T: Sieci wirtualne VPN w Windows Server 2019.

Cel ogólny lekcji:

Celem ogólnym lekcji jest nauczenie uczniów konfiguracji sieci wirtualnych VPN na serwerze Windows Server 2019 oraz kliencie Windows 10. Lekcja ma na celu przekazanie praktycznej wiedzy z zakresu tworzenia bezpiecznych połączeń VPN, zrozumienia korzyści i zastosowań sieci wirtualnych oraz umiejętności konfiguracji routerów NAT.

Cele szczegółowe:

1. Uczniowie powinni poznać pojęcie sieci wirtualnej VPN, zrozumieć zalety i różne zastosowania tego rozwiązania.
2. Uczniowie powinni opanować proces instalacji i konfiguracji wymaganych ról na serwerze Windows Server 2019.
3. Uczniowie powinni być w stanie poprawnie skonfigurować interfejsy sieciowe na serwerze i kliencie zgodnie z zadanymi wymaganiami, włączając w to nadanie nazw i adresów MAC adapterom.
4. Uczniowie powinni zdobyć umiejętność tworzenia migawek systemu przed rozpoczęciem konfiguracji VPN, co pozwoli na łatwiejszą diagnozę ewentualnych problemów.
5. Uczniowie powinni umieć dokonać zmiany ustawień DNS na kliencie Windows 10.
6. Uczniowie powinni być w stanie wyłączyć zapory na serwerze i kliencie zgodnie z zadanymi krokami.
7. Uczniowie powinni zrozumieć procedurę konfiguracji routerów NAT, a także potrafić zapisywać ją w zeszycie.
8. Uczniowie powinni być w stanie skonfigurować efektywną sieć VPN między serwerem a klientem, umożliwiającą bezpieczne przesyłanie danych przez Internet.

Ustawienia przed rozpoczęciem lekcji:

Sprawdzenie czy serwer z funkcją kontrolera domeny posiada dwie karty sieciowe. Jeśli nie, uczniowie powinni być w stanie dodać drugą kartę sieciową. W przypadku adresów IP, uczniowie powinni umieć ustawić adres statyczny lub skonfigurować serwer na DHCP. Adresy MAC powinny być dynamicznie uzyskiwane.

Zadania i zgłoszenia:

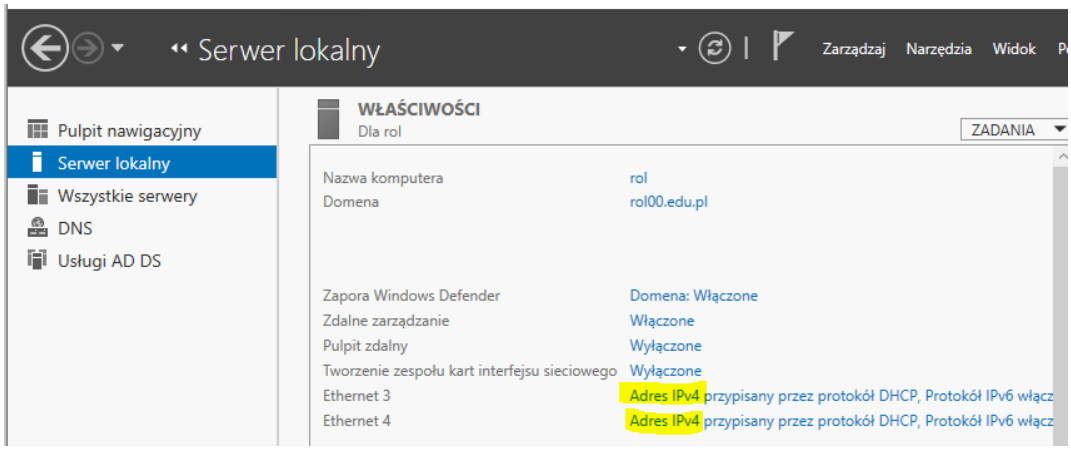
1. Uczniowie powinni krok po kroku dodawać rolę serwera "Dostęp zdalny" zgodnie z poleceniami, zapisując kolejne czynności w zeszycie.
2. Uczniowie powinni konfigurować usługę zasad i dostępu sieciowego, dodając interfejsy, modyfikując zasady sieciowe i sprawdzając reguły na zaporze.
3. Uczniowie powinni konfigurować adapter, tworzyć połączenie VPN, określać sposób łączenia, podawać poświadczenia użytkownika i sprawdzać parametry połączenia.

4. Uczniowie powinni sprawdzać połączonych klientów dostępu zdalnego, analizować tabelę mapowania sesji translatora adresów sieciowych oraz wykonywać pomiary parametrów związanych z połączeniem.
5. Uczniowie powinni wykonywać czynności związane z dołączaniem do domeny, analizować ruch za pomocą Wireshark i wyciągać wnioski z przeprowadzonych analiz.
6. Uczniowie powinni umieć dodawać domenowe konta użytkowników i określać uprawnienia dostępu do sieci.

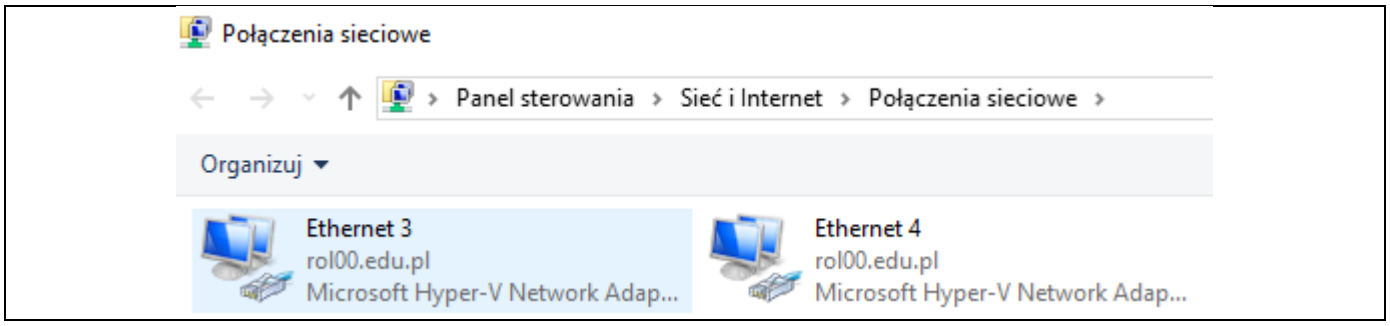
Efekt: Stworzenie funkcjonalnej i bezpiecznej sieci VPN między serwerem a klientem, a także zdobycie umiejętności konfiguracji, analizy oraz utrzymania tego rozwiązania.

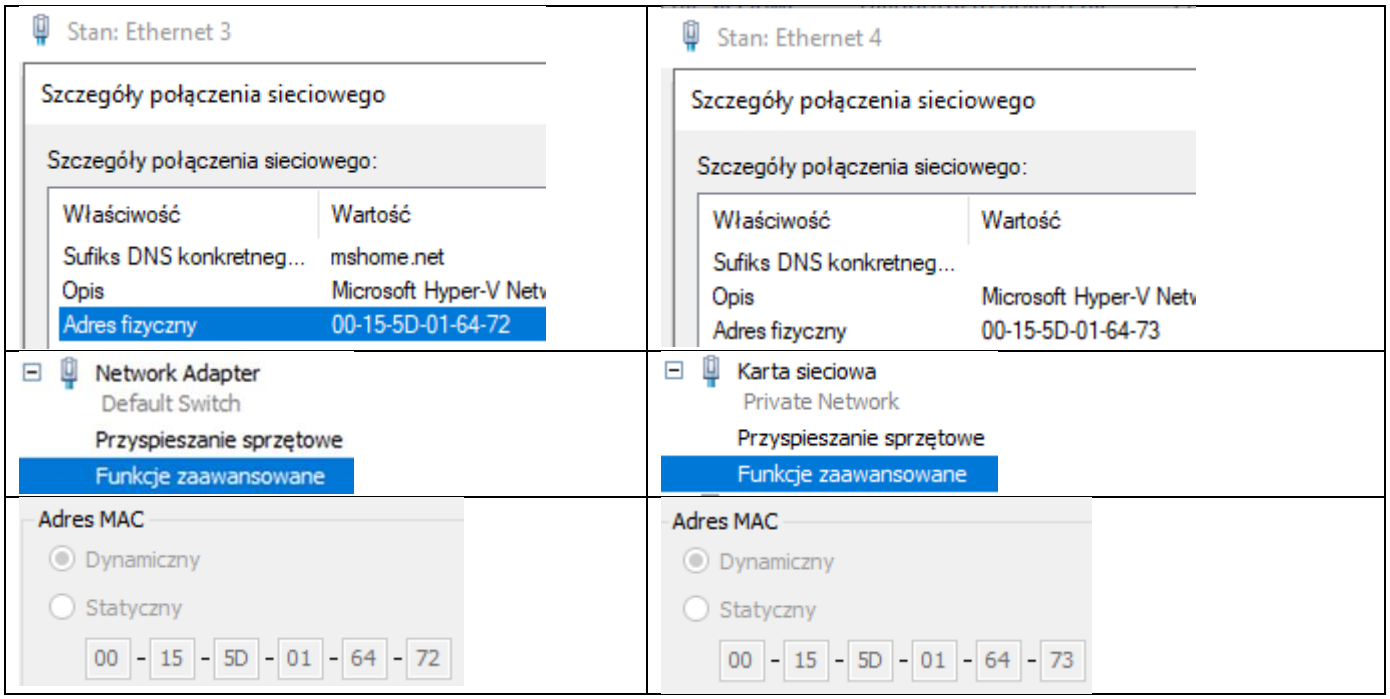
Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne ustawienia

Serwera **z funkcją kontrolera domeny** czy posiada dwie karty sieciowe, jeśli nie to dodaj



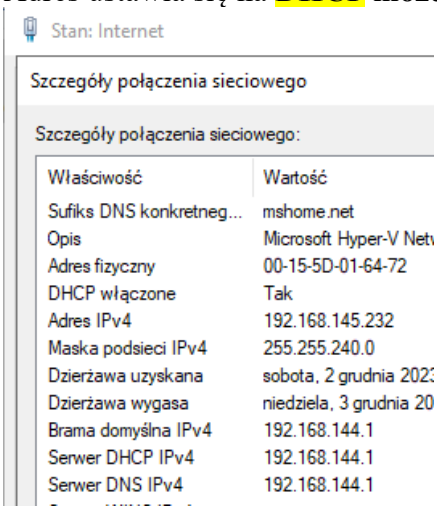
Po przejściu do Połączenia sieciowe patrz poniżej kliknij w jeden lub drugi Adres IPv4.



