link          127.0.0.1         4556
127.255.255.255             255.255.255.255  On-link          127.0.0.1         4556
192.168.100.28              255.255.255.255  On-link          192.168.100.28    281
224.0.0.0                   240.0.0.0        On-link          127.0.0.1         4556
224.0.0.0                   240.0.0.0        On-link          88.88.88.10      4506
224.0.0.0                   240.0.0.0        On-link          192.168.100.28    26
255.255.255.255             255.255.255.255  On-link          127.0.0.1         4556
255.255.255.255             255.255.255.255  On-link          88.88.88.10      4506
255.255.255.255             255.255.255.255  On-link          192.168.100.28    281
=====
Persistent Routes:
None
```

I po wyłączeniu:

IPv4 Route Table					
=====					
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	88.88.88.0	255.255.255.0	On-link	88.88.88.10	281
	88.88.88.10	255.255.255.255	On-link	88.88.88.10	281
	88.88.88.88	255.255.255.255	On-link	88.88.88.10	26
	88.88.88.255	255.255.255.255	On-link	88.88.88.10	281
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	192.168.100.0	255.255.255.0	192.168.100.20	192.168.100.29	26
	192.168.100.29	255.255.255.255	On-link	192.168.100.29	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
	224.0.0.0	240.0.0.0	On-link	88.88.88.10	281
	224.0.0.0	240.0.0.0	On-link	192.168.100.29	281
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	255.255.255.255	255.255.255.255	On-link	88.88.88.10	281
	255.255.255.255	255.255.255.255	On-link	192.168.100.29	281
=====					
Persistent Routes:					
None					

## Zadanie 3

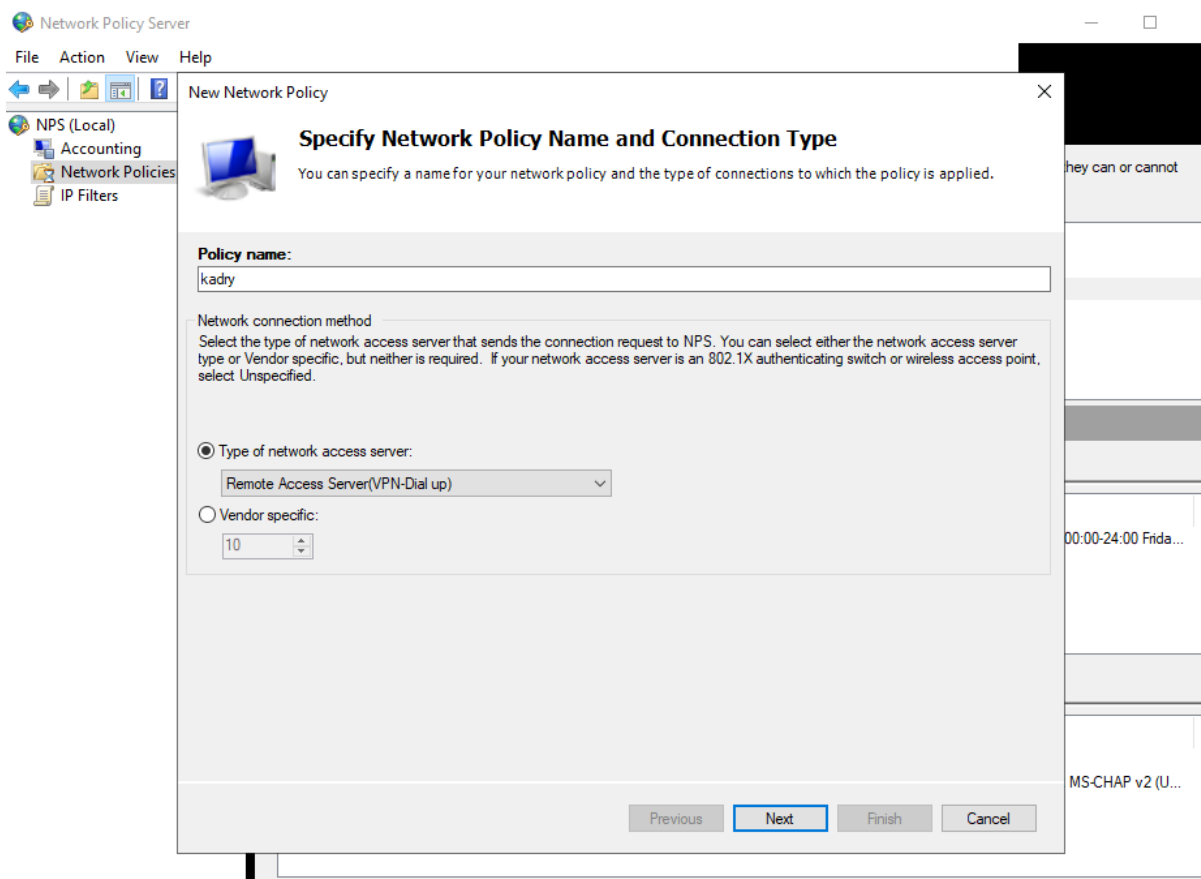
Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Otrzymałeś polecenie aby w zainstalowanym w systemie Windows Server "London" ustalić dla grupy "Kadry" zasady dostępu zdalnego poprzez usługę VPN w taki sposób, aby:


