Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-net-vpn

SIECI KOMPUTEROWE

VPN, czyli samochód zapakowany do ciężarówki

Witamy ponownie na Autostradzie Pakietów! Po ostatniej przygodzie z **za dużą ciężarówką pod wiaduktem** kierownik firmy transportowej ogłosił nową rewolucję. Tym razem nie chodzi o wielkość pojazdu. Chodzi o tajemnicę.

— Panowie! Koniec z publicznym pokazywaniem naszych transportów!
— Ale przecież jeździmy po publicznych drogach.
— WŁAŚNIE! Każdy może zobaczyć nasze samochody!
— To może kupimy ciężarówkę z zamkniętą naczepą?
— GENIALNE! ZAMAWIAĆ!

Następnego dnia przed magazyn przyjechała ogromna, zamknięta ciężarówka. Pracownicy otworzyli naczepę.

— Ładujemy towar?
— Nie! Ładujemy samochód!
— JAKI SAMOCHÓD?!
— Ten, który jeździ do naszego drugiego oddziału.
— Ale po co wkładać samochód do ciężarówki?
— Żeby na autostradzie nikt nie widział, czym jedzie!
— A nie wystarczy przyciemnić szyby?
— NIE DYSKUTOWAĆ! ŁADUJEMY!

🤣

VPN, czyli prywatna podróż po publicznej drodze

VPN (Virtual Private Network) to sposób stworzenia logicznego, prywatnego połączenia przez inną sieć, często publiczny Internet. Wyobraźmy sobie dwa firmowe biura: jedno w Warszawie, drugie w Krakowie. Każde ma swoje komputery i lokalną sieć. Chcemy, żeby mogły wymieniać dane tak, jakby łączyła je prywatna droga, choć między nimi biegnie zwykła publiczna autostrada.

Oryginalny samochód jest naszym pakietem. Wielka ciężarówka jest zewnętrznym transportem: zabiera samochód, przejeżdża publiczną drogą i wypuszcza go dopiero w odpowiednim miejscu. W sieci nazywamy to **tunelowaniem lub enkapsulacją** — umieszczeniem oryginalnych danych w dodatkowej „kopercie” potrzebnej do przewozu.

— Panie kierowniku, samochód dojechał do Krakowa!
— I nikt go nie widział?!
— Nie.
— DOSKONALE!
— Ale ciężarówkę widzieli wszyscy.
— CO?!
— Przecież jechała autostradą.
— TO CO TO ZA TAJNY TRANSPORT?!
— Tajny może być ładunek. Nie sam fakt, że ciężarówka istnieje.

Najważniejsza uwaga: **VPN nie czyni połączenia niewidzialnym**. Obserwator nadal może widzieć adresy końców tunelu, czas, ilość i charakterystykę ruchu. Zwykle nie widzi za to oryginalnych pakietów w postaci dostępnej bezpośrednio w sieci publicznej, jeśli tunel jest poprawnie zabezpieczony.

Tunelowanie i szyfrowanie to nie to samo

Kierownik ogląda nową ciężarówkę.

— Czy ona jest bezpieczna?
— Ma zamkniętą naczepę.
— Ale czy każdy może ją otworzyć?
— Jeśli nie zabezpieczymy drzwi, to tak.
— TO NA CO NAM TA TAJEMNICA?!
— Trzeba założyć porządny zamek.

Tunelowanie odpowiada za opakowanie i przewiezienie danych inną siecią. **Szyfrowanie** odpowiada za to, aby osoby bez odpowiednich kluczy nie mogły odczytać chronionej zawartości. To dwa różne pojęcia. Samo umieszczenie jednego pakietu w drugim nie daje jeszcze poufności: istnieją tunele bez **szyfrowania**.

W praktyce bezpieczne rozwiązania VPN mogą zapewniać poufność, integralność i uwierzytelnienie transmisji, zależnie od protokołu, trybu oraz konfiguracji. Ochrona przed nieuprawnioną zmianą danych jest równie ważna jak to, żeby nikt nie podglądał środka.

— A policjant na autostradzie ma klucz?
— Nie.
— A właściciel parkingu?
— Nie.
— A pan ze stacji benzynowej?
— Też nie.
— To skąd będą wiedzieli, co wieziemy?
— Nie będą.
— WRESZCIE KTOŚ ROZUMIE IDEĘ!

Kto odbiera ciężarówkę? Klucze, certyfikaty i tożsamość

Ciężarówka dociera do bramy krakowskiego oddziału. Ochroniarz wychodzi z budki.

— Kto jedzie?
— Tajna ciężarówka.
— Proszę potwierdzić tożsamość.

— Bardzo tajna ciężarówka.
— To nie potwierdzenie.
— Najbardziej tajna ciężarówka na świecie?!
— Proszę pana, potrzebuję właściwych dokumentów, a nie stopniowania przymiotników.

🤣

Urządzenia i użytkownicy łączący się przez VPN muszą wiedzieć, **z kim naprawdę zestawiają połączenie**. Wykorzystuje się do tego odpowiednie klucze, **certyfikaty** lub inne mechanizmy uwierzytelniania. Samo zaszyfrowanie transmisji do niezweryfikowanego odbiorcy nie wystarczy — można przecież bardzo bezpiecznie dostarczyć przesyłkę oszustowi.