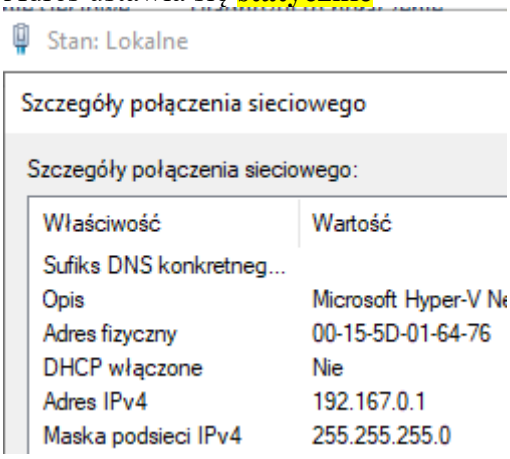


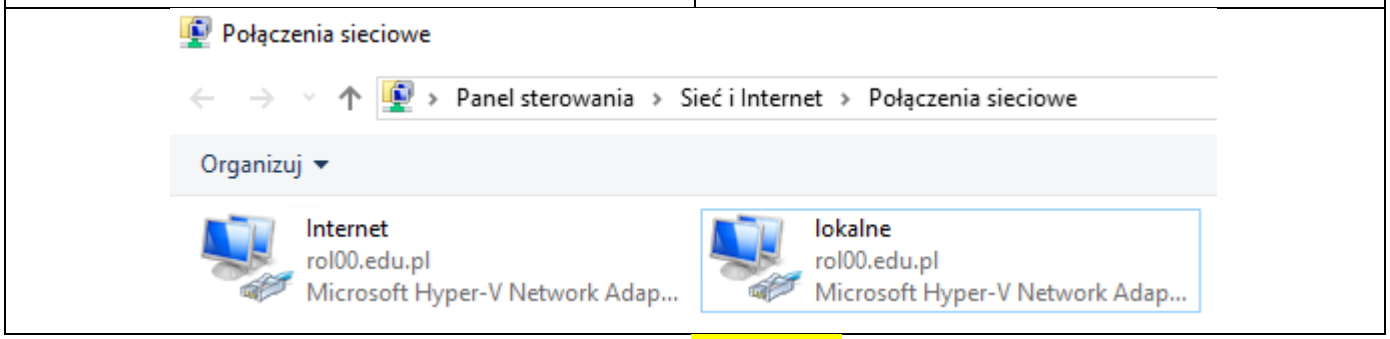
Adresy MAC w tabeli powyżej są dynamicznie uzyskiwane. Ważne, aby zidentyfikować kartę w systemie, że Adres fizyczny w zwirtualizowanym systemie odpowiada Adres MAC z Menedżer funkcji Hyper-V

Adres ustawia się na **DHCP może być inny**



Adres ustawia się **statycznie**





Utwórz punk kontrolny serwera z informacją o treści przed_VPN.

W zeszycie opisz procedurę wykonywania konfiguracji router NAT w Windows Server 2019.

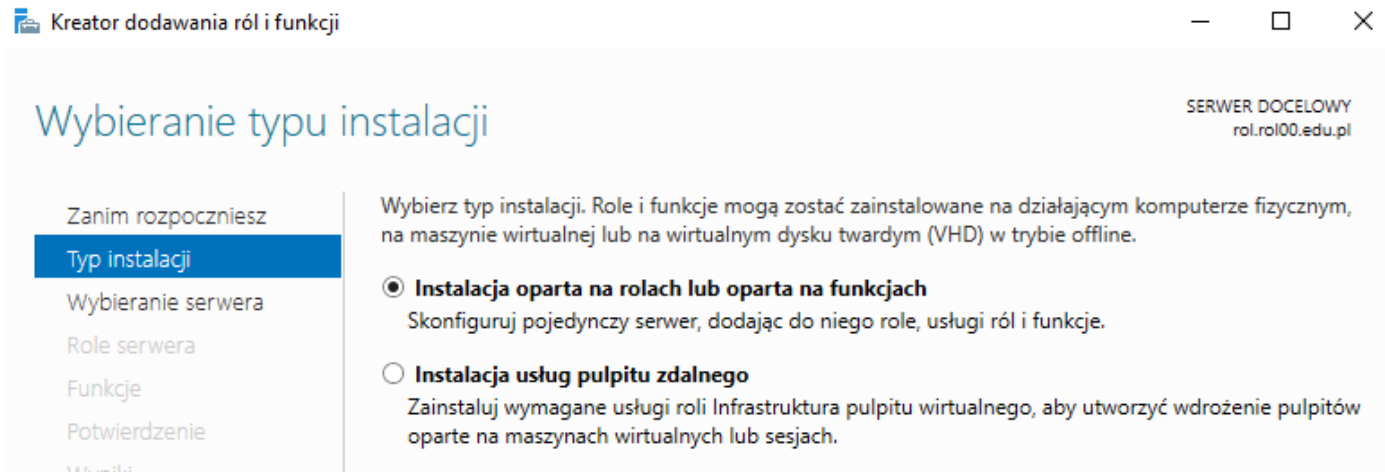
Wszystkie czynności konfiguracyjne należy kolejno zapisać w zeszycie.

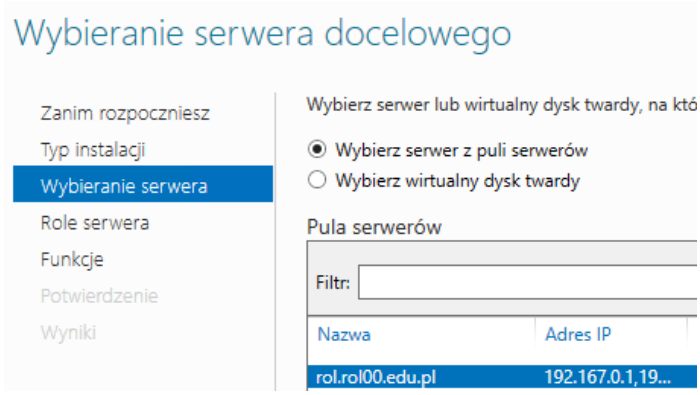
Włącz serwer Windows 2019

1. Dodanie roli serwera „Dostęp zdalny”

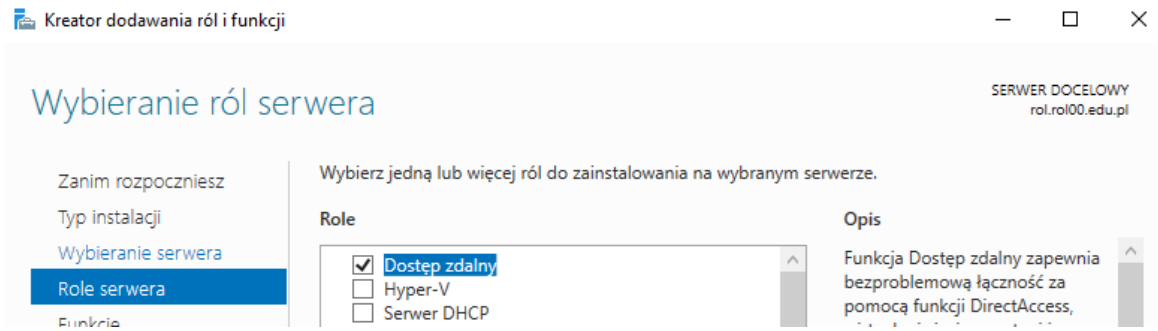
Otwórz Menedżera serwera i wybierz „Dodaj role i funkcje”.

Poniżej tylko istotne okna dla procedury instalacji i konfiguracji, jeśli okna niema poniżej wybierz Dalej



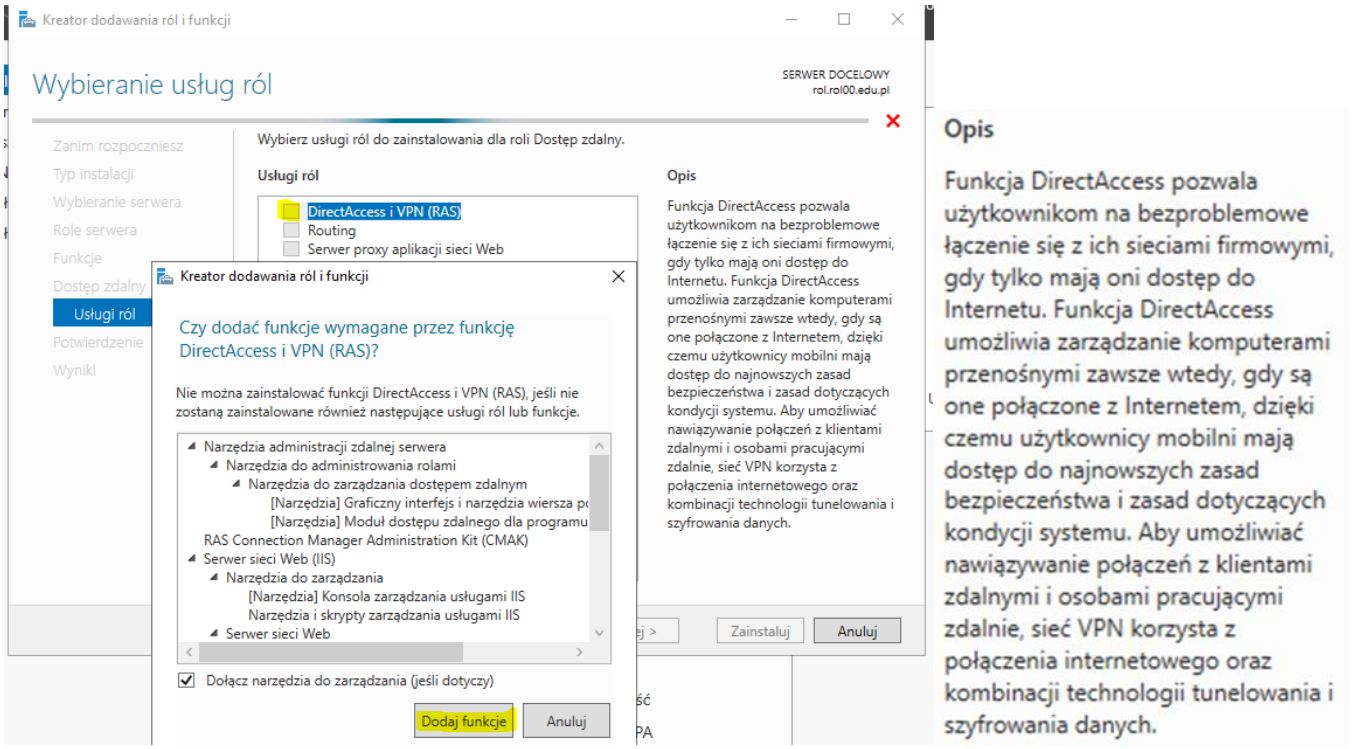


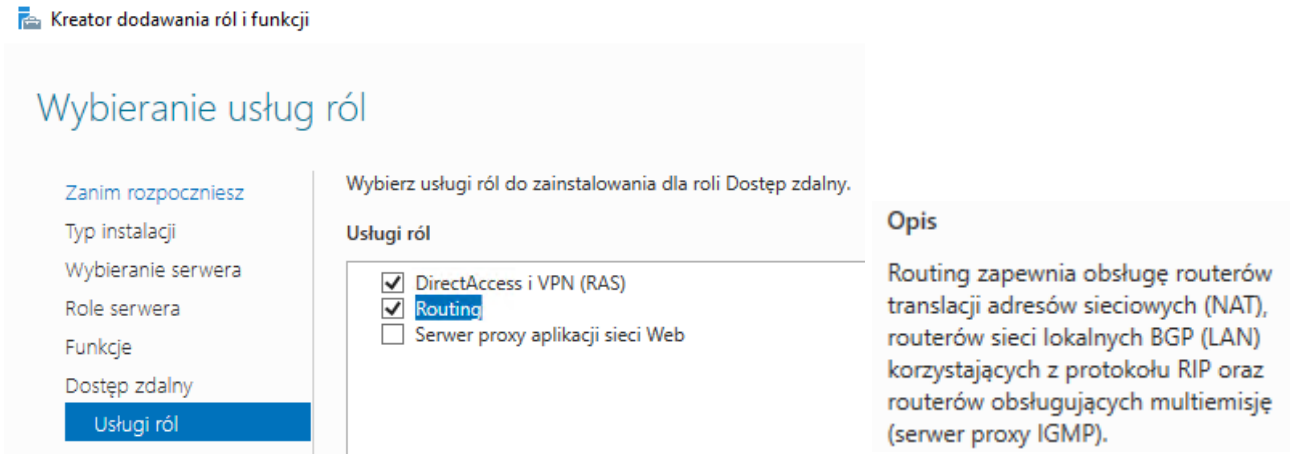
a. Zainstaluj rolę serwera „Dostęp zdalny”.



