

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 11. 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 11.
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.

ETAP 0 – Przegląd topologii i założenia

- Serwer Windows Server 2019 pełni role: AD DS, DNS, RRAS (VPN). Interfejsy: LAN = 192.167.0.1 (publikowany w DNS), WAN = 172.26.x.x (niepublikowany).
- Klient Windows 11 (po stronie Internetu/WAN) zestawia tunel do serwera RRAS.
- W ćwiczeniu używamy PPTP/MPPE – wyłącznie dydaktycznie; w produkcji preferuj IKEv2/SSTP/OpenVPN/WireGuard.

Przed przystąpieniem do ćwiczenia

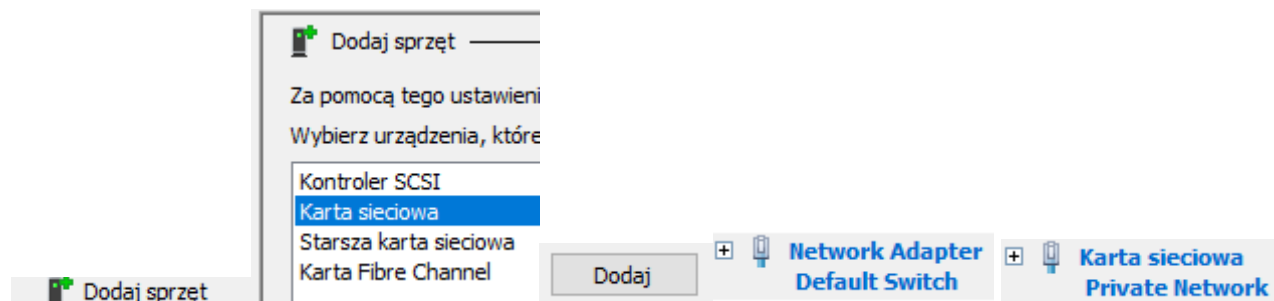
- a. Przywróć właściwy punkt kontrolny przed rozpoczęciem konfiguracji. W Hyper-V wykonaj:

Wybierz *nazwa twojej grupy_dc2019* → Punkty kontrolne → wybierz punkt kontrolny → Prawoklik → Zastosuj → Zastosuj.

- b. Upewnij się, że pracujesz na serwerze z **funkcją kontrolera domeny (DC)**

ETAP 1 – Przygotowanie środowiska (Serwer + Klient)

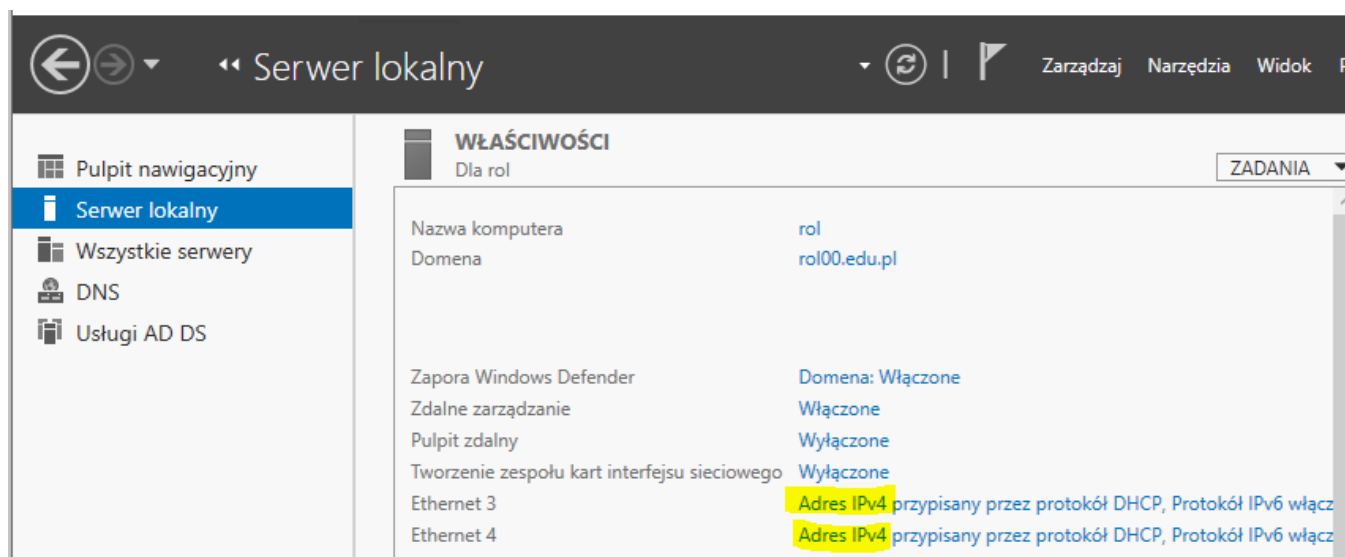
Przygotuj serwer Windows sprawdź, czy serwer posiada dwie karty sieciowe, jeśli nie to dodaj



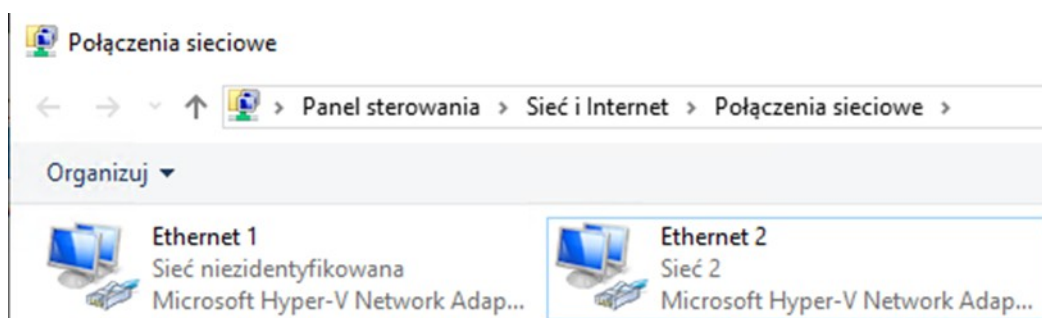
Uruchom maszynę właściwego serwera Windows dc2019 > Ctrl+Delete > Administrator > zaql@WSX

Po uruchomieniu pojawi się komunikat dotyczący sieci wybierz **Tak**.

Wybierz **Adres IPv4 przypisany ...** jak poniżej



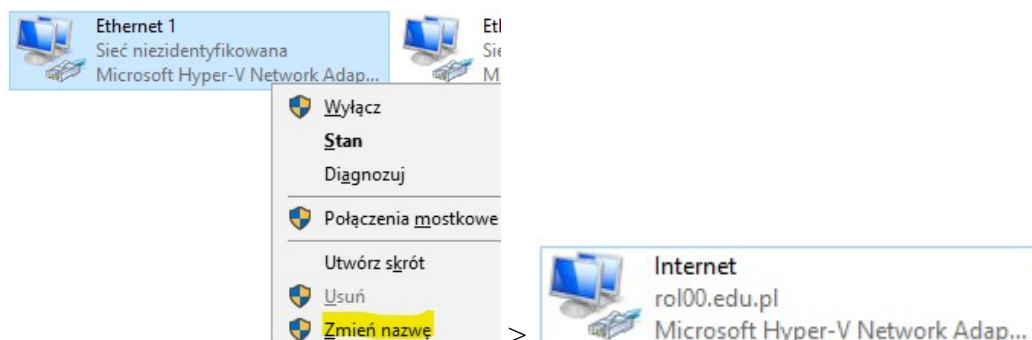
Otworzy się okno podobne do tego poniżej.



Wykonaj konfigurację interfejsów sieciowych serwera jak poniżej:

Internet (Default Switch → WAN)

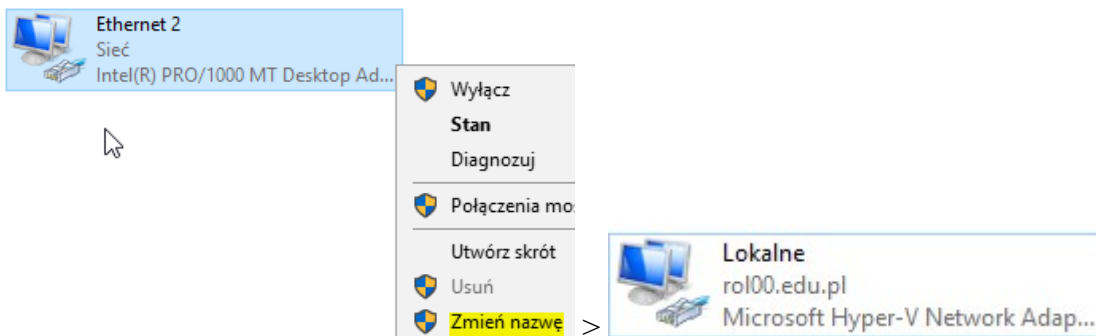
- Sprawdź MAC adaptera VM podłączonego w Hyper-V do przełącznika **Default Switch**.
- W Windows znajdź kartę z **tym samym adresem MAC** i nazwij ją.
- W oknie **Połączenia sieciowe**: wybierz kartę → **Zmień nazwę** → wpisz **Internet**:



Lokalne (Private Network → LAN)

- Sprawdź MAC adaptera VM podłączonego w Hyper-V do przełącznika **Private Network**.

- W Windows otwórz **Połączenia sieciowe**, znajdź kartę z **tym samym adresem MAC** i nazwij ją.
- W oknie **Połączenia sieciowe**: wybierz kartę → **Zmień nazwę** → wpisz **Lokalne**:



To powinno wyglądać tak:



Uwaga: Porównujesz MAC w Hyper-V z MAC w Windows, aby mieć pewność, że **to ten sam interfejs**.
Nie ustawiaj identycznego MAC na dwóch różnych kartach (LAN i WAN).

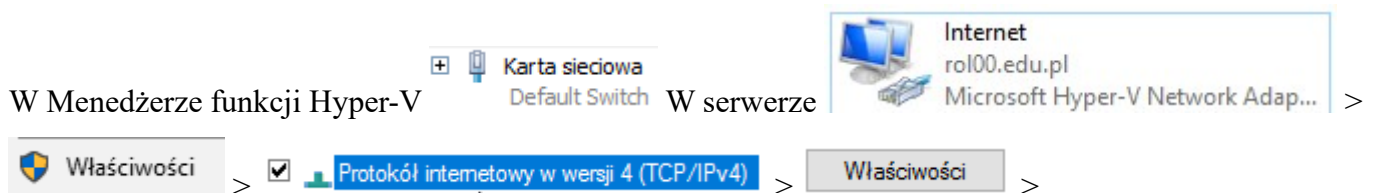
Powinno wyglądać tak:

- **Internet** – połączony z **Default Switch** (ten sam MAC w Hyper-V i Windows).
- **Lokalne** – połączony z **Private Network** (ten sam MAC w Hyper-V i Windows).

Adapter Lokalne musi być skonfigurowany ze statycznym adresem, adapter Internet powinien być ustawiony na DHCP.

Adres skonfigurowany na karcie Lokalne to adres, którego komputery klienckie będą używać jako bramy.

Internet	Adres IPv4 przypisany przez protokół DHCP, Protokół IPv6 włączony
Lokalne	192.167.0.1, Protokół IPv6 włączony



☒ Uzyskaj adres IP automatycznie ; ☒ Uzyskaj adres serwera DNS automatycznie > [Anuluj] > [Anuluj] > Stan >

Opis	Microsoft Hyper-V 1
Adres fizyczny	00-15-5D-07-2E-36
DHCP włączone	Tak
Adres IPv4	172.27.131.227
Maska podsieci IPv4	255.255.240.0
Dzierżawa uzyskana	wtorek, 3 stycznia
Dzierżawa wygasa	środa, 4 stycznia 21
Brama domyślna IPv4	172.27.128.1
Serwer DHCP IPv4	172.27.128.1
Serwer DNS IPv4	172.27.128.1

[Szczegóły...]

(przykładowe dane konfiguracyjne mogą się różnić).

W Menedżerze funkcji Hyper-V

Network Adapter
Private Network

W serwerze

Lokalne
rol00.edu.pl
Microsoft Hyper-V Network Adap...

Właściwości > ☒ Protokół internetowy w wersji 4 (TCP/IPv4) > Właściwości >

☒ Użyj następującego adresu IP:

Adres IP: 192 . 167 . 0 . 1
 Maska podsieci: 255 . 255 . 255 . 0
 Brama domyślna: . . .

☐ Uzyskaj adres serwera DNS automatycznie

☒ Użyj następujących adresów serwerów DNS:

Preferowany serwer DNS: 192 . 167 . 0 . 1

> OK > Zamknij.

DHCP włączone

Nie

Adres IPv4

192.167.0.1

Maska podsieci IPv4

255.255.255.0

Brama domyślna IPv4

Serwer DNS IPv4

192.167.0.1

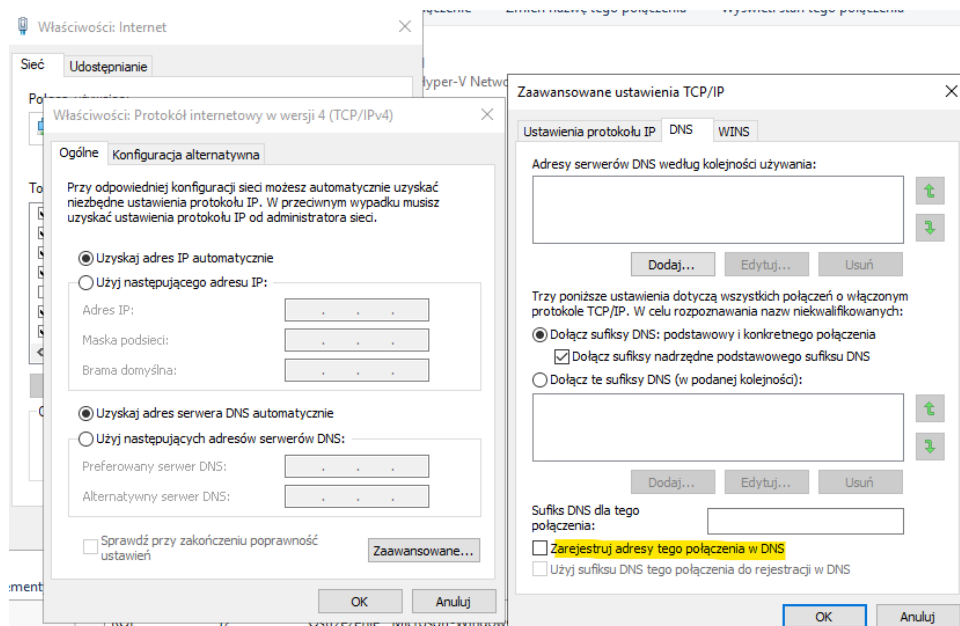
Zamknij.

Ethernet 1
 Sieć niezidentyfikowana
 Microsoft Hyper-V Network Adap...

> Stan >

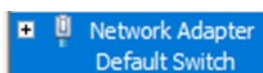
[Szczegóły...]

Na interfejsach Internet (WAN) i RAS (Dial-In) odznaczyć „Zarejestruj adresy tego połączenia w DNS”.

