


Techniki zwiększające prywatność

Julia Sadecka, Jakub Augustyn, Benjamin Jankowski

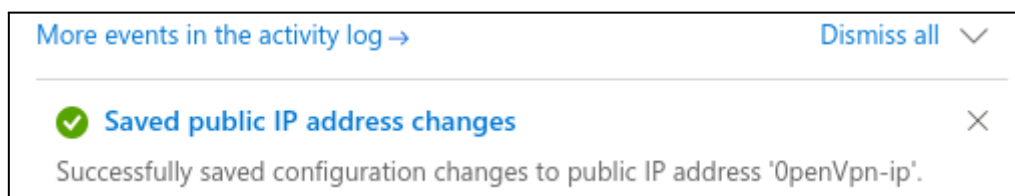
1. Domena dla wdrożonego wcześniej rozwiązania OPENVPN.

Domenę tworzymy na stronie Azure. Wchodzimy w panel konfiguracyjny maszyny (klikając w IP danej maszyny). W *DNS name label* wpisujemy domenę (należy pamiętać aby nie posiadała wielkich liter i znaków specjalnych).

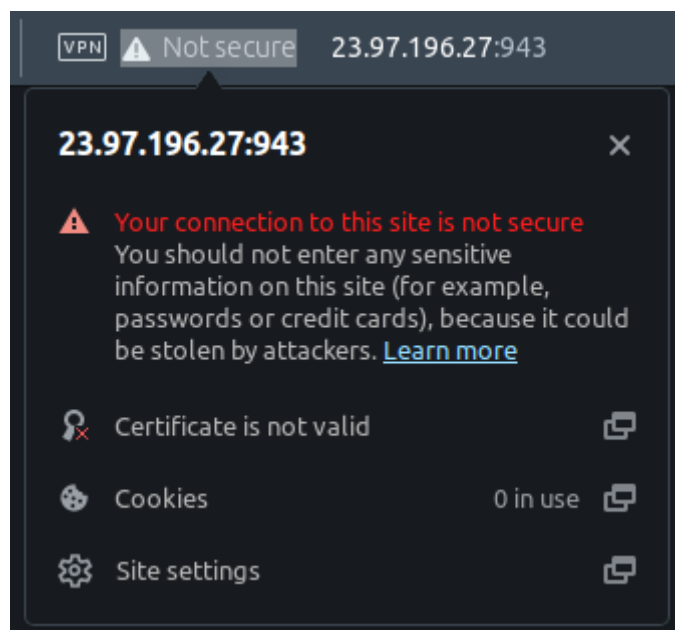
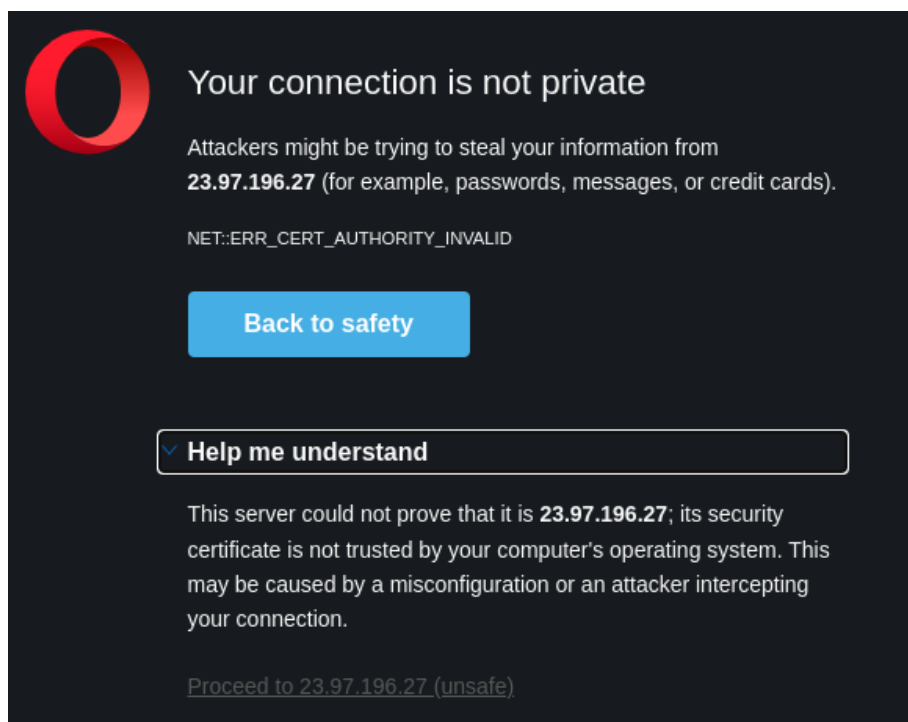


The screenshot shows the 'IP address assignment' configuration page in the Azure portal. It is set to 'Static' assignment. The 'IP address' is 23.97.196.27. The 'Idle timeout (minutes)' is set to 30 via a slider. The 'DNS name label (optional)' field contains 'odoitwpazure'. The domain '.westeurope.cloudapp.azure.com' is displayed at the bottom right.