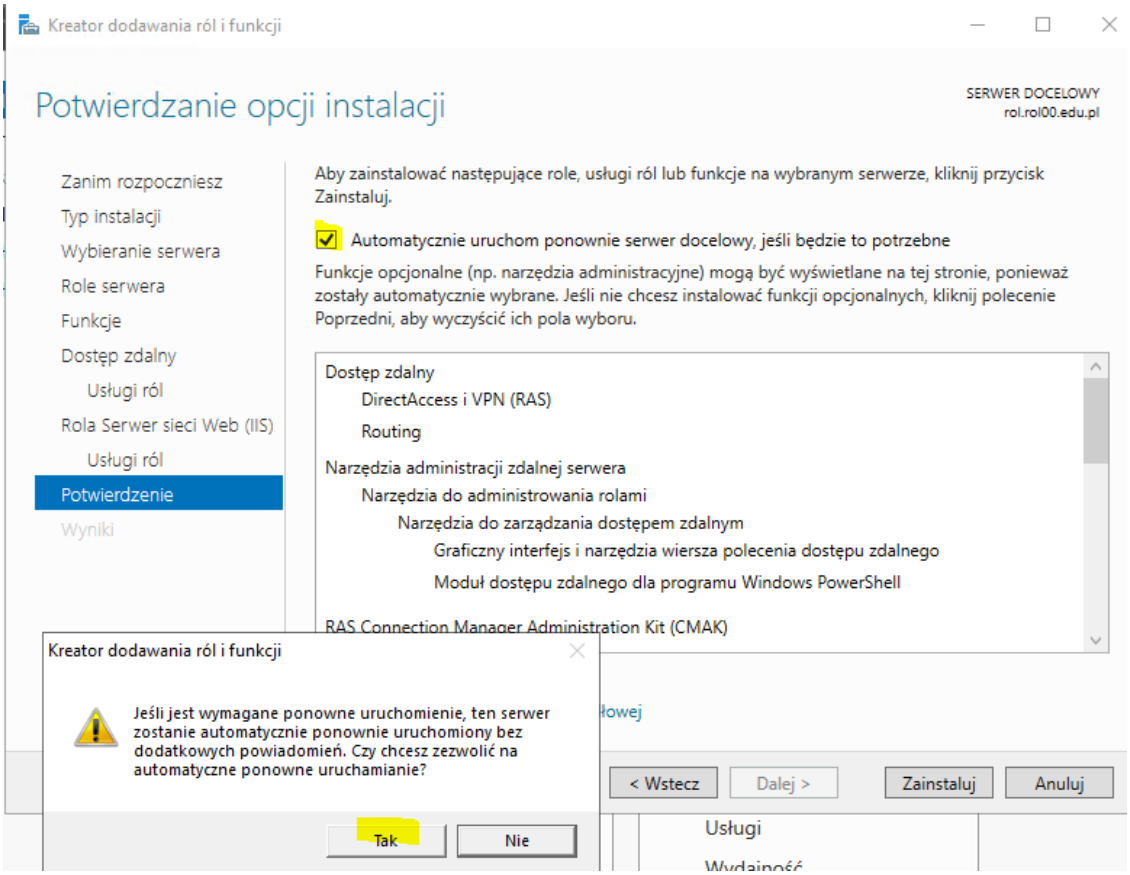
b. Sprecyzuj, które składowe usługi NPAS chcesz zainstalować. By obsłużyć połączenia VPN musisz zainstalować następujący składnik: **Usługi routingu i dostępu zdalnego** (RRAS, Routing and Remote Access) – instaluj obie funkcje, czyli **Routing** i **Usługę dostępu zdalnego**.

Zapisz ten opis w zeszycie. Zapoznaj się z zapisanymi informacjami, kliknij **Dalej**.





c. Po kliknięciu **Dalej** przechodzisz do ekranu potwierdzenia.



d. Gdy wszystko się zgadza, kliknij **Zainstaluj** i nastąpi instalacja roli.

Zgłoszenie 1

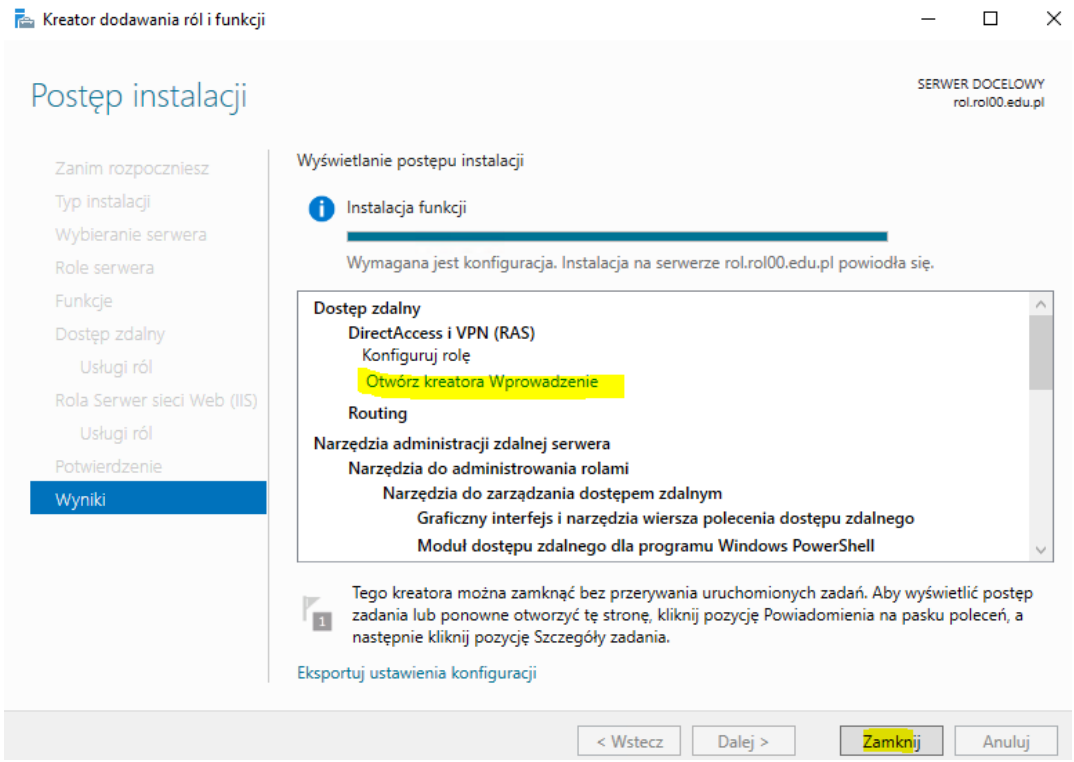
Praktyczna teoria o NAT

NAT to technika, która pozwala na mapowanie adresów IP i portów między dwoma różnymi domenami adresowymi. Jest używana, gdy prywatne adresy IP wewnętrznej sieci muszą komunikować się z zewnętrznymi sieciami, takimi jak Internet.

Urządzenia w sieci prywatnej mają adresy IP np. z zakresu 10.1.4.0/24, natomiast urządzenia w sieci publicznej mają adresy IP np. z zakresu 198.4.2.0/24. Aby umożliwić komunikację między tymi sieciami, router NAT mapuje adresy IP i porty źródłowe urządzeń prywatnych na adresy IP i porty docelowe urządzeń publicznych. W ten sposób, urządzenia prywatne mogą nawiązywać połączenia z urządzeniami publicznymi, a urządzenia publiczne mogą odbierać i odpowiadać na te połączenia.

Działanie VPN

Komputer kliencki łączy się do sieci publicznej, na przykład do Internetu, i inicjuje połączenie VPN do serwera zdalnego. Ten serwer zdalny zwykle znajduje się w podsieci brzegowej organizacji, z którą komputer kliencki próbuje uzyskać połączenie. Po wykonaniu połączenia tworzony jest zaszyfrowany tunel pomiędzy komputerem klienckim a serwerem VPN. Ten zaszyfrowany tunel przenosi ruch sieci lokalnej pomiędzy komputerem klienckim a siecią zdalną, do której komputer się połączył.



e. Sprawdź „!” Postępuj zgodnie z wskazówkami.

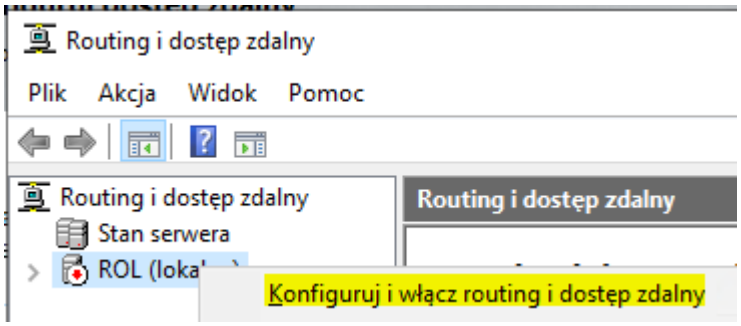
Otwórz kreator Wprowadzanie

Idź do końca kreatora, naciskając „Dalej”. Naciśnij „Zamknij” na ekranie postępu.

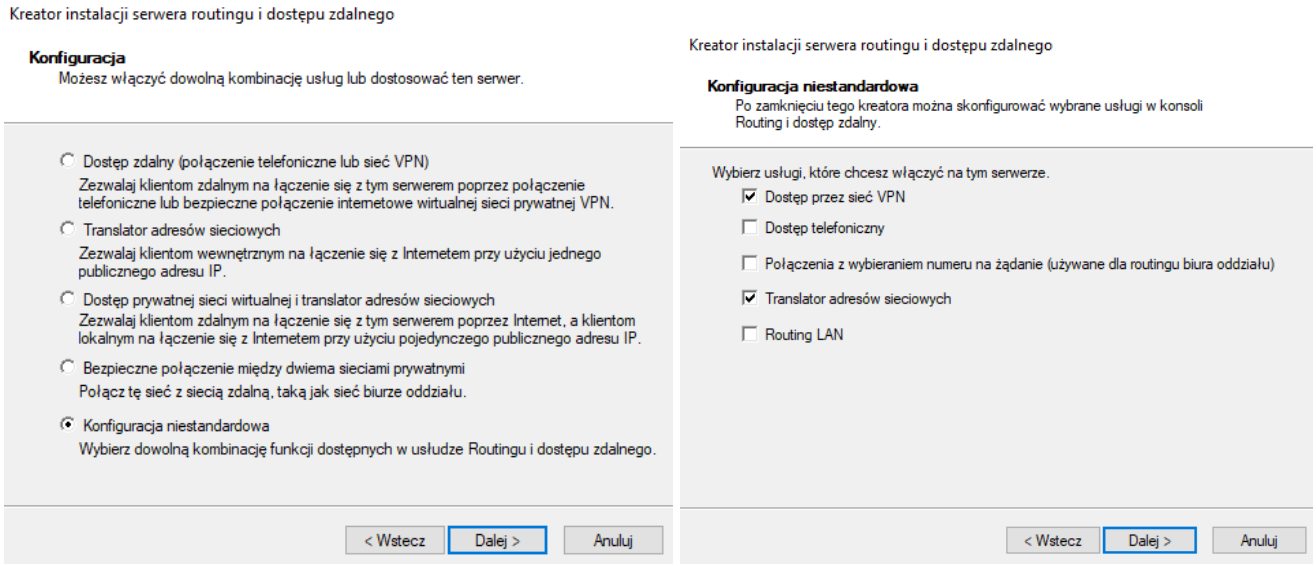
2. Procedura konfiguracji Usługi zasad i dostępu sieciowego.