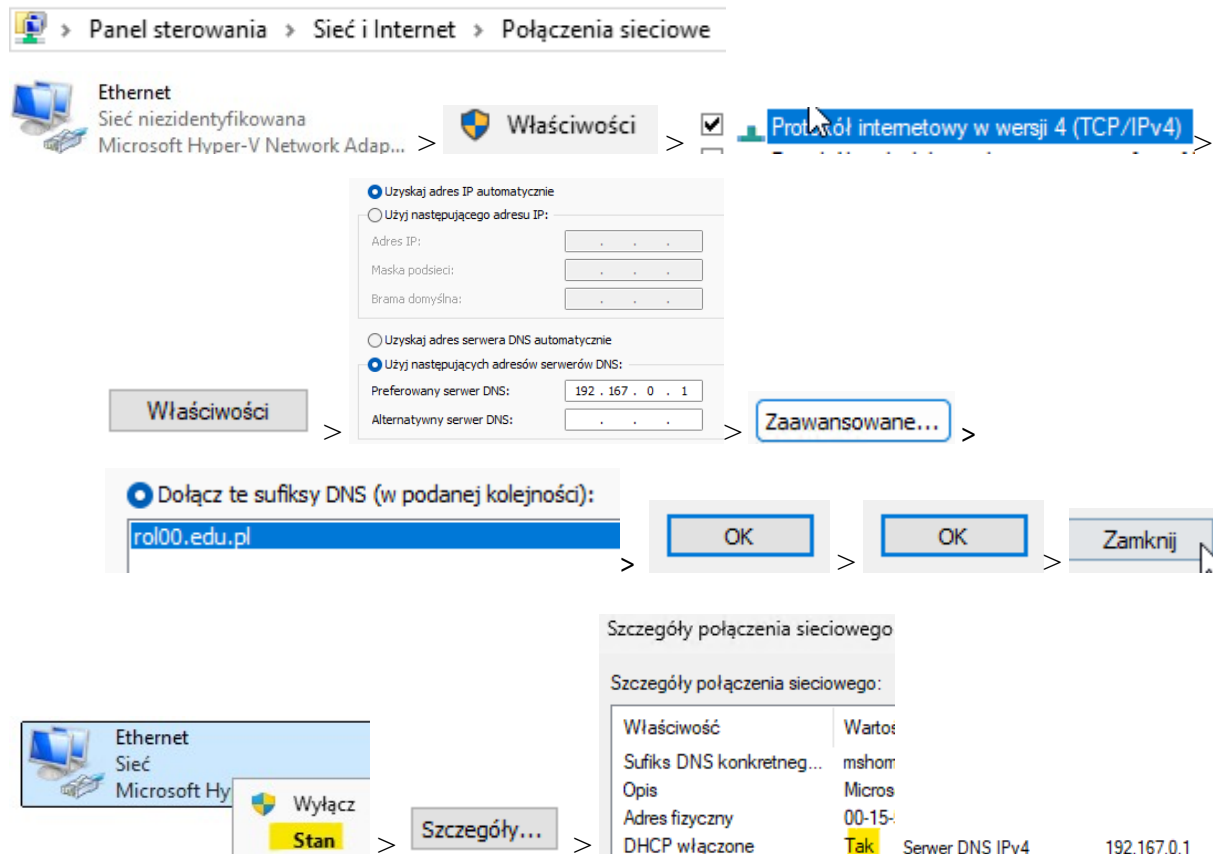


Przygotuj klienta Windows 11 jak poniżej:

W Hyper-V wybierz Ustawienia



Uruchom klienta Windows 11 Podaj login: admin > i hasło: zaq1@WSX



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

Wszystkie czynności konfiguracyjne należy kolejno zapisać w zeszycie.

Pozostaw włączony serwer.

Praktyczna teoria o NAT - wersja do tego zadania

NAT (Network Address Translation) to technika, która mapuje **adresy IP i porty** między dwiema domenami adresowymi. W naszym laboratorium NAT jest realizowany na serwerze **RRAS** i służy temu, aby **klienci z sieci prywatnej** mogli łączyć się z zasobami w **sieci zewnętrznej/WAN**.

- **Sieć prywatna (LAN):** 192.167.0.0/24 – serwer DC/RRAS ma adres **192.167.0.1** (to adres, który ma się publikować w DNS).
- **Sieć zewnętrzna/WAN:** 172.26.0.0/12 – interfejs WAN serwera RRAS posiada np. **172.26.99.7** (adres „publiczny” w naszym środowisku).
- **Klient po VPN (PPP)** otrzymuje adres z puli **172.26.105.x** (np. **172.26.105.187** lub **172.26.105.151**).

Gdy klient z sieci prywatnej lub klient VPN inicjuje połączenie do Internetu, **RRAS** dokonuje translacji:

- **adres prywatny/PPP** (np. 172.26.105.187) + **port prywatny** → **adres WAN serwera** (172.26.99.7) + **port publiczny** (dynamicznie przydzielany, np. 62122).

To nie tylko **NAT adresu**, ale także **PAT (Port Address Translation)** - wiele jednoczesnych sesji może korzystać z **tego samego adresu WAN**, a są rozróżniane **po różnych portach publicznych**. Dzięki temu pakiety wracające z Internetu trafiają poprawnie do właściwego klienta za RRAS.

Działanie VPN - wersja do tego zadania

Klient Windows 11 (po stronie **WAN/Internet**) łączy się do serwera **RRAS** na interfejsie **WAN** (np. 172.26.99.7) i zestawia **tunel VPN (PPTP/MPPE w ćwiczeniu)**. Po zestawieniu tunelu klient dostaje adres **PPP** z zakresu 172.26.105.x (np. 172.26.105.187), a ruch do zasobów sieci wewnętrznej jest **kapsułkowany** i przesyłany wewnątrz tunelu do serwera.

W efekcie:

- Klient **widzi zasoby LAN** (np. kontroler domeny pod 192.167.0.1) mimo że fizycznie znajduje się **poza** tą siecią.
- Ruch do Internetu może przechodzić przez NAT na RRAS: 172.26.105.187 → 172.26.99.7:port_publiczny → Internet, co zobaczysz w tabeli mapowań NAT (RRAS → IPv4 → Translator adresów sieciowych) jako wpisy „Wychodzące/UDP/TCP” z „Adres prywatny” = 172.26.105.x, „Adres publiczny” = 172.26.99.7 oraz „Port zdalny” zależny od usługi (np. 53 dla DNS, 443 dla HTTPS).

ETAP 2 – Konfiguracja sieci i DNS na kontrolerze domeny (DC)

Wymagane ustawienia DNS i rejestracji nazw na kontrolerze domeny (AD DS + DNS)

1) Na interfejsie LAN kontrolera domeny pozostaw: Preferowany DNS: 192.167.0.1 (lub 127.0.0.1) oraz Alternatywny DNS: - (puste).

2) Na interfejsach „Internet (WAN)” i „RAS (Dial-In Interface)”: pozostaw odznaczone „Zarejestruj adresy tego połączenia w DNS” (wyłącz rejestrację)

3) W strefie DNS pozostaw wyłącznie jeden rekord A hosta DC: rol.rol00.edu.pl → 192.167.0.1 oraz usuń wpisy 172.x.x.x, jeżeli istnieją.

4) Wymuś ponowną rejestrację:

```
ipconfig /flushdns
```

```
net stop netlogon
```

```
net start netlogon
```

```
ipconfig /registerdns
```

```
nltest /dsregdns
```

5) Weryfikacja na DC:

```
Resolve-DnsName rol.rol00.edu.pl -Server 127.0.0.1
```

```
Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.rol00.edu.pl -Server 127.0.0.1
```

Zgłoszenie 1.1

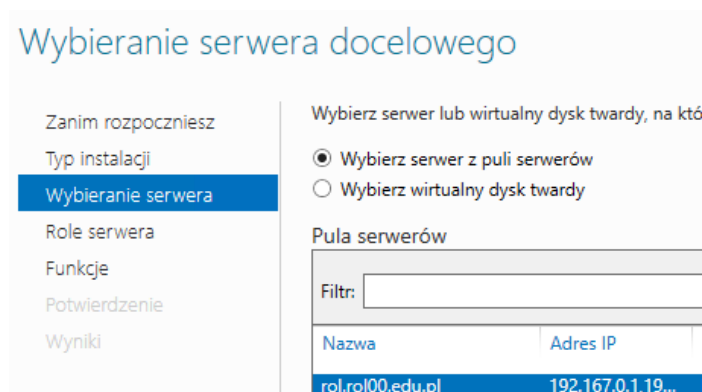
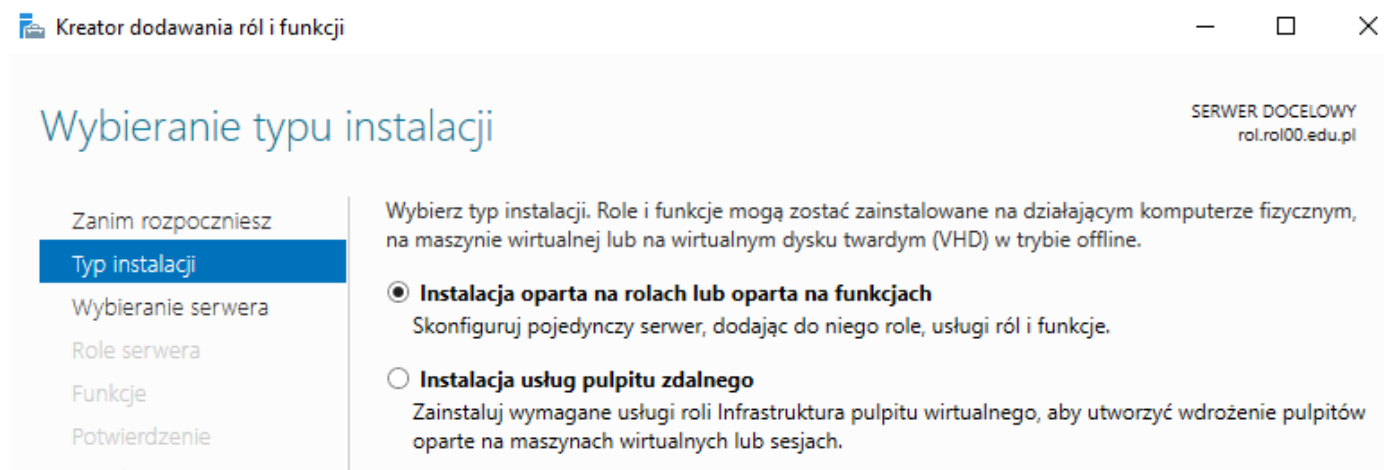
ETAP 3 – Instalacja roli „Dostęp zdalny” (RRAS)

1. Dodanie roli serwera „Dostęp zdalny”

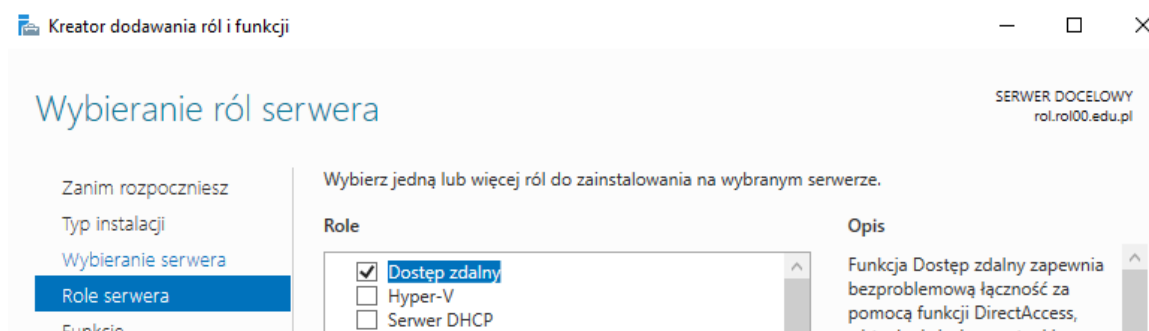
Otwórz Menedżer serwera → Dodaj role i funkcje → Rola „Dostęp zdalny”.



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

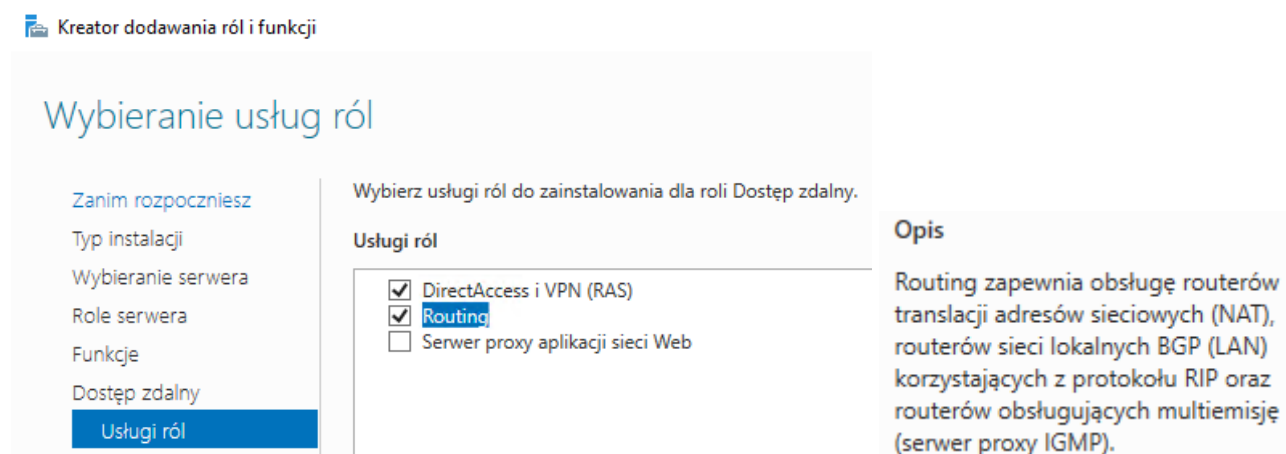
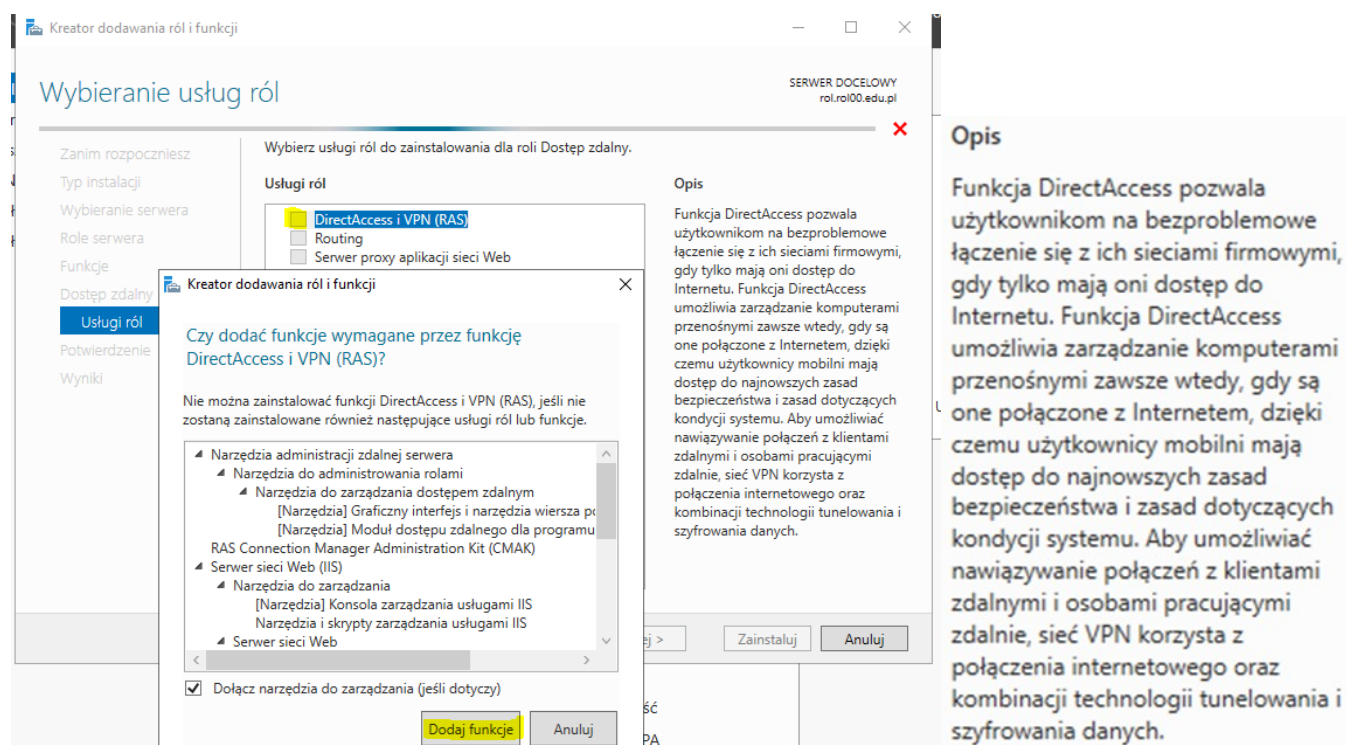


a. Zainstaluj rolę serwera „Dostęp zdalny”.

