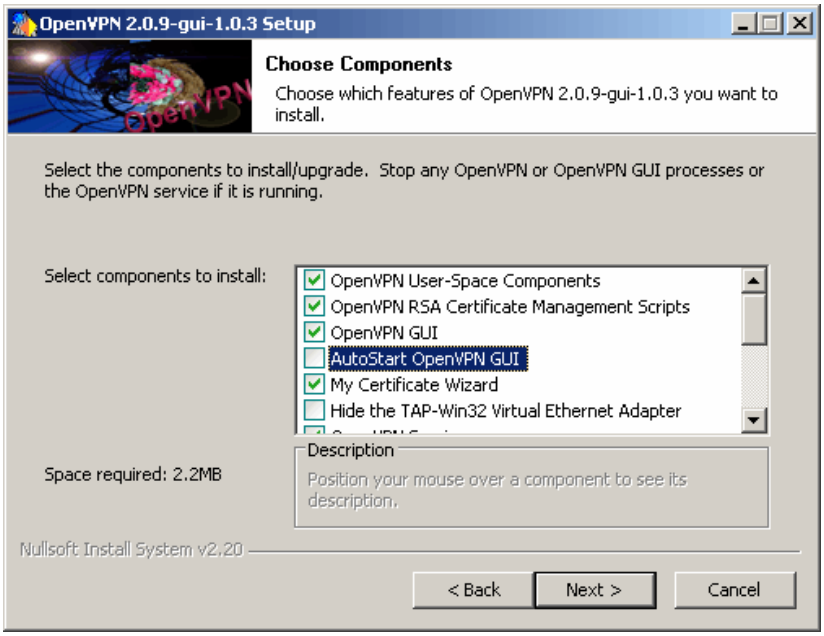
Parę słów o VPN i OpenVPN

VPN (Virtual Private Network) Wirtualna Sieć Prywatna to tunel łączący komputery lub sieci komputerowe biegnący przez inną sieć najczęściej Internet. Tunel jak sama nazwa wskazuje jest wirtualny, tzn fizycznie wykorzystuje inne fizyczne sieci i połączenia sieciowe. Połączenie takie może być szyfrowane, kompresowane i jest niedostępne dla komputerów lub sieci z poza końców tego tunelu. Sieci VPN stosuje się dla poprawienia bezpieczeństwa, łatwego dostępu do sieci firmowych lub pojedynczych komputerów. Najczęstszym zastosowaniem jest połączenie komputerów w różnych częściach internetu tak, aby mogły pracować ze sobą jak by były podłączone do jednej sieci LAN.

Jednym z rozwiązań do tworzenia sieci VPN jest OpenVPN. Oprogramowanie to jest wydawane na licencji GPL, jest darmowe i ma otwarty kod. Do budowania szyfrowanych tuneli w odróżnieniu od wielu innych rozwiązań nie jest wykorzystywany protokół IPSec, ale szyfrowanie oparte na bibliotekach OpenSSL. Wykorzystywany OpenSSL jest rozwijany na bieżąco co gwarantuje duże bezpieczeństwo i szybką reakcję na wykryte błędy. Wadą pakietu OpenVPN jest nigdzie nieopisany protokół komunikacji, który mimo wykorzystania OpenSSL'a może być powodem problemów z bezpieczeństwem.

Niewątpliwą zaletą programu jest dostępność binarnych pakietów na wiele platform i dla wielu systemów operacyjnych. OpenVPN można bez problemu uruchomić pod Windowsami, Linuksem czy Makiem. Istnieją też pakiety dla pracujących pod Linuksem routerów np. dla Linksysa.

Instalacja



Rozwiązanie oparte na OpenVPN wybrałem głównie, dlatego że do dyspozycji miałem Windows Server 2003 i klientów z Windows XP. Instalacja i konfiguracja nie są specjalnie skomplikowane, a dodatkowo oprogramowanie można zainstalować w trybie usługi, co ułatwia automatyczne zestawianie tunelu na komputerach użytkowników.