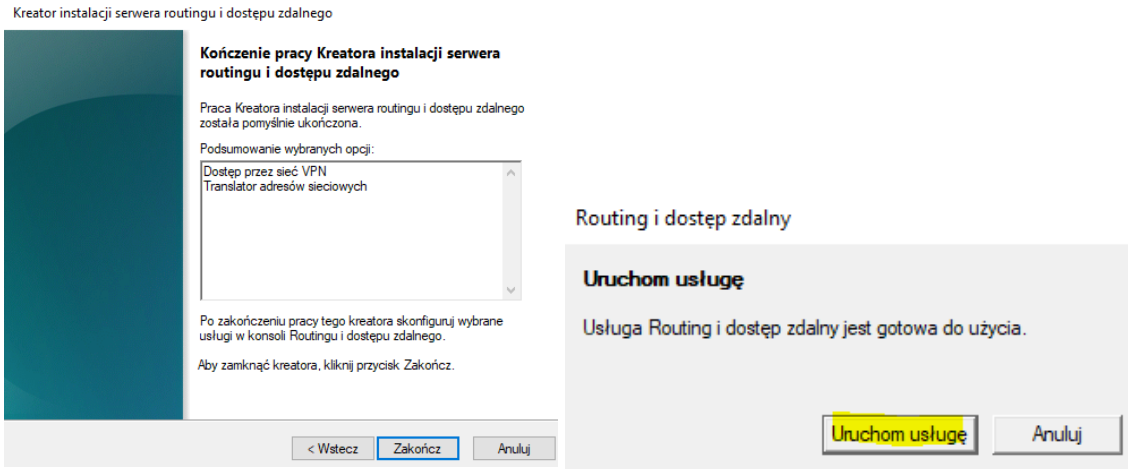
a. Przejdź do otwartego kreator Wprowadzanie

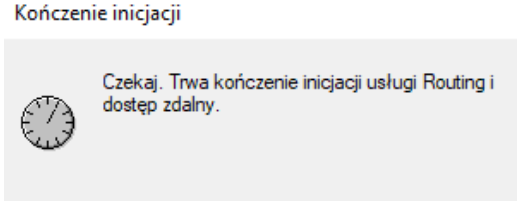
b. Kliknij prawym przyciskiem myszy nazwę serwera i wybierz „Konfiguruj i włącz routing i dostęp zdalny”.



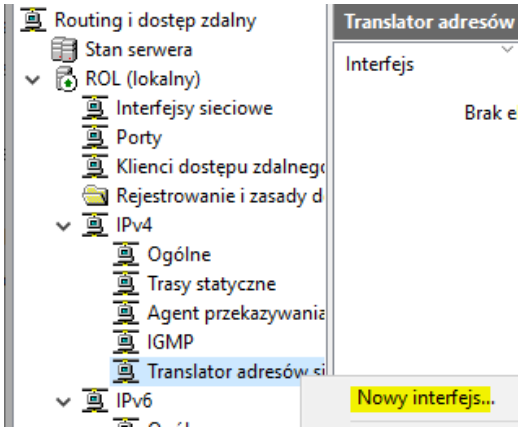
c. Wskaż sposób działania **serwera RRAS**. Priorytetem jest zapewnienie połączenia VPN dla użytkowników zdalnych, wybierz **Konfiguracja niestandardowa**.



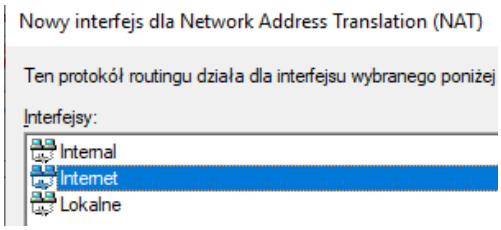




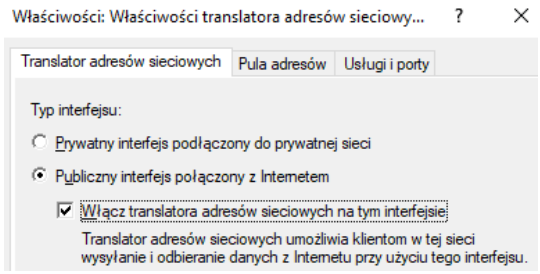
d. Dodaj nowe interfejsy



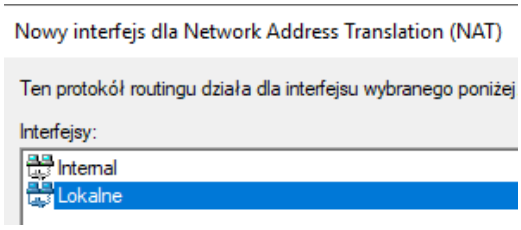
1. Internet



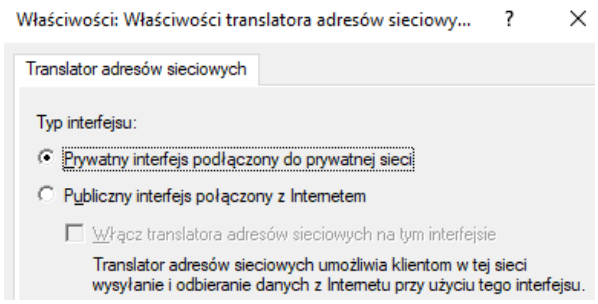
Jako publiczny



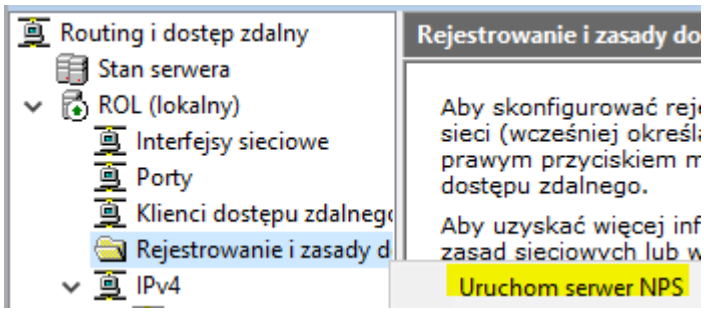
2. Lokalne



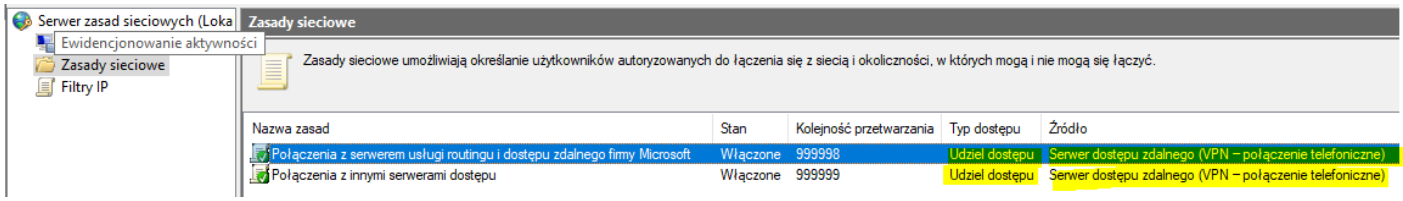
jako prywatny



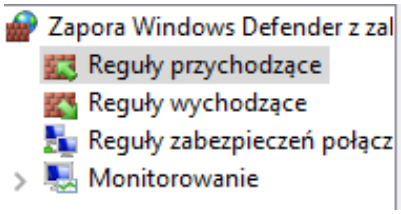
e. Po poprawnym zainstalowaniu i skonfigurowaniu **serwera RRAS**, system **zasad sieciowych** (NPS, Network Policy Server) domyślnie będzie blokował wszelkie próby dostępu do serwera RRAS. Aby zmienić tę zasadę, otwórz gałąź **Routing i dostęp zdalny**, a następnie PPM na **Rejestrowanie i zasady dostępu zdalnego** i **Uruchom serwer NPS**.

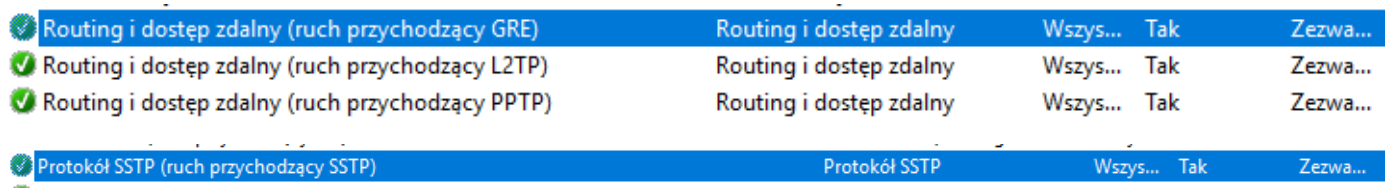


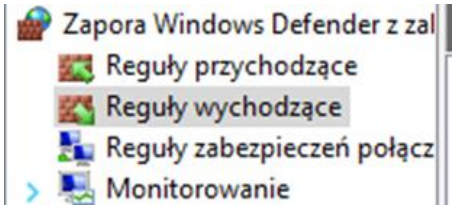
f. Zmodyfikuj i pozostaw jak poniżej ustawienia zasad sieciowych