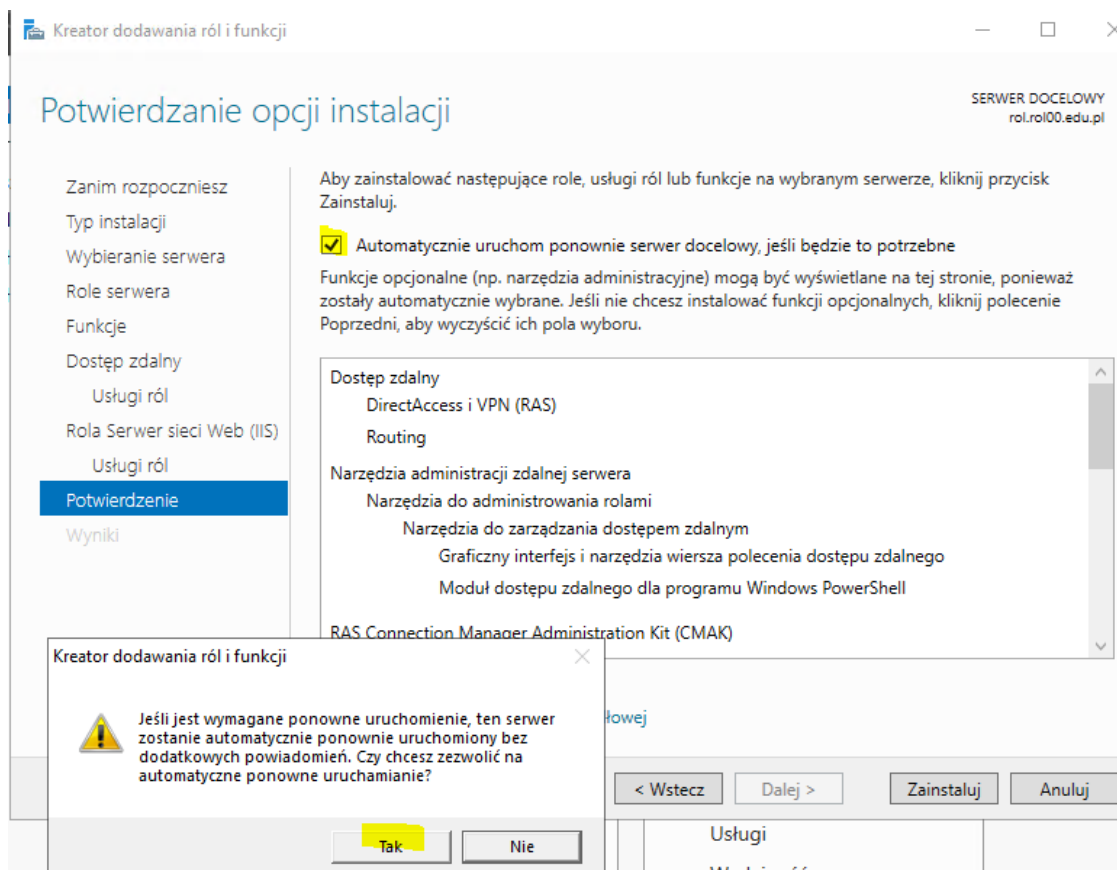


- b. Sprecyzuj, które składowe usługi NPAS chcesz zainstalować. By obsłużyć połączenia VPN musisz zainstalować następujący składnik: **Usługi routingu i dostępu zdalnego** (RRAS, Routing and Remote Access) – instaluj obie funkcje, czyli **Routing** i **Usługę dostępu zdalnego**.

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



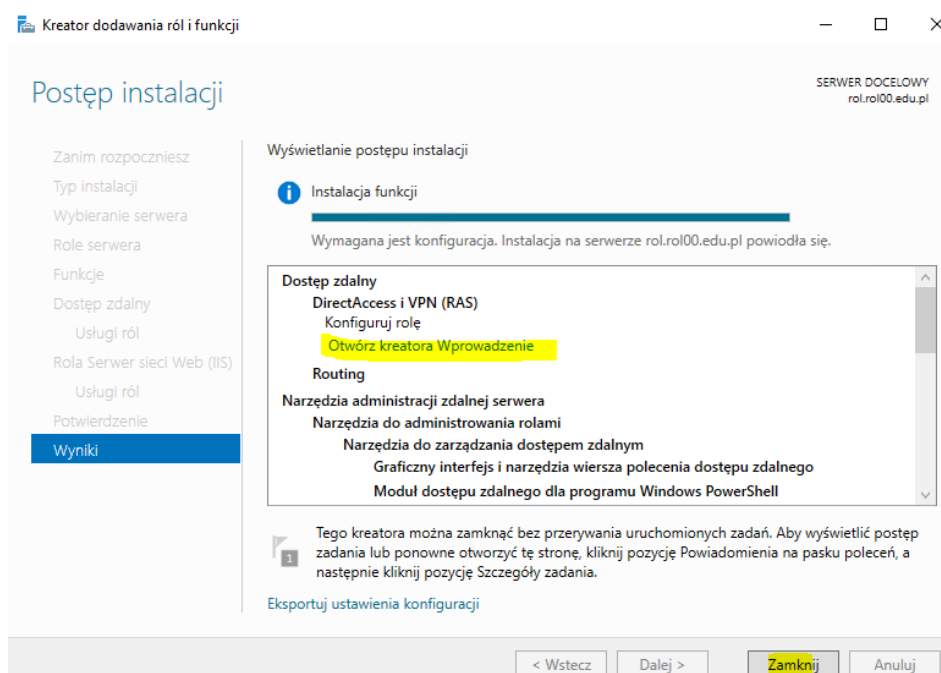
- c. Po kliknięciu **Dalej** przechodzisz do ekranu potwierdzenia.



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

Zgłoszenie 1.2

Kreator wyświetli okno z postępem instalacji. Poczekać, aż wszystkie wybrane role i funkcje zostaną zainstalowane. Po zakończeniu kliknij Zamknij, aby wrócić do głównego okna Menedżera serwera.



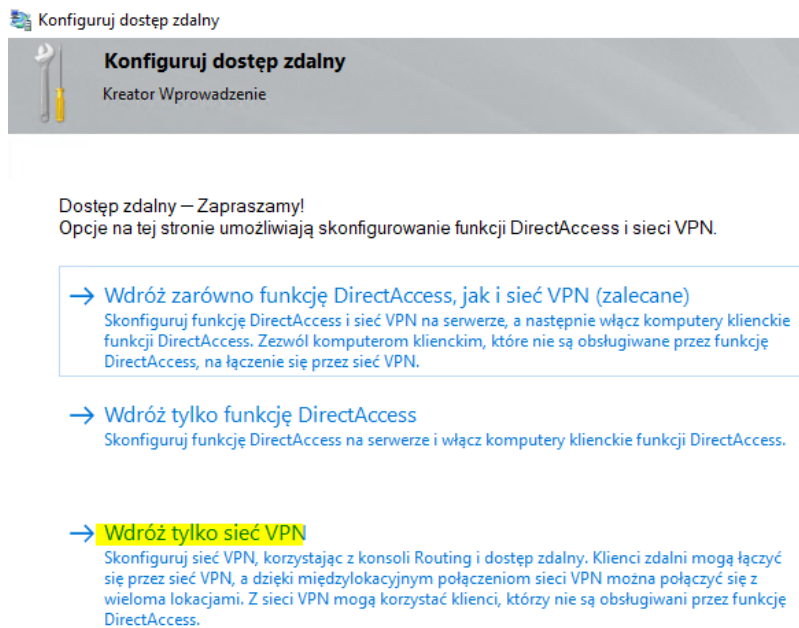
e. Sprawdź Kreator „Wprowadzenie” lub „!” Postępuj zgodnie z wskazówkami.

ETAP 4 – Konfiguracja RRAS: VPN + NAT + NPS + zaporą

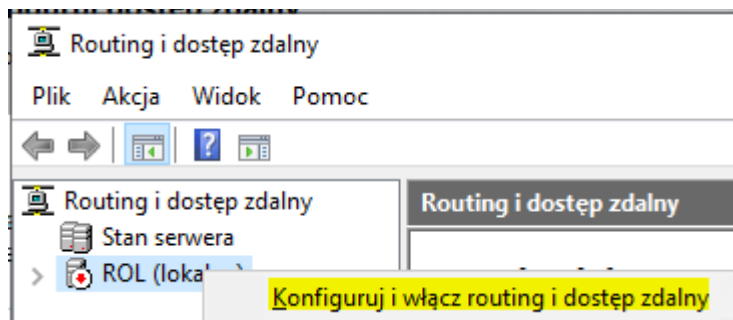
2. Procedura konfiguracji Usługi zasad i dostępu sieciowego.

Otwórz kreator Wprowadzanie. Kreator „Wprowadzenie” służy do późniejszej konfiguracji funkcji DirectAccess, VPN oraz routingu, dlatego w tym kroku jedynie **kontynuuj instalację**, czekając na jej pełne zakończenie. Idź do końca kreatora, naciskając „Dalej”. Naciśnij „Zamknij” na ekranie postępu.

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**.

Kreator instalacji serwera routingu i dostępu zdalnego

Konfiguracja

Możesz włączyć dowolną kombinację usług lub dostosować ten serwer.

- ☐ Dostęp zdalny (połączenie telefoniczne lub sieć VPN)
Zezwalaj klientom zdalnym na łączenie się z tym serwerem poprzez połączenie telefoniczne lub bezpieczne połączenie internetowe wirtualnej sieci prywatnej VPN.
- ☐ Translator adresów sieciowych
Zezwalaj klientom wewnętrznym na łączenie się z Internetem przy użyciu jednego publicznego adresu IP.
- ☐ Dostęp prywatnej sieci wirtualnej i translator adresów sieciowych
Zezwalaj klientom zdalnym na łączenie się z tym serwerem poprzez Internet, a klientom lokalnym na łączenie się z Internetem przy użyciu pojedynczego publicznego adresu IP.
- ☐ Bezpieczne połączenie między dwiema sieciami prywatnymi
Połącz tę sieć z siecią zdalną, taką jak sieć biurowa oddziału.
- ☒ Konfiguracja niestandardowa
Wybierz dowolną kombinację funkcji dostępnych w usłudze Routing i dostępu zdalnego.

< Wstecz Dalej > Anuluj

Kreator instalacji serwera routingu i dostępu zdalnego

Konfiguracja niestandardowa

Po zamknięciu tego kreatora można skonfigurować wybrane usługi w konsoli Routing i dostęp zdalny.

Wybierz usługi, które chcesz włączyć na tym serwerze.

- ☒ Dostęp przez sieć VPN
- ☐ Dostęp telefoniczny
- ☐ Połączenia z wybieraniem numeru na żądanie (używane dla routingu biura oddziału)
- ☒ Translator adresów sieciowych
- ☐ Routing LAN

< Wstecz Dalej > Anuluj

UWAGA: Gdy wystąpił problem z skonfigurowaniem połączenia VPN można tu wrócić i dodatkowo wybrać Routing LAN

Kreator instalacji serwera routingu i dostępu zdalnego

Kończenie pracy Kreatora instalacji serwera routingu i dostępu zdalnego

Praca Kreatora instalacji serwera routingu i dostępu zdalnego została pomyślnie ukończona.

Podsumowanie wybranych opcji:

Dostęp przez sieć VPN
Translator adresów sieciowych

Po zakończeniu pracy tego kreatora skonfiguruj wybrane usługi w konsoli Routing i dostępu zdalnego.

Aby zamknąć kreatora, kliknij przycisk Zakończ.

< Wstecz Zakończ Anuluj

Routing i dostęp zdalny

Uruchom usługę

Usługa Routing i dostęp zdalny jest gotowa do użycia.

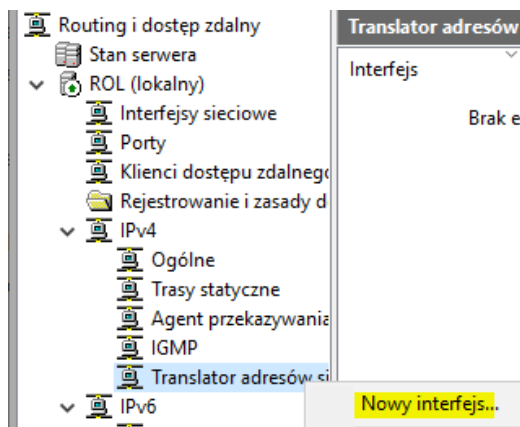
Uruchom usługę Anuluj

Kończenie inicjacji

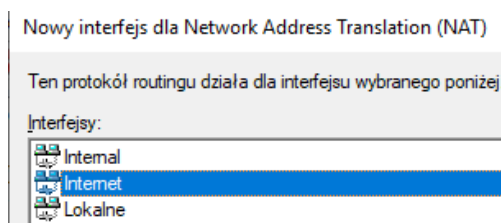


Czekaj. Trwa kończenie inicjacji usługi Routing i dostęp zdalny.