Na stronie domowej openvpn.net dostępne są binarna dla Windowsów, jest to wersja bez interfejsu graficznego. Przydatny jest pakiet zawierający nakładkę graficzną GUI (Graphical User Interface), można go pobrać ze strony openvpn.se. Osobiście proponuję wybrać pakiet z GUI. Podczas instalacji pamiętajmy o zainstalowaniu programu „My Certificate Wizard" ułatwi on generowanie certyfikatów. Można za to wyłączyć automatyczne startowanie OpenVPN GUI podczas uruchamiania Windowsów.

Certyfikaty

Będziemy potrzebowali przynajmniej trzy certyfikaty:

1. certyfikat urzędu certyfikacji CA (certificate authority), w opisanym rozwiązaniu sami będziemy podpisywać swoje certyfikaty;
2. certyfikat serwera VPN, czyli potrzebny będzie wniosek o wydanie certyfikatu i certyfikat wydany przez CA;
3. certyfikat klienta sieci VPN, czyli potrzebny będzie wniosek o wydanie certyfikatu i certyfikat wydany przez CA (w przypadku wielu klientów dla każdego potrzebny będzie osobny certyfikat)

Na początku należy skonfigurować OpenSSL'a którego zainstalowaliśmy razem z OpenVPN'em.

- W katalogu easy-rsa zmień nazwę pliku openssl.cnf.sample na openssl.cnf, zmień nazwę pliku vars.bat.sample na vars.bat i utwórz katalog keys.
- w pliku vars.bat zmień wpisy dotyczące ustawień certyfikatu (przyspieszy to wystawianie certyfikatów) np. :

```
set KEY_COUNTRY=PL
set KEY_PROVINCE=Mazowieckie
set KEY_CITY=Warszawa
set KEY_ORG=SerwerVPN
set KEY_EMAIL= vpn@ host.domain
```

- w katalogu keys utwórz pliki index.txt i serial, do pliku serial wpisz 00 (dwa zera)
- uruchom cmd.exe (interpreter poleceń) wejdź do katalogu easy-rsa i uruchom plik vars.bat, znajdują się w nim wartości zmiennych używanych w pozostałych plikach wsadowych znajdujących się w katalogu tym katalogu
-

Generacja kluczy:

- Na początek potrzebujemy klucza Diffiego-Hellmana który będzie używany przez protokół uzgadniania kluczy. Generujemy go uruchamiając plik build-dh.bat.
- Teraz wygenerujemy certyfikat urzędu certyfikacji uruchamiając plik build-ca.bat. W pliku bulid-ca.bat ustawiony jest okres ważności certyfikatu na 10 lat można to zmienić modyfikując parametr: -days 3650. W trakcie generowania certyfikatu należy odpowiedzieć na parę pytań:
-

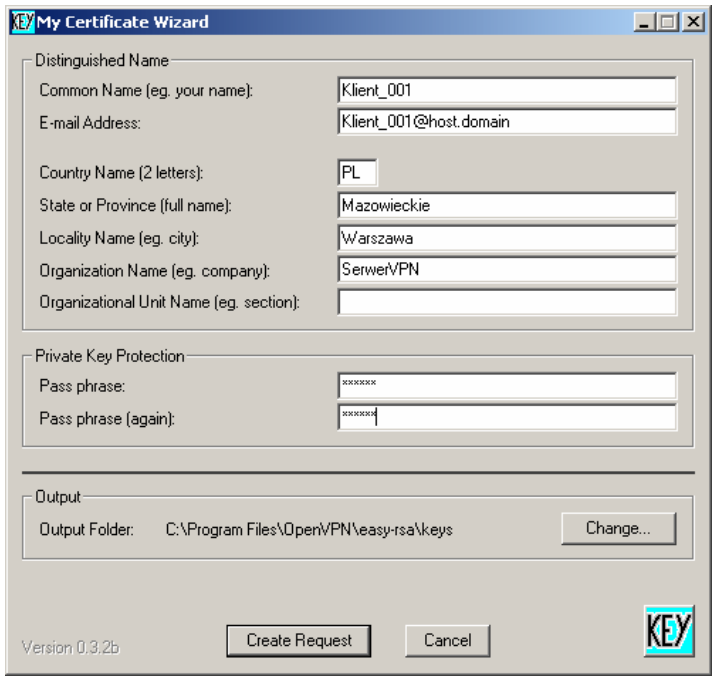
```
Country Name (2 letter code) [PL]:PL
State or Province Name (full name) [Mazowieckie]: Województwo
Locality Name (eg, city) [Warszawa]: Miasto
Organization Name (eg, company) [SerwerVPN]:Nazwa instytucji
Organizational Unit Name (eg, section) []:.
Common Name (eg, YOUR name) []:Imię i nazwisko lub nazwa firmy
Email Address [vpn@ host.domain]: adres mailowy
```