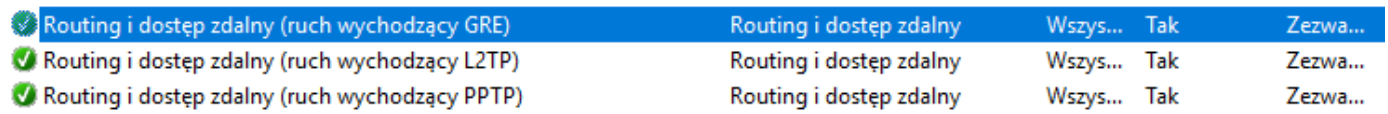


g. Sprawdź i upewnij się, że reguły na zaporze są jak poniżej









h. Wykonaj ping gogle.pl zakończony sukcesem

```
C:\Users\Administrator>ping google.pl

Pinging google.pl [142.250.186.195] with 32 bytes of data:
Reply from 142.250.186.195: bytes=32 time=17ms TTL=114
Reply from 142.250.186.195: bytes=32 time=17ms TTL=114
Reply from 142.250.186.195: bytes=32 time=16ms TTL=114
Reply from 142.250.186.195: bytes=32 time=19ms TTL=114

Ping statistics for 142.250.186.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 17ms
```

i. Wykonaj ipconfig zakończony sukcesem

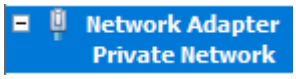
```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Internet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::e3:4ba7:e77:2f1b%17
   IPv4 Address. . . . . . . . . . . : 192.168.156.35
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 192.168.144.1

Ethernet adapter Lokalne:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b8fd:943a:fee7:1896%18
   IPv4 Address. . . . . . . . . . . : 192.167.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Zgłoszenie 2

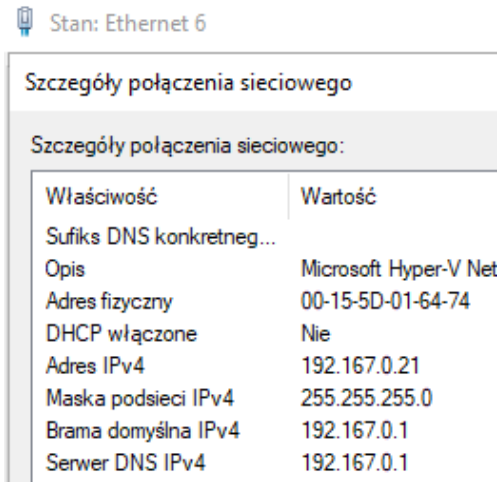
3. Konfiguracja Windows 10

Przejdź do Windows 10

a) Konfiguracja adaptera 1.



b) Ustawienia połączenia sieciowego.



c) Wykonaj ping do 192.167.0.1 zakończony sukcesem

```
C:\Users\admin>ping 192.167.0.1

Pinging 192.167.0.1 with 32 bytes of data:
Reply from 192.167.0.1: bytes=32 time<1ms TTL=128
Reply from 192.167.0.1: bytes=32 time<1ms TTL=128
Reply from 192.167.0.1: bytes=32 time<1ms TTL=128
Reply from 192.167.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.167.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

d) Wykonaj ping do 192.167.0.1 zakończony sukcesem

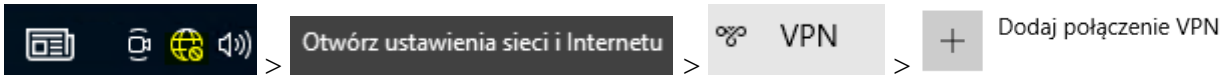
```
C:\Users\admin>ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=17ms TTL=113
Reply from 142.250.186.206: bytes=32 time=17ms TTL=113
Reply from 142.250.186.206: bytes=32 time=17ms TTL=113
Reply from 142.250.186.206: bytes=32 time=17ms TTL=113

Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms
```

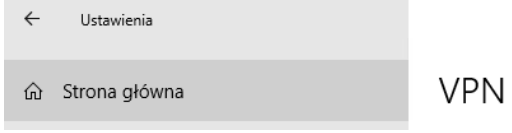
Zgłoszenie 3

4. Konfiguracja połączenia VPN.

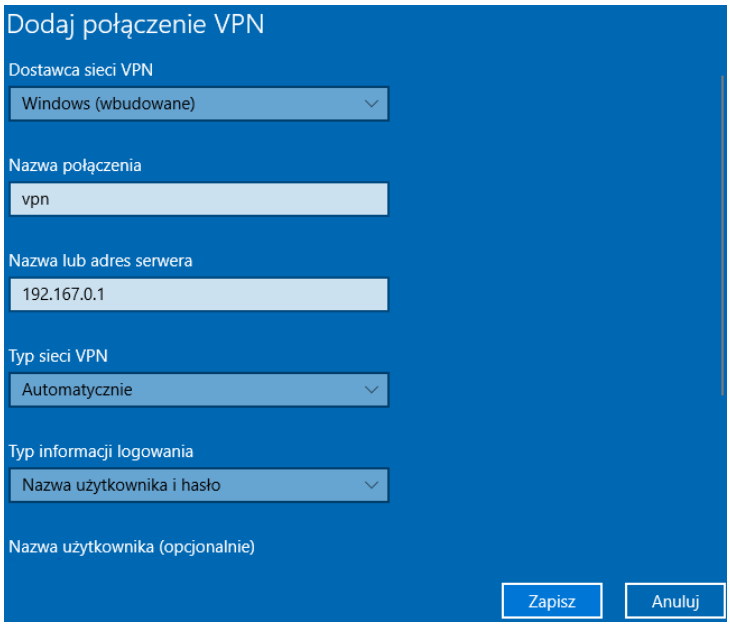
e) Skonfiguruj połączenie VPN.

Utwórz nowe połączenie, aby dołączyć do sieci VPN.



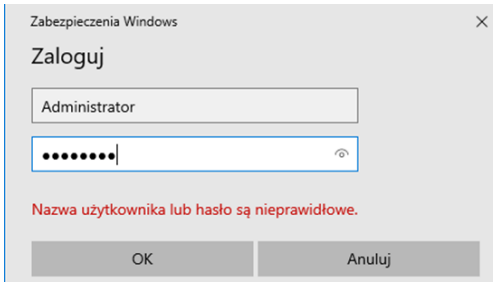


f) Określ sposób łączenia

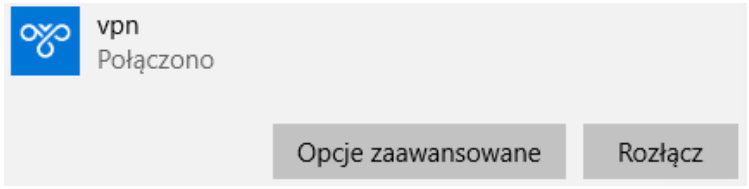


g) Wybierz opcję **Połącz**.

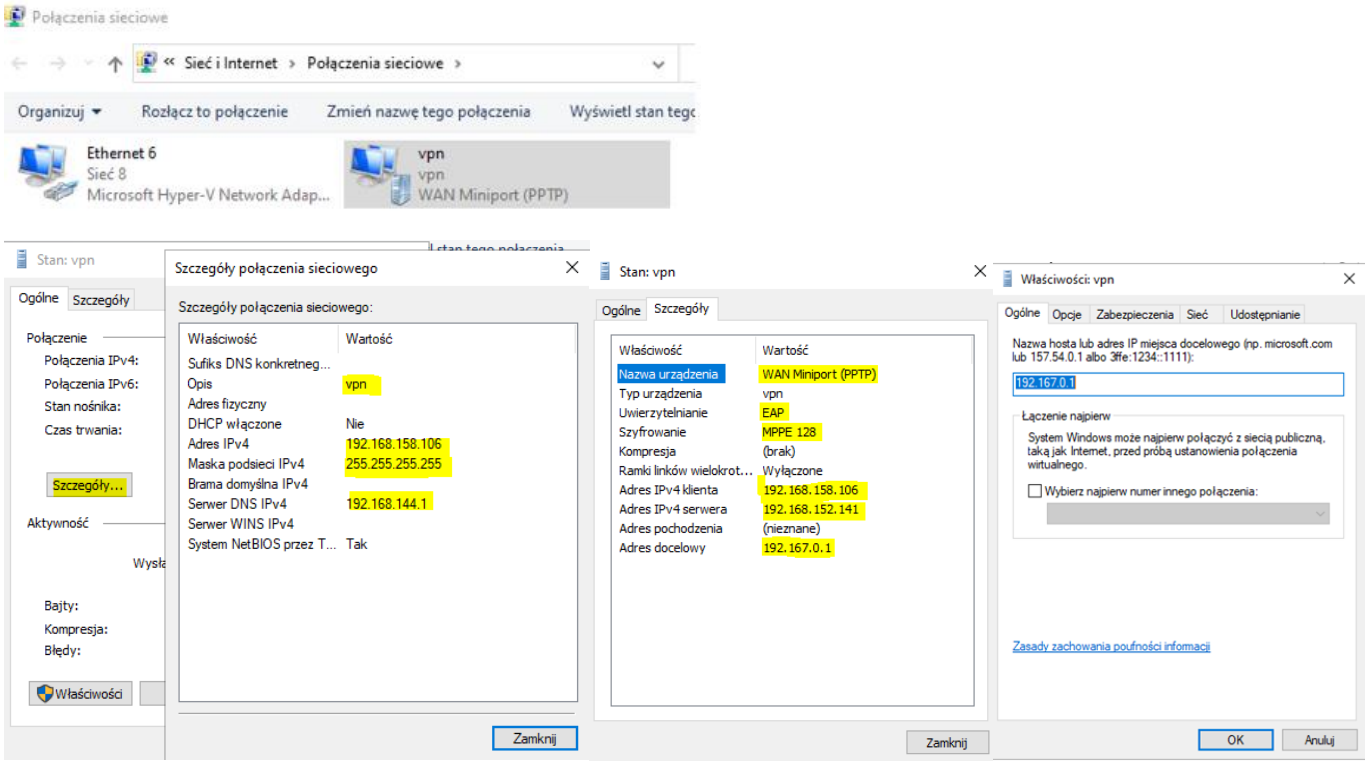
h) Podaj poświadczenie użytkownika, opcjonalnie możesz dodać nazwę domeny, z którą się łączysz.



i) Po poprawnym podaniu wszystkich niezbędnych danych zestawisz połączenie VPN. Efekt:



j) Sprawdź parametry połączenia. Opisany sposób będzie korzystał z szyfrowania MPPE, które zabezpiecza dane w połączeniu PPTP między klientem a serwerem sieci VPN. Zapisz w zeszycie parametry połączenia i ich interpretacje.



k) Wykonaj ping do 192.168.152.141 zakończony sukcesem

```
C:\Users\admin>ping 192.168.152.141

Pinging 192.168.152.141 with 32 bytes of data:
Reply from 192.168.152.141: bytes=32 time<1ms TTL=128
Reply from 192.168.152.141: bytes=32 time=1ms TTL=128
Reply from 192.168.152.141: bytes=32 time<1ms TTL=128
Reply from 192.168.152.141: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.152.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

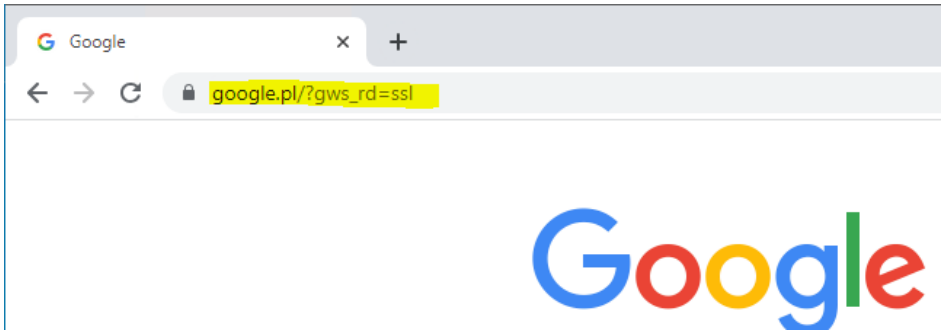
l) Wykonaj ipconfig /all jak poniżej

```
C:\Users\admin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : stacja
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Net
   Physical Address. . . . . . . . . : 00-15-5D-01-64-74
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a349:4a21:eec9:
   IPv4 Address. . . . . . . . . . . : 192.167.0.21(Preferre
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.167.0.1
   DHCPv6 IAID . . . . . . . . . . . : 335549789
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-AD-0F-
   DNS Servers . . . . . . . . . . . : 192.167.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

