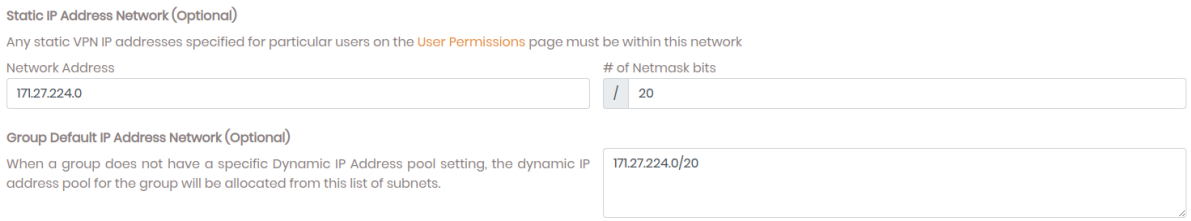
Kraków, 17.03.23

Kryptografia w służbie prywatności i techniki zwiększające prywatność użytkownika

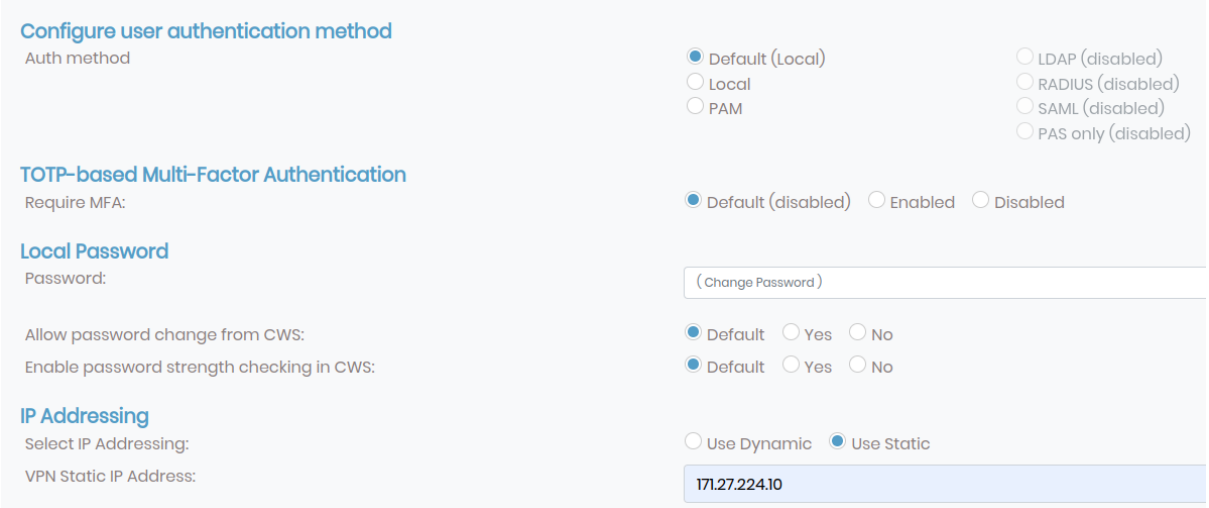
Julia Sadecka, Jakub Augustyn, Beniamin Jankowski

1. Konfiguracja maszyny

Po sukcesywnym założeniu maszyny wirtualnej w serwisie Azure wchodzimy na port 943 (Admin User Interface) i logujemy jako użytkownik *openvpn*.
W zakładce VPN Settings ustalamy odpowiednie dane sieci



Następnie dodaję użytkowników, tworząc certyfikaty dla nich oraz ustawiając metodę uwierzytelniania jako hasło.
Będą one potrzebne przy korzystaniu z sieci VPN.
Ponadto pamiętam o użyciu adresu statycznego:



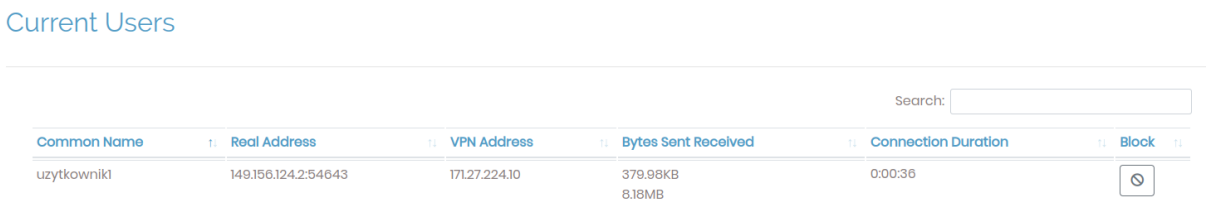
Po pobraniu certyfikatu należy otworzyć połączenie. W systemie UNIX jest to komenda:
$ sudo openvpn <certyfikat>
Następnie należy podać nazwę i hasło. Po tym połączenie zostaje nawiązane.

```
kuba@lenovo:~/Downloads$ sudo openvpn profile-4.ovpn
[sudo] password for kuba:
2023-03-08 10:33:42 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future
OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to
 --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2023-03-08 10:33:42 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 1
4 2022
2023-03-08 10:33:42 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Enter Auth Username: uzytkownik1
🔐 Enter Auth Password: **************
2023-03-08 10:34:08 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2023-03-08 10:34:08 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
```