W wyniku generacji otrzymamy w katalogu keys plik ca.crt - certyfikat CA i ca.key - klucz prywatny CA

- Następnie generujemy certyfikat dla serwera VPN uruchamiając plik build-key-server.bat. z parametrem określającym jak mają się nazywać pliki z certyfikatem i kluczem np.:
  build-key-server.bat Brama . W trakcie generowania certyfikatu będziemy proszeni o odpowiedzi na podobne pytania jak przy generowaniu certyfikatu CA.
  Po wygenerowaniu certyfikatu następuje jego podpisanie przez CA (jesteśmy pytani czy

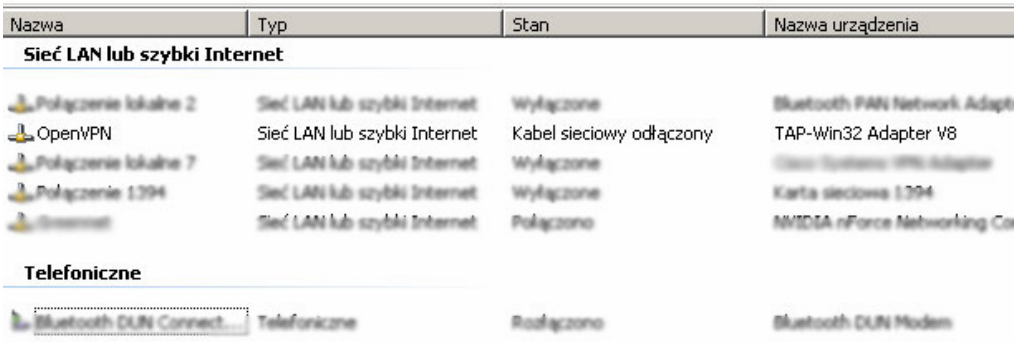
podpisać certyfikat) Do dyspozycji otrzymujemy pliki Brama.crt - certyfikat naszego serwera i Brama.key - klucz prywatny naszego serwera.

- Do generowania certyfikatu klienta sieci VPN wykorzystamy program „My Certificate Wizard". W polach: Country Name, State or Province Name, Locality Name, Organization Name wpisujemy identyczne dane, jakie podaliśmy podczas generowania certyfikatu CA. Ważne jest wpisanie odpowiedniego pola Common Name, dzięki niemu będziemy mogli rozpoznać na serwerze podłączających się klientów i np. ustawić dla nich indywidualną konfigurację. (w tym wypadku wpisałem Klient_001) Otrzymujemy plik Klient_001.key - klucz prywatny klienta i Klient_001.req - wniosek o wydanie certyfikatu. Teraz należy na podstawie wygenerowanego wniosku wystawić certyfikat dla klienta. Ja do tego używam skryptu podpisz.bat (listing na końcu dokumentu) w którym można określić czas na który podpiszemy certyfikat. Plik Klient_001.req znajduje się w katalogu keys, uruchamiamy cmd.exe wchodzimy do katalogu easy-rsa, uruchamiamy vars.bat następnie podpisz.bat z parametrem określającym klienta podpisz.bat Klient_001 Otrzymujemy plik Klient_001.crt który jest certyfikatem dla klienta VPN.



