Warstwa II - przełączanie / VPN tunele

VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna), można opisać jako "tunel", przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Taki kanał może opcjonalnie kompresować lub szyfrować w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa przesyłanych danych.

Określenie "wirtualna" oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Rozwiązania oparte na VPN powinny być stosowane np. w firmach, w których dosyć często pracuje się zdalnie ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie).

Protokoły VPN (1,2,3):

1. IPsec to zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy kodowych pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej (VPN).

VPN oparta na IPsec składa się z dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanał wymiany kluczy za pośrednictwem, którego przekazywane są dane związane z uwierzytelnianiem oraz kodowaniem (klucze) oraz kanału (jednego lub więcej), który niesie pakiety transmitowane poprzeć sieć prywatną. Kanał wymiany kluczy jest standardowym połączeniem UDP (port 500).

Protokoły wchodzące w skład architektury IPSec służą do bezpiecznego przesyłania przez sieć pakietów IP. Działają one na zasadzie enkapsulacji, tj. oryginalny (zabezpieczany) pakiet IP jest szyfrowany, otrzymuje nowy nagłówek protokołu IPSec i w takiej formie jest przesyłany przez sieć.

Bezpieczeństwo zapewniane przez IPSec może być dwojakie, w zależności od stosowanego protokołu. I tak: pojawia się problem dystrybucji kluczy symetrycznych. Narzuca się zastosowanie kryptografii asymetrycznej - ale jest ona o wiele wolniejsza od szybkich szyfrów symetrycznych i dodanie ich do protokołów niskiego poziomu jakimi są ESP i AH (Authentication Header) miałoby tragiczny wpływ na wydajność.

Te dwa protokoły pozostały więc relatywnie prostymi protokołami niskiego poziomu, a do skomplikowanych zadań dystrybucji klucza i uwierzytelniania stron stworzono oddzielny protokół IKE.

Kolejną istotną cechą kanałów IPSec jest ich jednokierunkowość - dany kanał obsługuje tylko ruch idący z hosta A do B. Jak więc realizowana jest dwukierunkowa komunikacja? Oczywiście każda pełna łączność wykorzystuje dwa kanały - jeden od A do B, drugi od B do A. Każdy z nich ma inne SPI, osobny licznik sekwencyjny, inne klucze kryptograficzne.

Taki jednokierunkowy kanał IPSec (ESP lub AH) jest określany nazwą Security Association (która nie ma dobrego polskiego tłumaczenia, stąd pozostaniemy przy określeniu "kanał"). Każde SA charakteryzuje się przez adresy IP początku i końca oraz SPI.

***

2. PPTP (ang. Point to Point Tunneling Protocol) to protokół komunikacyjny umożliwiający tworzenie wirtualnych sieci (VPN) wykorzystujących technologię tunelowania. Polega to na zdalnym dołączaniu się do stacji roboczych lub sieci (głównie opartych na systemie operacyjnym Windows) za pośrednictwem Internetu i tworzeniu pozorów połączenia z lokalną siecią, bez wychodzenia z domu zapewniając jednocześnie zachowanie bezpieczeństwa przy zdalnym przesyłaniu danych.

Najbardziej rozpowszechniona implementacja PPTP została opracowana przez firmę Microsoft. Protokół PPTP stanowi standardowe wyposażenie systemu operacyjnego Windows od wersji 98 i NT.

***

3. OpenVPN jest pakietem VPN stworzonym przez Jamesa Yonana. Umożliwia on tworzenie zaszyfrowanych połączeń między hostami. Pozwala to użytkownikom na autoryzację wejścia używając do tego celu specjalnych prywatnych kluczy, certyfikatów czy nazw użytkowników i haseł. Szeroko zastosowane są tu biblioteki szyfrujące OpenSSL oraz protokół SSLv3/TLSv1. Pakiet ten dostępny jest na platformach Linux, xBSD, Mac OS X oraz Windows 2000/XP. Oferuję on duże bezpieczeństwo i możliwości kontroli. Nie jest on kompatybilny z IPsec czy żadnym innym pakietem VPN. Cały pakiet

składa się z jednego kodu binarnego dla klienta i serwera, opcjonalnego pliku konfigurującego oraz z jednego lub więcej plików kluczy w zależności od metody autoryzacji.