- możliwe było połączenie z serwerem VPN tylko w godzinach od 8:00 do 18:00 w dni powszednie,
- jeżeli połączenie VPN będzie bezczynne (nie będzie żadnej transmisji danych poprzez to połączenie) przez 10 minut, to połączenie ma się automatycznie rozłączyć.




Twoim zadaniem jest więc:


- 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 bezczynne (nie będzie żadnej transmisji danych poprzez to połączenie) przez 10 minut, to połączenie ma się automatycznie rozłączyć
- zweryfikowanie działania utworzonej zasady dostępu zdalnego w systemie Windows "Nowak"



### Network Policies


 Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
 kadry	Enabled	1	Grant Access	Remote Access Serv...
 Connections to other access servers	Enabled	999999	Deny Access	Unspecified
 Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified

 kadry

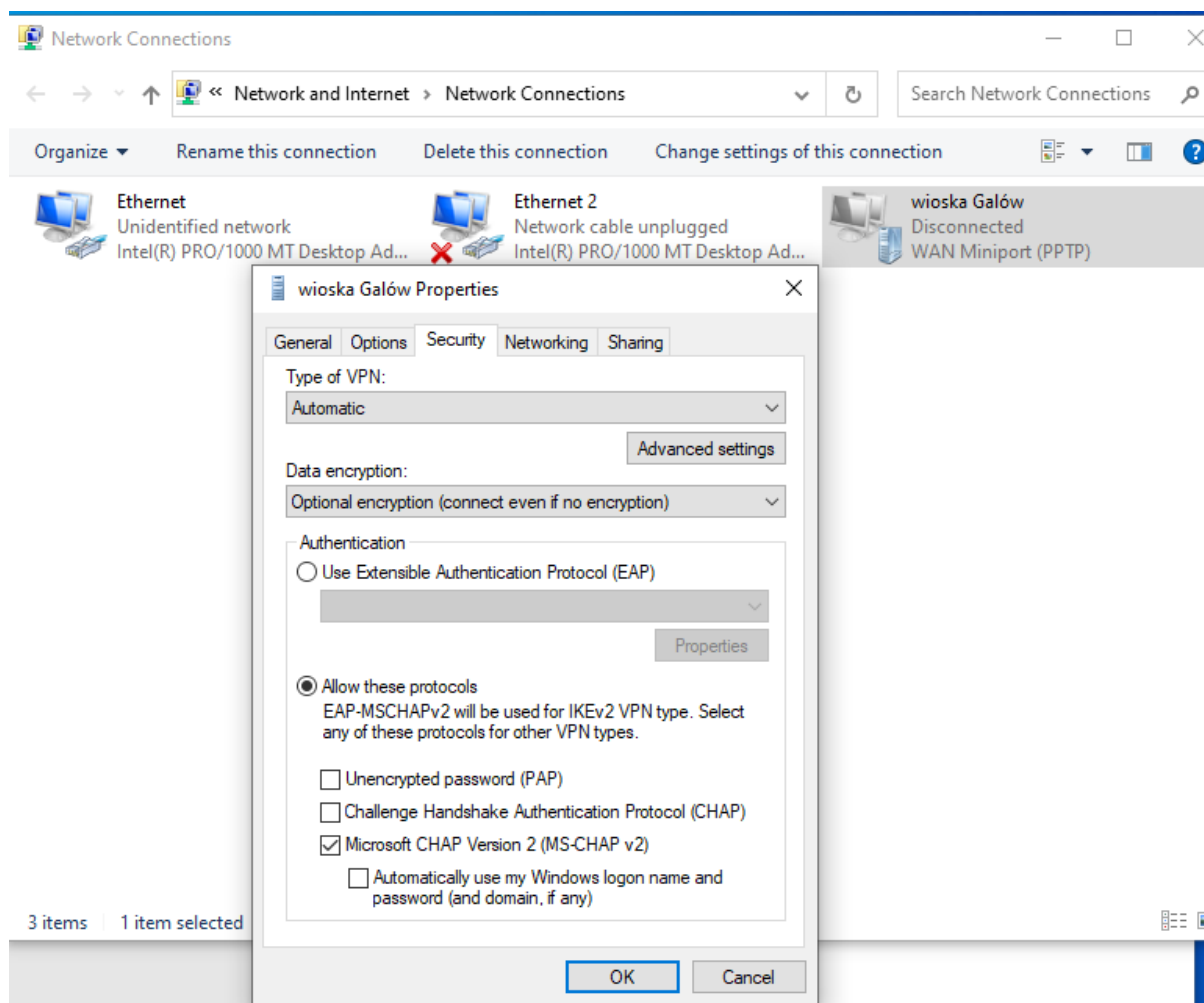
Conditions - If the following conditions are met:

Condition	Value
User Groups	CONTOSO\kadry

Settings - Then the following settings are applied:

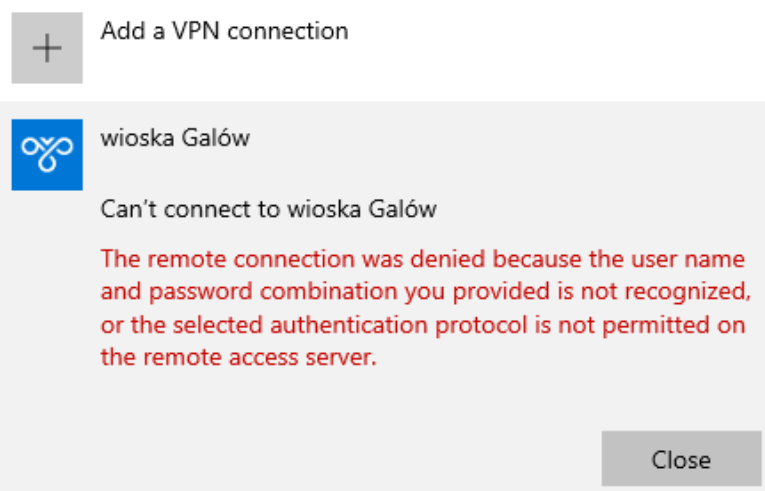
Setting	Value
Access Permission	Grant Access
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 O...
Framed-Protocol	PPP
Idle Timeout	10 minutes
Service-Type	Framed
Day and Time Restrictions	Monday 08:00-18:00 Tuesday 08:00-18:00 Wednesday 08:00-18:00 Thursday 08:00-18:00 Friday 08:...

ustawienie tymczasowe:



Próba połączenia na innych poświadczeniach konta z grupy kadry:

## VPN



nie można się połączyć ponieważ na serwerze jest inna godzina:



a jak ustaliliśmy można się łączyć od 8 do 18

## Zadanie 4

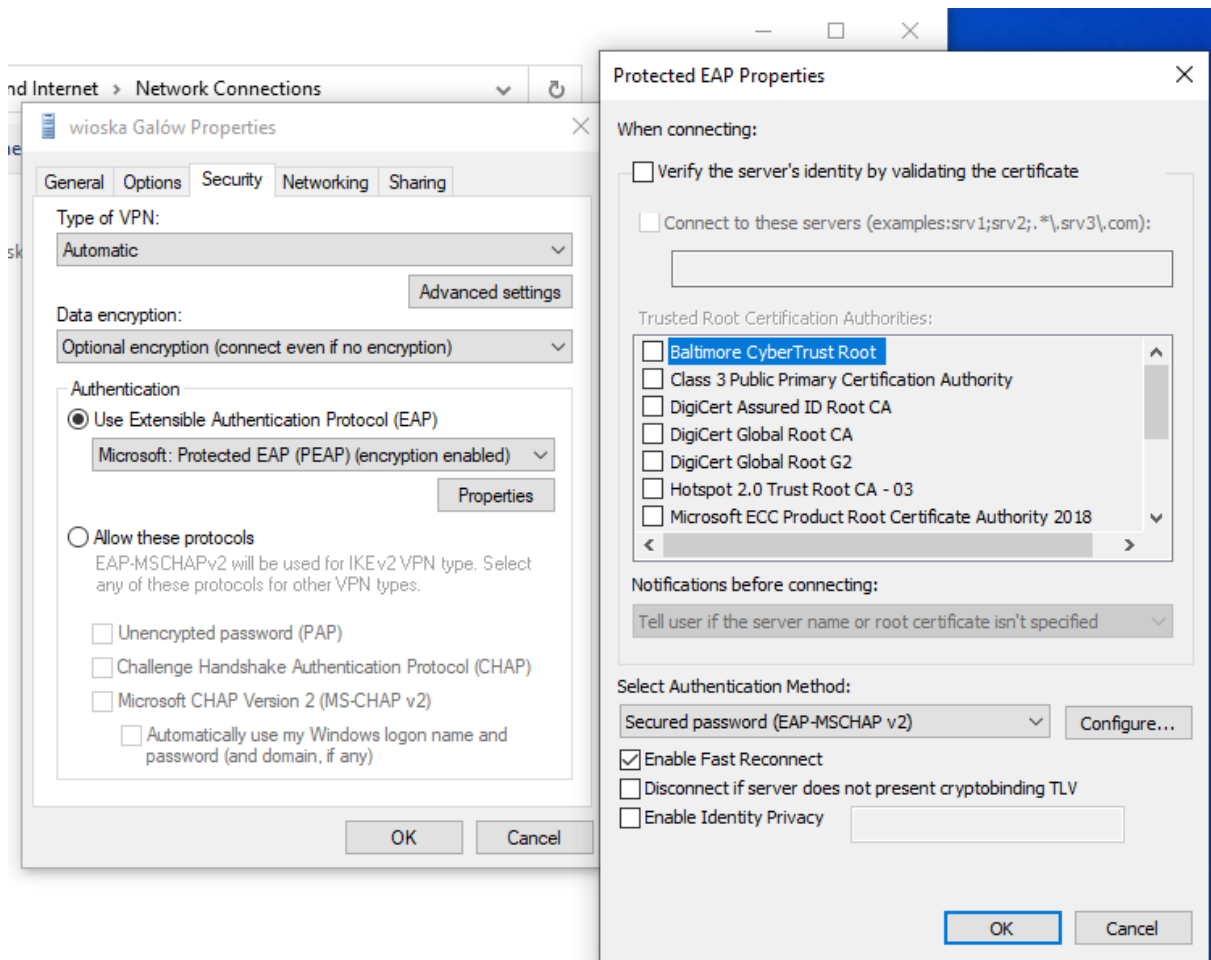
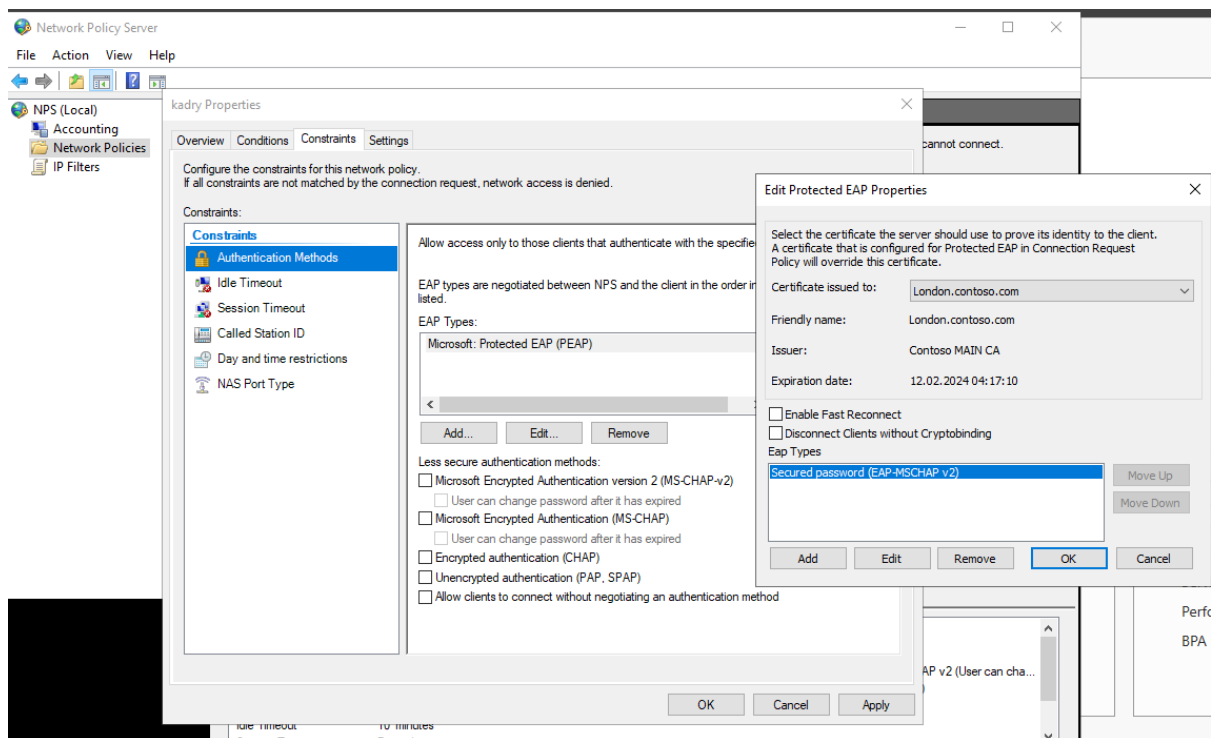
Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Przeczytałeś, że wdrożona przez ciebie usługa VPN typu client-to-site oparta na protokole PPTP oraz metodzie uwierzytelniania MS-CHAPv2 nie jest zbyt bezpieczna, a znacznie bezpieczniejszym rozwiązaniem jest oparcie jej na metodzie uwierzytelniania PEAP-MS-CHAPv2 wykorzystującej certyfikat serwera.

