**Dlaczego klient (np. przeglądarka) czasem wyświetla komunikat, że komunikacja z serwerem nie jest bezpieczna, pomimo tego, że jest szyfrowana (https)?**

Dlatego, iż w tym wypadku haker może przeprowadzić skuteczny atak typu „man in the middle”, poprzez usunięcie certyfikatu SSL, po uprzednim skonfigurowaniu własnego sprzętu (ustawienie trybu przechwytywania, konfiguracja zapory sieciowej iptables, przekierowanie ruchu w określone miejsce). Może on również podrobić owy certyfikat.