Instrukcja instalacji klienta OpenVPN w sieci WFAiIS UMK

operator@fizyka.umk.pl

2 lutego 2012

1 Informacje ogólne

1.1 Idea działania sieci VPN

Wirtualna sieć prywatna jest technologią pozwalającą w bezpieczny sposób łączyć komputery oraz sieci znajdujące się w różnych lokalizacjach geograficznych, używając do tego łącz publicznych (np. poprzez sieci publicznie działających dostawców internetowych). Połączenia tego typu realizowane są przy pomocy wirtualnych tuneli łączących pary hostów, na których pracuje usługa VPN. Przed ustanowieniem tunelu wymagane jest wcześniejsze uwierzytelnienie obydwu hostów, co pozwala później na autoryzację dostępu do usług. Poufność transmisji przechodzących przez tunel zapewnia silna kryptografia, dzięki czemu komunikacja poprzez VPN jest równie bezpieczna, jak transmisja prowadzona po dedykowanych łączach. Innymi słowami, VPN jest technologią pozwalająca utworzyć bezpieczny, wirtualny „dedykowany obwód" rozpięty po niezabezpieczonych łączach publicznych.

1.2 Usługi realizowane poprzez VPN w sieci IF

Pracownicy i goście

- Pełen dostęp do serwerów IF poprzez SSH spoza sieci IF.
- Dostęp do poczty elektronicznej (odbieranie i wysyłanie).

  Aby skonfigurować klienta poczty elektronicznej, należy postępować zgodnie ze wskazówkami dotyczącymi konfiguracji dla komputerów sieci lokalnej IF dostępnymi na stronie http://www.fizyka.umk.pl/fizyka/?q=node/141 (pkt. 3, także 1.2).
- Dostęp do usług pracujących na dowolnym komputerze dostępnym w sieci lokalnej.
- Dostęp do własnego komputera pracującego w sieci IF/KIS.

Studenci

Dostęp do wybranych serwerów sieci IF/KIS z sieci Eduroam i Internetu.

2 Uzyskiwanie certyfikatu

W celu uzyskania certyfikatu umożliwiającego połączenie się z usługą OpenVPN pracownicy Wydziału powinni skontaktować się z p. Pawłem Binnebeselem poprzez e-mail (bip@fizyka.umk.pl) lub telefonicznie (56 611 3265). W przypadku studentów konieczne jest złożenie w dzie-

kanacie Wydziału odpowiedniego wniosku, który można pobrać ze strony http://www.fizyka.-umk.pl/ftp/openvpn/wniosek.pdf.

W przeciągu 7 dni od dnia złożenia wniosku (a następnego dnia od momentu zarejestrowania użytkownika) w katalogu domowym użytkownika zostanie automatycznie utworzony katalog "openvpn", w którym będą znajdować się wymagane do instalacji pliki. Jeżeli w przeciagu 7 dni certyfikat nie pojawi się w w/w katalogu, to należy zgłosić ten fakt pisząc na adres operator@fizyka.umk.pl.

3 Instalacja klienta OpenVPN i jego uruchomienie

Użytkownicy systemów MS Windows powinni pobrać najnowszą wersję oprogramowania *OpenVPN Client for Windows* i ją zainstalować (http://openvpn.net/ → Community → Downloads). Następnie należy rozpakować pliki z otrzymanego od administratora pliku windows.zip. Jeżeli podczas instalacji program został umieszczony w katalogu *c:\Program Files\OpenVPN*, to pliki te należy rozpakować w katalogu *c:\Program Files\OpenVPN\config*.

W celu uruchomienia klienta OpenVPN należy kliknąć prawym klawiszem myszy na ikonę *OpenVPN GUI* i wybrać opcję "Connect".

3.1 System Linux

Większość aktualnie wydawanych dystrybucji posiada dołączony pakiet openvpn, więc należy go zainstalować wraz z pakietami zależnymi. Następnie należy w katalogu /etc/openvpn rozpakować zawartość pliku linux.zip:

```
# chmod 700 /etc/openvpn
# cd /etc/openvpn
# unzip linux.zip
```

Następnie można przystąpić do uruchomienia usługi openvpn. W tym celu warto wyłączyć zaporę ogniową, aby wykluczyć problemy wynikające z nadmiernego filtrowania ruchu wydając polecenie: `service iptables stop` (dystrybucje korzystające z systemu SysV) lub `systemctl stop iptables.service` (dystrybucje korzystające z systemu Upstart). Następnie należy wydać polecenie `service openvpn start` (`systemctl start openvpn`)

Po kilkunastu sekundach (w zależności od prędkości łącza) tunel powinien być gotowy do pracy. Aby to sprawdzić można uruchomić komendę `ping 172.20.0.1`. Zaporę ogniową należy zmodyfikować w taki sposób, aby nie blokować ruchu pakietów UDP do serwera 158.75.63.1 na port 1194 (pracownicy) lub 626 (studenci).