Chciałbyś więc zmodyfikować konfigurację usługi VPN w systemie Windows Server "London", tak aby użytkownicy w sposób wymuszony korzystali z połączenia w oparciu o metodę uwierzytelniania PEAP-MS-CHAPv2.

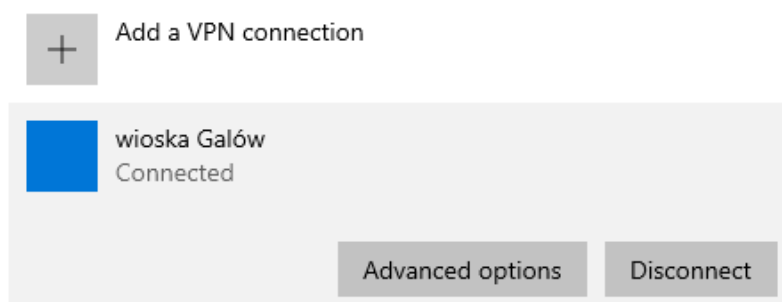
Twoim zadaniem jest więc:

- sprawdzenie w systemie Windows Server "London", 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 "*london.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 8





## VPN



## Zadanie 5

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Kilku pracowników przekazało, że niestety nie są w stanie uruchomić połączenia VPN gdy są w domu.

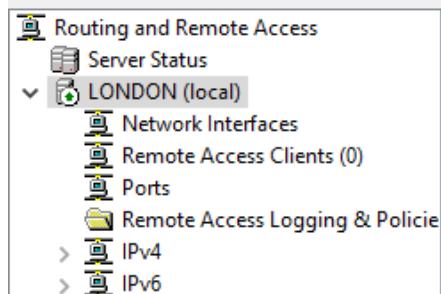
Szukając przyczyny, udało ci się wykryć, że problem stanowi zaporą ogniową blokująca ruch połączenia VPN uruchomiona u dostawcy internetowego tychże osób.

Przeczytałeś, że w rozwiązaniu problemu może pomóc wykorzystanie protokołu SSTP, co chciałbyś wdrożyć w swojej usłudze VPN.

Dodatkowo chciałbyś uniemożliwić użytkownikom łączenie się z wykorzystaniem mniej bezpiecznego protokołu PPTP.

Twoim zadaniem jest więc:

- powiązanie we właściwościach roli "Routing i dostęp zdalny" w ramach zabezpieczeń, certyfikatu SSL "london.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 firmy 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"



### LONDON (local) Properties

? X

General Security IPv4 IPv6 IKEv2 PPP Logging

The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider:  
 Windows Authentication Configure...

Authentication Methods...

The accounting provider maintains a log of connection requests and sessions.

Accounting provider:  
 Windows Accounting Configure...