W celu upewnienia się wchodzimy w konfigurację sieci.
Połączenie *tun0* posiada przydzielony adres IP z puli zadanej przez serwer openvpn.

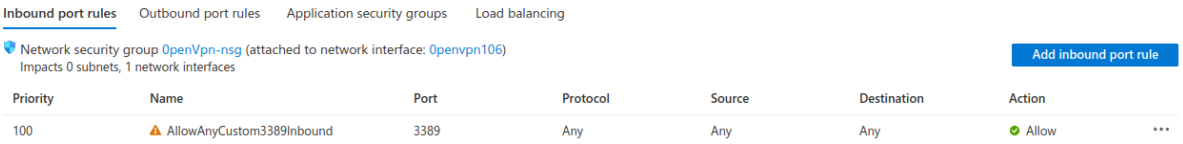
```
tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 171.27.224.10  netmask 255.255.240.0  destination 171.27.224.10
        inet6 fe80::ec28:2d1e:6e47:217b  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500
```

Połączenie widoczne jest także z panelu admina w serwisie openvpn.
Pokazuje on m. in. prawdziwy adres IP oraz ilość przesłanych danych.



2. Dostęp za pomocą RDP

Z powodu utrudnień które wystąpiły podczas prób nawiązania dostępu zastosowana została nietypowa metoda działania.
Ważną rzeczą było dodanie reguły w zakładce *Networking* zarządzania maszyną w serwisie Azure. Bez ww. reguły połączenia nie przyniosły zamierzonego skutku.



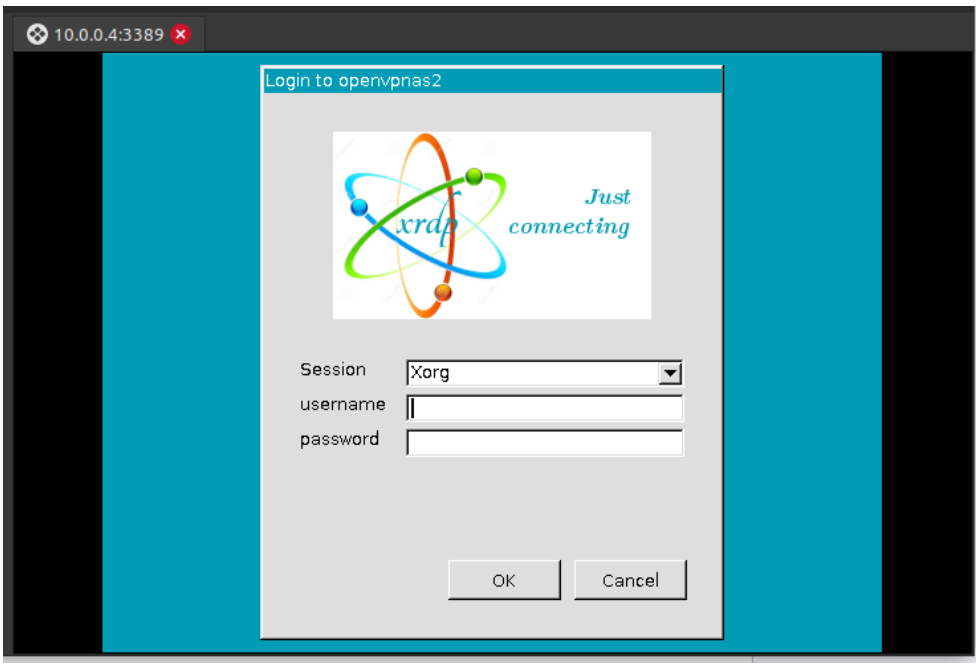
Reguła ta pozwala na przychodzące zapytania na port **3389** - stosowany głównie dla połączeń RDP (ang. *Remote Desktop Protocol*). Źródło oraz protokół zostały ustawione jako dowolne.

Następnie będąc połączonym z maszyną lokalnie za pomocą SSH instalujemy potrzebne pakiety do zdalnego dostępu komendą
$ sudo apt install xrdp
oraz pochodnymi tej komendy.
Sprawdzając status serwera widzimy, że działa on.

