Tworzenie sieci VPN w oparciu o OpenVPN.

1. Cel laboratorium

Celem jest stworzenie działającego połączenia pomiędzy dwoma komputerami (w tym wypadku maszynami wirtualnymi). Ćwiczenie należy wykonać w parach. Każda z osób konfiguruje własną sieć OpenVPN, po czym łączy się do sieci (jako klient) do osoby z pary.

2. Informacje wstępne

OpenVPN daje sporą swobodę przy tworzeniu połączeń VPN. Na pojedynczym komputerze można odpalić wiele instancji (serwerów) OpenVPN jednocześnie tworząc połączenie klienckie (przykładowo do innej sieci VPN). Ponadto (w bardziej zaawansowanej konfiguracji) możliwe jest połączenie tak zestawionych sieci VPN w jedną, dużą sieć. Wszystko zależy od naszych potrzeb gdyż OpenVPN, w przypadku konfiguracji, świetnie się dopasowuje do potrzeb każdego administratora.

Należy pamiętać, że każde połączenie VPN to jeden plik konfiguracyjny. Nazwy plików mogą być dowolne – demon OpenVPN na Linux (usługa na Windows) bez żadnego problemu poradzi sobie z wczytaniem każdego pliku conf znajdującego się w odpowiednim katalogu.

3. Wykonanie

Pierwszym ważnym krokiem jest pobranie OpenVPN do naszego systemu. Można oczywiście pobrać kod źródłowy, skompilować go i zacząć używać. Jednak, będąc administratorem sieci, cenimy swój czas. Pobierzemy gotową paczkę. Dla Windows znajdziemy je pod tym adresem: https://openvpn.net/index.php/open-source/downloads.html . Dla systemu Linux (z rodziny Debian) paczka znajduje się w repozytorium

apt-get install openvpn easy-rsa

Pakiet easy-rsa pełni tutaj rolę serwera certyfikacji naszego przyszłego VPN (bez niego nie wygenerujemy potrzebnych nam certyfikatów do ustanawiania i podtrzymywania połączeń).

Mając już pakiet przystępujemy do konfiguracji. Ponieważ nie mamy jeszcze swojego własnego pliku konfiguracyjnego pobieramy jeden z nich, dostępny w przykładach

gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf

Powyższy katalog zawiera także dodatkowe, przykładowe pliki konfiguracyjne dla klienta, serwera, konfiguracji zapory ogniowej i inne (można przejrzeć – zawsze to wzbogaca naszą wiedzę).

Kolejnym krokiem, który warto wykonać, jest skopiowanie konfiguracji serwera certyfikacji do katalogu openvpn. Oczywiście można je trzymać w dowolnym miejscu jednak należy mieć na uwadze, że w przyszłości możemy potrzebować dodatkowych centrów certyfikacji, niekoniecznie chcąc je ze sobą łączyć. Kopiujemy odpowiednie pliki (cały katalog)

cp -r /usr/share/easy-rsa/ /etc/openvpn

oraz tworzymy nowy katalog (we właśnie skopiowanym) celem przechowywania tworzonych kluczy. Katalog ten najlepiej będzie zabezpieczyć przed wszystkimi (tworzy go root, demona odpala root więc dostęp do katalogu powinien posiadać jedynie użytkownik root)