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☐ Allow custom IPsec policy for L2TP/IKEv2 connection

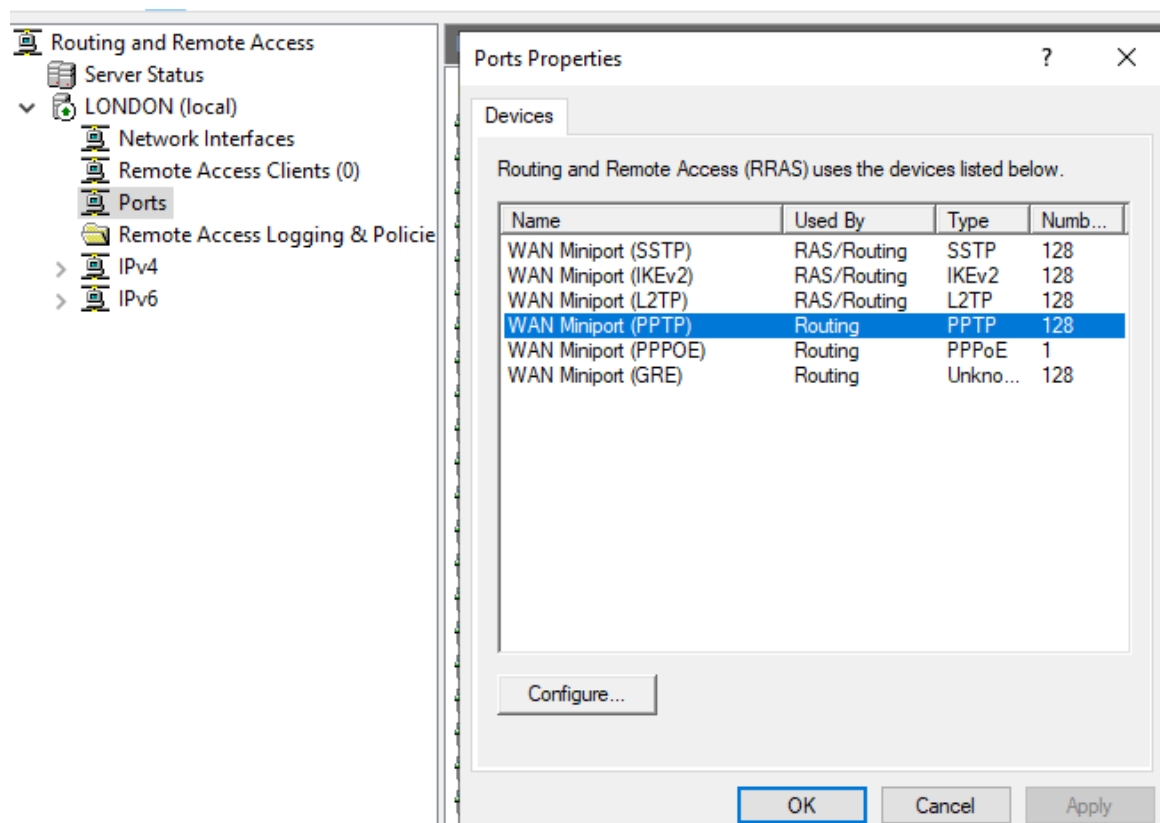
Preshared Key:

SSL Certificate Binding:  
☐ Use HTTP

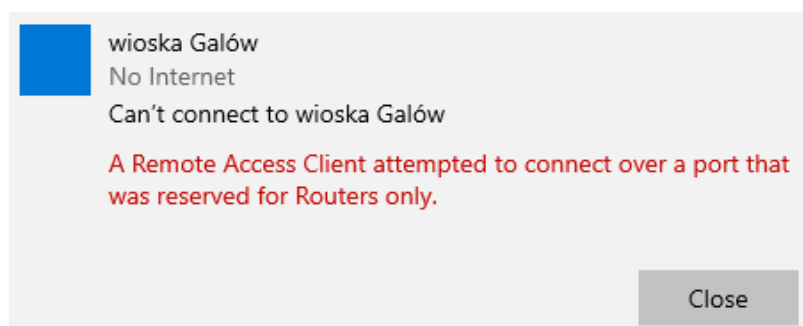
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

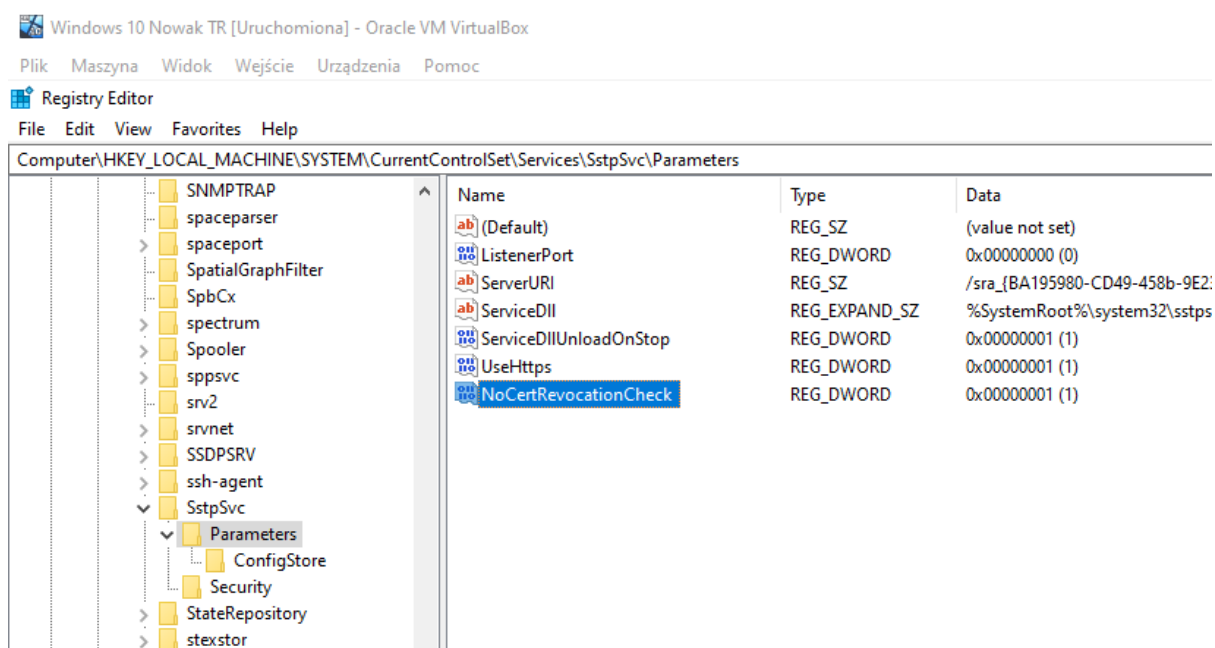
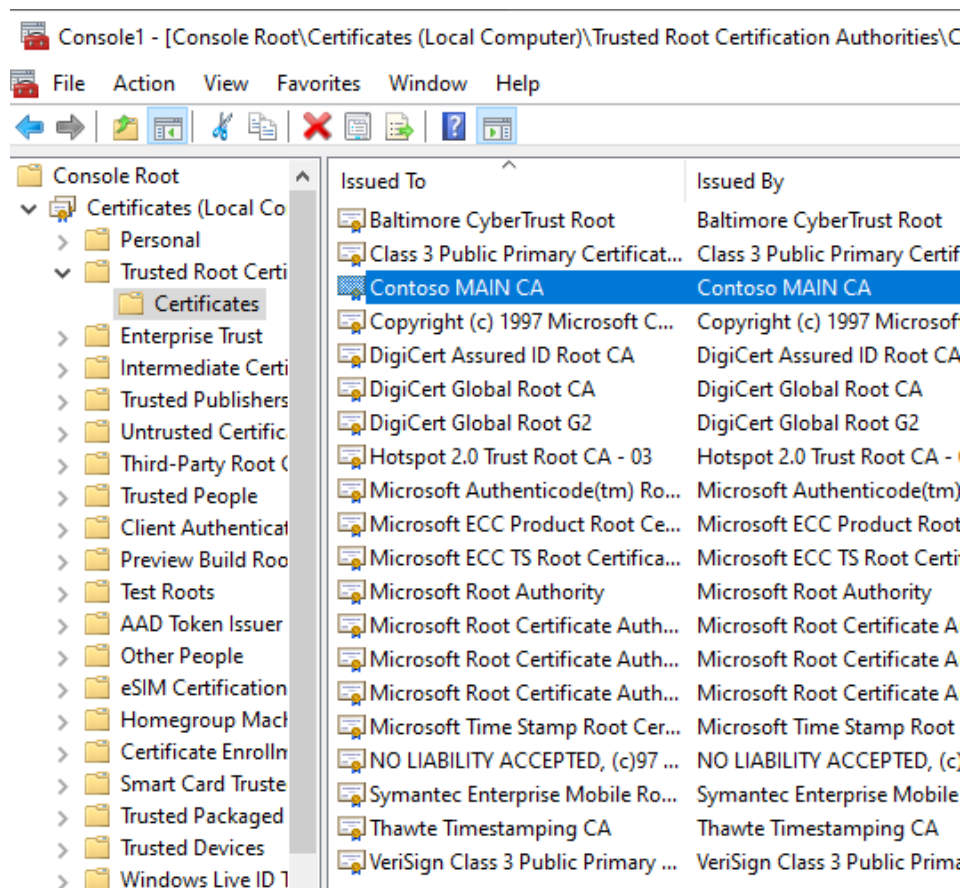
Certificate: London.contoso.com View

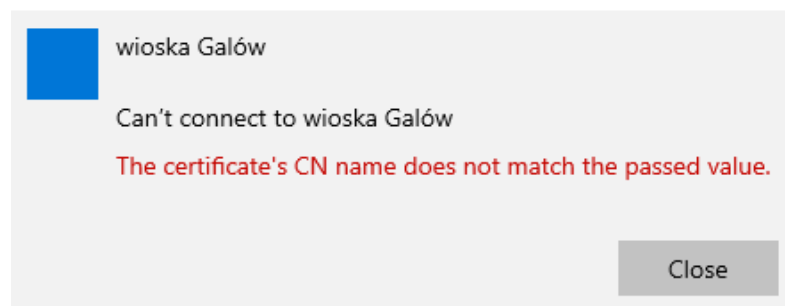
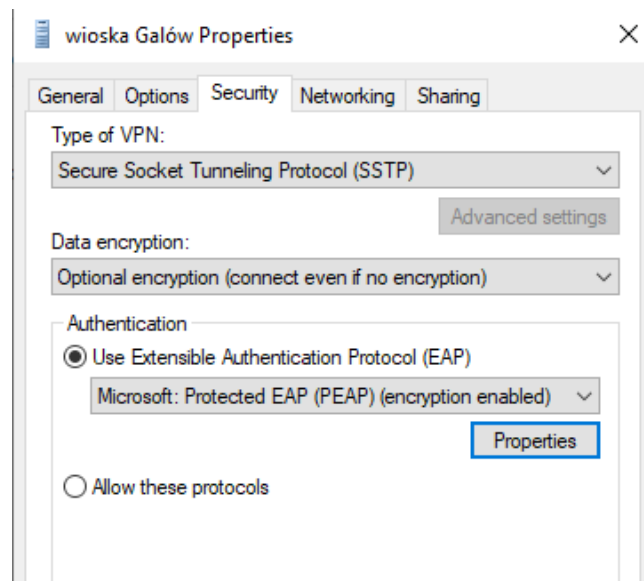
OK Cancel Apply



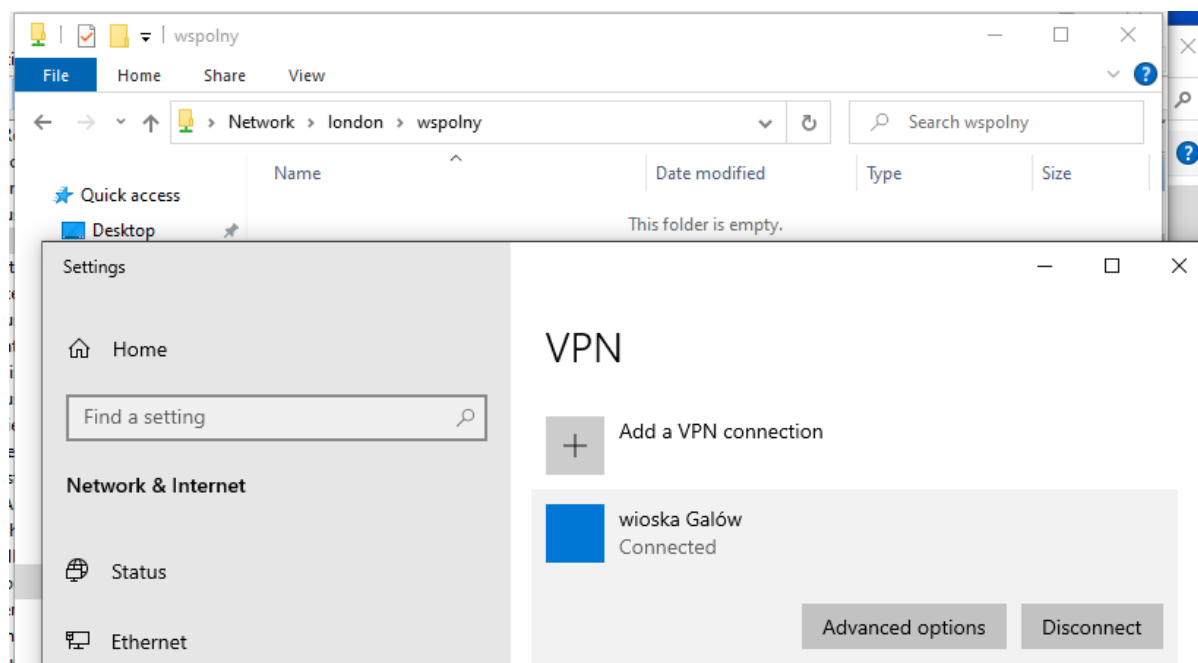
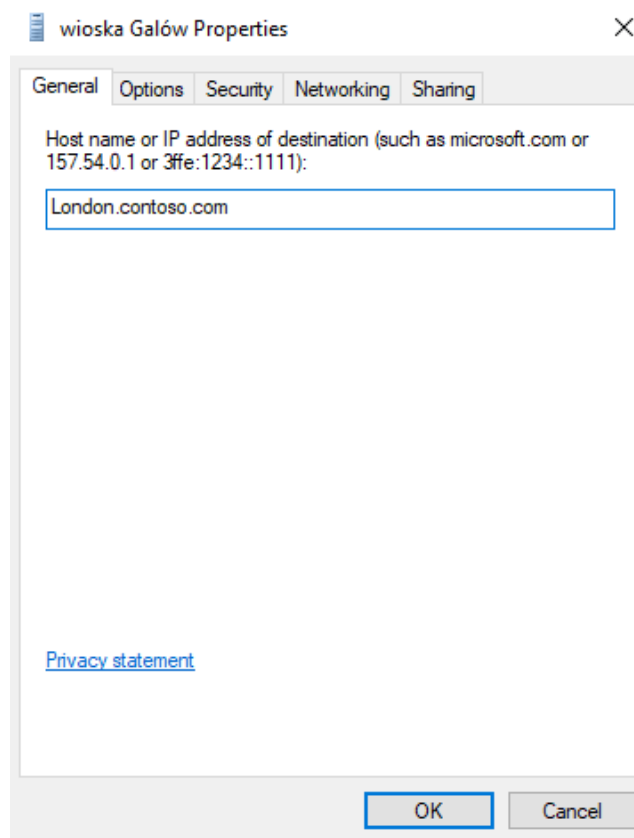
Teraz nie da się połączyć po PPTP:







dodanie do pliku hosts liniiki `88.88.88.88 London.contoso.com` oraz zmiana:



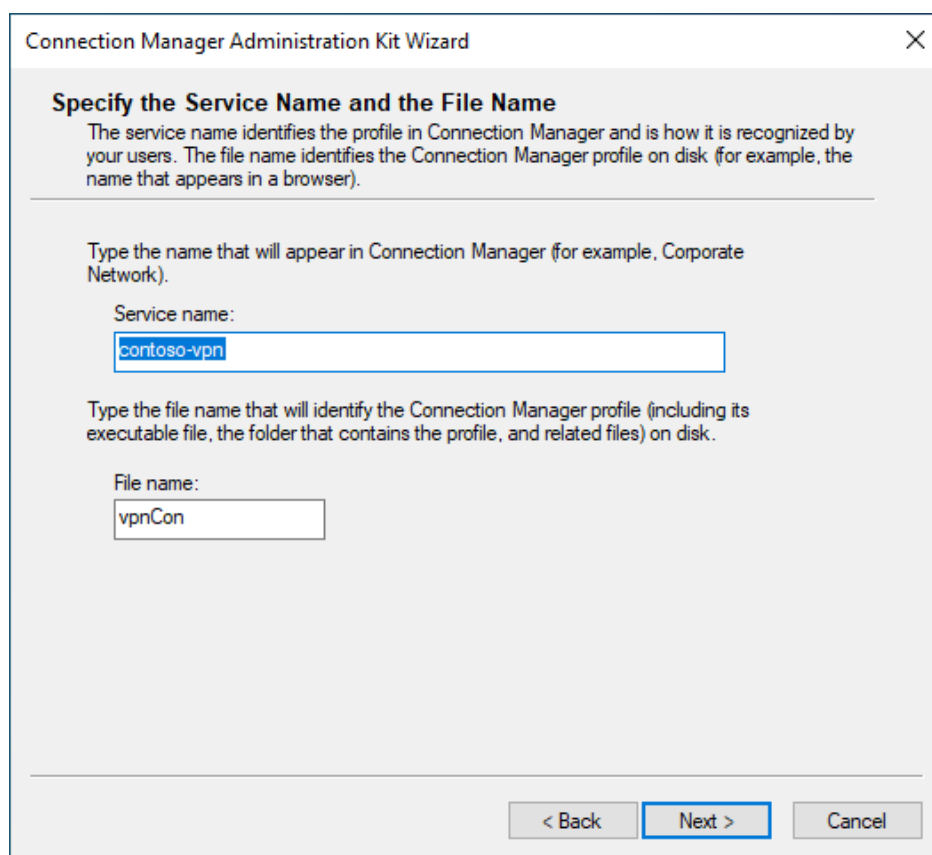
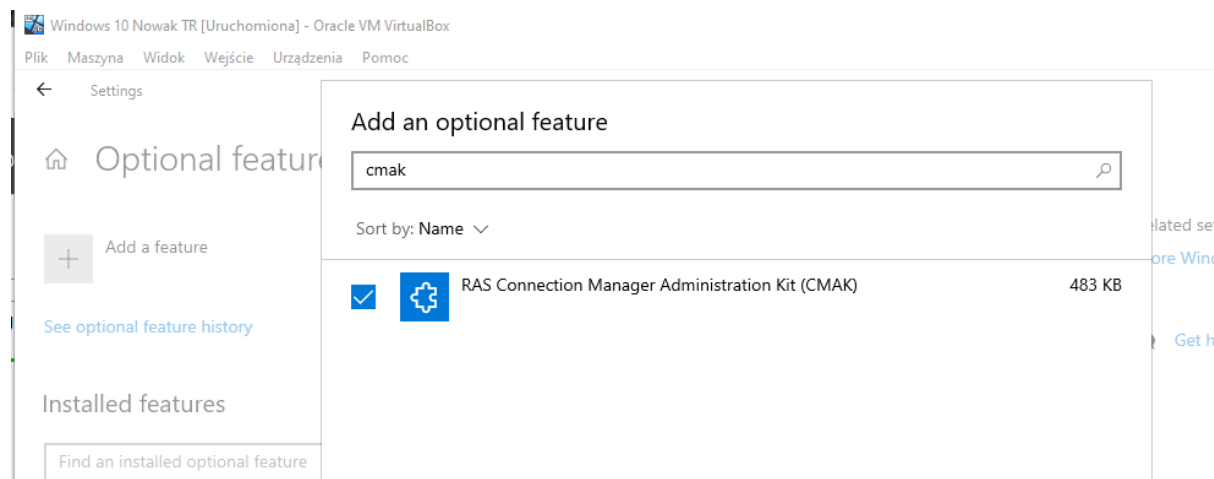
## Zadanie 6

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Otrzymałeś od przełożonego prośbę, aby dla uproszczenia użytkownikom konfiguracji połączeń VPN na ich komputerach domowych, przygotować plik automatyzujący tą czynność z wykorzystaniem narzędzia CMAK.

Twoim zadaniem jest więc:

- dodanie w systemie Windows "Nowak" 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



Connection Manager Administration Kit Wizard

### Add Support for VPN Connections

A Connection Manager profile can connect to a remote network by using a virtual private network (VPN) either through a dial-up connection or the Internet.

To add support for VPN connections to this profile, select the appropriate check box, and then provide the name or IP address of a VPN server.

☒ Phone book from this profile

☐ Phone books from the merged profiles

VPN server name or IP address

☒ Always use the same VPN server

London.contoso.com

☐ Allow the user to choose a VPN server before connecting

Browse...

☐ Use the same user name and password for VPN and dial-up connections

< Back Next > Cancel