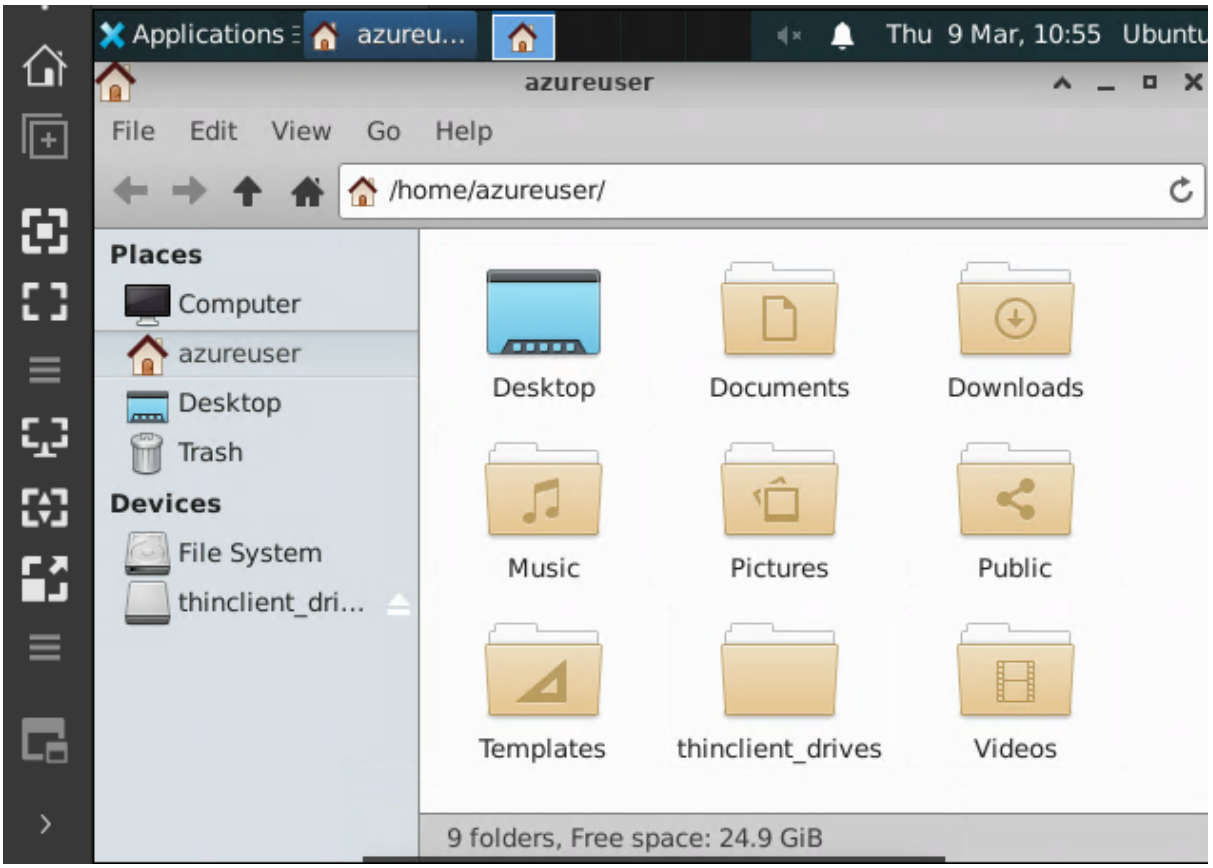
```
azureuser@openvpnas2:~$ sudo systemctl status xrdp
● xrdp.service - xrdp daemon
     Loaded: loaded (/lib/systemd/system/xrdp.service; enabled; vendor preset: >
     Active: active (running) since Wed 2023-03-08 10:04:53 UTC; 12h ago
       Docs: man:xrdp(8)
             man:xrdp.ini(5)
    Process: 10102 ExecStartPre=/bin/sh /usr/share/xrdp/socksetup (code=exited,>
    Process: 10110 ExecStart=/usr/sbin/xrdp $XRDP_OPTIONS (code=exited, status=>
   Main PID: 10111 (xrdp)
      Tasks: 1 (limit: 1077)
     Memory: 2.4M
        CPU: 5.416s
     CGroup: /system.slice/xrdp.service
             └─10111 /usr/sbin/xrdp
```

Skoro po stronie serwera wszystko jest jak powinno czas postawić się w roli klienta.
Po podłączeniu się do sieci VPN nawiązujemy połączenie z adresem **lokalnym maszyny**, w tym wypadku 10.0.0.4 na port **3389**. W systemie typu UNIX użyję do tego aplikacji remmina.