Kodowanie
OpenVPN używa bibliotek OpenSSL do kodowania danych i kanałów kontrolnych. Pozwala, aby OpenSSL dokonał całego kodowania umożliwiając pakietowi OpenVPN użycia szyfru wygenerowanego w OpenSSL. Może również korzystać z pakietu HMAC by stworzyć dodatkową warstwę zabezpieczenia połączenia. Pakiet jest w stanie również wykorzystać możliwość hardwarowe by polepszyć stopień i jakość kodowania.

Autoryzacja
OpenVPN oferuje kilka metod autoryzacji użytkowników. Oferuje klucze, certyfikaty oraz kontrole dostępu przy użyciu nazw użytkowników i haseł. Klucze są najłatwiejszym sposobem autoryzacji, certyfikaty charakteryzują się dużą solidnością i wiarygodnością. Opcja z nazwą użytkownika i hasłem jest nowa (wersja 2.0). Może być stosowana, w przypadku klienta, bez certyfikatu. (serwer musi posiadać certyfikat).

***

VLAN (Sieć wirtualna ang. Virtual Local Area Network) jest siecią komputerową wydzieloną logicznie w ramach innej, większej sieci fizycznej.

Do tworzenia VLAN-ów wykorzystuje się konfigurowalne lub zarządzalne switche, umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych, poprzez separację ruchu pomiędzy określonymi grupami portów. Komunikacja między VLAN-ami jest możliwa tylko wtedy, gdy w VLAN-ach tych partycypuje port należący do routera.

W przełącznikach konfigurowalnych zwykle spotyka się tylko najprostszą formę VLAN-ów, wykorzystującą separację grup portów.

W przełącznikach zarządzalnych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (tagowanie) poprzez doklejenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (trunking). W przypadku urządzeń zgodnych z ISL ramki są kapsulowane w całości.

Protokoły: IEEE 802.1Q, ISL (Inter-Switch Link, rozwiązanie Cisco).

***

Tunel - zestawienie połączenia między dwoma odległymi hostami tak, by stworzyć wrażenie że są połączone bezpośrednio.

W miarę rozwoju sieci komputerowych najpierw lokalnych, a następnie rozległych, powstało zapotrzebowanie na łączenie ze sobą różnych sieci lokalnych za pośrednictwem publicznych sieci rozległych. Sieci lokalne korzystają jednak z innych protokołów sieciowych niż sieci rozległe. Na przykład popularne sieci lokalne firmy Novell pracują w protokole IPX, sieci rozległe wykorzystują natomiast protokoły Frame-Relay, ATM, X.25, a na nich często IP (np. Internet). Łączenie sieci wykorzystujących inny protokół niż sieć rozległą, za pomocą której łączymy sieci rozległe w sieć wirtualną, nie jest jedynym przesłaniem wykorzystywania tunelowania. Drugim i często istotniejszym jest bezpieczeństwo. Szczególnie ostatnio tunelowanie bywa często łączone z wykorzystaniem metod kryptograficznych. Często zwykli użytkownicy Internetu stosują tę technikę do własnych potrzeb. Przykładem jest korzystanie z dostępnego w Internecie oprogramowania szyfrującego o nazwie SSH. Oprogramowanie to, oprócz bezpiecznej pracy zdalnej, umożliwia tworzenie dodatkowego kanału szyfrowanego, przez który użytkownik może "tunelować" dowolną inną - potencjalnie narażoną na niebezpieczeństwo podsłuchu - usługę TCP/IP (np. FTP, telnet, IRC). Warunkiem jest jedynie zainstalowane SSH na obu końcach połączenia.

Generalnie można stwierdzić, iż tunelowanie umożliwia przesyłanie pewnych usług sieciowych za pośrednictwem innych, często odmiennych usług sieci, pracujących w różnych standardach.