Connection Manager Administration Kit Wizard

### Your Connection Manager Profile is Complete and Ready to Distribute

Your Connection Manager profile has been successfully compiled into a self-installing executable (.exe) file, which is located at:

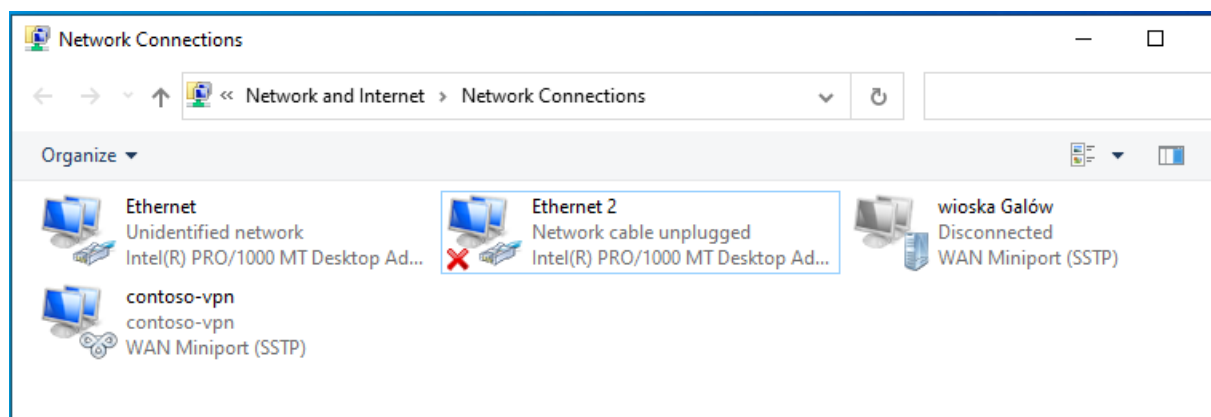
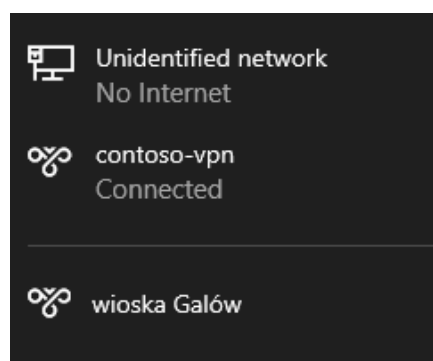
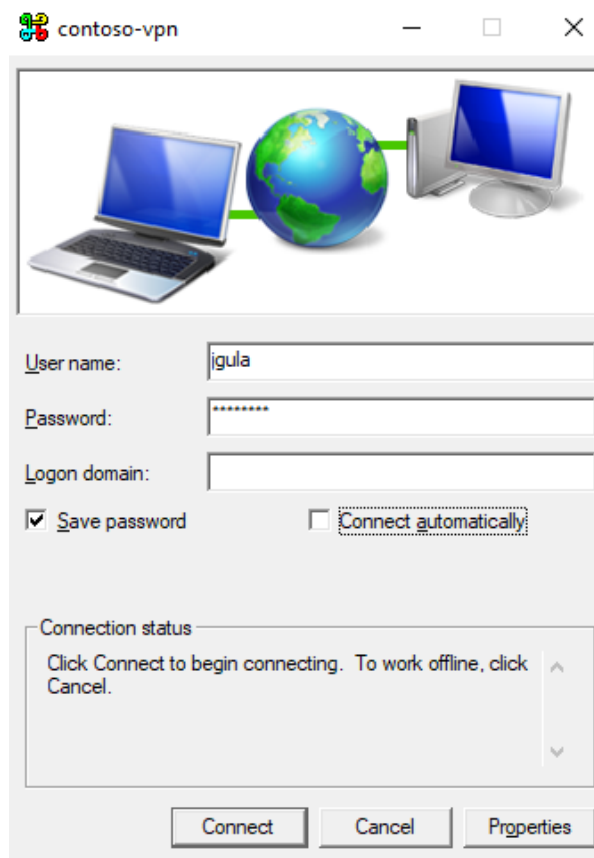
AK\Profiles\Windows Vista and above\vpnCon\vpnCon.exe

To close this wizard, click Finish.

< Back Finish Cancel

Ctrl+C, Ctrl+V do eksploratora plików i samo zacznij instalację.





## Zadanie 7

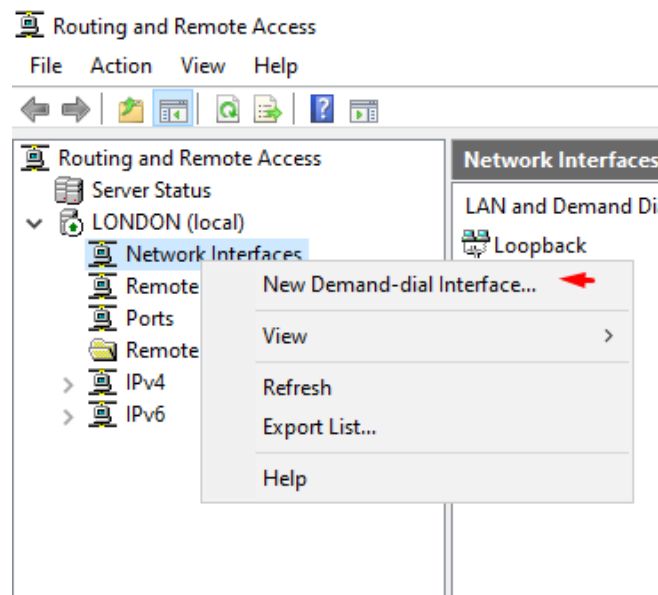
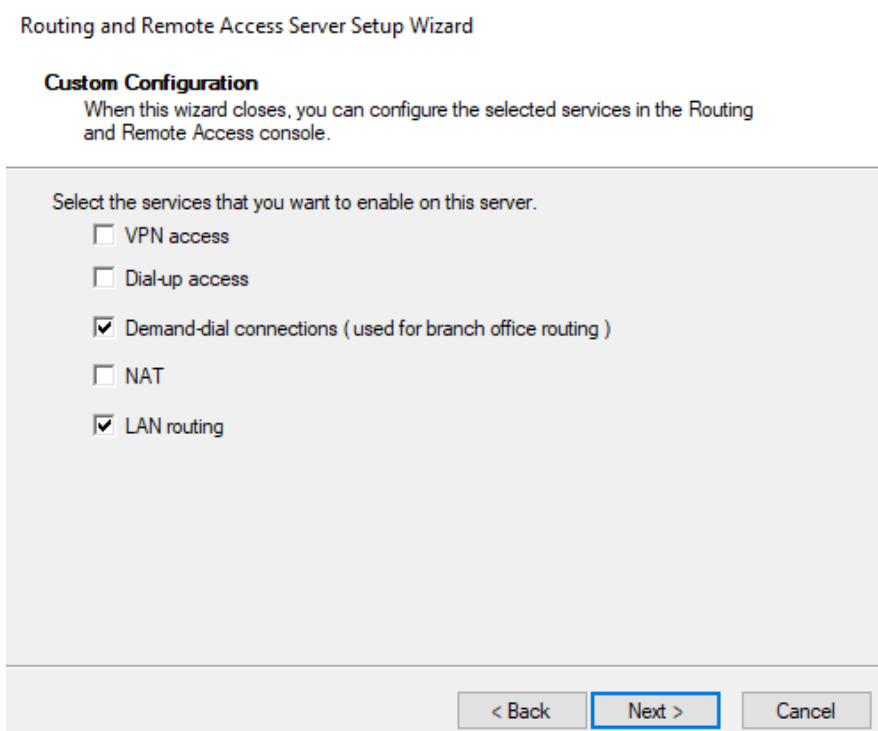
Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Otrzymałeś polecenie, aby skonfigurować możliwość komunikacji między komputerami w London oraz w Glasgow, korzystającymi z we. adresów IP (London - 192.168.100.0/24, Glasgow - 172.16.0.0/24), za pomocą tunelu VPN typu site-to-site, z wykorzystaniem lokalnych systemów Windows Server "London", oraz Windows Server "Glasgow"

Twoim zadaniem jest więc:

- zainstalować w systemie Windows Server "Glasgow" rolę "Remote Access"
- włączyć w "Remote Access" usługę "Routing LAN" oraz usługę "Połączenia z wybieraniem numeru na żądanie" (w ramach konfiguracji niestandardowej)
- skonfigurować w "Usłudze 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: *london.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: *192.168.100.0/24*
  - Poświadczenia telefonowania: *vpn1/Zaq12wsx*
  - Poświadczenia połączeń wychodzących: *vpn1/Zaq12wsx*
- w ramach właściwości utworzonego interfejsu zaznaczyć opcję "Połączenie trwałe", która pozwoli na automatyczne uruchamianie tunelu VPN przy starcie systemu operacyjnego
- w systemie Windows Server "London" skonfigurować w "Usłudze 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: *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: *172.16.0.0/24*