Po wpisaniu danych pojawia się okienko z prośbą o uwierzytelnienie.



Finalnie mamy dostęp do maszyny wraz z GUI, co jest wygodne dla użytkownika końcowego. :>



VPN (virtual private network) jest to technologia, która chroni połączenia internetowe. VPN tworzy zaszyfrowany tunel pomiędzy dwoma punktami. Najważniejszymi cechami sieci VPN są: bezpieczeństwo (VPN wykorzystuje protokoły szyfrowania np. SSL/TLS, IKEv2, aby połączenie było bezpieczne przed zagrożeniami z sieci publicznej), prywatność (ukrywa prawdziwy adres IP, przez co chroni przed śledzeniem), współdzielenie zasobów (każda osoba z dowolnego miejsca na świecie może korzystać z zasobów np. plików czy baz danych). Dzięki VPN możemy także zmienić geolokalizację, dzięki czemu uzyskamy dostęp do treści, które w niektórych częściach świata są zablokowane, albo niedostępne

3. Możliwe zastosowania sieci VPN.

Przykładami zastosowania sieci VPN są:

- Bezpieczne połączenie z siecią firmową: Pracownicy korzystający z sieci VPN mogą zdalnie łączyć się z siecią firmy, aby mieć dostęp do jej zasobów, takich jak bazy danych, pliki, itp. Wszystkie połączenia są szyfrowane i chronione przed zagrożeniami z sieci publicznej.

- Ochrona prywatności: VPN umożliwia użytkownikom ukrycie swojego prawdziwego adresu IP, co zapewnia większą prywatność i ochronę przed śledzeniem przez reklamodawców i innych użytkowników sieci.

- Odblokowywanie treści geograficznie ograniczonych: VPN umożliwia użytkownikom uzyskanie dostępu do treści internetowych, które są ograniczone geograficznie, np. treści dostępnych tylko w USA lub w Europie.

- Bezpieczne korzystanie z sieci publicznych: Użytkownicy korzystający z sieci publicznych, takich jak lotniska, hotele, kawiarnie, itp., mogą skorzystać z VPN, aby zabezpieczyć swoje połączenia przed niepowołanym dostępem i kradzieżą danych.

- Ochrona przed cyberprzestępczością: VPN zapewnia ochronę przed atakami cyberprzestępców, takich jak phishing, ransomware, itp., ponieważ połączenia są szyfrowane i chronione przed zagrożeniami z sieci publicznej.

- Korzystanie z usług, które są blokowane w określonych częściach świata np. Skype w krajach Bliskiego Wschodu czy w Chinach

4. Dane dostępu:

IP Maszyny:

Publiczny: 23.97.196.27
Prywatny: 10.0.0.4

Użytkownik maszyny:
login: azureuser
hasło: Virtual!Mach1n3

Użytkownik 1 VPN:
login: uzytkownik1
hasło: Virtual!Mach1n3

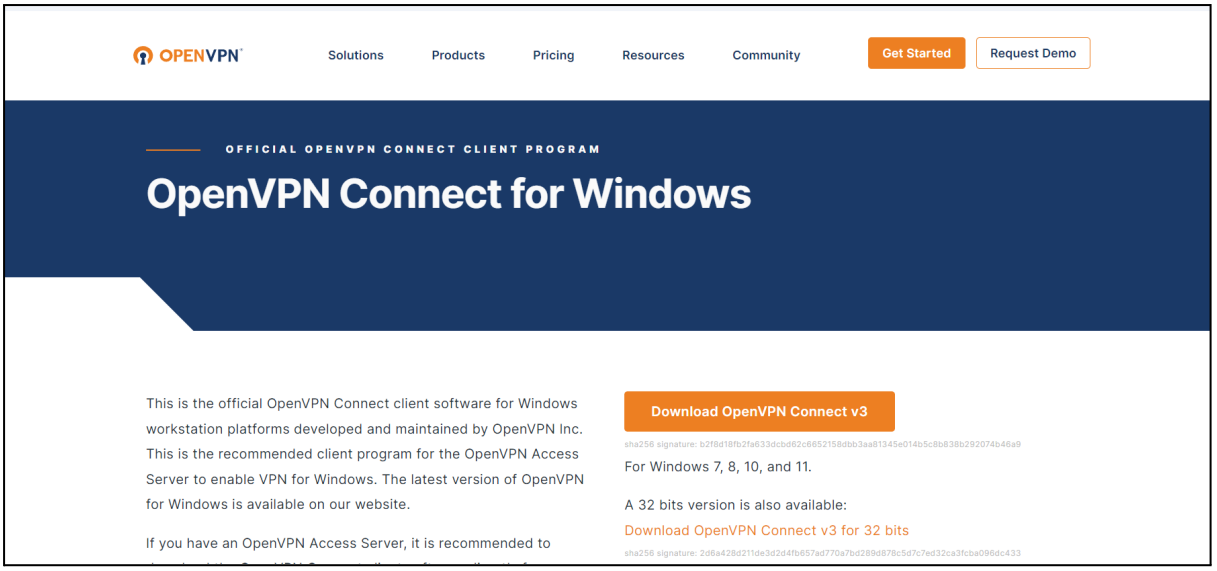
Użytkownik 2 VPN:
login: uzytkownik2
hasło: Virtual!Mach1n3