mkdir /etc/openvpn/easy-rsa/keys

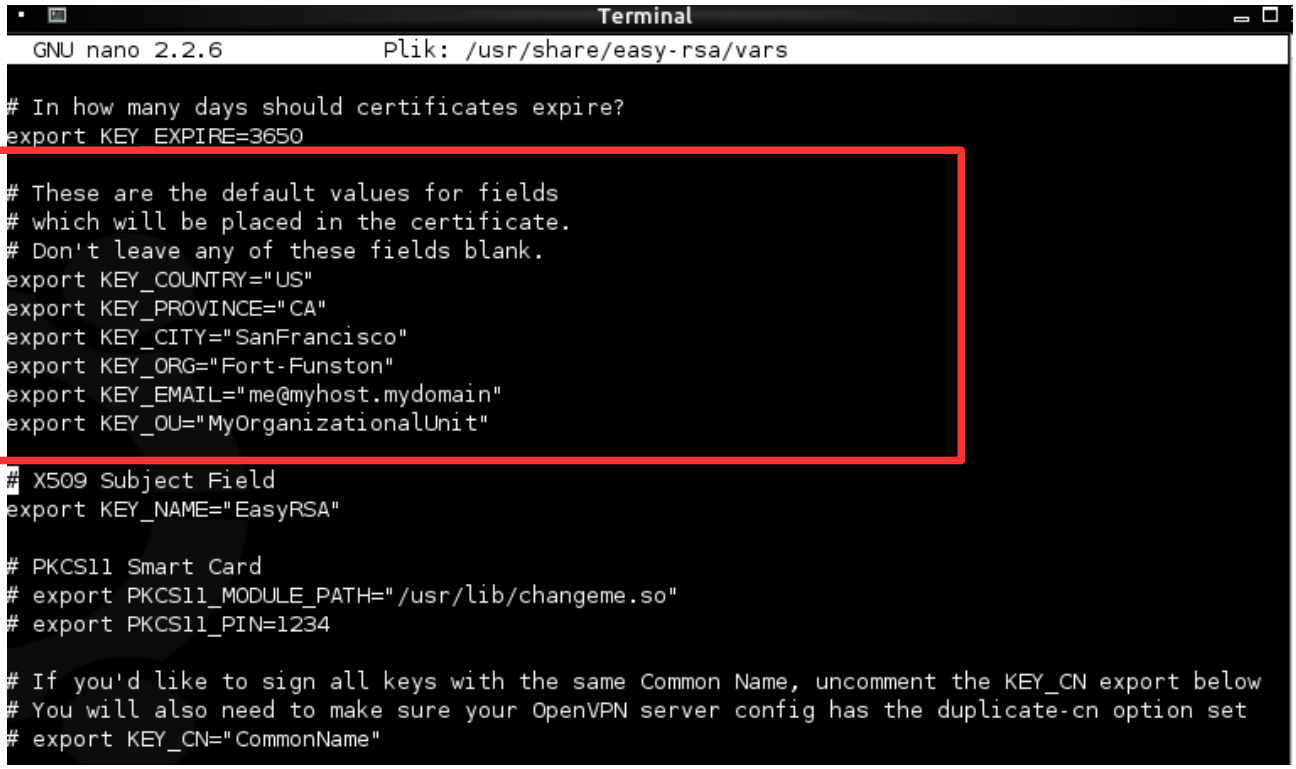
chmod 700 /etc/openvpn/easy-rsa/keys

Następnie należy przekopiować odpowiedni plik certyfikatu dla zainstalowanej wersji OpenSSL. W wypadku nowszych wersji systemu Linux będzie to zawsze wersja powyżej 1 toteż wykonujemy polecenie:

cp /etc/openvpn/easy-rsa/openssl-1.0.0.cnf /etc/openvpn/easy-rsa/openssl.cnf

Teraz czas na edycję zmiennych naszego centrum autoryzacji. Edytujemy plik vars (w poniższym wypadku użyto edytora nano, można użyć dowolnego innego)

nano /etc/openvpn/easy-rsa/vars



Edytujemy (opcjonalnie) zmienne zaznaczone w ramce, np. jako kraj podajemy wartość PL, podajemy miasto, organizację itp. Jednak jedną zmienną musimy edytować OBOWIĄZKOWO – to wartość KEY_EMAIL. Jeżeli pozostawimy ją nienaruszoną, klucze nie będą się generować. Jeżeli z jakichś przyczyn klucze nie będą się generować będzie to znaczyło o złym ustawieniu wskazanych zmiennych (proces trzeba będzie powtórzyć po zmianie wartości!)
INFORMACJA: Niektórzy zalecają także zmianę wartości KEY_NAME. Nie jest to jednak obligatoryjne. Natomiast warto w powyższym pliku upewnić się, że wartość KEY_SIZE to 2048 (jeżeli nie to należy ją zmienić).