Konfiguracja

OpenVPN umożliwia konfigurację w trybie router i bridge. Konfiguracja w trybie router to połączenie IP jeden do jednego. Jeden nr IP otrzymuje serwer drugi klient, umożliwienie widzenia się wielu klientów między sobą realizowane jest odpowiednią konfiguracją routingu. Konfiguracja w trybie bridge umożliwia podłączenie wielu klientów do jednego IP serwera. Brigde przekazuje wszystkie pakiety pomiędzy klientami i umożliwia komunikację innymi protokołami niż TCP np. IPX czy NetBIOS. Wadą takiego rozwiązania jest znaczne zwiększenie ruchu, co może powodować przytkanie słabszych łącz.



Podczas instalacji powstaje w Windowsach nowe „połączenie lokalne”. Dla ułatwienia rozpoznania można zmienić mu nazwę na np. OpenVPN. W katalogu bin znajdują się pliki bat do usuwania (deltapall.bat) i tworzenia (addtap.bat) wirtualnych interfejsów.

Tryb router
W trybie routera używamy wirtualny interfejs tun. Konfiguracja serwera znajdować się będzie w pliku server.ovpn w katalogu config. W tym samym katalogu potrzebujemy certyfikat CA (ca.crt), certyfikat serwera (Brama.crt) i klucz prywatny serwera (Brama.key).

```
dev tun #urządzenie tun czyli tryb pracy router
dev-node OpenVPN # nazwa wirtualnego interfejsu sieciowego
port 4215 # port na którym nasłuchuje serwer
mode server
server 10.2.1.0 255.255.255.0
dh dh1024.pem
ca ca.crt # certyfikat CA
cert Brama.crt # certyfikat bramy
key Brama.key #klucz prywatny bramy
proto tcp-server
verb 1 # poziom logowania
keepalive 10 900
inactive 3600
comp-lzo
status "C:\\Program Files\\OpenVPN\\log\\status.log"
client-config-dir "C:\\Program Files\\OpenVPN\\vpn_clients"
ccd-exclusive
```

Taka konfiguracja nada interfejsowi OpenVPN nr IP 10.2.1.1 jeżeli fizyczny interfejs komputera będzie z tej samej sieci i będzie podłączony do sieci LAN to klienci podłączeni do VPN’a będą mieli dostęp do komputerów w LAN’ie.

W katalogu vpn_clients (trzeba go utworzyć) będą pliki o nazwach zgodnych z polem Common Name certyfikatu klienta. W plikach będzie znajdować się konfiguracja dla poszczególnych klientów. Konfigurację taką można też umieścić w pliku konfiguracyjnym klienta, ale trzymanie wszystkiego na serwerze ułatwia zarządzanie klientami VPN. W tym przypadku utworzymy plik Klient_001

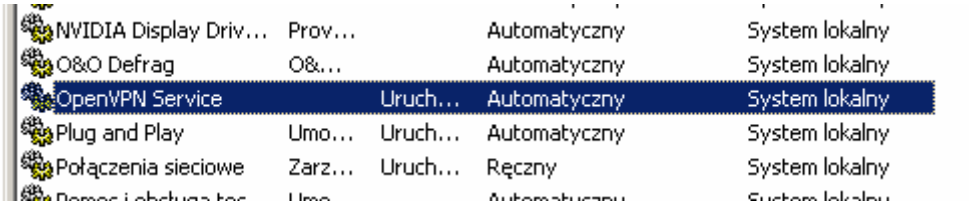
```
ifconfig-push 10.2.1.253 10.2.1.254
push "route 10.2.1.0 255.255.255.0"
```

W pierwszej linijce pierwszy nr IP to nr klienta drugi to nr IP serwera. Druga linijka umożliwia routing do całej sieci VPN, zmieniając wielkość podanej sieci można ustawić routing tylko do części komputerów. Oczywiście żeby mieć pewność, że klient nie ma dostępu do danych komputerów trzeba o to zadbać ustawiając odpowiednio zaporę sieciową na serwerze VPN.