Port dostępu usługi RDP: 3389

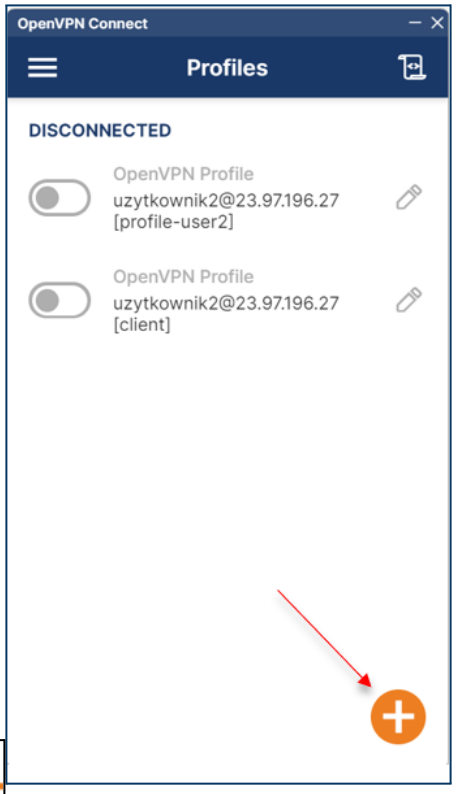
5. Konfiguracja klienta przez VPN i RDP na podstawie użytkownika 2 VPN.

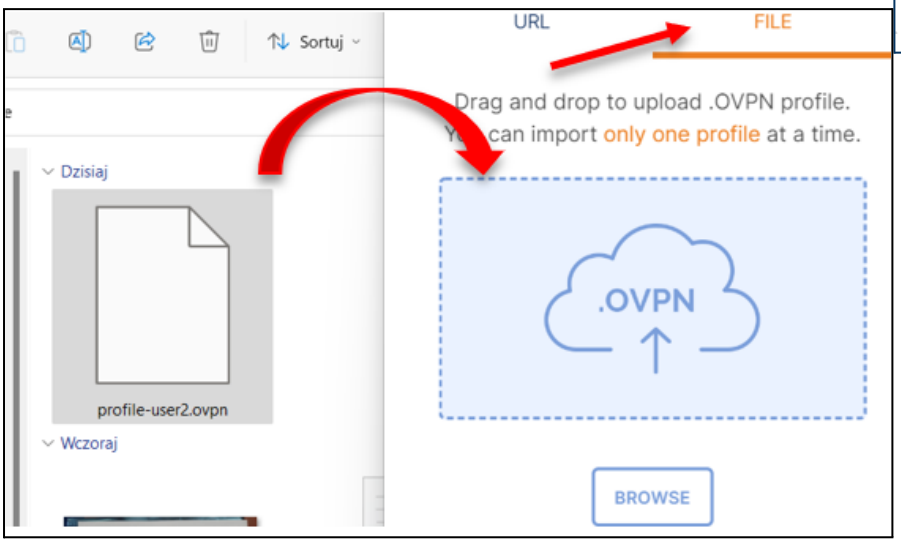
Konfiguracja VPN

1) Pobranie detykowanej aplikacji OpenVPN Connects ze strony: https://openvpn.net/client-connect-vpn-for-windows/



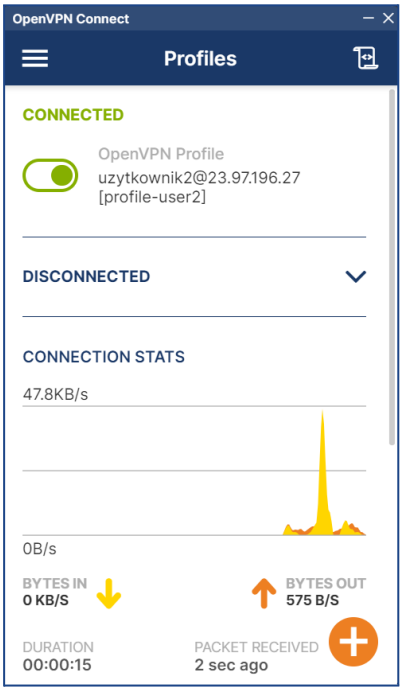
2) Po włączeniu aplikacji dodajemy profil użytkownika poprzez kliknięcie “+”