Tunelowanie, czyli inaczej przekierowywanie portów polega na przesyłaniu niezabezpieczonych pakietów protokołów TCP (POP3, SMTP czy HTTP) przez bezpieczny protokół SSH.

Istnieją dwa rodzaje przekierowania portów: lokalne (wychodzące) oraz zdalne (przychodzące).
Lokalne – przekierowuje ruch przychodzący na port lokalny na odpowiedni port zdalny. Na przykład ruch przychodzący na port 1234 klienta może zostać przekierowany na port 23 na serwerze.
Zdalne – przekierowuje ruch przychodzący na port na serwerze na odpowiedni port lokalny. Na przykład ruch przychodzący na port 1234 na serwerze może zostać przekierowany na port 23 na komputerze lokalnym.

***

Switch (z ang., w jęz. polskim przełącznik, przełącznica, także komutator) to urządzenie łączące segmenty sieci komputerowej. Switch pracuje w warstwie drugiej modelu OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami.

Switche określa się też mianem wieloportowych mostów (ang. bridge) lub inteligentnych hubów - switch używa logiki podobnej jak w przypadku mostu do przekazywania ramek tylko do docelowego segmentu sieci (a nie do wszystkich segmentów jak hub), ale umożliwia połączenie wielu segmentów sieci w gwiazdę jak hub (nie jest ograniczony do łączenia dwóch segmentów jak most).

W celu ustalenia fizycznego adresata używają docelowego adresu MAC zawartego w nagłówku ramki Ethernet. Jeśli switch nie wie, do którego portu powinien wysłać konkretną ramkę, zalewa (flooding) wszystkie porty za wyjątkiem portu, z którego ramkę otrzymał. Switche utrzymują tablicę mapowań adres MAC<->port fizyczny, której pojemność jest zwykle określona na 4096, 8192 lub 16384 wpisów. Po przepełnieniu tej tablicy nowe wpisy nie są dodawane (chyba że któryś stary wygaśnie), a ramki 'zalewane' są do wszystkich portów (za wyjątkiem portu, którym ramka dotarła do switcha).

Switche ograniczają domenę kolizyjną do pojedynczego portu, dzięki czemu są w stanie zapewnić każdemu hostowi podłączonemu do portu osobny kanał transmisyjno-nadawczy, a nie współdzielony, tak jak huby.

Na switchach zarządzalnych można również wydzielać VLAN-y, czyli wirtualne podsieci LAN. Porty należące do różnych VLANów nie 'widzą' swoich transmisji - do wymiany informacji pomiędzy różnymi VLANami używa się routerów. Porty do VLANów przypisywane są statycznie lub na podstawie adresu MAC podłączonej stacji (opisuje to protokół GVRP, Generic VLAN Registration Protocol, dostępny na większych switchach). VLANy pomiędzy dwoma podłączonymi do siebie switchami przenosi specjalny rodzaj połączenia - trunk. W standardzie IEEE 802.1Q każda ramka wysyłana przez trunk opatrzona zostaje 4-bajtowym polem, w ramach którego przenoszony jest również identyfikator VLANu (tak, by odbierający ramki przełącznik był w stanie wysłać ramkę do odpowiedniego VLANu). W związku z tym ramki tzw. tagowane, czyli oznaczane, mogą mieć maksymalnie długość do 1523 bajtów.

Obecnie na rynku obecne są również switche routujące (tzw. przełączniki 3 warstwy modelu OSI).

Tryby przekazywania ramek:
Przekazywanie ramek przez switcha może się odbywać w róznych trybach. W przełącznikach zarządzalnych istnieje możliwość wyboru odpowiedniego trybu. Dostępne tryby to:

- Cut-through - wprowadza najmniejsze opóźnienie, brak sprawdzania poprawności ramek.
- Store and forward - wprowadza największe opóźnienie, sprawdza sumy kontrolne (CRC) ramek.
- Fragment free - rozwiązanie pośrednie sprawdzające tylko poprawność nagłówka ramki.
- Przełączanie adaptacyjne - na podstawie ruchu wybierany jest jeden z powyższych trybów.