PPP adapter vpn:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vpn
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.158.106(Prefe
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.144.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

m)Wykonaj ping do gogle.com zakończony sukcesem

```
C:\Users\admin>ping google.com

Pinging google.com [142.250.186.206] with 32 bytes of data:
Reply from 142.250.186.206: bytes=32 time=18ms TTL=113
Reply from 142.250.186.206: bytes=32 time=18ms TTL=113
Reply from 142.250.186.206: bytes=32 time=18ms TTL=113
Reply from 142.250.186.206: bytes=32 time=17ms TTL=113

Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms
```

n) Otwórz w przeglądarce gogle.com zakończony sukcesem

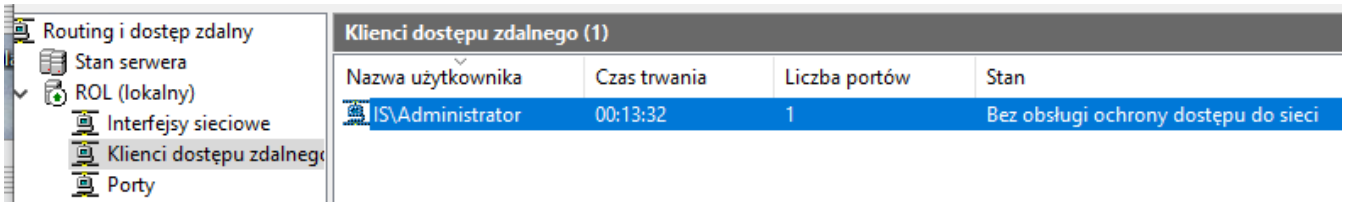


Zgłoszenie 4

5. Analiza parametrów serwera Windows 2019

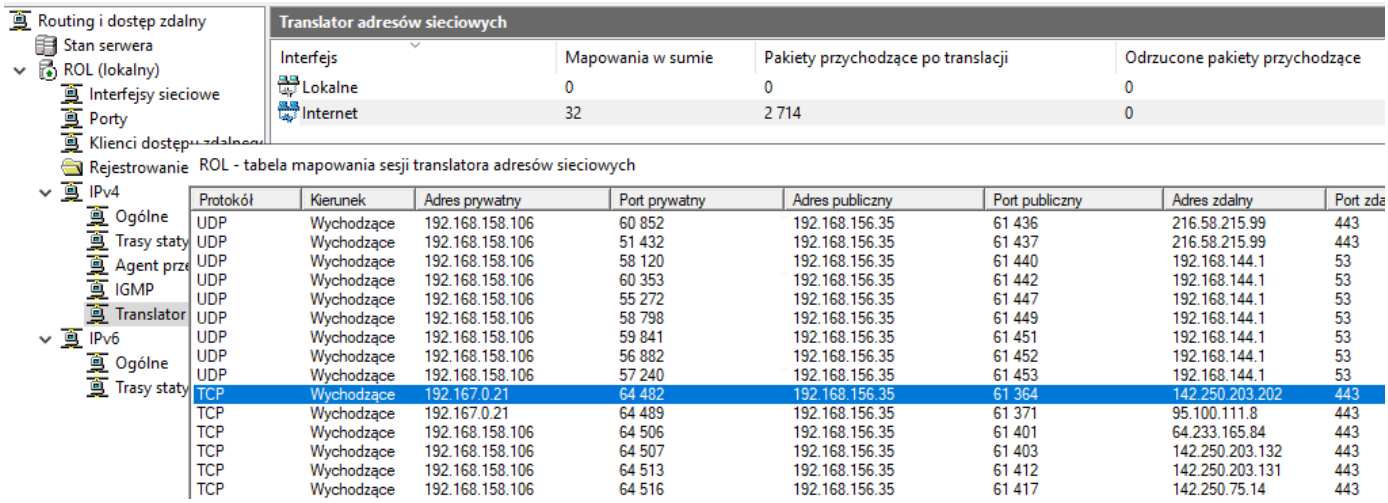
Przejdź do serwera

a) Sprawdź połączonych klientów dostępu zdalnego



b) Przeanalizuj na interfejsie Internet tabelę mapowania sesji translatora adresów sieciowych.

Zapisz w zeszycie wnioski.



c) Wykonaj ipconfig /all jak poniżej

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Internet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::e3:4ba7:e77:2f1b%17
   IPv4 Address. . . . . . . . . . . : 192.168.156.35
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 192.168.144.1

Ethernet adapter Lokalne:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b8fd:943a:fee7:1896%18
   IPv4 Address. . . . . . . . . . . : 192.167.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

PPP adapter RAS (Dial In) Interface:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.152.141
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :
```

Zgłoszenie 5

6. Analiza parametrów Windows 10

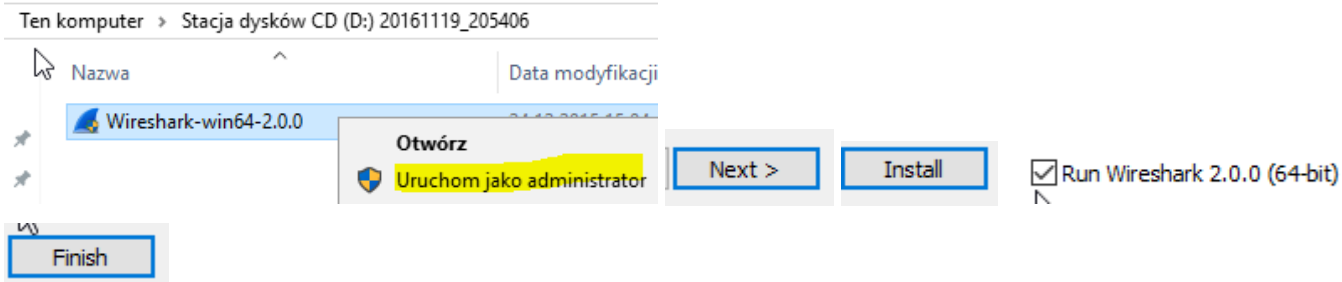
Przejdź do Windows 10

a) Wykonaj ping do 192.168.152.141 z parametrem -t zakończony sukcesem

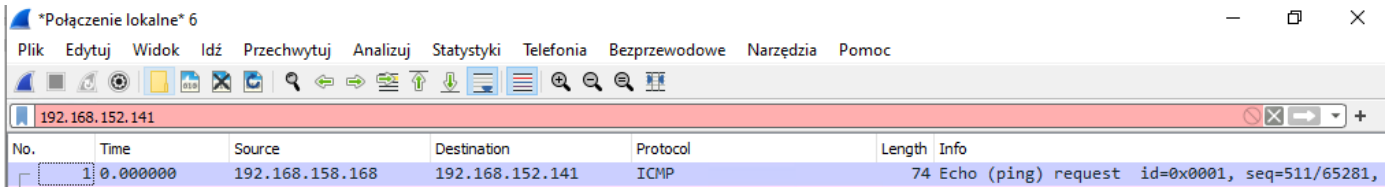
```
PPP adapter vpn:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vpn
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.158.168(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.144.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\admin>ping 192.168.152.141 -t
```

b) Pobierz Wireshark.iso podłącz go i zainstaluj Wireshark.

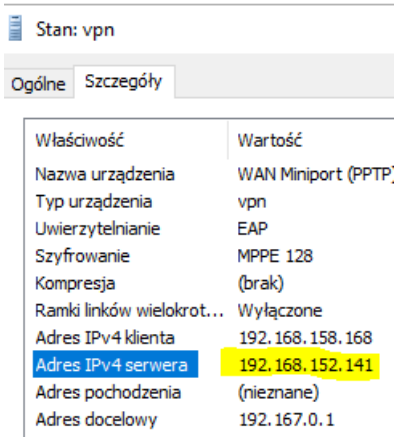
z menu Menedżer funkcji Hyper-V > Nośnik > Stacja dysków DVD > Włóż dysk … > Pobrane >



c) Uruchom Wireshark, uruchom podsłuch połączenia lokalnego.



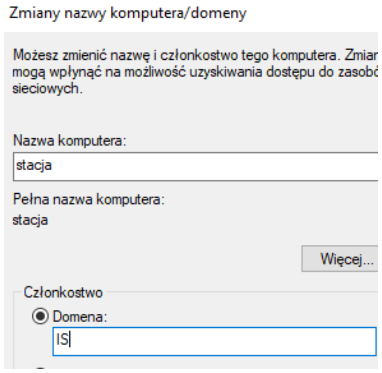
d) Zatrzymaj podsłuch za pomocą Wireshark. Przeanalizuj wynik. Protokoły wykorzystane do zbudowania połączenia zdradzi nam również przechwycony pakiet - komunikacja pomiędzy klientem a serwerem VPN. Podczas analizy wykorzystaj Stan: vpn. Zapisz w zeszycie wnioski.



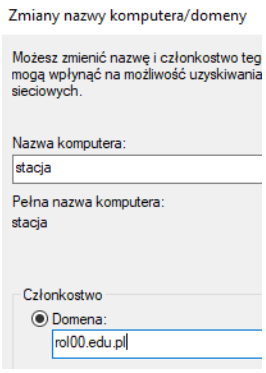
Zgłoszenie 6

7. Podłączenie Windows 10 do domeny z włączonym VPN i analiza.

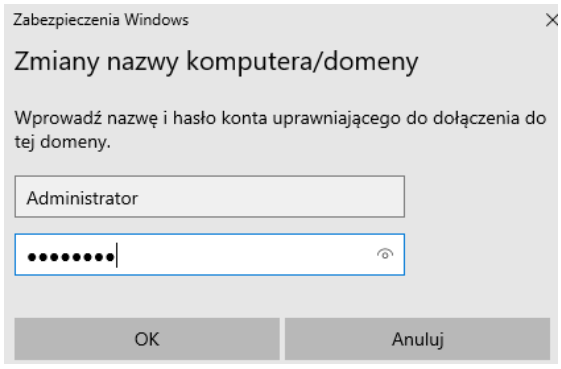
a) Podaj nazwę domeny

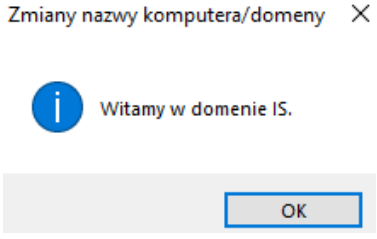


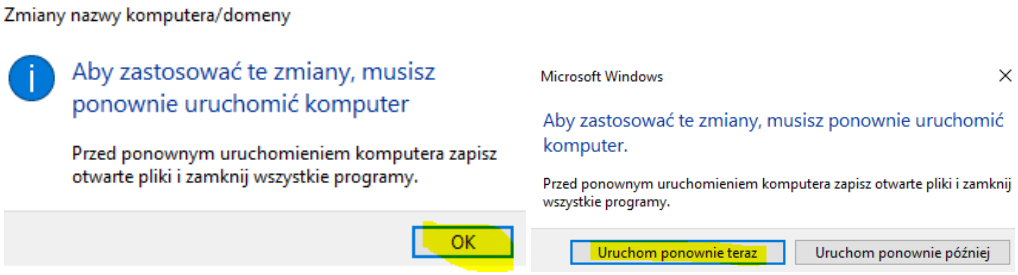
lub



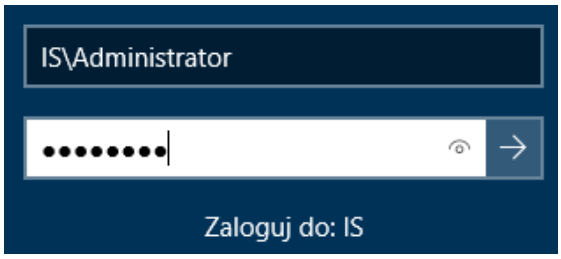
b) Podaj nazwę i hasło konta uprawniającego do dołączenia do domeny





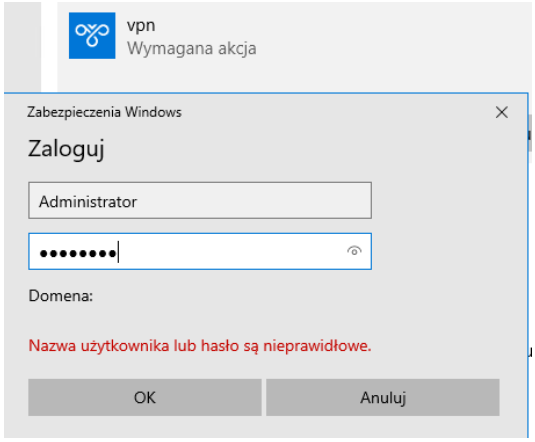


c) Na Windows 10 zaloguj się jako Administrator do domeny



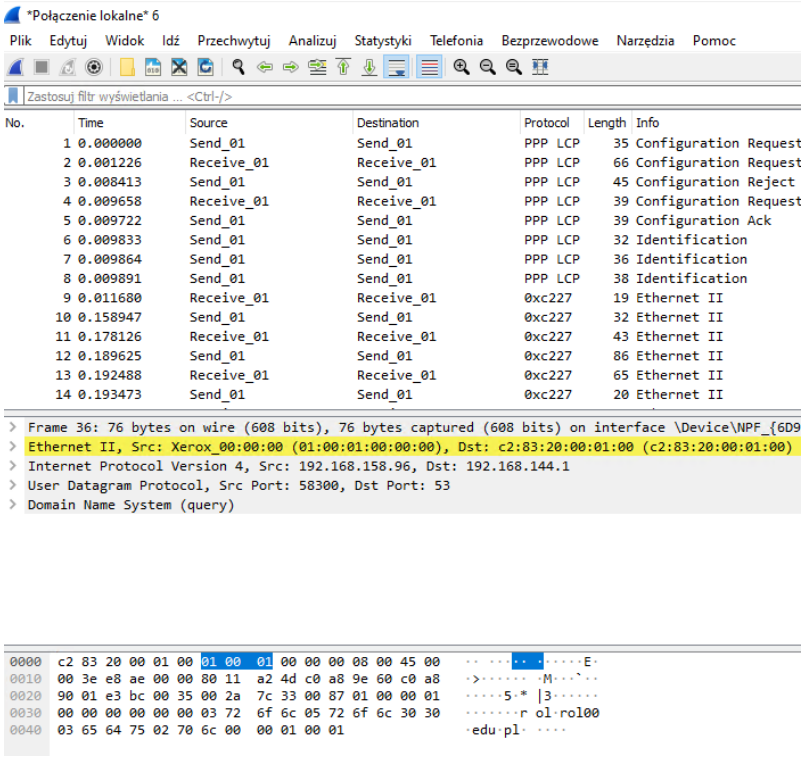
d) Włącz Wireshark, przejmij kartę sieciową

e) Podłącz się jako vpn



f) Zatrzymaj podsłuch w Wireshark

g) Przenalizuj przechwycony ruch. Zapisz w zeszycie wnioski z analizy wynik podsłuchu sieci wykonanego za pomocą Wireshark. Oraz przedstaw wnioski z zadania.



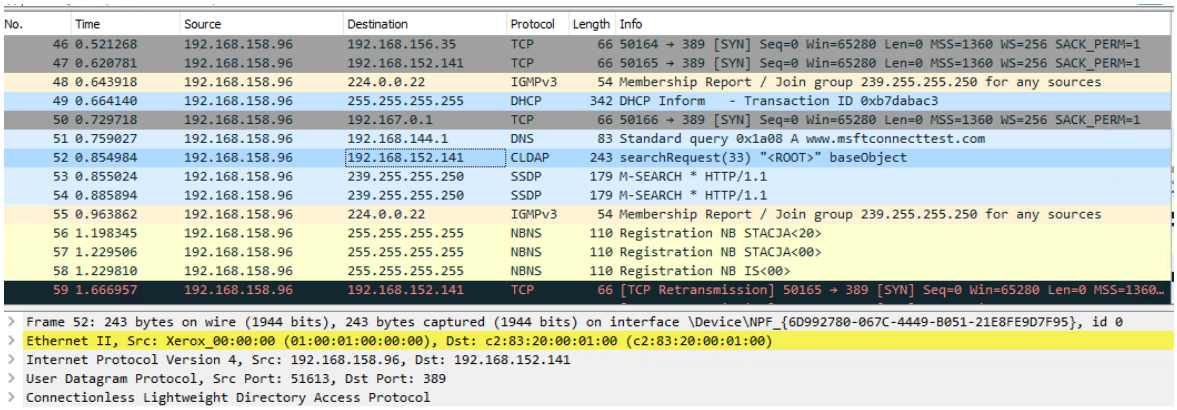
h) Wykonaj ipconfig /all jak poniżej

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : stacja
   Primary Dns Suffix  . . . . . . . : rol00.edu.pl
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : rol00.edu.pl

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Net
   Physical Address. . . . . . . . . : 00-15-5D-01-64-74
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a349:4a21:eec9:
   IPv4 Address. . . . . . . . . . . : 192.167.0.21(Preferre
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.167.0.1
   DHCPv6 IAID . . . . . . . . . . . : 335549789
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-AD-0F-
   DNS Servers . . . . . . . . . . . : 192.167.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

PPP adapter vpn:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vpn
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.158.96(Prefer
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
```