  - Poświadczenia telefonowania: *vpn1/Zaq12wsx*

- Poświadczenia połączeń wychodzących: *vpn1/Zaq12wsx*
- w ramach właściwości utworzonego interfejsu zaznaczyć opcję "*Połączenie trwałe*", która pozwoli na automatyczne uruchamianie tunelu VPN przy starcie systemu operacyjnego
- przetestować połączenie VPN



Demand-Dial Interface Wizard

**Interface Name**  
You can type a friendly name for this connection.

Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.

Interface name:

vpn1

< Back Next > Cancel

Demand-Dial Interface Wizard

**Connection Type**

Select the type of demand-dial interface you want to create.

- ☐ Connect using a modem, ISDN adapter, or other device
- ☒ Connect using virtual private networking (VPN)
- ☐ Connect using PPP over Ethernet (PPPoE)

Demand-Dial Interface Wizard

**VPN Type**

Select the type of VPN connection you want to create.

- ☐ Automatic selection
- ☒ Point to Point Tunneling Protocol (PPTP)
- ☐ Layer 2 Tunneling Protocol (L2TP)
- ☐ IKEv2

## Demand-Dial Interface Wizard

### Destination Address

What is the name or address of the remote router?



Enter the name or IP address of the router you are connecting to.

Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

london.contoso.com

## Demand-Dial Interface Wizard

### Protocols and Security

Select transports and security options for this connection.



Select all that apply:

- ☒ Route IP packets on this interface.
- ☒ Add a user account so a remote router can dial in
- ☐ Send a plain-text password if that is the only way to connect
- ☐ Use scripting to complete the connection with the remote router

## Demand-Dial Interface Wizard



### Static Routes for Remote Networks

A static route is a manually defined, permanent route between two networks.