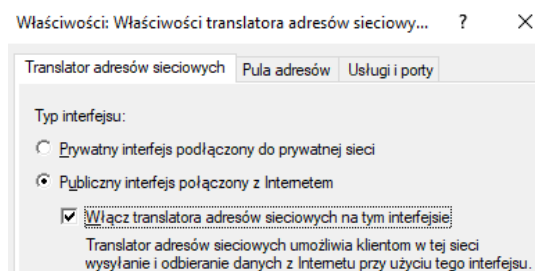
d. W RRAS dodaj nowe interfejsy



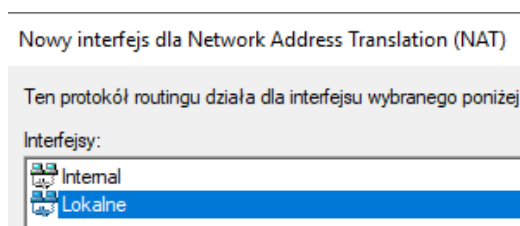
1. „Internet”



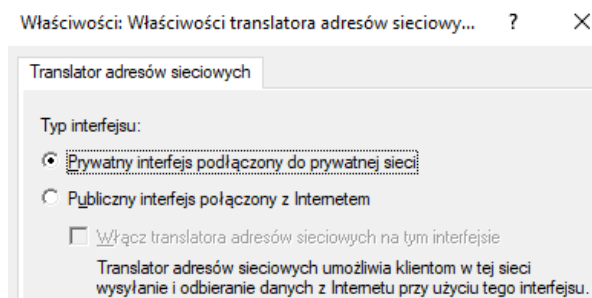
jako PUBLICZNY



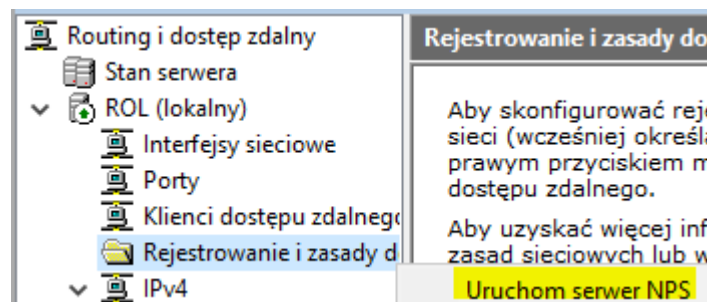
2. „Lokalne”



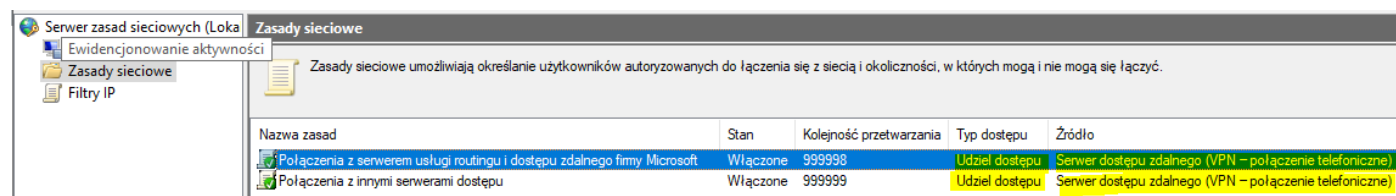
jako PRYWATNY



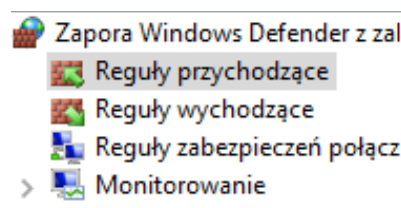
- e. Po poprawnym zainstalowaniu i skonfigurowaniu **serwera RRAS**, system **zasad sieciowych** (NPS, Network Policy Server) domyślnie będzie blokował wszelkie próby dostępu do serwera RRAS. Aby zmienić tę zasadę, otwórz gałąź **Routing i dostęp zdalny**, a następnie PPM na **Rejestrowanie i zasady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



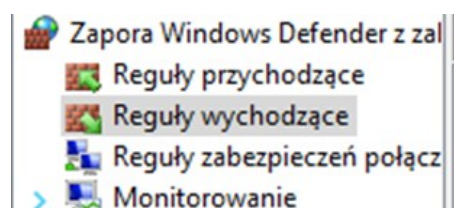
- f. Zmodyfikuj i pozostaw jak poniżej ustawienia zasad sieciowych „Udziel dostępu”



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



Routing i dostęp zdalny (ruch przychodzący GRE)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...
Routing i dostęp zdalny (ruch przychodzący L2TP)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...
Routing i dostęp zdalny (ruch przychodzący PPTP)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...
Protokół SSTP (ruch przychodzący SSTP)	Protokół SSTP	Wszys...	Tak	Zezwa...



Routing i dostęp zdalny (ruch wychodzący GRE)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...
Routing i dostęp zdalny (ruch wychodzący L2TP)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...
Routing i dostęp zdalny (ruch wychodzący PPTP)	Routing i dostęp zdalny	Wszys...	Tak	Zezwa...

- h. Wykonaj **ping google.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 (efekt podobny)

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Internet:

    Connection-specific DNS Suffix  . : mshome.net
    Link-local IPv6 Address . . . . . : fe80::d45d:fa11:1c2d:82eb%6
    IPv4 Address. . . . . : 172.18.201.161
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 172.18.192.1

Ethernet adapter Lokalne:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::bd26:5703:e8b1:8315%15
    IPv4 Address. . . . . : 192.167.0.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Zgłoszenie 2

ETAP 5 – Konfiguracja klienta Windows 11 (Ethernet + VPN)

3. Konfiguracja Windows 11 (klient)

Przejdź do Windows 11

a) Wykonaj polecenie **ping 192.167.0.1**. Ping powinien zakończyć się powodzeniem. Wyjaśnij, dlaczego.

```
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
```

Ping 192.167.0.1 działa, ponieważ jest to bezpośredni ping do adresu IP, który nie wymaga DNS. Adres ten jest osiągalny w sieci, a host odpowiada na żądania ICMP, dlatego polecenie kończy się sukcesem.

b) Wymuszenie błędnego DNS na interfejsie WAN klienta (symulacja braku poprawnego DNS przed zestawieniem VPN). Na kliencie Windows 11: Ustawienia > Sieć i Internet > Ethernet > Edytuj serwery DNS > Tryb: Ręczny > IPv4 → Włącz > Preferowany DNS: 0.0.0.0; Alternatywny DNS: 127.0.0.99

Zapisz

PowerShell: `ipconfig /flushdns`

Wykonaj `ping google.com` zakończony „Ping request could not find host google.com. Please check the name and try again”. Wyjaśnij, dlaczego.

Ping nie działa, ponieważ komputer nie jest w stanie rozwiązać nazwy google.com na adres IP. Oznacza to problem z usługą DNS - brak poprawnej konfiguracji DNS, niedziałający serwer DNS lub brak połączenia z siecią, które uniemożliwia wykonanie zapytania DNS.

ETAP 6 – Polityka DNS przez tunel (NRPT) – wymuszenie DNS domenowego

Polityka DNS przez tunel (NRPT) – wymuszenie zapytań domenowych do DC

NRPT to skrót od **Name Resolution Policy Table**, czyli **Tabela Zasad Rozpoznawania Nazw** w systemie Windows.

To mechanizm, który pozwala wymusić, *dokąd* klient Windows ma kierować zapytania DNS dla określonych domen - niezależnie od tego, jakie serwery DNS ma ustawione na karcie sieciowej.

NRPT to tabela zasad DNS, która mówi komputerowi: „jeśli zapytanie dotyczy konkretnej domeny, wysyłaj je do konkretnego serwera DNS”. Przykład z Twojego zadania: Namespace: .rol00.edu.pl, NameServer: 192.167.0.1

To znaczy: **każde zapytanie dotyczące domeny rol00.edu.pl ma iść DO TUNELU VPN, do serwera DNS kontrolera domeny 192.167.0.1**, nawet jeśli na karcie sieciowej ustawiony jest DNS 8.8.8.8 lub inny.

Po co używa się NRPT?

NRPT jest używany, żeby: **wymusić domenowy DNS, zapobiec wyciekom DNS, obsługiwać domenę po VPN, zapewnić, że klient znajdzie kontroler domeny przez tunel, rozwiązywać SRV, A, CNAME z domeny firmowej.**

Kiedy NRPT działa? Zawsze na **klientach Windows** (Win10, Win11). Nie działa na serwerach Windows - tylko na klientach. Działa zarówno pod VPN, jak i bez niego (np. dla DirectAccess).

NRPT to tabela zasad DNS w Windows, która wymusza wysyłanie zapytań do wybranego serwera DNS dla określonej domeny - dzięki temu klient po VPN korzysta z domenowego DNS, a nie z publicznych serwerów.

Po zestawieniu usług RRAS trzeba wymusić, by **klienci VPN pytali DNS domenowy (DC)**, a nie publiczne resolvery.

Nie zamykaj żadnych okien z efektami aż do zgłoszenia lub zrób wycinki z ekranu.

PowerShell (uruchom jako Administrator) na kliencie Windows 11:

1. Wyczyść starą regułę dla domeny (jeśli była)

```
Get-DnsClientNrptRule | Where-Object { $_.Namespace -eq ".rol00.edu.pl" } | Remove-DnsClientNrptRule -Force -ErrorAction SilentlyContinue
```

UWAGA: Ten etap pomijamy jak wyświetli błąd.

2. Dodaj wymuszenie DNS dla domeny przez tunel

```
Add-DnsClientNrptRule -Namespace ".rol00.edu.pl" -NameServers 192.167.0.1
```