i) Włącz Wireshark, przejmij kartę sieciową

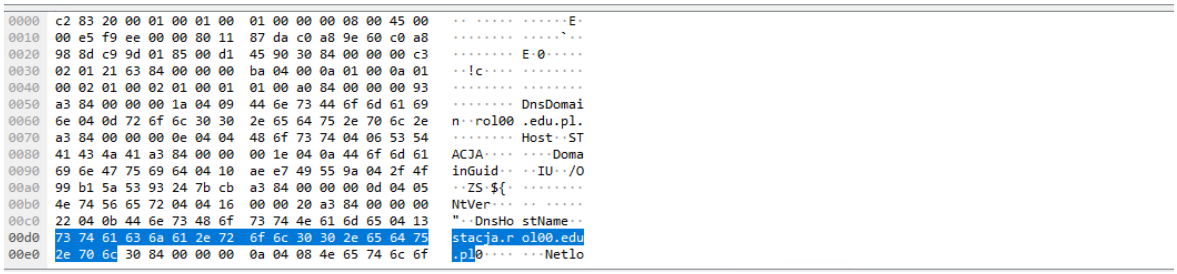
j) Wykonaj ping do 192.168.158.96 z parametrem -t zakończony sukcesem

k) Zatrzymaj podsłuch za pomocą Wireshark. Przenalizuj przechwycony ruch



No.	Time	Source	Destination	Protocol	Length	Info
46	0.521268	192.168.158.96	192.168.156.35	TCP	66	50164 → 389 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 WS=256 SACK_PERM=1
47	0.620781	192.168.158.96	192.168.152.141	TCP	66	50165 → 389 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 WS=256 SACK_PERM=1
48	0.643918	192.168.158.96	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
49	0.664140	192.168.158.96	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xb7dabac3
50	0.729718	192.168.158.96	192.167.0.1	TCP	66	50166 → 389 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 WS=256 SACK_PERM=1
51	0.759027	192.168.158.96	192.168.144.1	DNS	83	Standard query 0x1a08 A www.msftconnecttest.com
52	0.854984	192.168.158.96	192.168.152.141	CLDAP	243	searchRequest(33) "<ROOT>" baseObject
53	0.855024	192.168.158.96	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
54	0.885894	192.168.158.96	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
55	0.963862	192.168.158.96	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
56	1.198345	192.168.158.96	255.255.255.255	NBNS	110	Registration NB STACJA<20>
57	1.229506	192.168.158.96	255.255.255.255	NBNS	110	Registration NB STACJA<00>
58	1.229810	192.168.158.96	255.255.255.255	NBNS	110	Registration NB IS<00>
59	1.666957	192.168.158.96	192.168.152.141	TCP	66	[TCP Retransmission] 50165 → 389 [SYN] Seq=0 Win=65280 Len=0 MSS=1360…

```
> Frame 52: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{6D992780-067C-4449-B051-21E8FE9D7F95}, id 0
> Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: c2:83:20:00:01:00 (c2:83:20:00:01:00)
> Internet Protocol Version 4, Src: 192.168.158.96, Dst: 192.168.152.141
> User Datagram Protocol, Src Port: 51613, Dst Port: 389
> Connectionless Lightweight Directory Access Protocol
```



```
0000  c2 83 20 00 01 00 01 00  01 00 00 00 08 00 45 00   ·· ····· ·····E·
0010  00 e5 f9 ee 00 00 80 11  87 da c0 a8 9e 60 c0 a8   ········ ·····`··
0020  98 8d c9 9d 01 85 00 d1  45 90 30 84 00 00 00 c3   ········ E·0·····
0030  02 01 21 63 84 00 00 00  ba 04 00 0a 01 00 0a 01   ··!c···· ········
0040  00 02 01 00 02 01 00 01  01 00 a0 84 00 00 00 93   ········ ········
0050  a3 84 00 00 00 1a 04 09  44 6e 73 44 6f 6d 61 69   ········ DnsDomai
0060  6e 04 0d 72 6f 6c 30 30  2e 65 64 75 2e 70 6c 2e   n··rol00 .edu.pl.
0070  a3 84 00 00 00 0e 04 04  48 6f 73 74 04 06 53 54   ········ Host··ST
0080  41 43 4a 41 a3 84 00 00  00 1e 04 0a 44 6f 6d 61   ACJA···· ····Doma
0090  69 6e 47 75 69 64 04 10  ae e7 49 55 9a 04 2f 4f   inGuid·· ··IU··/O
00a0  99 b1 5a 53 93 24 7b cb  a3 84 00 00 00 0d 04 05   ··ZS·${· ········
00b0  4e 74 56 65 72 04 04 16  00 00 20 a3 84 00 00 00   NtVer··· ·· ·····
00c0  22 04 0b 44 6e 73 48 6f  73 74 4e 61 6d 65 04 13   "··DnsHo stName··
00d0  73 74 61 63 6a 61 2e 72  6f 6c 30 30 2e 65 64 75   stacja.r ol00.edu
00e0  2e 70 6c 30 84 00 00 00  0a 04 08 4e 65 74 6c 6f   .pl0···· ···Netlo
```