Tryb router w tej konfiguracji umożliwia podłączenie maksymalnie 127 klientów, dla każdego wykorzystane są 2 adresy IP jeden dla serwera drugi dla klienta (1-2, 3-4, 5-6 … 249-250, 251-252, 253-254). Żeby zwiększyć ilość klientów należ zmienić maskę sieci.

Uruchomienie serwera można wykonać na dwa sposoby. Używając programu „OpenVPN GUI”, który widać po uruchomieniu na trayu.

Drugim sposobem jest uruchomienie usługi „OpenVPN Service” np. poleceniem `net start "OpenVPN Service"`. Ustawienie sposobu uruchamiania usługi na automatyczny spowoduje startowanie VPN’a przy uruchamianiu systemu.



Konfiguracja klienta

Na komputerze klienta instalujemy OpenVPN i w katalogu config umieszczamy certyfikat CA (ca.crt), certyfikat klienta (Klient_001.crt) i klucz prywatny klienta (Klient_001.key)

```
client
dev tun #urządzenie tun czyli tryb pracy router
port 4215 # port na którym nasłuchuje serwer
remote 70.71.72.73 # nr IP serwera VPN
resolv-retry infinite
proto tcp-client
ip-win32 dynamic
ca ca.crt
cert Klient_001.crt
key Klient_001.key
ping 10
ping-restart 60
comp-lzo
verb 1
```

Uruchomienie połączenia klienta VPN przy pomocy OpenVPN GUI wymaga uprawnień administratora. Instalując usługę "OpenVPN Service" można ominąć wymagania administratora jednak wtedy nie jesteśmy pytani o hasło do certyfikatu i połączenia się nie zestawia. Wyjściem z sytuacji jest zapisanie do certyfikatu klienta hasła na stałe lub nadanie użytkownikowi praw administratora. Wpisanie hasła można wykonać takim poleceniem:
`openssl rsa -in Klient_001.key -out Klient_001.key_bez`
Otrzymamy plik Klient_001.key_bez przy którym nie występuje pytanie o hasło. Plikiem zastępujemy dotychczasowy plik `Klient_001.key`. Problem z prawami dotyczy stabilnej wersji 2.0.9 OpenVPN, w wersji 2.1 problem ten nie występuje jednak na dzień dzisiejszy jest to wersja testowa nie polecana do zastosowań produkcyjnych.

Tryb bridge
Poniższa konfiguracja pokazuje ustawienie dla serwera, którego jeden interfejs fizyczny podłączony jest do internetu a drugi do sieci LAN. W oknie połączenia sieciowe należy zaznaczyć wirtualny interfejs OpenVPN i fizyczny interfejs podłączony do LAN’u a następnie wybrać opcję „Połączenie mostkowe”. Utworzonemu interfejsowi mostkowemu trzeba nadać taki sam nr IP jaki ma fizyczny interfejs podłączony do LAN’u. W tym wypadku zgodnie z plikiem konfiguracyjnym 10.2.1.25/255.255.255.0.

```
dev tap
dev-node OpenVPN
port 4215
```

```
server-bridge 10.2.1.25 255.255.255.0 10.2.1.60 10.2.1.80
push "dhcp-option DNS 10.2.1.1"
push "dhcp-option WINS 10.2.1.1"
push "route-gateway 10.2.1.50"
dh dh1024.pem
ca ca.crt
cert Brama.crt
key Brama.key
proto tcp-server
verb 1
keepalive 10 900
inactive 3600
comp-lzo
ifconfig-pool-persist "C:\\Program Files\\OpenVPN\\config\\ipp.txt"
status "C:\\Program Files\\OpenVPN\\log\\status.log"
client-config-dir "C:\\Program Files\\OpenVPN\\bridge_clients"
ccd-exclusive
```

Linijka server-bridge określa nr IP serwera (taki sam nr IP jak fizycznego interfejsu podłączonego do lanu) , maskę sieci i zakres nr IP przydzielanych klientom VPN'a. Opcje push wysyłają do klientów informacje na temat konfiguracji ich interfejsów przekazując ustawienia DNS, WINS i bramy.