— Ale przecież ma naszą firmową nalepkę!
— Panie kierowniku, drukarka do nalepek stoi w każdym sklepie papierniczym.
— Cholera. To proszę sprawdzić dokumenty.

Dwa biura albo jeden człowiek z laptopem

W firmie są dwa rodzaje zleceń. Pierwsze: połączyć całe biuro w Warszawie z całym biurem w Krakowie. Drugie: umożliwić pracownikowi z laptopem dostęp do firmowych zasobów, gdy jest poza biurem.

W pierwszym przypadku mówimy zwykle o **site-to-site VPN**: dwa routery albo bramy VPN łączą sieci w obu lokalizacjach. Samochody z całych osiedli korzystają ze wspólnego transportu. W drugim przypadku mamy **remote-access VPN**: pojedynczy komputer lub telefon zestawia własne połączenie z siecią firmy.

— Panie kierowniku, z parkingu dzwoni pracownik.
— Z którego oddziału?
— Z hotelu nad morzem.
— A co tam robi?!
— Ma laptop i chce dostać się do firmowego serwera.
— To niech prześle laptop ciężarówką do Krakowa!
— Albo po prostu uruchomi klienta VPN.
— Zawsze musicie psuć mi genialne pomysły!

VPN nie oznacza jednak automatycznego dostępu do wszystkiego. Nadal działają uprawnienia, firewalle i zasady **bezpieczeństwa**. Prywatna droga nie jest przepustką do każdego pokoju w budynku.

Trasy: skąd kierowca wie, do której ciężarówki wsiąść?

Pewnego ranka samochód z Warszawy zamiast do krakowskiego oddziału pojechał zwykłą drogą.

— Dlaczego nie skorzystał z VPN?!
— Bo w jego instrukcji jazdy nie ma takiej trasy.
— ALE PRZECIEŻ KUPILIŚMY CIĘŻARÓWKĘ!
— Sama ciężarówka nie wpisuje tras do mapy.

W sieci o wyborze drogi decydują **routing** oraz reguły sieciowe. Trzeba określić, które adresy i sieci są osiągalne przez tunel. W połączeniu dwóch firmowych sieci potrzebne są właściwe trasy po obu stronach, a także odpowiednie reguły ruchu. Samo ustanowienie tunelu nie oznacza, że każdy pakiet zacznie nim jechać.

— A czy mogę skierować samochody przez tunel, ale odpowiedzi kazać wracać zwykłą drogą?
— Może pan. Tylko proszę się potem nie dziwić, że część rozmów się rozsypie.
— Czyli muszę sprawdzić również drogę powrotną?
— Brawo, panie kierowniku.

Full tunnel i split tunnel, czyli bułki za tysiąc dwieście złotych

Kierownik ogłasza kolejną zasadę.

— OD DZISIAJ WSZYSTKIE SAMOCHODY JADĄ TAJNĄ CIĘŻARÓWKĄ!
— Nawet ten, który jedzie po bułki?
— WSZYSTKIE!
— Ale piekarnia jest po drugiej stronie ulicy.
— NIE INTERESUJE MNIE TO!

Samochód z Warszawy wjeżdża do ciężarówki. Ciężarówka jedzie do Krakowa. Samochód wyjeżdża, kupuje bułki i wraca tą samą drogą.

— Panie kierowniku, bułki dotarły!
— Doskonale! Ile kosztowały?
— Osiem złotych.
— A transport?
— Tysiąc dwieście.
— ...
— Ale nikt po drodze nie widział, jakie kupiliśmy bułki!

🤣🤣🤣

Full tunnel oznacza w typowej konfiguracji zdalnego klienta, że ruch do Internetu również jest kierowany przez VPN. **Split tunnel** kieruje przez VPN tylko wybrane zasoby, a pozostały ruch może wychodzić bezpośrednio przez lokalne łącze. To wynik konfiguracji tras i polityk, a nie magia włączana samą nazwą.

Jedno ustawienie nie zawsze jest lepsze od drugiego. Full tunnel daje firmie większą kontrolę nad ruchem, ale może zwiększać obciążenie i opóźnienia. Split tunnel oszczędza zasoby i pozwala korzystać z lokalnego połączenia, ale wymaga starannego przemyślenia zasad bezpieczeństwa.

Jest jeszcze **DNS**, czyli nasza **książka adresowa Internetu**. To, którędy jedzie pytanie o nazwę serwera, również zależy od ustawień. Włączony VPN nie daje automatycznej gwarancji, że każdy **DNS** przechodzi przez tunel.

— Panie kierowniku, po co wysyłamy bułki do Krakowa?
— Bo tak napisałem w regulaminie.
— A kto napisał regulamin?
— JA!
— To mamy odpowiedź.

Kto teraz widzi ruch? VPN nie jest peleryną niewidką

Kierownik składa zamówienie na jeszcze większy napis „ANONIMOWY TRANSPORT”.