***

Router (ruter, trasownik) to urządzenie sieciowe, które określa następny punkt sieciowy do którego należy skierować pakiet danych (np. datagram IP). Ten proces nazywa się routingiem (rutingiem) bądź trasowaniem. Routing odbywa się w warstwie trzeciej modelu OSI.

Router używany jest przede wszystkim do łączenia ze sobą sieci WAN, MAN i LAN.
Routing jest najczęściej kojarzony z protokołem IP, choć procesowi trasowania można poddać datagramy dowolnego protokołu routowalnego np. protokołu IPX w sieciach obsługiwanych przez NetWare (sieci Novell).

Pierwotne routery z lat sześćdziesiątych były komputerami ogólnego przeznaczenia. Chociaż w roli routerów można używać zwykłych komputerów, nowoczesne szybkie routery to wysoce wyspecjalizowane urządzenia, w których interfejsy sieciowe są połączone bardzo szybką magistralą wewnętrzną. Zazwyczaj mają wbudowane dodatkowe elementy (takie jak pamięć podręczna czy układy wyręczające procesor w pakowaniu i odpakowywaniu ramek warstwy drugiej) w celu przyspieszenia typowych czynności, takich jak przekazywanie pakietów.

Wprowadzono również inne zmiany w celu zwiększenia pewności działania, takie jak zasilanie z baterii oraz pamięć trwała zamiast magnetycznej. Nowoczesne routery zaczynają więc przypominać centrale telefoniczne, a obie te technologie coraz bardziej się upodabniają i prawdopodobnie wkrótce się połączą.
Aby mógł zajść routing, router musi być podłączony przynajmniej do dwóch podsieci (które można określić w ramach jednej sieci komputerowej).

Szczególnym przypadkiem routera jest **przełącznik warstwy trzeciej**, czyli urządzenie z jednym interfejsem sieciowym, które routuje pomiędzy dwoma lub większą ilością sieci wydzielonych logicznie na tym pojedynczym interfejsie. Dla sieci Ethernet są to VLAN-y (wirtualne sieci lokalne), dla sieci ATM czy Frame Relay kanały PVC/SVC (Permanent Virtual Circuit/Switched Virtual Circuit, stałe bądź komutowane kanały wirtualne).

Router tworzy i utrzymuje tablicę routingu, która przechowuje ścieżki do konkretnych obszarów sieci i metryki związane z tymi ścieżkami.

Aby router mógł trasować pakiety i wybierać optymalne marszruty niezbędna jest mu wiedza na temat otaczających go urządzeń (m.in. innych routerów i przełączników). Wiedza ta może być dostarczona w sposób statyczny przez administratora i nosi wówczas nazwę trasy statycznej lub router może ją pozyskać dynamicznie od innych urządzeń warstwy 3 - trasy takie nazywane są dynamicznymi. Do wyznaczania i obsługi tras dynamicznych router wykorzystuje protokoły routingu.

***

Routowanie polega na wyszukiwaniu w tablicy odpowiedniej informacji dot. miejsca docelowego pakietu, tzn. trasy jaką ma przebyć dany pakiet, aby dotrzeć do celu. Każdy wpis trasy musi zawierać dwie informacje:

- adres docelowy – to jest adres sieci, z jaką router jest bezpośrednio połączony; czasem może się zdarzyć, ze urządzenie zna kilka tras dojścia do danej sieci (w takim przypadku wyboru tej najwłaściwszej dokonuje się za pomocą metryk, ale to już temat dotyczący protokołów routingu);
- wskaźnik do celu – informacja, czy router jest bezpośrednio podłączony do sieci docelowej, lub adres innego routera bezpośrednio połączonego z szukaną siecią (tzw. "next-hop router");

Istnieją dwa sposoby dobierania trasy: klasowy (protokół RIP) oraz bezklasowy (protokoły: RIPv2, RIPng, Classless Routing).