3. Uporządkuj listę przyrostków DNS

```
Set-DnsClientGlobalSetting -SuffixSearchList @("rol00.edu.pl")
```

4. Reset cache i szybka kontrola

```
ipconfig /flushdns
```

```
nslookup rol.rol00.edu.pl. 192.167.0.1
```

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.rol00.edu.pl. 192.167.0.1
```

Komunikatu: DNS request timed out. Server: Unknown Address: 192.167.0.1 jest PRAWIDŁOWY efekt na tym etapie ćwiczenia!

UWAGA – ważne na tym etapie ćwiczenia

W instrukcji przewidziano, że polecenie: nslookup rol.rol00.edu.pl 192.167.0.1

ma zwrócić komunikat: DNS request timed out. Server: Unknown Address: 192.167.0.1

i ma to być prawidłowy wynik przed zestawieniem VPN, ponieważ klient znajduje się w sieci WAN i nie powinien mieć dostępu do DNS kontrolera domeny.

W naszej szkolnej sieci WAN działa jednak publiczny serwer DNS, który automatycznie przechwytuje i obsługuje wszystkie zapytania DNS.

Dlatego możesz zobaczyć wynik inny niż w instrukcji, np.: odpowiedź z publicznego DNS, nazwy serwerów Cloudflare, lub brak timeoutu. **Nie jest to błąd w Twojej konfiguracji.**

To zachowanie wynika z działania szkolnej infrastruktury DNS i różni się od środowiska, w którym była przygotowana pierwotna instrukcja.

Ćwiczenie wykonuj dalej normalnie - kolejne kroki (NRPT, VPN, SRV) nadal zadziałają prawidłowo.

W tym momencie lekcji: masz tylko **połączenie sieciowe WAN**, serwer RRAS jest po stronie LAN, **DNS serwera (192.167.0.1) NIE jest osiągalny przez WAN**, więc nslookup **musi** dać timeout.

Sprawdź, czy skonfigurowałeś NRPT, aby klient VPN zawsze kierował zapytania DNS domeny rol00.edu.pl do serwera DNS kontrolera domeny.

1) Menedżer DNS – czy serwer DNS odpowiada i jakie są rekordy

1. Menedżer serwera → Narzędzia → DNS

2. W drzewie: [Nazwa_serwera] → Strefy wyszukiwania do przodu → rol00.edu.pl

- **Sprawdź rekordy SRV** (ważne dla LDAP/DC):

Przejdź do strefy **_msdcs.rol00.edu.pl** (jeśli jest osobną strefą) lub do folderów **_sites**, **_tcp**, **_udp** wewnątrz strefy i upewnij się, że istnieją rekordy:

- **_ldap._tcp.dc._msdcs.rol00.edu.pl** (typ **SRV**) – to ten, o który pytasz w komendzie nslookup -type=SRV

3. Właściwości serwera DNS → karta **Monitorowanie**

- Kliknij **Przeprowadź prosty test zapytań** oraz **Przeprowadź test rekursji**, aby potwierdzić sprawność serwera.

Po Twoich poleceniach na kliencie (nslookup rol.rol00.edu.pl 192.167.0.1 i SRV) tu zweryfikujesz, że odpowiednie rekordy istnieją i mogą być zwracane.

2) Menedżer DNS – włącz „Rejestrowanie debugowania” i Podgląd zdarzeń

Jeśli chcesz wizualnie potwierdzić, że zapytania od klientów VPN faktycznie docierają:

1. **Menedżer serwera** → **Narzędzia** → **DNS**
2. Prawy przycisk na [Nazwa_serwera] → **Właściwości** → karta **Rejestrowanie debugowania**
 - Zaznacz: **Zaznacz wszystko** (lub przynajmniej *Zapytania, Odpowiedzi*).
 - Wskaż plik dziennika (domyślnie C:\Windows\System32\Dns\Dns.log).
 - Zastosuj.
3. Otwórz **Podgląd zdarzeń**: **Narzędzia** → **Podgląd zdarzeń** → **Dzienniki aplikacji i usług** → **Microsoft** → **Windows** → **DNS-Server** → **Analiza i debugowanie / Zdarzenia operacyjne**
 - Tu zobaczysz (**graficznie w dzienniku**) przychodzące zapytania, adresy źródłowe (powinny to być adresy puli VPN z RRAS) i rozwiązywane nazwy (np. rol.rol00.edu.pl).

To najpewniejsze potwierdzenie „że NRPT działa”, bo pokazuje realny ruch DNS od klientów przez tunel do DC.

3) RRAS – czy klient VPN jest rzeczywiście połączony (adres źródłowy dla logów DNS)

1. **Menedżer serwera** → **Narzędzia** → **Routing i dostęp zdalny**
2. [Nazwa_serwera] → **Stan** → **Klienci zdalni**
 - Widzisz listę aktywnych połączeń, przypisane **adresy IP puli VPN** i czas połączenia.
 - Te adresy powinny pojawiać się jako **źródła** w logach DNS (pkt 2).

4) Zasady grupy (jeśli NRPT dystrybuujesz przez GPO, a nie tylko ręcznie)

Jeżeli zamiast ręcznie na kliencie chcesz rozsyłać NRPT z DC:

1. **Menedżer serwera** → **Narzędzia** → **Zarządzanie zasadami grupy**
2. Otwórz odpowiednie **GPO** przypięte do OU z komputerami/VPN-klientami:
 - **Konfiguracja komputera** → **Zasady** → **Ustawienia systemu Windows** → **Zasady rozpoznawania nazw** (*Name Resolution Policy*)
3. W edytorze zobaczysz skonfigurowane **reguły NRPT** dla przestrzeni nazw (np. .rol00.edu.pl) i wskazane **serwery DNS** (np. 192.167.0.1).
4. Na kliencie możesz graficznie sprawdzić zastosowanie GPO:
 - Win+R → rsop.msc (lub gpresult /h raport.html) – pokazuje, czy GPO z NRPT się zastosowało.

Uwaga: Twoje aktualne komendy PowerShell ustawiają NRPT **lokalnie na kliencie**, więc na **serwerze nie zobaczysz** tej lokalnej tabeli; w GPMC zobaczysz ją tylko wtedy, gdy **tworzysz NRPT jako ustawienie GPO**.

5) Dodatkowe „wizualne” potwierdzenia na serwerze

- **Menedżer DNS** → **Statystyki** (prawy przycisk na serwerze DNS → **Wyczyść statystyki / Odśwież**) – rosnące liczniki zapytań po zestawieniu VPN.
- **Zapora systemu Windows z zabezpieczeniami zaawansowanymi** → **Monitorowanie** → sesje i reguły dla **UDP/TCP 53** (opcjonalnie).
- **Wydajność systemu** (perfmon.msc) → **Dodaj liczniki** → **DNS** (np. *Total Query Received/sec*) – wykresy aktywności.

Krótką „ściągą” – gdzie kliknąć (PL GUI)

- **DNS (MMC):** *Menedżer serwera* → *Narzędzia* → *DNS* → [serwer] → *Właściwości* → *Monitorowanie / Rejestrowanie debugowania*
- **Podgląd zdarzeń (DNS):** *Narzędzia* → *Podgląd zdarzeń* → *Dzienniki aplikacji i usług* → *Microsoft* → *Windows* → *DNS-Server* → *Zdarzenia operacyjne / Analiza i debugowanie*
- **RRAS:** *Narzędzia* → *Routing i dostęp zdalny* → *Stan* → *Klienci zdalni*
- **GPO (NRPT przez politykę):** *Narzędzia* → *Zarządzanie zasadami grupy* → [GPO] → *Konfiguracja komputera* → *Zasady* → *Ustawienia systemu Windows* → *Zasady rozpoznawania nazw*

Zgłoszenie 3

UWAGA BEZPIECZEŃSTWA (ważne): PPTP (MPPE) używane w ćwiczeniu jest przestarzałe i niezalecane do środowisk produkcyjnych z uwagi na znane słabości kryptograficzne.

W zastosowaniach rzeczywistych stosuj: IKEv2 (z EAP-TLS), SSTP (TLS 1.2+), OpenVPN / WireGuard.

ETAP 7 – Konfiguracja połączenia VPN i testy łączności (ipconfig, ping, nslookup, Wireshark)

4. Konfiguracja statycznej puli adresów IPv4 w RRAS (VPN) (domena)

Otwórz:

Menedżer serwera → Narzędzia → Routing i dostęp zdalny (RRAS)

Następnie: Kliknij PPM na ROL (lokalny)

Wybierz: Właściwości

Przejdź do zakładki IPv4

Zaznacz opcję: **Statyczna pula adresów**

Kliknij Dodaj...

W oknie „Edytuj zakres adresów IPv4” wpisz:

Początkowy adres IP: 192.167.0.20

Końcowy adres IP: 192.167.0.30

Maska doda się sama: 255.255.255.0

Następnie kliknij OK → Zastosuj → OK.

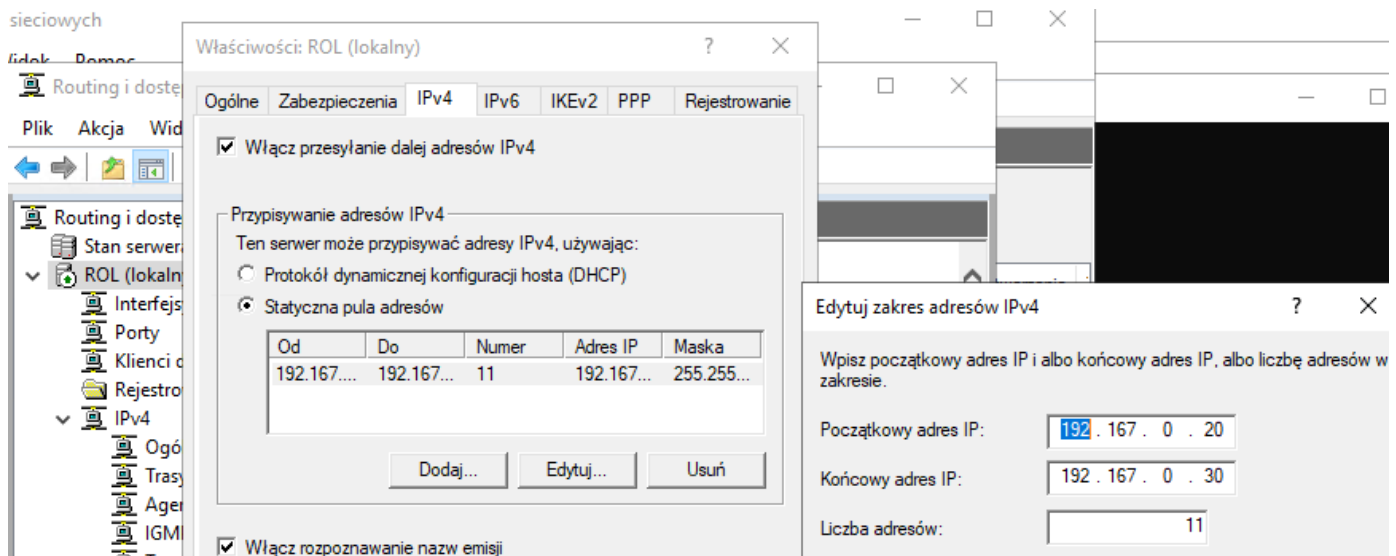
RRAS będzie teraz przydzielał klientom VPN adresy z zakresu: 192.167.0.20 – 192.167.0.30

Polecenie PowerShell (opcjonalne)

Uczniowie tego nie muszą robić, wariant PS:

Set-VpnIPAddressAssignment -IPAddressRange "192.167.0.20","192.167.0.30"

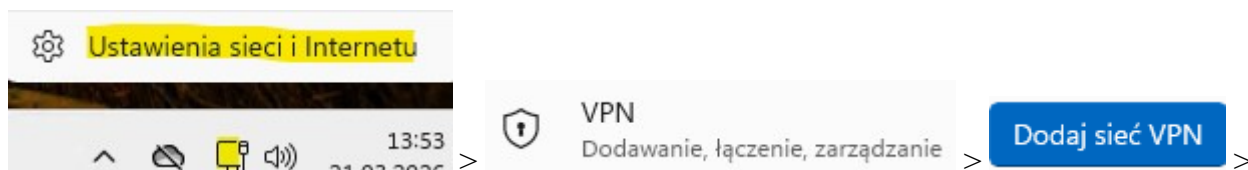
(Działa tylko w środowiskach z pełnym modułem RRAS.)



5. Konfiguracja połączenia VPN a Windows 11.

b) Skonfiguruj połączenie VPN.

Utwórz nowe połączenie, aby dołączyć do sieci VPN.



c) Określ sposób łączenia

Adres serwera sprawdź w ustawieniach serwera na karcie „Internet”.

Dodaj połączenie VPN

Dostawca sieci VPN

Windows (wbudowane)

Nazwa połączenia

vpn

Nazwa lub adres serwera

[Redacted]

Typ sieci VPN

Automatycznie

Typ informacji logowania

Nazwa użytkownika i hasło

Nazwa użytkownika (opcjonalnie)

Zapisz

Anuluj

d) Wybierz opcję **Połącz**.



vpn

Nie połączono

Połącz



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



Zabezpieczenia Windows

Zaloguj

Nazwa użytkownika

Administrator

Hasło

••••••••



Domena:

Nazwa użytkownika lub hasło są niepoprawne.

OK

Anuluj

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



vpn

Połączono

Rozłącz



g) 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 interpretację. Co uczeń powinien zapisać w zeszycie:

Parametry połączenia PPTP + MPPE:

PPTP – protokół tunelowania VPN

MPPE 128-bit – szyfrowanie danych w tunelu

MS-CHAPv2 – uwierzytelnianie użytkownika

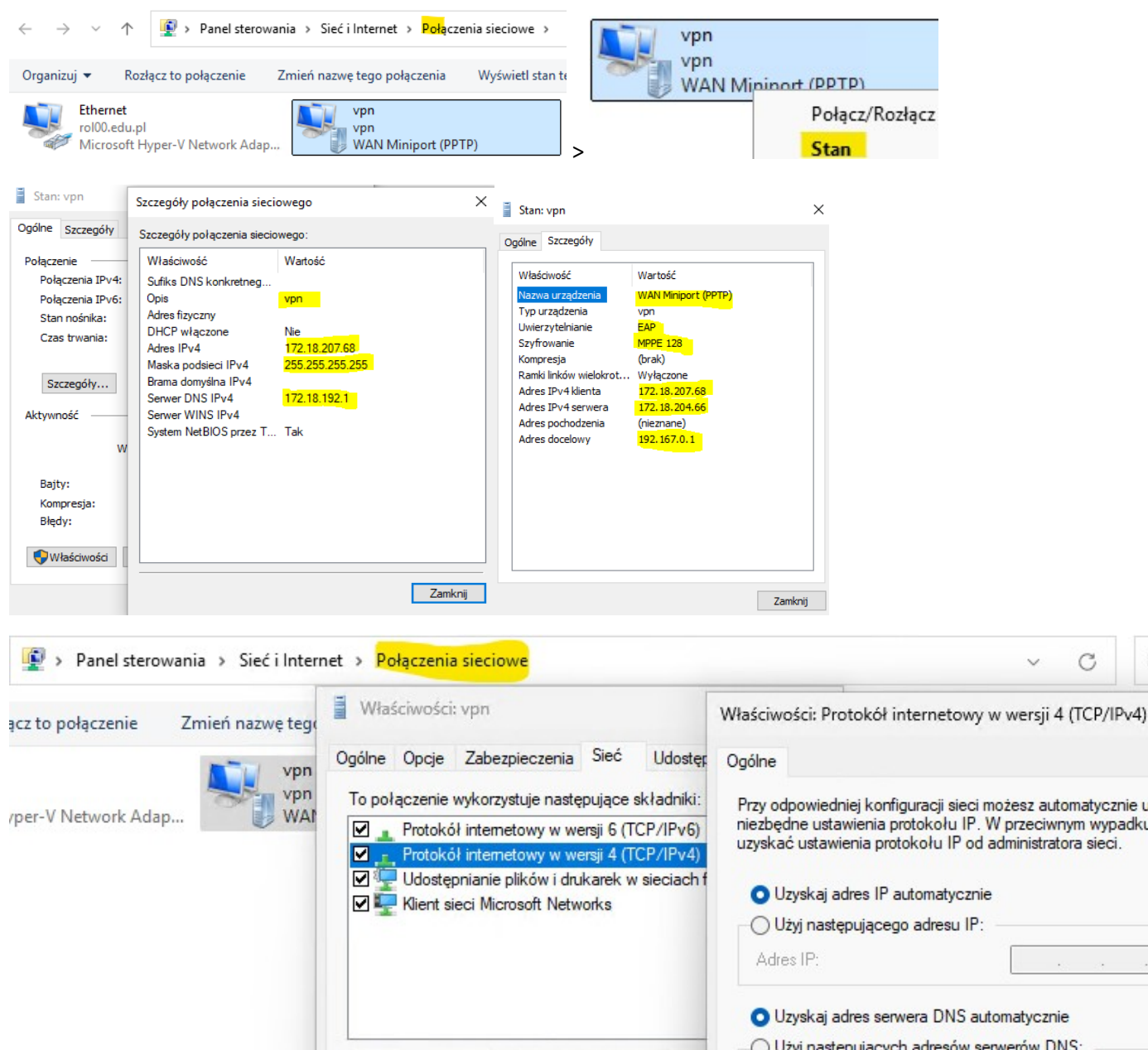
GRE – kapsułkowanie ruchu

IP klienta VPN – adres z puli RRAS

IP serwera VPN – adres routera RRAS

Szyfrowanie: włączone – tunel zabezpieczony

Na Windows 11:



h) Wykonaj `ipconfig /all` i zapisz adresy interfejsów: Ethernet (WAN) i PPP/vpn (tunel).

Przykładowe:

Ethernet adapter Ethernet:

DHCP Enabled. : Yes

Autoconfiguration Enabled : Yes

IPv4 Address. : 172.26.110.203(Preferred)

Default Gateway : 172.26.96.1

DHCP Server : 172.26.96.1

DNS Servers : 172.26.96.1

NetBIOS over Tcpip. : Enabled

PPP adapter vpn:

Description : vpn

DHCP Enabled. : No

Autoconfiguration Enabled : Yes

IPv4 Address. : 172.26.105.151(Preferred)

Subnet Mask : 255.255.255.255

Default Gateway : 0.0.0.0

DNS Servers : 172.26.96.1

i) Wykonaj ping do adresu IPv4 na **PPP adapter vpn** zakończony sukcesem. Wyjaśnij, dlaczego.

Ping działa, ponieważ tunel VPN jest zestawiony, a klient ma własny adres IP na interfejsie PPP, dzięki czemu może komunikować się z serwerem przez tunel.

j) Wykonaj **ping google.com** zakończony sukcesem. Wyjaśnij, dlaczego.