Dostajemy potwierdzenie stworzenia domeny.
(odoitwpazure.westeurope.cloudapp.azure.com)



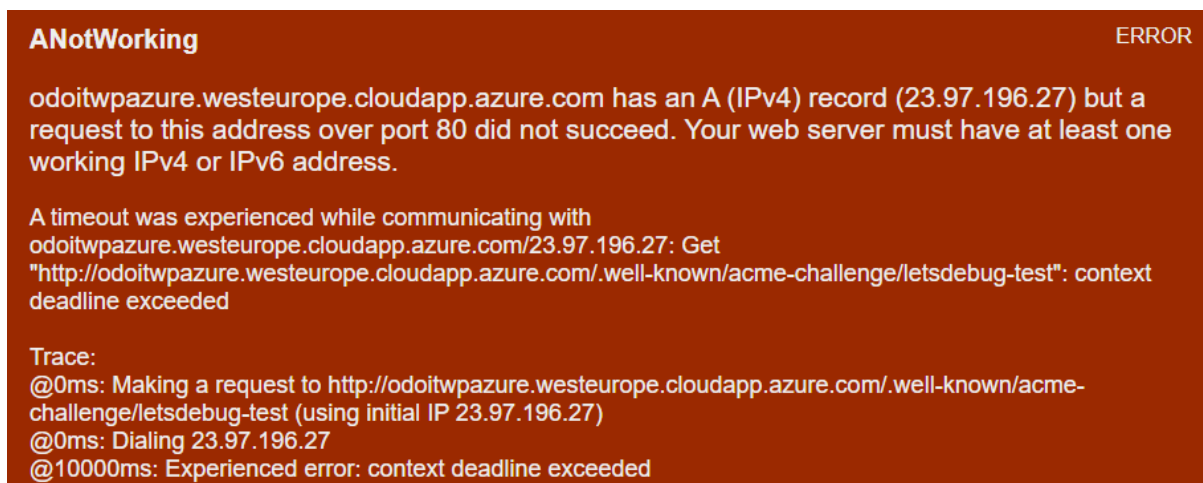
Po wejściu na serwer DNS dostajemy informację, że strona jest niebezpieczna. Należy więc wygenerować certyfikat dla danego adresu.



2. Instalacja certyfikatu SSL dla własnego serwera.

Do tego celu użyjemy *certbota* (<https://certbot.eff.org/>). Jest to opensourcowy software tool, który tworzy certyfikaty dzięki stronie *Let's Encrypt* (<https://letsencrypt.org/>) na manualnie zarządzanych stronach internetowych, aby włączyć HTTPS. Jest on dosyć wygodnym narzędziem, które ułatwia sam proces, ale sam nie jest niezbędny do zainstalowania certyfikatu SSL. Poniżej podaliśmy kroki, które trzeba podjąć, aby zainstalować certyfikat na stronie <http://odoitwpazuree.westeurope.cloudapp.azure.com/>.

1. Wpierw, należy połączyć się z maszyną za pomocą SSH (można również przez protokół RDP - natomiast przy użyciu pierwszej opcji, cała procedura będzie nieco szybsza).
2. Następnie otwieramy port 80. Bez tego kroku Let's encrypt (certbot) nie będzie w stanie zainstalować certyfikatu.



Wobec powyższego dodaję regułę w panelu Azure zezwalającą na połączenie na port 80 z dowolnego źródła.

AllowAnyCustom80Inbound ×
OpenVpn-nsg

Source ⓘ

Source port ranges * ⓘ

Destination ⓘ

Service ⓘ

Destination port ranges * ⓘ

Protocol
☒ Any
☐ TCP
☐ UDP
☐ ICMP

Action
☒ Allow
☐ Deny

Priority * ⓘ
 ✓

3. Należy teraz zainstalować poniższe rzeczy:

- `sudo snap install core`
- `sudo snap install refresh core`
- `sudo snap install --classic certbot`

```
azureuser@openvpnas2:~$ sudo snap install core
core 16-2.58.3 from Canonical✓ installed
azureuser@openvpnas2:~$ sudo snap refresh core
snap "core" has no updates available
azureuser@openvpnas2:~$ sudo snap install --classic certbot
certbot 2.4.0 from Certbot Project (certbot-eff✓) installed
```