To activate this demand-dial connection, you must add a static route to the network. Specify the IP address of the remote networks this network will communicate with.

Static Routes:

Destination	Network Mask/Prefix length	Metric
192.168.100.0	255.255.255.0	1

Add

Remove

## Demand-Dial Interface Wizard

### Dial-In Credentials

Configure the user name and password that the remote router will use when it dials in to this server.



You need to set the dial-in credentials that remote routers will use when connecting to this interface. A user account will be created on this router with the information that you enter here.

User name:

Password:

Confirm password:

## Demand-Dial Interface Wizard

### Dial-Out Credentials

Supply the user name and password to be used when connecting to the remote router.



You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.

User name:

Domain:

Password:

Confirm password:

### vpn1 Properties

General Options Security Networking

Connection type

☐ Demand-dial  
Idle time before hanging up:

☒ Persistent connection

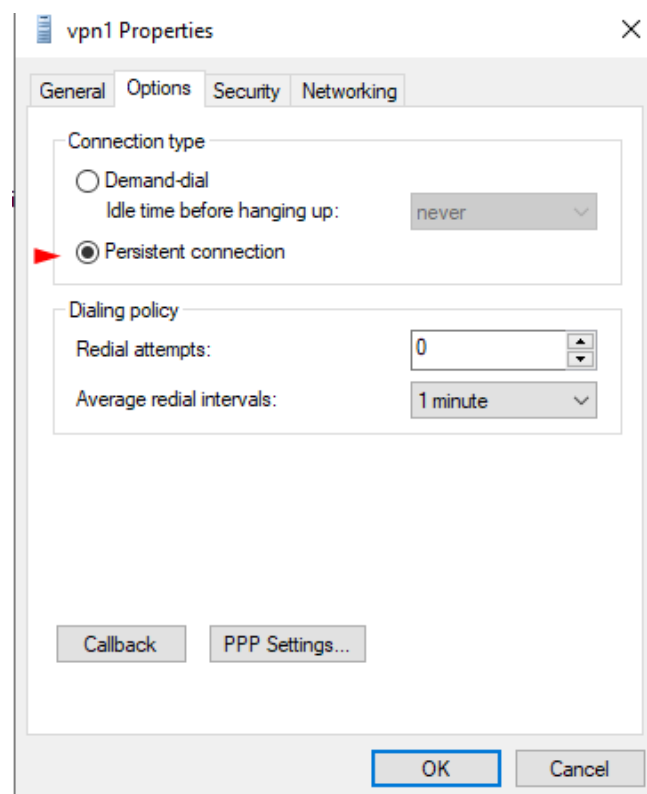
Dialing policy

Redial attempts:

Average redial intervals:

Callback PPP Settings...

Podobna konfiguracja na drugim serwerze



Routing and Remote Access		Network Interfaces		
Server Status				
LONDON (local)				
Network Interfaces				
Remote Access Clients (0)				
Ports				
Remote Access Logging & Policies				
IPv4				
General				
Static Routes				
DHCP Relay Agent				
IGMP				

LAN and Demand Dial Interfaces		Type	Status	Connection State
vpn1		Demand-dial	Enabled	Connected
Loopback		Loopback	Enabled	Connected
Internal		Internal	Enabled	Connected
Ethernet 2		Dedicated	Enabled	Connected
Ethernet		Dedicated	Enabled	Connected

sprawdzenie czy połączenie działa:

Network Interfaces			
LAN and Demand Dial Interfaces	Type	Status	Connection Sta
vpn1	Demand-dial	Enabled	Connected