```
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

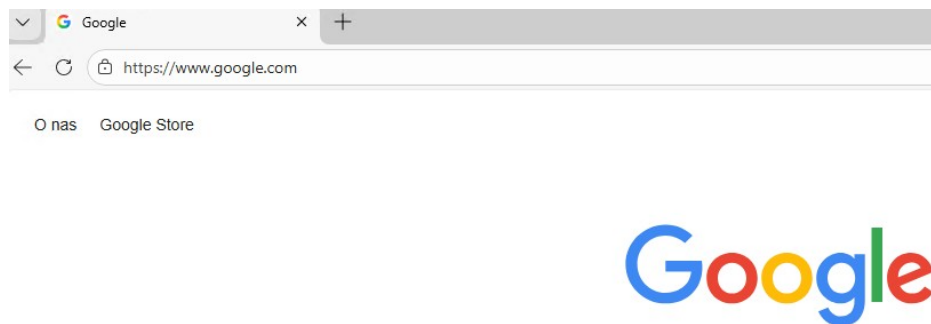
Ping statistics for 142.250.186.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 18ms, Average = 17ms
```

Ping działa poprawnie, ponieważ komputer ma teraz prawidłową konfigurację DNS i potrafi rozwiązać nazwę google.com na adres IP. Oznacza to, że zapytania DNS są kierowane do właściwego serwera DNS (lokalnego lub publicznego), który zwraca poprawne rekordy, dzięki czemu możliwa jest komunikacja z hostem w Internecie. Spójność z wcześniejszą odpowiedzią (b):

W b) ping nie działał, bo DNS nie działał.

W k) ping działa, bo DNS już działa poprawnie.

k) Otwórz w przeglądarce google.com zakończony sukcesem



Zgłoszenie 4

6. Analiza parametrów sieci za pomocą tabeli mapowania sesji translatora adresów sieciowych na serwerze Windows 2019

Przejdź do serwera

a) Sprawdź połączonych klientów dostępu zdalnego. Co to oznacza?

Nazwa użytkownika	Czas trwania	Liczba portów	Stan
IS\Administrator	00:13:32	1	Bez obsługi ochrony dostępu do sieci

Oznacza to, że użytkownik *Administrator* jest aktualnie połączony z serwerem VPN, a tunel działa poprawnie. Czas trwania sesji jest zmienny.

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

Zapisz w zeszycie wnioski. Uwaga: adresy IP widoczne na zrzutach ekranu mogą różnić się od tych, które pojawią się u Ciebie podczas ćwiczenia.

Interfejs	Mapowania w sumie	Pakiety przychodzące po translacji	Odrzucone pakiety przychodzące	Pakiety wychodzące po translacji
Lokalne	0	0	0	0
Internet	56	19 177	0	15 472

Protokół	Kierunek	Adres prywatny	Adres publiczny	Port publiczny	Adres zdalny	Port zdalny	Czas bezczynności
TCP	Wchodzący	63 647	172.26.99.7	63 647	150.171.109.53	443	73
TCP	Wchodzący	60 865	172.26.99.7	62 084	52.182.141.63	443	37
TCP	Wchodzący	50 249	172.26.99.7	62 085	104.81.60.57	443	42
TCP	Wchodzący	53 348	172.26.99.7	62 086	92.123.189.179	443	40
TCP	Wychodzący	63 331	172.26.99.7	63 331	95.101.61.219	443	39
TCP	Wychodzący	51 323	172.26.99.7	62 089	204.79.197.203	443	39
TCP	Wychodzący	56 614	172.26.99.7	62 090	151.101.65.44	443	39
TCP	Wychodzący	50 019	172.26.99.7	62 091	185.89.210.82	443	39

Serwer RRAS wykonuje NAT dla klientów VPN. W tabeli widać, że prywatne adresy z puli VPN (172.26.105.x) są tłumaczone na publiczny adres serwera (172.26.99.77). Oznacza to, że klienci VPN korzystają z Internetu przez NAT serwera, a wiele aktywnych sesji TCP potwierdza prawidłowe działanie translacji adresów.

Zgłoszenie 5

Krótką ściągą do korelacji z Wireshark i NAT (dla ucznia)

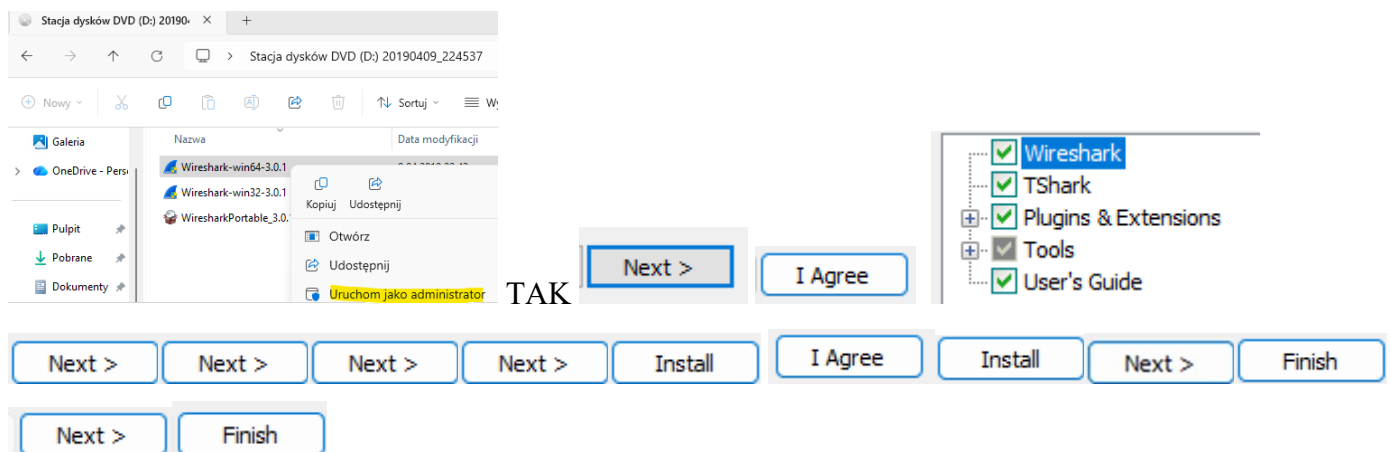
- Po `ipconfig /all` odczytaj: **Ethernet (WAN)** – np. 172.26.110.203 **PPP/vpn (tunel)** – np. 172.26.105.187
- W **Wireshark** filtruj: `ip.addr == 172.26.110.203 || ip.addr == 172.26.105.187` – zobaczysz, które ramki dotyczą **WAN**, a które **tunelu**.
- W **RRAS** → **IPv4** → **Translator adresów sieciowych (interfejs „Internet”)** sprawdź, jak Twój adres **PPP** (172.26.105.x) mapuje się na adres **WAN** (172.26.99.7) z różnymi portami publicznymi (to właśnie **PAT**).

7. Analiza parametrów sieci za pomocą Wireshark na Windows 11

Przejdź do Windows 11

- Wykonaj ping na adres publiczny serwera z parametrem `-t` zakończony sukcesem (tu 172.26.99.7) wyjaśnij efekt.
- Wykonaj ping na adres publiczny bramy serwera z parametrem `-t` zakończony sukcesem (tu 172.26.96.1) wyjaśnij efekt.
- Wykonaj ping na adres *PPP adapter RAS (Dial In) Interface* (tu 172.26.110.190) wyjaśnij efekt.
- Pobierz [Wireshark.iso](#) podłącz go i zainstaluj Wireshark.

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



- Uruchom Wireshark, uruchom podsłuch połączenia lokalnego.

*5 interfaces

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

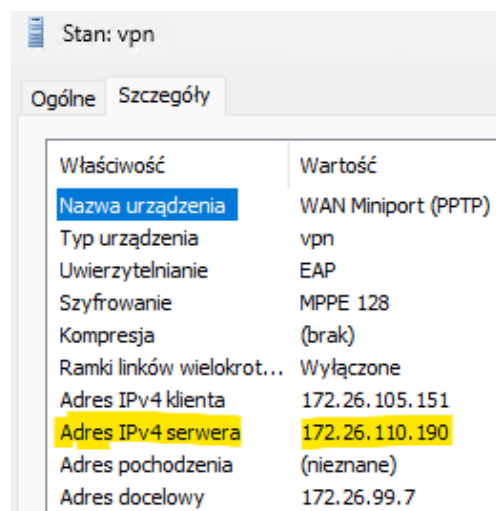
pptp

No.	Time	Source	Destination	Protocol	Length	Info
5	2.155208	172.26.99.7	172.26.110.203	PPTP	70	Echo-Request
6	2.155298	172.26.110.203	172.26.99.7	PPTP	74	Echo-Reply

Adresy IP i pakiety w Wiresharku mogą być inne niż na przykładzie - zależą od Twojego faktycznego połączenia VPN. To normalne - wartości te zależą od aktualnego połączenia VPN, adresu przydzielonego przez serwer RRAS oraz tego, jakie pakiety zostaną przechwycone w czasie podglądu. Najważniejsze, abyś

potrafił rozpoznać ogólny kierunek komunikacji: ruch między Twoim adresem PPP (klient VPN) a adresem serwera VPN.

f) 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.



Właściwość	Wartość
Nazwa urządzenia	WAN Miniport (PPTP)
Typ urządzenia	vpn
Uwierzytelnianie	EAP
Szyfrowanie	MPPE 128
Kompresja	(brak)
Ramki linków wielokrot...	Wyłączone
Adres IPv4 klienta	172.26.105.151
Adres IPv4 serwera	172.26.110.190
Adres pochodzenia	(nieznane)
Adres docelowy	172.26.99.7

Uczeń zapisuje:

Widzę pakiety PPTP/PPP między moim adresem PPP a adresem serwera VPN.

Adresy IP mogą być u mnie inne (dynamiczne przydzielanie).

Protokół: PPTP + PPP, szyfrowanie MPPE 128-bit.

Stan VPN potwierdza poprawne zestawienie tunelu.

Zgłoszenie 6

ETAP 8 – Dołączenie do domeny przez VPN

8. Podłączenie Windows 11 do domeny z włączonym VPN i analiza.

- Pozostaw DNS na interfejsie „Ethernet”
 - Preferowany serwer DNS: 192.167.0.1
 - Alternatywny serwer DNS: (pusty)
- Pozostaw “Dołącz te Suffixy DNS” (w podanej kolejności): rol00.edu.pl
 - Wejdź w **Ustawienia** → **Sieć i Internet** → **Ethernet**.
 - Otwórz **Zmień opcje karty** i kliknij prawym na swoją kartę sieciową → **Właściwości**.
 - Kliknij **IPv4** → **Właściwości**.
 - Wybierz **Zaawansowane** → **DNS**, gdzie ustawisz serwery DNS i sufiksy domeny.
- Testy poprawności i braku wycieku DNS

Sprawdzenie, że **DNS naprawdę idzie tunelem** i że SRV są widoczne z klienta. Testy poprawności i braku wycieku DNS Na kliencie (po zestawieniu VPN):

```
nslookup rol.rol00.edu.pl 192.167.0.1
```

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.rol00.edu.pl 192.167.0.1
```

Przykładowy prawidłowy wynik:

```
C:\Users\admin>nslookup -type=SRV _ldap._tcp.dc._msdcs.rol00.edu.pl 192.167.0.1
```

```
Server: topolino.ct.infn.it
```

```
Address: 192.167.0.1
```

```
_ldap._tcp.dc._msdcs.rol00.edu.pl    SRV service location:
```

```
priority    = 0
```

```
weight      = 100
```

```
port        = 389
```

```
svr hostname = rol.rol00.edu.pl
```

```
rol.rol00.edu.pl    internet address = 172.25.173.5
```

```
rol.rol00.edu.pl    internet address = 172.25.162.24
```

```
rol.rol00.edu.pl    internet address = 192.167.0.1
```

Jeśli wynik jest taki jak u Ciebie → NIC nie poprawiasz. Jest dobrze.

Komunikat “Jeżeli odpowiedzi nie pochodzą z 192.167.0.1 – popraw NRPT” odnosi się tylko do sytuacji, gdy:

- odpowiedzi przychodzą z 8.8.8.8,
- lub innego DNS z karty fizycznej,
- lub Server: pokazuje coś innego niż **192.167.0.1**.

U Ciebie wszystko jest OK.

Wniosek, dla ucznia: Test potwierdził, że zapytania DNS są kierowane przez tunel VPN do serwera 192.167.0.1, a klient poprawnie pobiera rekordy SRV kontrolera domeny, co oznacza brak wycieku DNS i prawidłowe działanie NRPT.

Jeżeli odpowiedzi nie pochodzą z 192.167.0.1 – popraw regułę NRPT / metryki interfejsów.

Wireshark (klient):

- na interfejsie PPP/vpn sprawdź, że zapytania DNS (UDP/53) wychodzą tunelem,
- na interfejsie Ethernet (WAN) nie powinno być zapytań DNS do Internetu.

d) Zmiana metryki interfejsów

- a. Ustaw VPN jako interfejs o niższej metryce

Panel sterowania → Sieć i Internet → Połączenia sieciowe → Zmień ustawienia karty sieciowej → **vpn** → Właściwości → Sieć > ... IPv4 → Właściwości → Zaawansowane → odznacz „Metryka automatyczna” → Metryka interfejsu > wpisz > **1**

Dla Ethernetu ustaw np. **50**.

b. Wyłącz IPv6 na karcie fizycznej (na czas testu)

Bo Windows potrafi próbować dołączać „po IPv6”, którego nie masz.

c. Upewnij się, że z klienta pingujesz DC po tunelu, np.:

ping 192.167.0.1

ping (tu wpisz adres ip WAN z serwer)

Oba wracają z adresu VPN, nie fizycznego. Zdanie „oba wracają z adresu VPN, nie fizycznego” oznacza, że cały ruch do domeny rol00.edu.pl (pingi, DNS, SRV) przechodzi przez skonfigurowany tunel VPN (interfejs PPP), a nie wychodzi interfejsem Ethernet WAN. Dzięki temu klient może komunikować się z kontrolerem domeny znajdującym się w sieci LAN serwera RRAS. Jest to dowód poprawnego działania konfiguracji VPN + NRPT.

d. TEST KLUCZOWY – to zdecyduje:

nltest /dsgetdc:rol00.edu.pl

Jeśli zwróci DC → możesz dołączyć do domeny.

Jeśli zwróci błąd → Windows nadal używa złego interfejsu.

e) Ustawienie puli adresów IPv4 dla połączeń VPN

a. W RRAS → IPv4:

Zaznacz: Statyczna pula adresów

Dodaj: od: 192.167.0.20 do: 192.167.0.30

b. Zastosuj zmiany.

c. Rozłącz i ponownie połącz VPN.

Po połączeniu klient powinien dostać:

adres w zakresie 192.167.0.20–30

maskę 255.255.255.0

DNS = 192.167.0.1

brama NIE jest potrzebna do DC

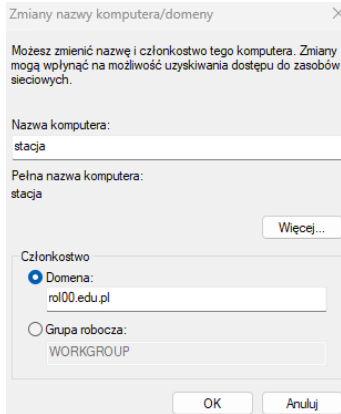
d. Dla pewności ustaw poprawny DNS na kliencie ręcznie. Wpisz w PowerShell (Admin):

Set-DnsClientServerAddress -InterfaceAlias "vpn" -ServerAddresses 192.167.0.1

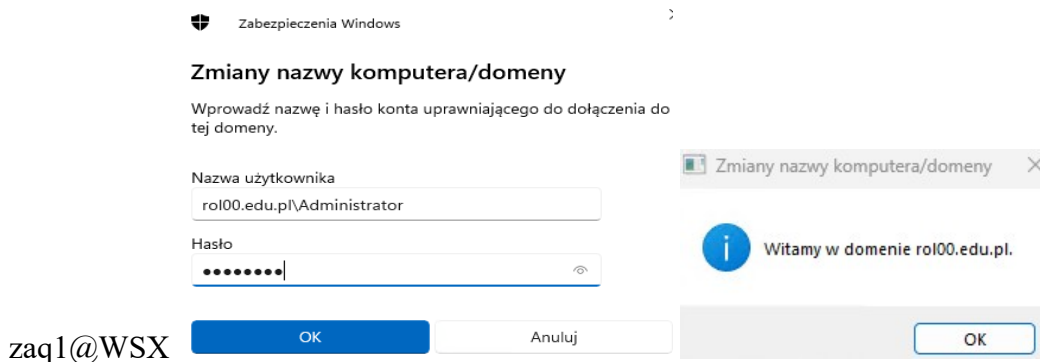
f) Właściwe dołączenie do domeny

a. Podaj nazwę domeny

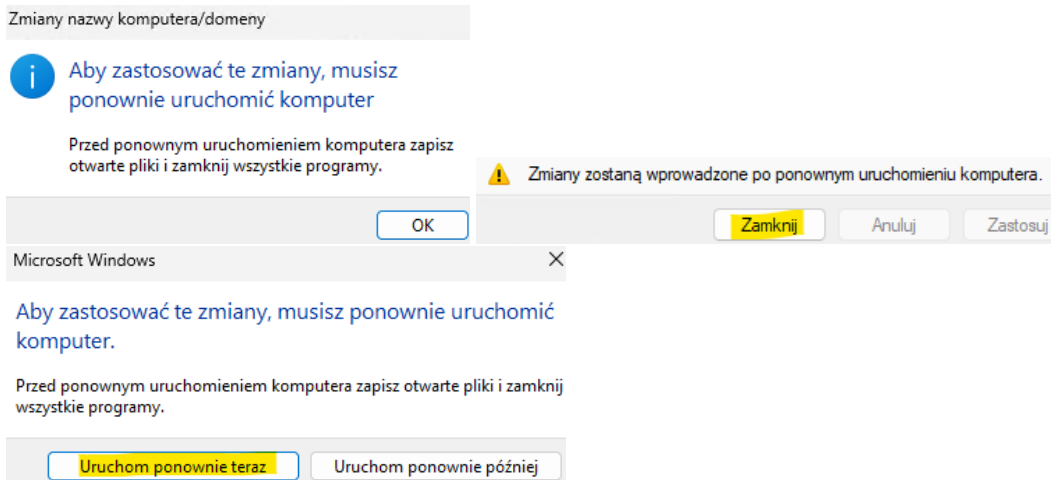
Flaga + Pause > Zaawansowane ustawienia systemu > Nazwa komputera > Zmień >



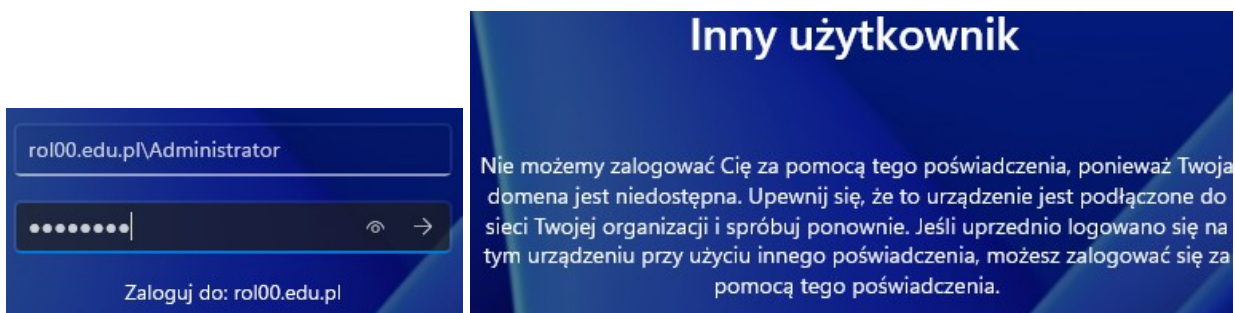
b. Podaj nazwę i hasło konta uprawniającego do dołączenia do domeny: rol00.edu.pl\Administrator