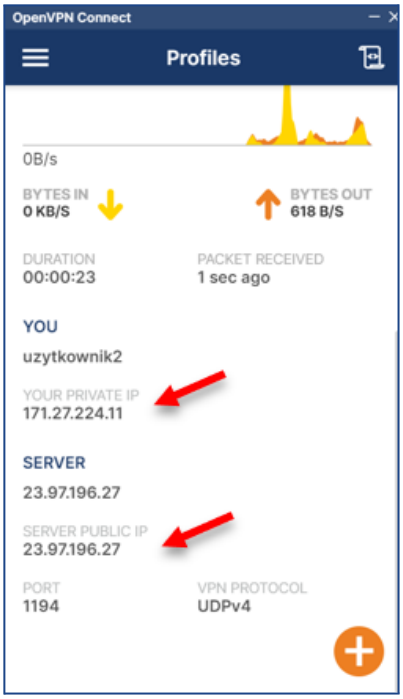




3) Przechodzimy do zakładki file i przeciągamy tam plik z certyfikatem (.ovpn), który dostaliśmy od serwera.

4) Klikamy ‘Connect’, a następnie system nas prosi o hasło, które jest także podane przez serwer. Hasło z punktu 4 dla użytkownika 2: Virtual!Mach1n3
5) Dostajemy taki widok, gdzie widzimy prywatne IP naszego komputera, a także publiczne IP serwera.





Dostęp zdalny RDP

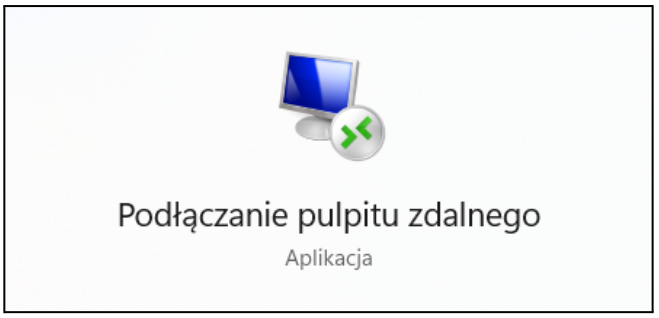
1) Aby połączyć się zdalnie potrzebujemy drugiego użytkownika także zalogowanego do naszego VPNa, musimy znać jego prywatny adres IP (w naszym przypadku 171.27.224.10), port dostępu usługi RDP (3389), a także hasło (Virtual!Mach1n3).
2) Aby sprawdzić czy użytkownik jest dostępny możemy spingować jego adres IP -> dla Windowsa: wchodzimy do cmd, wpisujemy ping <adres prywatny, dla nas 171.27.224.10>, klikamy Enter. Jeżeli w ‘Received’ jest wartość większa niż 0 to znaczy, że jest on dostępny.

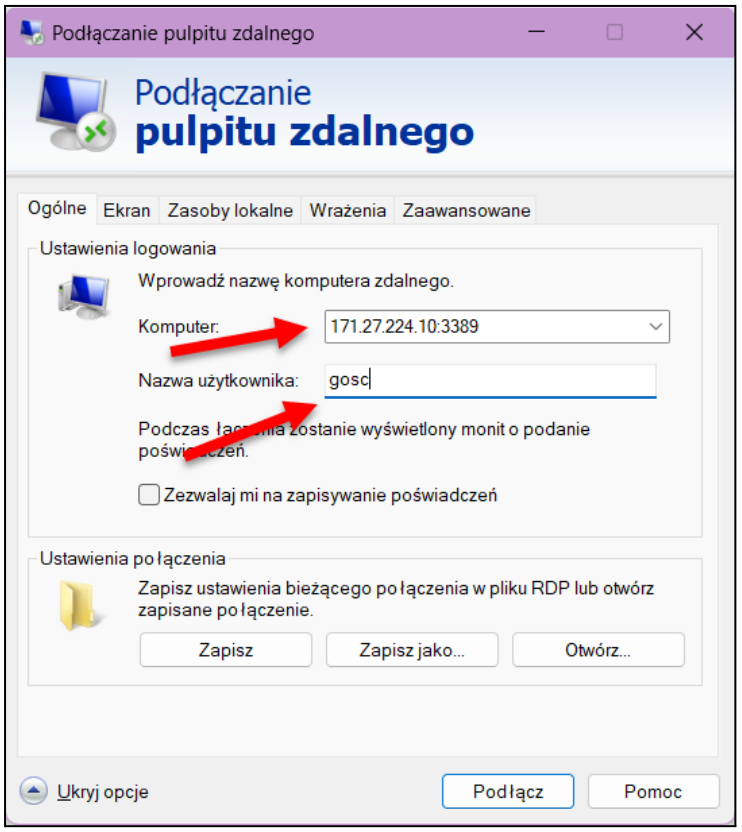
```
C:\Users\PC>ping 171.27.224.10

Pinging 171.27.224.10 with 32 bytes of data:
Request timed out.
Reply from 171.27.224.10: bytes=32 time=81ms TTL=63
Reply from 171.27.224.10: bytes=32 time=81ms TTL=63
Reply from 171.27.224.10: bytes=32 time=81ms TTL=63

Ping statistics for 171.27.224.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 81ms, Maximum = 81ms, Average = 81ms
```