```

C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time=3ms TTL=126
Reply from 172.16.0.1: bytes=32 time=2ms TTL=126
Reply from 172.16.0.1: bytes=32 time=14ms TTL=126
Reply from 172.16.0.1: bytes=32 time=3ms TTL=126

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\Users\Administrator>

```

przy wyłączeniu połączenia:

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Request timed out.
Reply from 172.16.0.1: bytes=32 time=3ms TTL=126
Reply from 172.16.0.1: bytes=32 time=2ms TTL=126
Reply from 172.16.0.1: bytes=32 time=2ms TTL=126

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Request timed out.
Reply from 88.88.88.88: Destination host unreachable.
Reply from 172.16.0.1: bytes=32 time=2ms TTL=126
Reply from 172.16.0.1: bytes=32 time=3ms TTL=126

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

```

Przy czym gdy mamy włączoną opcję "Persistent connection", połączenie po chwili zostaje wznowione.



## Zadanie 8

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

Przeczytałeś, że wdrożona przez ciebie usługa VPN typu site-to-site oparta na protokole PPTP nie jest zbyt bezpieczna, a znacznie bezpieczniejszym rozwiązaniem jest oparcie jej na protokole L2TP wykorzystującym certyfikaty.

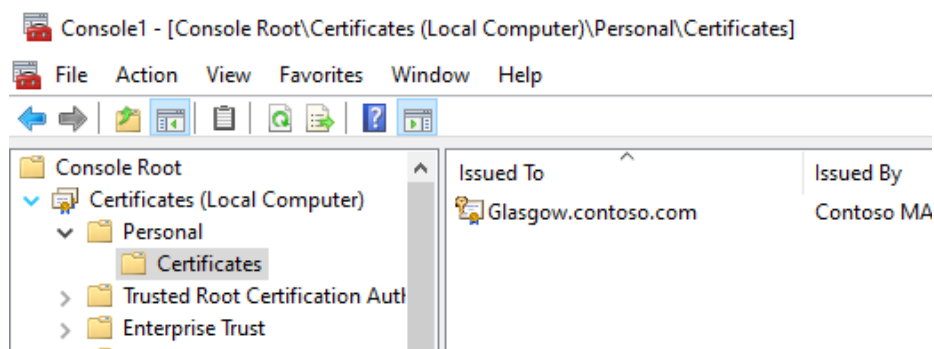
Chciałbyś więc zmodyfikować konfigurację usługi VPN w systemie Windows Server "London" oraz Windows Server "Glasgow" tak, aby serwery te korzystały z połączenia w oparciu o protokół L2TP.

Twoim zadaniem jest więc:

- 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 "London" oraz Windows Server "Glasgow" zmiana we właściwościach interfejsu sieciowego o nazwie *vpn1*, w ramach zabezpieczeń, typu wirtualnej sieci prywatnej na "Protokół L2TP/IPsec" używającego certyfikatów do uwierzytelnienia

---

Generowanie certyfikatu dla glasgow:



---

Konfiguracja na obu serwerach