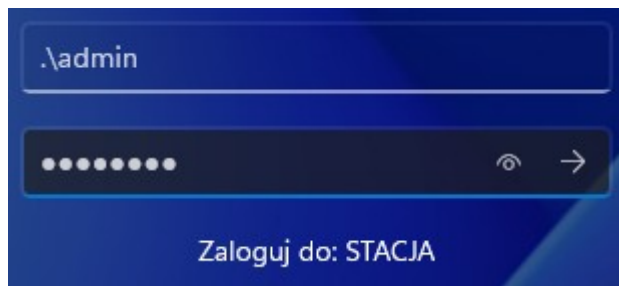
zaq1@WSX



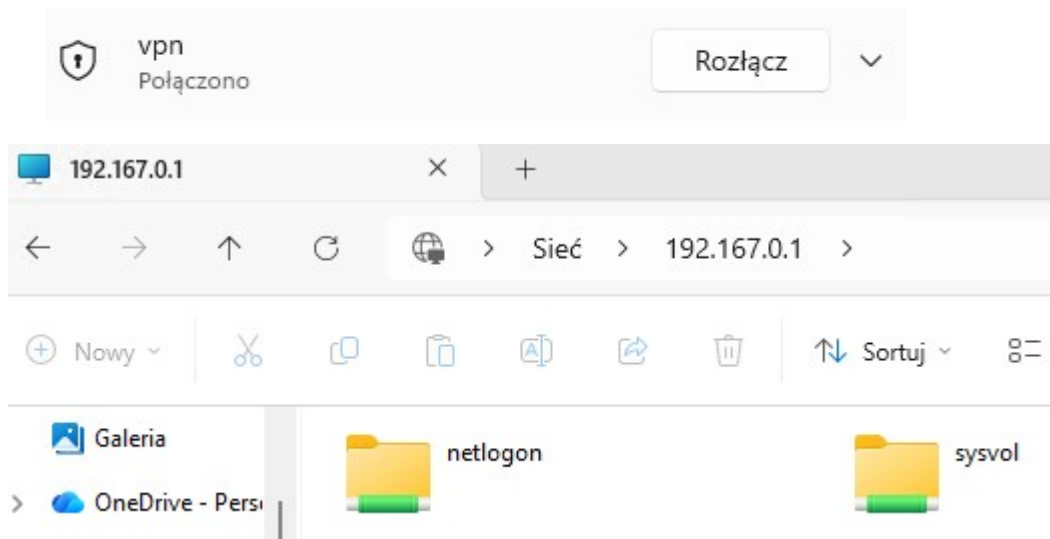
c. Po restarcie Na Windows 11 zaloguj się kontem domenowym.



d. Na Windows 11 zaloguj się jako .\admin

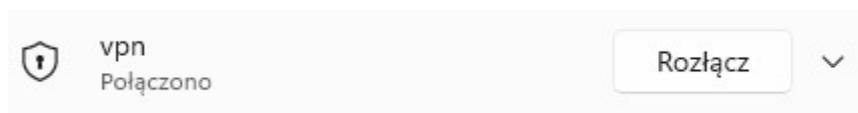


e. Na Windows 11 podłącz się jako vpn i zweryfikuj dostęp do zasobów domenowych.

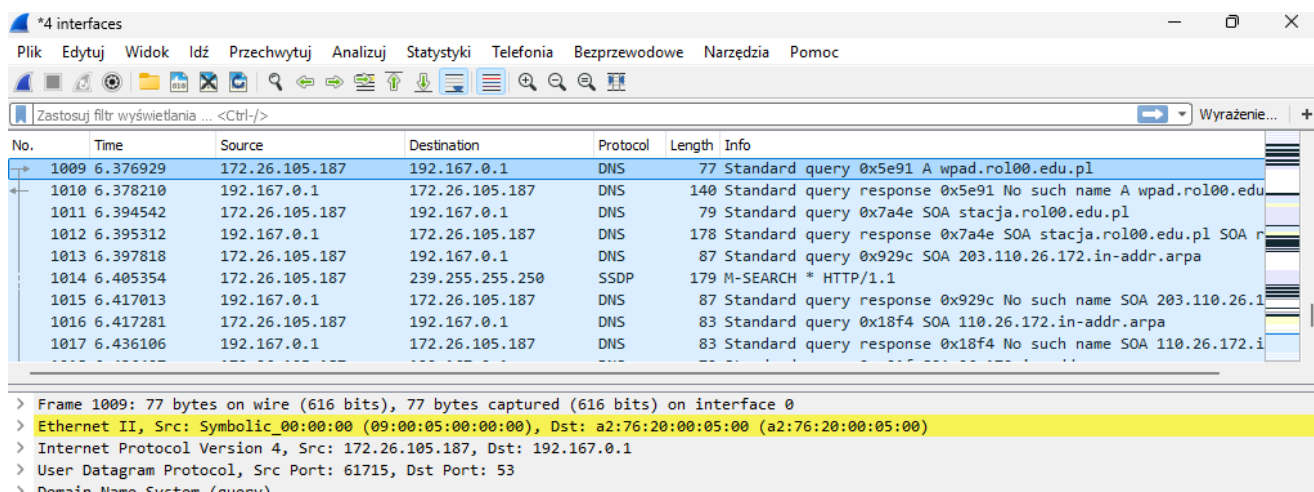


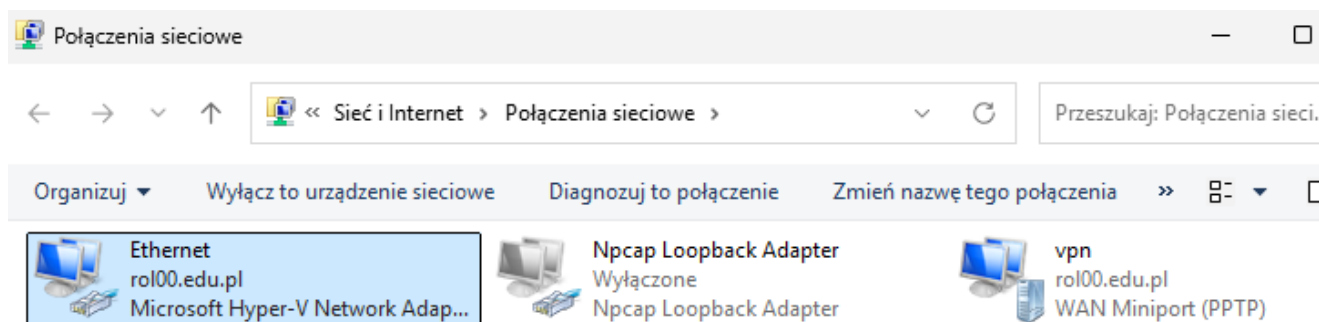
g) Praca z Wireshark

- Włącz Wireshark, przejmij wszystkie karty sieciowe
- Podłącz się jako vpn



- Zatrzymaj podsłuch w Wireshark
- Przeanalizuj przechwycony ruch. Zapisz w zeszycie wnioski z analizy wynik podsłuchu sieci wykonanego za pomocą Wireshark. Oraz przedstaw wnioski z zadania.





e. Wykonaj `ipconfig /all` i odczytaj adresy IPv4 dwóch interfejsów widocznych po zestawieniu VPN: Ethernet (sieć zewnętrzna/WAN) oraz PPP/vpn (tunel VPN).

Przykład: `172.26.110.203` (Ethernet) i `172.26.105.187` (PPP).

f. Następnie w Wireshark odfiltruj ruch po tych adresach, aby zobaczyć, które pakiety wychodzą bezpośrednio przez WAN, a które przez tunel VPN.

Filtry przykładowe (wklej jeden z nich w pasku filtra):

`ip.addr == 172.26.110.203 || ip.addr == 172.26.105.187`

Lub – jeśli chcesz zobaczyć oddzielnie ruch dla każdego interfejsu:

`ip.addr == 172.26.110.203`

`ip.addr == 172.26.105.187`

Wskazówka dla ucznia:

- Pakiety z adresem źródłowym/docelowym `172.26.110.203` to ruch idący interfejsem **Ethernet (WAN)**.
- Pakiety z adresem `172.26.105.187` to ruch przechodzący przez **tunel VPN (PPP)**.
- Zrób krótki zrzut ekranu (screen) z Wiresharka z widocznym filtrem i kilkoma pasującymi pakietami dla obu adresów.

g. Pozostaw włączonego Wireshark, przejmij karty sieciowe

h. Wykonaj ping do `172.26.105.187` z parametrem `-t` zakończony sukcesem

1) Filtry wyświetlania (Display Filter) – wpisujesz w górnym pasku „Display Filter”

Tylko ICMP (ping) do/z adresu `172.26.105.187`:

`icmp && ip.addr == 172.26.105.187`

Wyłącznie żądania echa (Echo Request) do `172.26.105.187`:

`icmp.type == 8 && ip.dst == 172.26.105.187`

Wyłącznie odpowiedzi echa (Echo Reply) od `172.26.105.187`:

`icmp.type == 0 && ip.src == 172.26.105.187`

Widok porównawczy dla obu interfejsów (tunel i WAN) - jeśli znasz oba adresy klienta z `ipconfig /all`, np.:

- Ethernet (WAN) = `172.26.110.203`

- PPP/vpn (tunel) = 172.26.105.187

Złap ICMP związany z jednym adresem (tunel):

```
icmp && ip.addr == 172.26.105.187
```

Lub równocześnie pokaż ruch związany z oboma:

```
icmp && (ip.addr == 172.26.110.203 || ip.addr == 172.26.105.187)
```

Wskazówka dydaktyczna:

- Jeśli przechwytujesz na **PPP/vpn**, zobaczysz ruch ICMP „po tunelu” (adres klienta z interfejsu PPP i adres docelowy).
- Jeśli przechwytujesz na **Ethernet**, zobaczysz ruch ICMP „po WAN” (z adresem przypisanym karcie Ethernet).

2) Filtry przechwytywania (Capture Filter) – ustawiasz w oknie wyboru interfejsu (ikona „zębatego”) przed kliknięciem Start

Tylko ping do/z 172.26.105.187:

```
icmp and host 172.26.105.187
```

Tylko ping wychodzący do 172.26.105.187:

```
icmp and dst host 172.26.105.187
```

Tylko ping przychodzący z 172.26.105.187:

```
icmp and src host 172.26.105.187
```

Kiedy używać?

Capture Filter ogranicza ilość danych już na etapie przechwytywania (mniejszy plik, mniej szumu).

Display Filter działa po fakcie (pełny zrzut, a potem odsiewasz).

- Zatrzymaj podsłuch i przeanalizuj przechwycony ruch
 - Zatrzymaj przechwytywanie (**Stop**).
 - Wpisz odpowiedni **Display Filter** (jeśli jeszcze nie był ustawiony) – np.

```
icmp && ip.addr == 172.26.105.187
```

3. Co sprawdzić i zapisać we wnioskach:

- Wiersze **Echo (ping) request** i **Echo reply** (kolumna *Info*): czasy RTT, numery identyfikatorów/seq.
- **Warstwa IP**: czy źródłowy adres klienta zgadza się z adresem karty, którą chcesz testować (Ethernet vs PPP)?
 - Na **interfejsie PPP/vpn** źródłem będzie adres z interfejsu PPP (tunel).
 - Na **interfejsie Ethernet** źródłem będzie adres z karty WAN.
- Czy występuje **ICMP Port Unreachable / Destination Unreachable** (błędy sieciowe)?
- Czy są **straty** (brak Echo reply) lub **wysokie opóźnienia**?

- j. Pozostaw uruchomionego Wiresharka i wybierz interfejs PPP/vpn (tunel) lub Ethernet (WAN).
- k. W wierszu polecenia wykonaj ping 172.26.105.187 -t. W Wireshark zastosuj filtr:

icmp && ip.addr == 172.26.105.187

- l. (alternatywnie tylko zapytania/odpowiedzi: icmp.type == 8 && ip.dst == 172.26.105.187 / icmp.type == 0 && ip.src == 172.26.105.187)

n) Zatrzymaj przechwytywanie i opisz wynik:

- adres źródłowy/destynacji w ramach ICMP,
- RTT, ewentualne straty,
- różnice między przechwytem na **PPP** a na **Ethernet** (który interfejs generuje dany ruch).

Zapisz w zeszycie wnioski z analizy wynik podsłuchu sieci wykonanego za pomocą Wireshark.

Oraz przedstaw wnioski z zadania.

Zgłoszenie 7

ETAP 9 – Analiza NAT (tabela mapowania sesji) na RRAS

9. Analiza parametrów serwera Windows 2019

Przejdź do Windows Server 2019

- a) Na serwerze RRAS przejdź do IPv4 → Translator adresów sieciowych i wybierz interfejs Internet. Odczytaj bieżące wpisy w „ROL – tabela mapowania sesji translatora adresów sieciowych”. Przeanalizuj na interfejsie Internet tabelę mapowania sesji translatora adresów sieciowych

Routing i dostęp zdalny		Translator adresów sieciowych					
Stan serwera							
ROL (lokalny)							
Interfejsy sieciowe							
Porty							
Klienci dostępu zdalnego (1)							
Rejestrowanie i zasady dost							
IPv4							
Ogólne							
Trasy statyczne							
Agent przekazywania DI							
IGMP							

Interfejs	Mapowania w sumie	Pakiety przychodzące po translacji	Odrzucone pakiety przychodzące	Pakiety wychodzące po translacji	Odrzuc
Lokalne	0	0	0	0	0
Internet	24	188 130	6	110 487	1

ROL - tabela mapowania sesji translatora adresów sieciowych							
Protokół	Kierunek	Adres prywatny	Port prywatny	Adres publiczny	Port publiczny	Adres zdalny	Port zdalny
UDP	Wychodzące	172.26.105.151	49 842	172.26.99.7	62 102	142.251.151.119	443
UDP	Wychodzące	172.26.105.151	51 158	172.26.99.7	62 119	172.26.96.1	53
UDP	Wychodzące	172.26.105.151	61 137	172.26.99.7	62 122	172.26.96.1	53
UDP	Wychodzące	172.26.105.151	61 588	172.26.99.7	62 124	172.26.96.1	53

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

1) Odczyt i identyfikacja (wypełnij poniższe)

- a) **Liczba aktywnych mapowań** na interfejsie **Internet**:
- b) **Protokół** ruchu dla wybranych 3 wpisów (np. zaznaczonych): (np. UDP/UDP/UDP)
- c) **Kierunek** ruchu: (np. „Wychodzące” dla wszystkich)
- d) **Adres prywatny** (klienta VPN) we wpisach: (np. 172.26.105.151)
- e) **Adres publiczny** (RRAS po stronie WAN): (np. 172.26.99.7)
- f) **Para portów** (prywatny → publiczny) dla każdego z wpisów:
- wpis 1: →

- wpis 2: →
- wpis 3: →

g) **Adres zdalny i port zdalny (cel):**

- wpis 1: : (np. 142.251.151.119:443)
- wpis 2: : (np. 172.26.96.1:53)
- wpis 3: : (np. 172.26.96.1:53)

Wskazówka: Widzisz mechanikę PAT (Port Address Translation) – **ten sam adres prywatny** (172.26.105.151) jest mapowany na **ten sam adres publiczny** (172.26.99.7), ale **różne porty publiczne** (np. 62102, 62119, 62122, ...). Dzięki temu wiele jednoczesnych sesji z jednego hosta prywatnego może iść na zewnątrz.

2) Interpretacja techniczna (krótkie odpowiedzi)

h) **Co oznacza, że wpis ma „Kierunek = Wychodzące”?**

.....

i) **Dlaczego port publiczny różni się od portu prywatnego?**

(opisz w 1–2 zdaniach działanie PAT/NAPT)

.....

j) **Które wpisy odpowiadają za rozwiązywanie nazw (DNS)?**

(podaj po czym to rozpoznajesz)

.....

k) **Który wpis wskazuje na ruch HTTPS do Internetu?**

(uzasadnij na podstawie pola „Port zdalny”)

.....

l) **Wyjaśnij, co zobaczysz w Wireshark na kliencie przy takiej sesji DNS/HTTPS.**

(na jakich adresach/portach, które IP będzie źródłowe po stronie klienta, a co po stronie RRAS)

.....