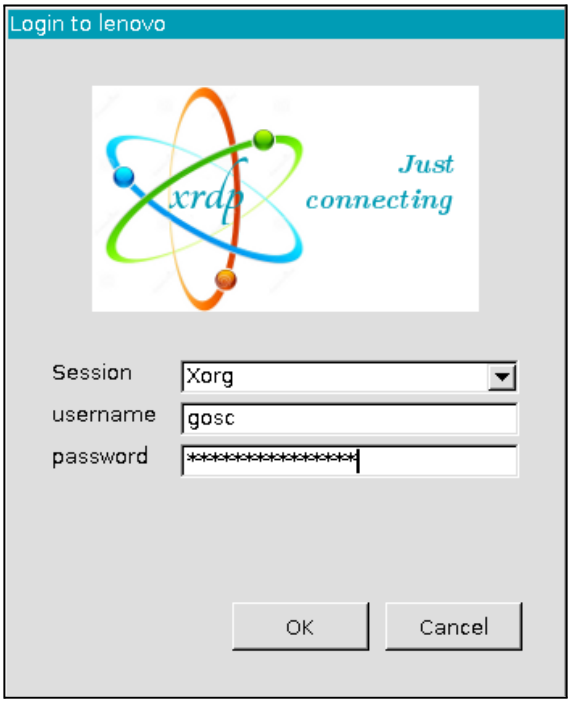
3) Wchodzimy do aplikacji pulpitu zdalnego.





4) W miejsce komputer wpisujemy adres IP komputera do którego chcemy się dostać, a także port w postaci: *IP:port* (171.27.224.10:3389). A w Nazwie użytkownika ‘gosc’.

5) Username wypełni się automatycznie, hasło jest podane przez serwer (Virtual!Mach1n3). Klikamy OK i tym sposobem dostajemy się do maszyny drugiego użytkownika



6. Metody zwiększenia poziomu bezpieczeństwa dla wdrożonego rozwiązania zdalnego dostępu VPN.

1. Stosowanie bezpiecznych haseł - NIST sugeruje:
    - co najmniej 8-znakowe hasła (im dłuższe tym lepsze)
    - omijanie wszelkich wzorców jak np. 12345
    - mieszanie dużych i małych liter, używanie cyfr i znaków specjalnych
    - nie używanie tych samych haseł do wszystkich kont
2. Zastosowanie firewalli, aby ograniczyć dostęp napływającego ruchu sieciowego tylko do niezbędnych portów.
3. Ustawienie odpowiedniego limitu użytkowników - w pewnym stopniu utrudnia dostęp do sieci.
4. Postawienie systemu SIEM, który będzie zbierał i analizował logi dot. połączeń z siecią (droższe rozwiązanie). W ten sposób będzie mogli monitorować wymianę informacji między użytkownikami oraz w łatwiejszy sposób wykryjemy wszelkie próby uszkodzenia czy zaatakowania sieci.
5. Ciągła edukacja użytkowników korzystając ze zdalnego dostępu (dosyć ogólne spostrzeżenie, natomiast wciąż bardzo ważne).
6. Można również tak zmienić ustawienia serwera, aby inni użytkownicy nie wiedzieli siebie nawzajem w danej sieci (ta opcja jest już zależna od tego, co chcemy osiągnąć w danej sieci VPN).
7. Ciągłe aktualizowanie serwera oraz sprawdzenie wszelkich luk bezpieczeństwa (wszelkie zero-day bugi itp.).
8. Możliwe również wprowadzenie RBAC (Role-based access control) - autoryzacja użytkowników bazowała by na ich rolach czy stanowiskach, jakie posiadają. W ten sposób różni użytkownicy będą mogli posiadać dostęp tylko do określonych usług w ramach właśnie ich roli.
9. Zablokowanie tzw. *split-tunneling*, gdzie przy włączonej tej funkcji, cały wymieniany ruch sieciowy nie ogranicza się tylko do połączenia między użytkownikiem, a serwerem. Czysty VPN z kolei potrafi szyfrować cały wymieniany ruch, nie zważając na docelowy adres wysyłanych danych.