4. Następnie wpisujemy poniższą komendę, aby uzyskać potrzebne pliki certyfikacyjne:

```
azureuser@openvpnas2:~$ sudo certbot certonly --standalone
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): odoitwpazuree.westeurope.cloudapp.azure.com
Requesting a certificate for odoitwpazuree.westeurope.cloudapp.azure.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/odoitwpazuree.westeurope.cloudapp.azure.com/fullchain.pem
Key is saved at: /etc/letsencrypt/live/odoitwpazuree.westeurope.cloudapp.azure.com/privkey.pem
This certificate expires on 2023-06-21.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

- - - - -
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
- - - - -
azureuser@openvpnas2:~$
```

5. Należy teraz przekazać pliki fullchain.pem, cert.pem oraz privkey.pem na odpowiednio *CA Bundle*, *Certificate* oraz *Private Key*:

```
root@openvpnas2:/etc/letsencrypt/live/odoitwpazuree.westeurope.cloudapp.azure.com# ll
total 28
drwxr-xr-x 2 root root 4096 Mar 23 19:08 ./
drwx----- 3 root root 4096 Mar 23 19:08 ../
-rw-r--r-- 1 root root 692 Mar 23 19:08 README
lrwxrwxrwx 1 root root 67 Mar 23 19:08 cert.pem -> ../../archive/odoitwpazuree.westeurope.cloudapp.azure.com/cert1.pem
lrwxrwxrwx 1 root root 68 Mar 23 19:08 chain.pem -> ../../archive/odoitwpazuree.westeurope.cloudapp.azure.com/chain1.pem
lrwxrwxrwx 1 root root 72 Mar 23 19:08 fullchain.pem -> ../../archive/odoitwpazuree.westeurope.cloudapp.azure.com/fullchain1.pem
lrwxrwxrwx 1 root root 70 Mar 23 19:08 privkey.pem -> ../../archive/odoitwpazuree.westeurope.cloudapp.azure.com/privkey1.pem
```

Please Provide:

CA Bundle

Provide a concatenated list of CA certificates that validates your web server certificate.

Select CA Bundle file

fullchain.pem

Certificate

Provide web certificate file here.