3) Korelacja z Wireshark (dowód)

- **Na kliencie (Windows 11)** uruchom Wireshark i przechwyć minimum 30 s ruchu podczas:
 - pingowania/otwarcia strony www,
 - wykonania nslookup (np. nslookup microsoft.com).
- **Zastosuj filtry wyświetlania** (w pasku „Display filter”):

DNS (UDP/53) – cały ruch klienta:

`(udp.port == 53) && (ip.src == 172.26.105.151 || ip.dst == 172.26.105.151)`

HTTPS (TCP/443) – cały ruch klienta:

`(tcp.port == 443) && (ip.src == 172.26.105.151 || ip.dst == 172.26.105.151)`

(Zastąp 172.26.105.151 rzeczywistym adresem **PPP/vpn** klienta z ipconfig /all.)

Zapisz 2 zrzuty ekranu:

1. DNS – 2–3 ramki z widocznym adresem źródłowym klienta (PPP) i portem **53** po drugiej stronie.
2. HTTPS – 2–3 ramki do dowolnego IP z Internetu na **443**.

Wnioski (2–3 zdania): Opisz, w jaki sposób **port publiczny** na RRAS (np. 62102) pozwala rozróżnić jednocześnie sesje, mimo że wychodzą przez **ten sam** adres publiczny (172.26.99.7).

4) Mini-quiz (sprawdzenie zrozumienia)

1. Gdy wielu klientów prywatnych łączy się do tego samego serwera DNS na porcie 53, jak RRAS odróżnia ich sesje po stronie **Internet**?

Odp.: (po porcie publicznym = PAT)

2. Co by się stało, gdyby interfejs **Internet** nie wykonywał translacji portów (tylko adresu)?

Odp.: (konflikt sesji, brak rozróżnienia jednoczesnych połączeń)

3. W tablicy widzisz wpis „UDP → Adres zdalny 142.251.151.119:443”. Co to za typ ruchu i jak prawdopodobnie powstał?

Odp.: (HTTPS przez QUIC/UDP lub specyficzny serwis; odnieś do portu 443 i protokołu UDP z Twojego przykładu)

Przedstaw wnioski z zadania.

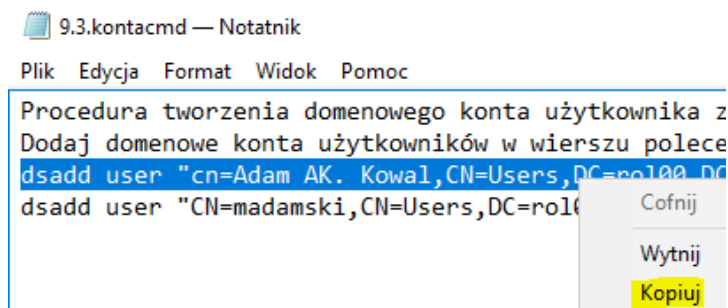
Zgłoszenie 8

ETAP 10 – Kontrola dostępu: konta użytkowników VPN w AD/NPS

10. Dodanie domenowego konta użytkownika uprawnionego do korzystania z VPN

a) Pobierz [9.3kontacm.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**

```

Administrator: Wiersz polecenia
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Administrator>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
dsadd succeeded:cn=Adam AK. Kowal,CN=Users,DC=rol00,DC=edu,DC=pl

```

d) Dodane zostanie domenowe konto 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

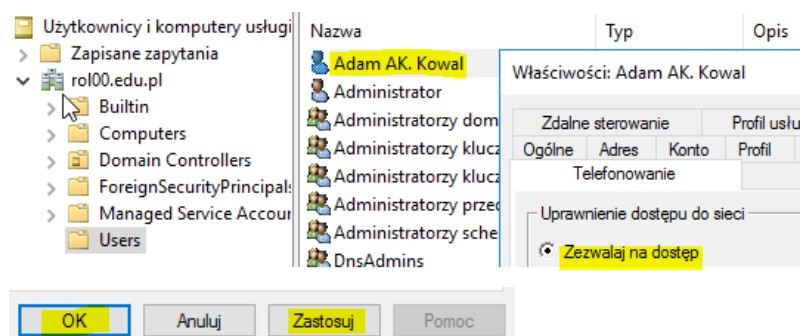
```

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

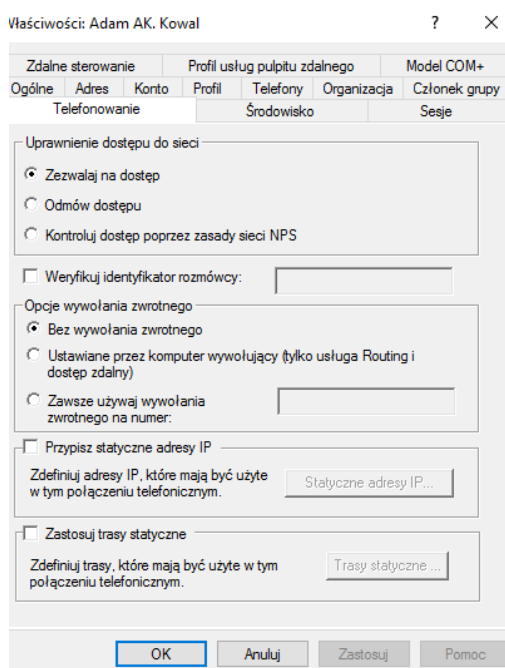
e) Określ użytkowników, którzy mogą łączyć się z serwerem.

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.



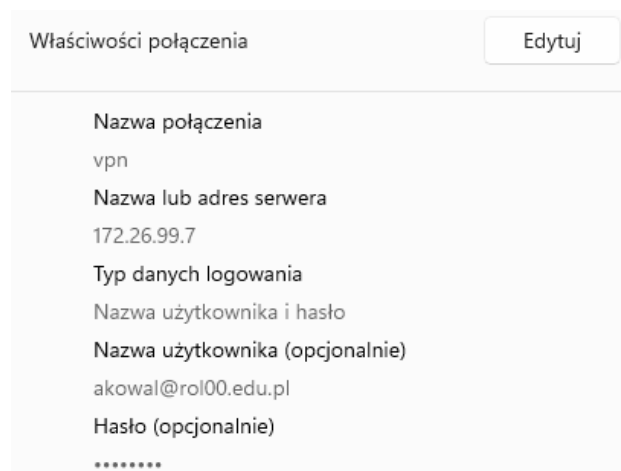
Efekt:



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

Kontrola dostępu: tylko wybrani użytkownicy mogą łączyć się z VPN

- 1) W konsoli „Użytkownicy i komputery AD” otwórz właściwości konta ucznia/użytkownika.
- 2) Karta „Telefonowanie” → „Uprawnienie dostępu do sieci” → zaznacz „Zezwalaj na dostęp”.
- 3) W NPS pozostaw zasadę, która dopuszcza połączenia wyłącznie dla tak oznaczonych kont (lub dla grupy domenowej „VPN_Users” – zalecane w większych środowiskach).
- f) W Windows 11 wyczyść informacje logowania
- g) W Windows 11 edytuj właściwości połączenia VPN
- h) Połącz ponownie używając dodanego konta akowal@rol00.edu.pl



Właściwości połączenia		Edytuj
Nazwa połączenia	vpn	
Nazwa lub adres serwera	172.26.99.7	
Typ danych logowania		
Nazwa użytkownika i hasło		
Nazwa użytkownika (opcjonalnie)	akowal@rol00.edu.pl	
Hasło (opcjonalnie)	*****	

Efekt polecenia ipconfig /all:

PPP adapter vpn:

Connection-specific DNS Suffix . :

Description : vpn

Physical Address. :

DHCP Enabled. : No

Autoconfiguration Enabled . . . : Yes

IPv4 Address. : 172.26.99.41(Preferred)

Subnet Mask : 255.255.255.255

Default Gateway : 0.0.0.0

DNS Servers : 172.26.96.1

NetBIOS over Tcpip. : Enabled

Zgłoszenie 9

11. Na Windows 11 zaloguj się kontem domenowym

Połączenia utworzone w Ustawieniach:

NIE pojawiają się na ekranie logowania

NIE utrzymują tunelu przy „Przełącz użytkownika”

NIE działają dla użytkownika przed zalogowaniem

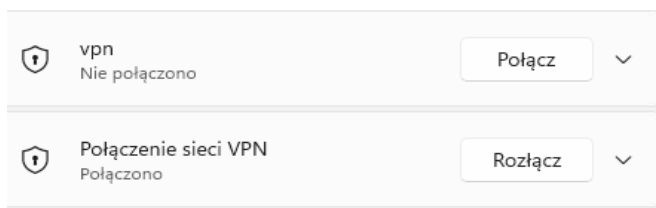
NIE zestawiają tunelu w czasie logowania do domeny

a) Utwórz połączenie VPN SYSTEMOWE

Tylko takie połączenie: pojawi się na ekranie logowania, pozwoli połączyć VPN przed wpisaniem hasła, umożliwi logowanie domenowe

- Otwórz klasyczne narzędzie sieciowe (nie Ustawienia!) Naciśnij: Win + R wpisz: **ncpa.cpl**
- Kliknij: „Skonfiguruj nowe połączenie lub nową sieć”
- Wybierz: „Połącz z miejscem pracy”
- Wybierz: „Użyj mojego połączenia internetowego (VPN)”
- Wpisz dane serwera Adres: sprawdź w ustawieniach serwera i Nazwa połączenia: **Połączenie sieci VPN**.
- Pojawi się opcjonalny check-box: „Zezwalaj innym użytkownikom na używanie tego połączenia” **ZAZNACZ** to. To uczyni połączenie systemowym. Bez tego Windows **NIGDY** nie pozwoli logować się przez VPN.
- Zakończ, a potem skonfiguruj: Zabezpieczenia: PPTP + MSCHAPv2, IPv4: DNS = 192.167.0.1, IPv4 → Zaawansowane → Użyj domyślnej bramy w sieci zdalnej

The screenshot shows the 'Network Setup' window in Windows. The title bar reads 'Sieć i Internet > Centrum sieci i udostępniania'. Below the title bar, there's a search bar 'Szukaj w Panelu sterowania'. The main content area is titled 'Wyświetl podstawowe informacje o sieci i skonfiguruj połączenia'. Underneath, there's a section 'Połącz z miejscem pracy'. The instruction says 'Wpisz adres internetowy, z którym chcesz się połączyć'. Below this, it says 'Ten adres można uzyskać od administratora sieci.' There are two input fields: 'Adres internetowy:' with the value '172.25.173.5' and 'Nazwa miejsca docelowego:' with the value 'Połączenie sieci VPN'. At the bottom, there are three checkboxes: 'Użyj karty inteligentnej' (unchecked), 'Zapamiętaj moje poświadczenia' (checked), and 'Zezwalaj innym osobom na korzystanie z tego połączenia' (checked). A note below the last checkbox says 'Ta opcja zezwala dowolnej osobie z dostępem do tego komputera na używanie tego połączenia.' At the very bottom, there are two buttons: 'Utwórz' and 'Anuluj'.



b) Na Windows 11 zaloguj się kontem domenowym i zweryfikuj dostęp do zasobów domenowych.

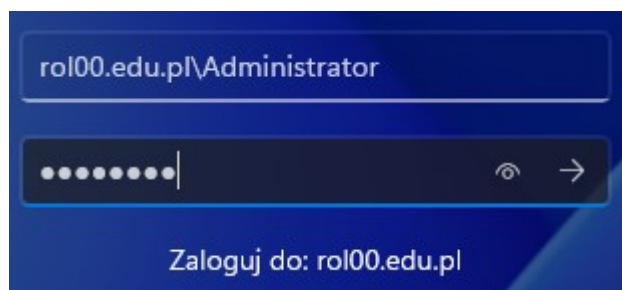
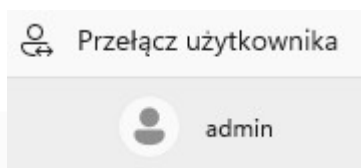
Zmiany nazwy komputera/domeny

Wprowadź nazwę i hasło konta uprawniającego do dołączenia do tej domeny.

Nazwa użytkownika
rol00.edu.pl\Administrator

Hasło
••••••••

OK Anuluj



Efekt 1:

Administrator
Administrator@rol00.edu.pl

Znajdź ustawienie

System
Bluetooth i urządzenia
Sieć i Internet
Personalizacja
Aplikacje
Konta
Czas i język
Ułatwienia dostępu
Prywatność i zabezpieczenia
Windows Update

Sieć i Internet > VPN

Połączenia sieci VPN

Połączenie sieci VPN
Nie połączono

Połącz

Dodaj sieć VPN

Ustawienia zaawansowane dla wszystkich połączeń sieci VPN

Zezwalaj na połączenia VPN w sieciach taryfowych

Włączone

Zezwalaj na połączenia VPN podczas korzystania z roamingu

Włączone

Uzyskaj pomoc

Przełącz opinię

(c) Microsoft Corporation. Wszelkie prawa zastrzeżone

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:

Connection-specific DNS Suffix . : mshome.net
Description : Microsoft Hype
Physical Address. : 00-15-5D-01-64
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IPv4 Address. : 172.25.78.115
Subnet Mask : 255.255.240.0
Lease Obtained. : niedziela, 22
Lease Expires : poniedziałek,
Default Gateway : 172.25.64.1
DHCP Server : 172.25.64.1
DNS Servers : 192.167.0.1
NetBIOS over Tcpip. : Enabled

Efekt 2:

Zaloguj

Nazwa użytkownika

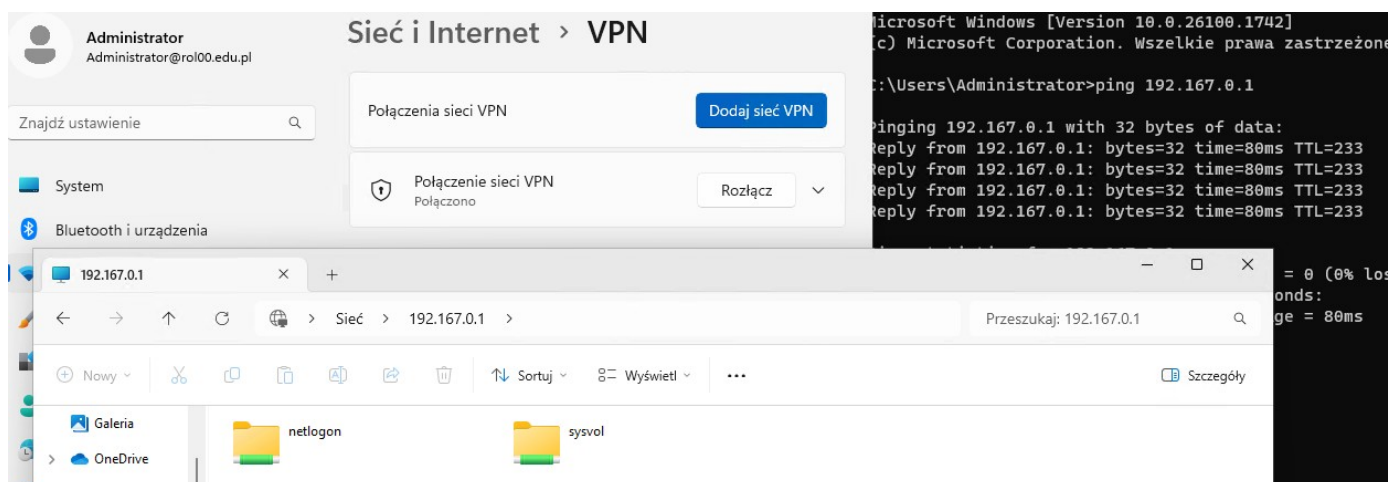
rol00.edu.pl\Administrator

Hasło

••••••••

Domena: rol00.edu.pl

Nazwa użytkownika lub hasło są niepoprawne.



12. 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 wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.