Konfiguracja klienta

```
client
dev tap
port 4215
remote 70.71.72.73
resolv-retry infinite
proto tcp-client
ip-win32 dynamic
ca ca.crt
cert Klient_001.crt
key Klient_001.key
ping 10
ping-restart 60
comp-lzo
verb 1
```

Uruchomienie w trybie bridge jest identyczne jak w trybie router.

Powyższe konfiguracje nie opisują oczywiści wszystkich możliwości OpenVPN'a. Więcej opcji można znaleźć na stronie domowej programu. Niestety dokumentacja w paru miejscach nie pokrywa się z tym, co możemy uzyskać w rzeczywistości. Zdarzają się opcje nie dostępne w wersji dla Windows lub opcje które po prostu nie działają.

Różnice router - bridge
Główną różnicę pomiędzy trybem router i bridge widać bardzo dobrze w pliku status.log. W przypadku trybu bridge wygląda tak:

```
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
00:ff:a9:6c:22:46,Klient_001,83.99.177.3:1531,Sat Aug 02 19:22:15 2008
```

a w przypadku trybu router wygląda tak:

```
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
10.2.1.60,Klient_001,83.99.177.3:4183,Sat Aug 02 19:10:35 2008
```

Jak widać tablica routingu do klienta w trybie bridge zawiera jego MAC address czyli logicznie podłączony jest on tak jak każdy komputer w „zwykłym „ LAN'ie. W przypadku trybu router jest to tablica routingu podobna do tablicy routingu IP.

Uwagi
Błąd: `failed to update database TXT_DB error number 2`
Może okazać się, że musimy wystawić certyfikat z takim samym polem Common Name jeszcze przed wygaśnięciem poprzedniego. Należy wtedy zmienić wpis i pliku easy-rsa\keys\index.txt.attr z unique_subject = yes na unique_subject = no.

Dla klientów, którzy są za NAT'em nieobsługującym --state ESTABLISHED,RELATED musimy określić lokalny port, na którym będzie zestawiane połączenie VPN. Port musi być taki sam jak ten, na którym następuje wywołanie do serwera w tym przypadku 4215. Robimy to poleceniem `lport 4215` w pliku konfiguracyjnym klienta, nie udało mi się tego skonfigurować z wersjami poniżej 2.1 OpenVPN.

W razie problemów z zestawieniem połączenia warto testowo wyłączyć wszystkie zapory sieciowe.

Opis niektórych parametrów
Opcje `ccd-exclusive` zastosowałem z dwóch powodów w przypadku trybu router umożliwia trzymanie konfiguracji klientów na serwerze, a nie w plikach klientów oraz wyklucza możliwość podłączenia się do sieci VPN klientów którzy nie mają swojego pliku w katalogu wymienionym w opcji `client-config-dir.` W przypadku trybu bridge pliki klientów są puste i opcja ta jest zastosowana tylko po to żeby mieć kontrolę nad listą podłączających się klientów.

`crl-verify crl.pem` - umożliwia zarządzanie listą certyfikatów uprawnionych do podłączenia się do serwera VPN. Plik crl.pem należy skopiować z katalogu keys do katalogu config. Usuwanie certyfikatów z listy uprawnionych wykonuje się skryptem revoke-full.bat.