Select Certificate file

cert.pem

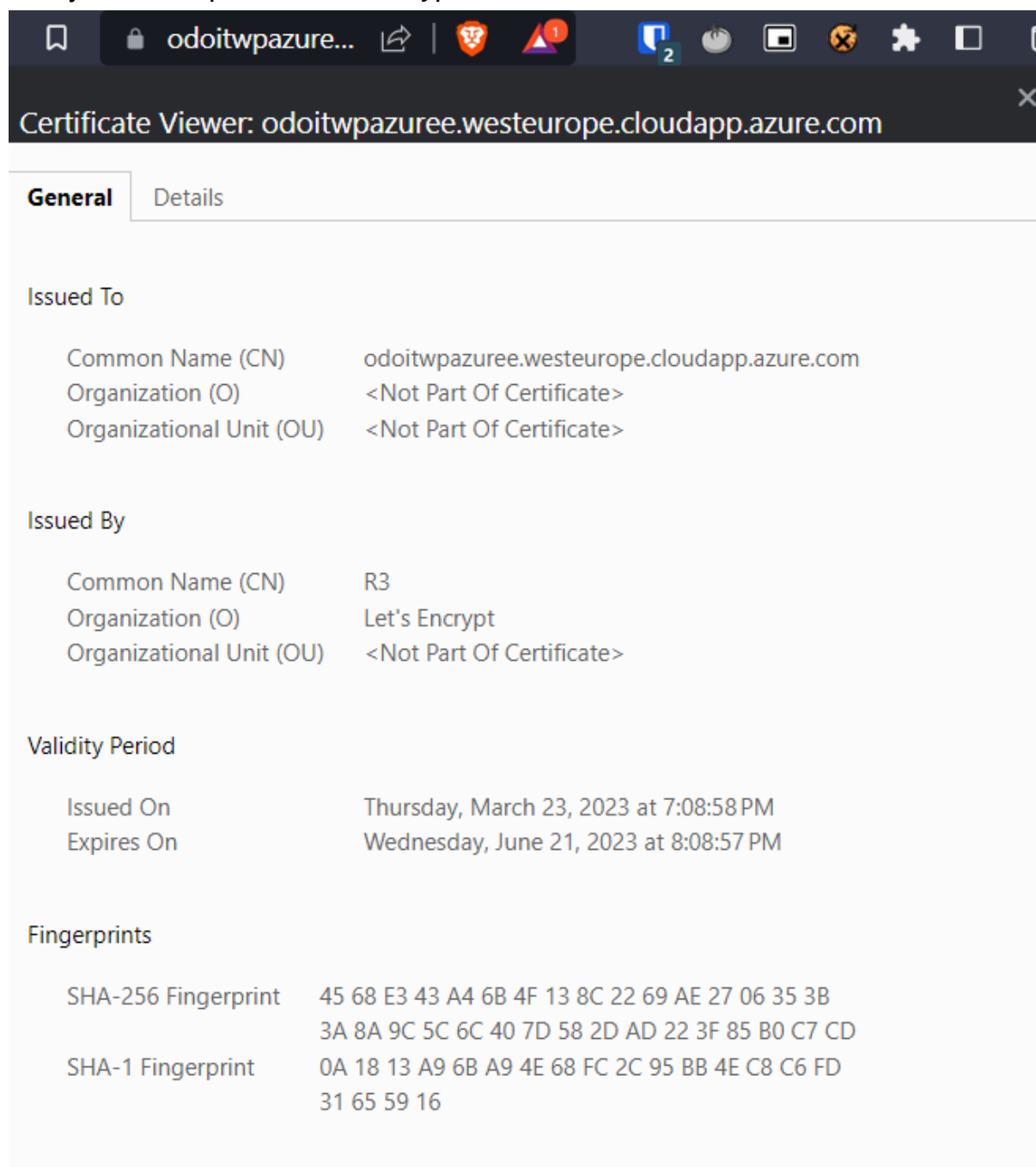
Private Key

Provide web certificate private key here.

Select Private Key file

privkey.pem

Po powyższych krokach, przeglądarka nie oznacza strony jako niebezpieczna, a także pokazywana jest informacja, że strona została zweryfikowana przez *Let's Encrypt*.



3. Adres logowania www. do swojego serwera VPN.

Poniżej znajduje się link do strony, dzięki której możemy pobrać plik konfiguracyjny dostępu do VPN:

<https://odoitwpazuree.westeurope.cloudapp.azure.com/>

Dalej logujemy się loginem i hasłem takim, jak podaliśmy już w poprzednim sprawozdaniu:

IP Maszyny:

Publiczny: 23.97.196.27

Prywatny: 10.0.0.4

Użytkownik 1 VPN:

login: uzytkownik1

hasło: Virtual!Mach1n3

Użytkownik 2 VPN:

login: uzytkownik2

hasło: Virtual!Mach1n3

4. Dostępne rodzaje certyfikatów SSL i zasady działania rozwiązań SSL.

Certyfikaty SSL (Secure Sockets Layer) są używane do zabezpieczenia połączeń internetowych. Stosowane są przez banki czy sklepy internetowe do ochrony danych logowania. Ich podstawową funkcją jest zabezpieczenie danych przesyłanych między serwerem a klientem poprzez szyfrowanie informacji. Protokół SSL zapewnia poufność przesyłanych informacji przez ich szyfrowanie, pozwala zweryfikować tożsamość stron komunikacji oraz gwarantuje integralność otrzymanych danych. Certyfikaty te są wydawane przez organizacje certyfikujące w celu potwierdzenia autentyczności serwerów internetowych.

Obecnie wyróżniamy trzy typy certyfikatów SSL do ochrony serwerów internetowych:

-1- Certyfikat weryfikacji domeny (DV) - potwierdza jedynie autentyczność domeny, na której działa serwer. Dla jego wydania nie jest wymagana szczegółowa weryfikacja właściciela domeny czy firmy, co sprawia, że jest najprostszym i najtańszym w użyciu rodzajem certyfikatu SSL. Ten typ nie mówi nic o właścicielu, który się nim posługuje, lecz gwarantuje bezpieczeństwo, poufność i integralność transmisji danych.

-2- Certyfikat weryfikacji organizacji (OV) - oprócz potwierdzenia autentyczności domeny, certyfikat OV wymaga także weryfikacji firmy

lub organizacji, która jest jej właścicielem. Wymagana jest tu szczegółowa weryfikacja informacji o firmie oraz jej właścicielach, co powoduje, że certyfikat OV jest bardziej zaufany niż DV.

-3- Certyfikat rozszerzonej weryfikacji (EV) - najbardziej zaawansowany rodzaj certyfikatu SSL. Oprócz weryfikacji domeny i organizacji, certyfikat EV wymaga dokładnej weryfikacji tożsamości firmy, w tym jej prawnej struktury oraz autentyczności informacji o niej. Certyfikat EV wyróżnia się w przeglądarkach internetowych zielonym paskiem adresu oraz wyświetleniem nazwy firmy przy zamkniętej kłódce.

Zasada działania protokołu SSL polega na:

- ustanowieniu *bezpiecznego kanału* komunikacji między serwerem a klientem, co zapewnia prywatność i integralność przesyłanych informacji
- po nawiązaniu połączenia między serwerem a klientem, protokół SSL wymienia *klucze publiczne*, które służą do szyfrowania i deszyfrowania przesyłanych informacji.
- na podstawie tych kluczy, wyznaczany *jest symetryczny klucz szyfrujący*, który jest używany do szyfrowania danych przesyłanych między stronami. W trakcie tego procesu, protokół SSL wykorzystuje certyfikaty SSL, aby potwierdzić autentyczność serwera oraz zaszyfrować klucze publiczne.