Protokoły routingu dynamicznego: **RIP, IGRP, EIGRP, OSPF, BGP, IS-IS**

***

Certyfikat w kryptografii to dane podpisane cyfrowo przez stronę, której ufamy (Certificate Authority). Dane te zawierają takie informacje jak:

- klucz publiczny właściciela certyfikatu,
- nazwa zwyczajowa (np. imię i nazwisko, pseudonim, nazwa firmy),
- nazwa organizacji,
- jednostka organizacyjna,
- zakres stosowania (podpisywanie, szyfrowanie, autoryzacji dostępu itp.),
- czas w jakim certyfikat jest ważny,
- informacje o wystawcy certyfikatów,
- sposób weryfikacji certyfikatu (np. adres pod którym można znaleźć listy CRL),
- adres, pod którym znajduje się polityka certyfikacji, jaką zastosowano przy wydawaniu tego certyfikatu,
- inne dane - struktura certyfikatu jest płynna i może przechowywać praktycznie dowolne dane, takie jak np. fotografia właściciela, próbka jego głosu, informacje biometryczne.

Typowe zastosowania certyfikatów to potwierdzenie tożsamości serwerów / autoryzacja dostępu w protokole SSL, potwierdzenie autentyczności podpisu elektronicznego, potwierdzenie autentyczności klucza publicznego adresata wiadomości.
Należy pamiętać, że samo istnienie certyfikatu nie informuje nas o poziomie bezpieczeństwa. Każdorazowo, przy korzystaniu z kanału komunikacji zabezpieczonego certyfikatem, należy również zapoznać się z informacjami przechowywanymi wewnątrz certyfikatu.

***

SSH (ang. secure shell) to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP-IP, w architekturze klient-serwer. W ścisłym znaczeniu SSH to tylko następca protokołu telnet, służącego do terminalowego łączenia się ze zdalnym komputerem. SSH różni się od telnetu tym, że transfer wszelkich danych jest zaszyfrowany, oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów. W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań. Wspólną cechą wszystkich tych protokołów jest identyczna z ssh technika szyfrowania danych i rozpoznawania użytkownika. Obecnie protokoły z rodziny SSH praktycznie wyparły wszystkie inne "bezpieczne" protokoły takie jak np: Rlogin i RSH.

Ogólne założenia protokołu SSH powstały w grupie roboczej IETF. Istnieją jego dwie wersje SSH1 i SSH2. W jego wersji 2, możliwe jest użycie dowolnych sposobów szyfrowania danych i 4 różnych sposobów rozpoznawania użytkownika, podczas gdy SSH1 obsługiwał tylko stałą listę kilku sposobów szyfrowania i 2 sposoby rozpoznawania użytkownika (klucz RSA i zwykłe hasło).

Najczęściej współcześnie stosowany sposób szyfrowania to AES, choć nadal część serwerów używa szyfrowania Blowfish i technik z rodziny DES.

Rozpoznawanie użytkownika może się opierać na tradycyjnym pytaniu o hasło, klucz (RSA lub DSA) lub z użyciem protokołu Kerberos.

Trzy najbardziej znane implementacje SSH to zamknięty ssh.com, oparty na licencji Open Source OpenSSH oraz wersja protokołu stosowana w programie PuTTY.

Protokoły z rodziny SSH korzystają zwyczajowo z portu 22 protokołu TCP, choć w wielu zastosowaniach celowo stosuje się port o innym numerze w celu zwiększenia bezpieczeństwa serwera. Sama rodzina SSH znajduje się w warstwie aplikacji modelu OSI, ale do połączenia korzysta z protokołu TCP.

***

SSL (ang. Secure Socket Layer) - protokół, w swojej pierwotnej wersji zaprojektowany przez firmę Netscape Communications Corporation zapewniający poufność i integralność transmisji danych oraz zapewnienie uwierzytelnienia, opierający się na szyfrach asymetrycznych oraz tzw. certyfikatach standardu X.509.
Zaletą protokołu jest fakt, że działa on na warstwie TCP, a więc można łatwo zastosować do zabezpieczenia protokołów warstwy aplikacyjnej (np.: telnet, HTTP, gopher, POP3).