Następne polecenia OBOWIĄZKOWO należy wykonywać jako root (zalogowanie się na jego konto lub użycie sudo -i !!)

Przechodzimy do katalogu easy-rsa

cd /etc/openvpn/easy-rsa

Teraz wydajemy serię poleceń

```
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
```

Pierwsza linia pobiera wszystkie zmienne z pliku vars celem wykorzystania przy generowaniu certyfikatu.
Skrypt clean-all wyrzuca wszystko z katalogu WSZYSTKIE certyfikaty i pliki, jakie znajdowały się w naszym katalogu kluczy (utworzony keys, więc nic w nim nie powinno być).
build-dh tworzy parametry Diffie-Hellman, które posłużą do wygenerowania klucza szyfrującego SSL/TLS.
pkitool tworzy nam klucz autoryzujący nasze centrum certyfikacji (z ustawianych wcześniej zmiennych).
Druga linia z tym skryptem tworzy certyfikat naszego serwera.
Przechodzimy do katalogu keys (w którym będziemy przechowywać nasze klucze)
Ostatnie polecenie generuje nam nasz klucz szyfrujący transmisję. Nie jest on obowiązkowy jednak w aktualnej sytuacji pełnej inwigilacji dobrze jest skonfigurować połączenie dodatkowym kluczem.

Ponieważ nasz późniejszy skrypt nie będzie zaglądał do katalogu keys toteż kopiujemy wygenerowane pliki do głównego katalogu openvpn (gdzie mamy już plik konfiguracyjny serwera)

```
cp server.crt server.key ca.crt dh2048.pem ta.key /etc/openvpn/
```

Od tego momentu nasz serwer może już działać i przyjmować połączenia od klientów! (warunek – musi posiadać odpowiednią konfigurację serwera – na razie jest domyślna).

Generowanie kluczy dla poszczególnych klientów wygląda następująco:

```
source vars
./pkitool [nazwa_komputera]
```

gdzie nazwa komputera musi zostać uzupełniona (nie może być w kwadratowych nawiasach!). Nazwą może też być imię_nazwisko użytkownika, jego pseudonim czy cokolwiek innego, jednoznacznie wskazującego na klienta (nazwy nie mogą się powtórzyć)

Po wygenerowaniu musimy skopiować odpowiednie pliki na komputer naszego klienta – bez nich nie nastąpi połączenie. Plikami tymi są:

```
/etc/openvpn/easy-rsa/keys/ca.crt
/etc/openvpn/easy-rsa/keys/[nazwa_komputera].crt
/etc/openvpn/easy-rsa/keys/[nazwa_komputera].key
/etc/openvpn/easy-rsa/keys/ta.key
```

Najlepiej skopiować je do swojego katalogu domowego (celem późniejszego doręczenia odpowiedniemu klientowi).

Pozostałą konfigurację sieci należy wykonać samodzielnie, w oparciu o dostępne materiały Internetowe. Przy czym ważne jest by klienckie maszyny mogły osiągnąć sieć za NAT. W związku

z powyższym niezbędnie stanie się skonfigurowanie przekazywanie adresów IP oraz odpowiednia reguła w zaporze sieciowej. Dobrze byłoby też gdyby klienci VPN mogli widzieć siebie nawzajem.

Po przetestowaniu konfiguracji, jako dodatkowe zadanie, można wykonać przemieszczenie aktualnej konfiguracji na system z rodziny Windows (powinno się to obyć bez specjalnych zmian, za pomocą kopiuj/wklej).

Sprawozdanie, wraz z plikami konfiguracyjnymi (i certyfikatami) należy dostarczyć w pliku zip/7z/gz/tar (bądź dowolnym innym) na adres poczty elektronicznej.

Materiały:
http://ubuntuguide.org/wiki/OpenVPN_server
https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-debian-8
http://sekurak.pl/praktyczna-implementacja-sieci-vpn-na-przykladzie-openvpn/