7. Techniki zwiększające prywatność, przy administracji systemami informatycznymi

- Monitorowanie dostępów - ważnym krokiem w zwiększeniu prywatności jest monitorowanie dostępów do systemów informatycznych. Dzięki temu administratorzy wiedzą do jakich zasobów dane osoby miały dostęp (pliki, foldery, aplikacje). Przykładami monitorowania dostępu są:
    - Logi systemowe - są to pliki zawierające informacje o zdarzeniach i działaniach systemowych, takich jak logowanie użytkowników, zmiana ustawień systemowych czy dostęp do plików. W tym celu używają oni różnego rodzaju aplikacji typu SIEM, które automatycznie analizują logi i ostrzegają przed podejrzanym ruchem.
    - Audyty dostępu - to mechanizmy, które umożliwiają śledzenie działań użytkowników w systemie informatycznym, takich jak odczyt, zapis czy modyfikacja plików. Audyty dostępu pozwalają na śledzenie aktywności użytkowników i wykrywanie prób naruszenia prywatności czy bezpieczeństwa systemu.
    - Innym rozwiązaniem jest monitorowanie ruchu sieciowego. Wtedy można wyciągnąć takie informacje jak przesyłanie plików czy korzystanie z aplikacji internetowych.

- Bazy danych i aplikacje:
    - Jedną z najważniejszych rzeczy jest zapewnienie *bezpiecznej konfiguracji i administrowania* baz danych i aplikacji. W ramach konfiguracji administratorzy powinni ustawić odpowiednie uprawnienia dostępu do danych (odczyt, zapis czy modyfikacja) oraz chronić dane przed nieautoryzowanym dostępem poprzez stosowanie szyfrowania.
    - Należy też regularnie wykonywać *kopie zapasowe danych*, aby w przypadku awarii lub utraty danych możliwe było ich przywrócenie.
    - W przypadku aplikacji webowych, które często są narażone na ataki (SQL Injection, XSS), należy stosować dodatkowe zabezpieczenia, takie jak *filtracja danych wejściowych i ich walidacja*.

- Urządzenia sieciowe - są to: routery, przełączniki, punkty dostępu itp.
    - W ich przypadku ważne jest przede wszystkim zapewnienie bezpiecznej konfiguracji, co oznacza m.in. zmianę domyślnych

haseł i nazw użytkownika, a także zablokowanie niepotrzebnych portów i protokołów.
    - Kolejnym ważnym krokiem jest aktualizacja oprogramowania urządzeń sieciowych. Regularne aktualizacje zapewniają, że urządzenia są zabezpieczone przed znanymi lukami w zabezpieczeniach i innymi zagrożeniami.
    - Dla większej ochrony prywatności użytkowników warto stosować szyfrowanie danych przesyłanych przez urządzenia sieciowe. Przykładami takich protokołów są SSL czy TLS.
    - Ważne jest również monitorowanie aktywności urządzeń sieciowych. Logi systemowe urządzeń sieciowych mogą zawierać cenne informacje o wykorzystaniu podatności przez atakujących. Dobrą praktyką jest także stosowanie firewalli.

- Zdalny dostęp i dostęp nadzorowany. Aby zwiększyć jego bezpieczeństwo należy zwrócić uwagę czy zawiera takie rzeczy jak:
    - Autentykacja dwuskładnikowa - umożliwia to dodatkową ochronę przed nieuprawnionym dostępem.
    - Kontrola sesji - umożliwia to kontrolowanie sesji, w której użytkownik uzyskał dostęp do danych, co pozwala na wykrycie próby nieuprawnionego dostępu.
    - Audytowanie - umożliwia to monitorowanie działań użytkowników w systemie, co pozwala na wykrycie próby nieuprawnionego dostępu lub innych działań naruszających prywatność.

- Jako administrator dobrze zwrócić także uwagę na takie aspekty jak:
    - Anonimizacja danych - pozwala na ochronę danych osobowych poprzez zamianę danych identyfikujących na dane anonimowe, które nie identyfikowały by żadnej osoby.
    - Należy też usuwać stare czy niepotrzebne dane, ponieważ wtedy uniemożliwiają nieuprawniony dostęp do nich.