Istnieją trzy wersje protokołu – wersja 1 miała poważną dziurę w bezpieczeństwie biorącą się z nieweryfikowania procedury uzgadniania szyfru – atakujący mógł wymusić używanie przez strony najsłabszego szyfru obsługiwanego przez obie strony, ze złamaniem którego mógł sobie poradzić znacznie łatwiej niż z szyfrem, który strony wybrałyby normalnie. Wersja 2 weryfikuje procedurę negocjacyjną.

Obecnie najczęściej używaną wersją jest SSL 3. Aktualnie uważany jako standard bezpiecznej transmisji danych w internecie i rozwijany jako TLS (ang. Transport Layer Security).

***

Klucz (ang. key) – w kryptografii informacja umożliwiająca wykonywanie pewnej czynności kryptograficznej – szyfrowania, deszyfrowania, podpisywania, weryfikacji podpisu itp.

Kryptografia symetryczna
W kryptografii symetrycznej klucz służy do szyfrowania i deszyfrowania wiadomości. Do obu tych czynności używa się tego samego klucza, dlatego powinien być znany tylko uczestnikom. Taki klucz jest przypisany do danej komunikacji, nie do posiadacza, dlatego zwykle do każdego połączenia jest generowany nowy klucz. Może do tego służyć np. (oparty na kryptografii asymetrycznej) protokół Diffiego-Hellmana.

Kryptografia asymetryczna
W kryptosystemach asymetrycznych wyróżniamy klucz publiczny oraz prywatny. Ten pierwszy może być zupełnie jawny, drugi powiniem znać tylko właściciel. Matematyczna konstrukcja kluczy powinna być taka, żeby wygenerowanie prywatnego na podstawie publicznego było jak najtrudniejsze obliczeniowo. Zależnie od kryptosystemu, wygenerowanie klucza publicznego na podstawie prywatnego również może być trudne (RSA), lub trywialne (ElGamal).
Dwie najważniejsze funkcje kryptografii asymetrycznej to:

- **szyfrowanie** – wtedy klucz publiczny służy do szyfrowania, a prywatny do deszyfrowania
- **podpisy cyfrowe** – klucz prywatny służy do generacji podpisów, klucz publiczny do ich weryfikacji

Klucze asymetryczne są zwykle przypisane do uczestnika (osoby, programu itp.), nie do kanału komunikacji.
Dwa najpopularniejsze systemy kryptografii asymetrycznej to RSA i ElGamal. Inne to m.in. DSA i ECC.

***

Przykład 1: Prosty tunel bez zabezpieczeń

StudentA:

```
# openvpn --remote studentb --dev tun1 --ifconfig 10.4.0.1 10.4.0.2 --verb 9
```

StudentB:

```
# openvpn --remote studenta --dev tun1 --ifconfig 10.4.0.2 10.4.0.1 --verb 9
```

Zweryfikować czy tunel działa za pomocą programu ping.

na StudentA:

```
$ ping 10.4.0.2
```

na StudentB:

```
$ ping 10.4.0.1
```

Opcja --verb 9 powoduje wyprowadzanie dużych ilości informacji w formie podobnej do programu tcpdump(8). Jeżeli działa można opcję --verb 9 pominąć.

Przykład 2: Tunel z kluczem statycznym

Wygenerować klucz statyczny.

```
# openvpn --genkey --secret key
```

Komenda powoduje wygenerowanie losowego klucza w pliku key (w formacie ascii). Skopiować key bezpiecznym połączeniem np programem scp(1) na drugi komputer.

Na StudentA:

```
# openvpn --remote studentb --dev tun1 --ifconfig 10.4.0.1 10.4.0.2\ --
verb 5 --secret key
```

Na StudentB:

```
# openvpn --remote studenta --dev tun1 --ifconfig 10.4.0.2 10.4.0.1\ --
verb 5 --secret key
```

Zweryfikować czy tunel działa za pomocą programu ping.

na StudentA:

```
$ ping 10.4.0.2
```

na StudentB:

```
$ ping 10.4.0.1
```