Opis niektórych plików wsadowych (.bat)

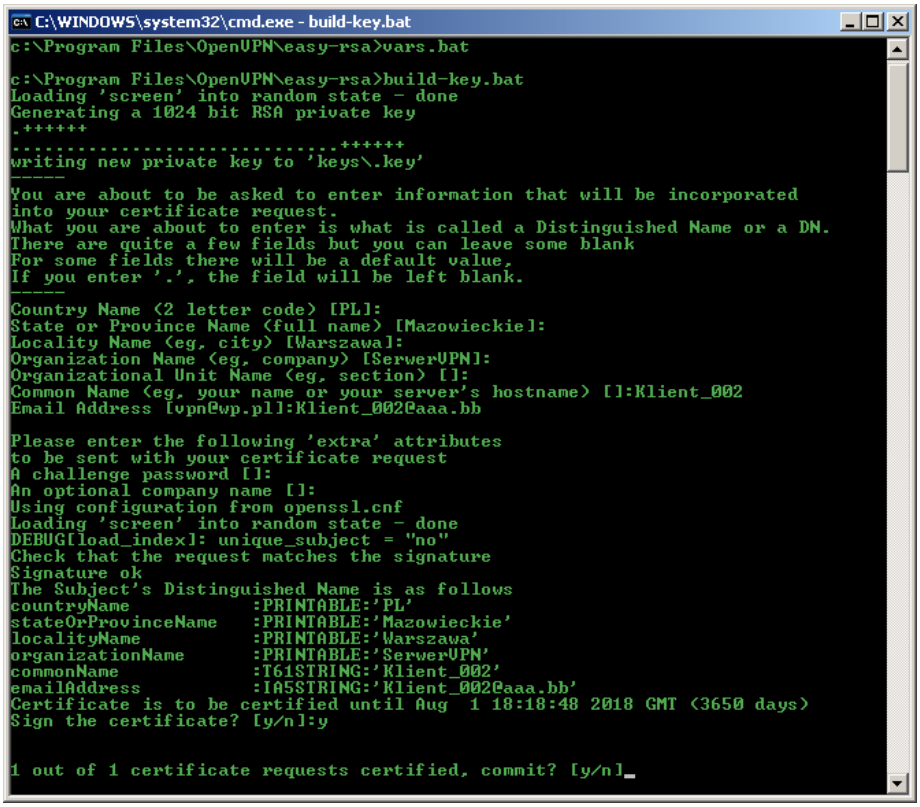
addtap.bat -	dodanie kolejnego wirtualnego interfejsu sieciowego
deltapall.bat -	usunięcie wszystkich wirtualnych interfejsów sieciowych
build-ca.bat -	generowanie certyfikatu urzędu certyfikacji
build-dh.bat -	generowanie pliku z kluczem DH
build-key-server.bat -	generowanie certyfikatu dla serwera VPN
build-key.bat -	generowanie i podpisanie klucza dla klienta VPN, generuje się certyfikat bez hasła / `build-key.bat kazwa_klienta` /
clean-all.bat -	wyczyszczenie katalogu keys, utworzenie nowych plików index.txt i serial
init-config.bat -	inicjowanie konfiguracji, nadpisanie plików vars.bat i openssl.cnf plikami przykładowymi

revoke-full.bat - usunięcie certyfikatu klienta z listy uprawnionych do korzystania z połączenia VPN, w katalogu keys powstaje plik crl.pem który należy skopiować do katalogi config. Żeby serwer sprawdzał listę uprawnionych klientów w konfiguracji trzeba dopisać crl-verify crl.pem / `revoke-full.bat nazwa klienta` /

vars.bat - zmienne używane w pozostałych skryptach

podpisz.bat - plik do wystawiania certyfikatów na podstawie plików .req dostarczonych od klientów VPN / `podpisz.bat nazwa_klienta` /

Przykładowa wykorzystanie skryptu: wystawianie i podpisywanie certyfikatu przy pomocy bulid-key.bat



podpisz.bat

```
@echo off
rem ====================================
rem ILE DNI
set DNI=90
rem ====================================
set PARAM1=a%1a
if %PARAM1%==aa (
echo PODAJ PARAMETR Common Name
pause
exit )
echo CERTYFIKAT DLA %1 ZOSTANIE WYSTAWIONY NA %DNI%
pause
cd %HOME%
rem sign the cert request with our ca, creating a cert/key pair
openssl ca -days %DNI% -out %KEY_DIR%\%1.crt -in %KEY_DIR%\%1.req -config %KEY_CONFIG%
del /q %KEY_DIR%\*.old
pause
```