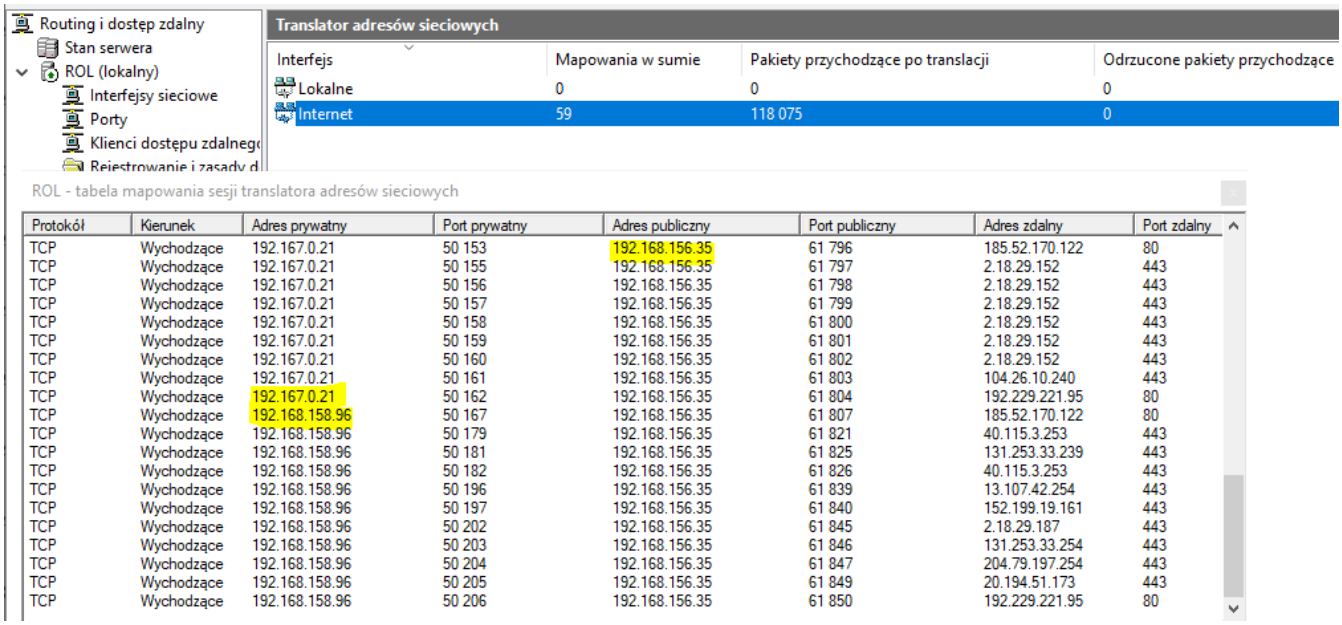
l) Zapisz w zeszycie wnioski z analizy wynik podsłuchu sieci wykonanego za pomocą Wireshark. Oraz przedstaw wnioski z zadania.

Zgłoszenie 7

8. Analiza parametrów serwera Windows 2019

Przejdź do Windows Serwer 2019

a) Przeanalizuj na interfejsie Internet tabelę mapowania sesji translatora adresów sieciowych



Interfejs	Mapowania w sumie	Pakiety przychodzące po translacji	Odrzucone pakiety przychodzące
Lokalne	0	0	0
Internet	59	118 075	0

ROL - tabela mapowania sesji translatora adresów sieciowych

Protokół	Kierunek	Adres prywatny	Port prywatny	Adres publiczny	Port publiczny	Adres zdalny	Port zdalny
TCP	Wychodzące	192.167.0.21	50 153	192.168.156.35	61 796	185.52.170.122	80
TCP	Wychodzące	192.167.0.21	50 155	192.168.156.35	61 797	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 156	192.168.156.35	61 798	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 157	192.168.156.35	61 799	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 158	192.168.156.35	61 800	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 159	192.168.156.35	61 801	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 160	192.168.156.35	61 802	2.18.29.152	443
TCP	Wychodzące	192.167.0.21	50 161	192.168.156.35	61 803	104.26.10.240	443
TCP	Wychodzące	192.167.0.21	50 162	192.168.156.35	61 804	192.229.221.95	80
TCP	Wychodzące	192.168.158.96	50 167	192.168.156.35	61 807	185.52.170.122	80
TCP	Wychodzące	192.168.158.96	50 179	192.168.156.35	61 821	40.115.3.253	443
TCP	Wychodzące	192.168.158.96	50 181	192.168.156.35	61 825	131.253.33.239	443
TCP	Wychodzące	192.168.158.96	50 182	192.168.156.35	61 826	40.115.3.253	443
TCP	Wychodzące	192.168.158.96	50 196	192.168.156.35	61 839	13.107.42.254	443
TCP	Wychodzące	192.168.158.96	50 197	192.168.156.35	61 840	152.199.19.161	443
TCP	Wychodzące	192.168.158.96	50 202	192.168.156.35	61 845	2.18.29.187	443
TCP	Wychodzące	192.168.158.96	50 203	192.168.156.35	61 846	131.253.33.254	443
TCP	Wychodzące	192.168.158.96	50 204	192.168.156.35	61 847	204.79.197.254	443
TCP	Wychodzące	192.168.158.96	50 205	192.168.156.35	61 849	20.194.51.173	443
TCP	Wychodzące	192.168.158.96	50 206	192.168.156.35	61 850	192.229.221.95	80

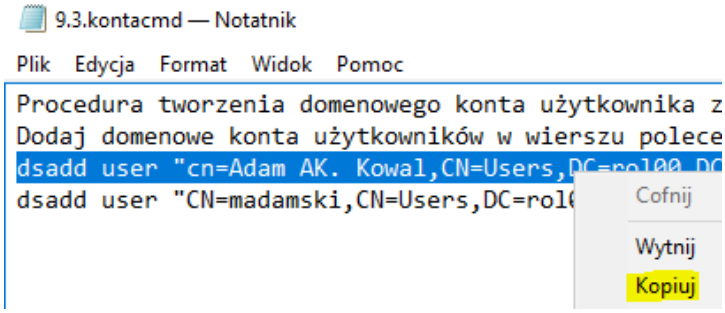
b) Zapisz w zeszycie wnioski z analizy na interfejsie Internet tabeli mapowania sesji translatora adresów sieciowych. Przedstaw wnioski z zadania.

Zgłoszenie 8

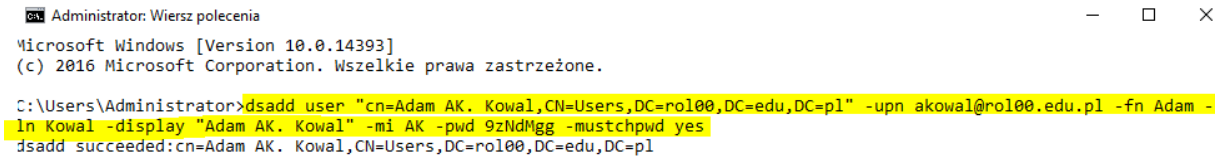
9. Dodanie domenowego konta użytkownika uprawnionego do korzystania z VPN

a) Pobierz 9.3kontacmd.iso i podłącz do serwera z menu Menedżer funkcji Hyper-V > Nośnik > Stacja dysków DVD > Włóż dysk … > Pobrane > 9.3.kontacmd.iso

b) Otwórz Stacja dysków DVD > Skopiuj zaznaczoną poniżej linie.



c) W cmd wklej zaznaczoną powyżej linie. Prawo klik Wklej



d) Dodane zostanie domenowe konta użytkownika w wierszu polecenia jak poniżej.

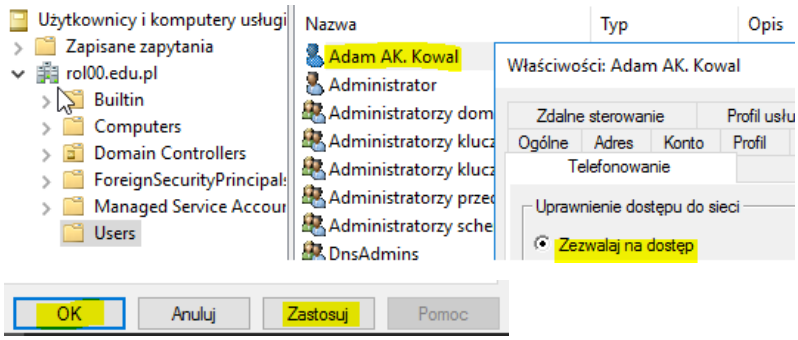
dsadd user "cn=Adam AK. Kowal,CN=Users,DC=rol00,DC=edu,DC=pl" -upn akowal@rol00.edu.pl -fn Adam -ln Kowal -display "Adam AK. Kowal" -mi AK -pwd 9zNdMgg -mustchpwd yes

Serwer RRAS może obsługiwać klientów. Administrator może połączyć się do serwera VPN.

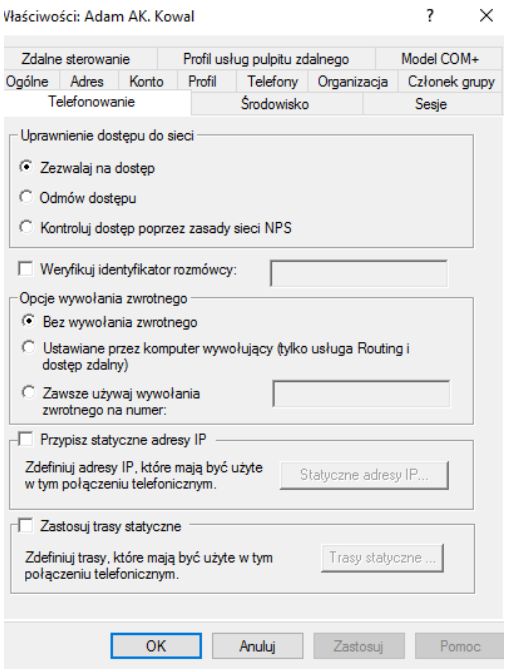
e) Określ użytkowników, którzy mogą łączyć się z serwerem.

Otwórz przystawkę **Użytkownicy i komputery usług Active Directory** i wyszukaj użytkownika, któremu chcemy dać prawo korzystania z połączenia VPN.

Po wybraniu danego użytkownika, wybierz **Właściwości** i przejdź na kartę **Telefonowanie**. Odszukaj sekcję **Uprawnienie dostępu do sieci** i kliknij na **Zezwalaj na dostęp**. Od tej pory użytkownik wykorzystujący swoje poświadczenia (logowanie do domeny) będzie mógł łączyć się z **serwerem RRAS**.



Efekt:



Serwer został skonfigurowany tak by konkretnemu użytkownikowi dać możliwość skorzystania z tunelu VPN.

f) Wykonaj logowanie do Windows 10 do konta użytkownika uprawnionego do korzystania z VPN

Efekt:

```
C:\Users\Adam AK. Kowal>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : stacja
   Primary Dns Suffix  . . . . . . . : rol00.edu.pl
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : rol00.edu.pl

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V
   Physical Address. . . . . . . . . : 00-15-5D-01-64-74
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a349:4a21:ee
   IPv4 Address. . . . . . . . . . . : 192.167.0.21(Prefe
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.167.0.1
   DHCPv6 IAID . . . . . . . . . . . : 335549789
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-AD-
   DNS Servers . . . . . . . . . . . : 192.167.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

PPP adapter vpn:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vpn
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.157.75(Pre
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.144.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Zgłoszenie 9

10. Podaj ogólne wnioski z wykonanego zadania.

Zgłoszenie 10

Przywróć pierwszy punkt kontrolny

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.