— Teraz nikt nie dowie się, dokąd jadę!
— Operator lokalnego łącza może widzieć połączenie do bramy VPN.
— Ale nie widzi wnętrza zaplombowanej ciężarówki?
— Przy prawidłowym **szyfrowaniu** nie powinien móc go odczytać.
— A operator po drugiej stronie tunelu?
— Może widzieć ruch wychodzący z jego sieci, zależnie od tego, co jest dalej **szyfrowane**.
— A strona, do której się loguję?
— Nadal może wiedzieć, że to pan.
— TO GDZIE TA ANONIMOWOŚĆ?!
— W ulotce marketingowej, panie kierowniku.

🤣

VPN może chronić dane na określonym odcinku i zmieniać widoczny na zewnątrz **adres IP**, jeśli ruch wychodzi do Internetu przez bramę VPN. Nie usuwa jednak ciasteczek, logowania na konta, identyfikatorów przeglądarki ani innych metod rozpoznawania użytkownika. **VPN to narzędzie sieciowe, nie obietnica pełnej anonimowości.**

Ochrona VPN obejmuje konkretny odcinek połączenia. Jeśli ruch po wyjściu z tunelu nie jest dodatkowo zabezpieczony, operator tej części trasy może zobaczyć więcej. Dlatego **HTTPS** nadal jest potrzebny.

OpenVPN, WireGuard, IPsec: różne ciężarówki, wspólny cel

Do magazynu przyjeżdża trzech przedstawicieli handlowych.

— Nasza ciężarówka nazywa się OpenVPN!
— Nasza WireGuard!
— A nasza używa IPsec!
— KTÓRA JEST NAJLEPSZA?! — pyta kierownik.
— To zależy od wymagań, urządzeń i konfiguracji — odpowiada administrator.
— Nienawidzę odpowiedzi „to zależy”.
— Witamy w informatyce.

OpenVPN, WireGuard i IPsec to różne technologie realizujące bezpieczne połączenia. Różnią się m.in. sposobem zestawiania sesji, zarządzaniem kluczami, możliwościami i wymaganiami wdrożenia. Samo słowo „VPN” nie mówi, którego rozwiązania użyto ani czy ustawiono je poprawnie.

MTU wraca: samochód w ciężarówce pod wiaduktem

Wszystko działało znakomicie, aż do momentu, gdy zaplombowana ciężarówka dojechała do znajomego wiaduktu.

— PANIE KIEROWNIKU! ZNOWU SIĘ NIE MIEŚCIMY!
— Jak to?! Przecież wczoraj zmniejszyliśmy samochód!
— Tak, ale dzisiaj zapakowaliśmy go do ciężarówki!
— TO WYJMIJCIE GO Z CIĘŻARÓWKI!
— Ale wtedy nie będzie tunelu VPN.
— TO ZMNIEJSZCIE CIĘŻARÓWKĘ!
— Trzeba zmniejszyć ładunek i uwzględnić dodatkowe opakowanie.
— CHOLERA, ZNOWU MATEMATYKA!

🤣🤣

Tunel zwykle dodaje swoje nagłówki, co zmniejsza miejsce na oryginalny pakiet. Dlatego VPN bywa miejscem, w którym pojawiają się problemy opisane w artykule o **MTU i MSS**: małe pakiety działają, a duże transmisje się zawieszają. Trzeba uwzględnić rzeczywiste **MTU** trasy, narzut tunelu, komunikaty ICMP i ewentualne **MSS** clamping dla **TCP**.

Nie ma jednego magicznego **MTU** ani **MSS** pasującego do każdego VPN. Zależy to od konkretnego protokołu, łącza i sposobu opakowania danych.

A co, jeśli ciężarówka nie przyjedzie?

— Panie kierowniku, tunel przestał działać!
— To niech samochody jadą zwykłą drogą.
— Ale miały wozić poufne dokumenty!
— To może jednak nie?
— WŁAŚNIE.

Po awarii VPN ruch może zostać zablokowany, skierowany inną trasą albo wypłynąć zwykłym łączem — zależnie od konfiguracji. Jeśli określone dane **muszą** pozostać w tunelu, należy świadomie skonfigurować zasady blokowania ruchu poza nim, często nazywane **kill switch** lub odpowiednią polityką firewalla.

— Czyli trzeba przewidzieć awarię?
— Tak.
— A nie wystarczy napisać „bezawaryjne” w reklamie?
— Niestety nie.

Finał: tajny transport dotarł

Po tygodniu konfiguracji pierwsza zaplombowana ciężarówka poprawnie dotarła z Warszawy do Krakowa. Dokumenty zostały sprawdzone, klucze pasowały, trasy były właściwe, a pod wiaduktem nikt nie zostawił połowy naczepy.

— Panie kierowniku, połączenie działa!
— I nikt nie widział naszego samochodu?
— Tak.
— I nikt nie otworzył naczepy?
— Tak.
— I wszystko przyjechało na czas?
— Tak.
— DOSKONALE! Proszę zamówić jeszcze pięć takich ciężarówek!
— Ale potrzebujemy tylko jednej.
— Nie szkodzi. Firma musi się rozwijać!

🤣

Dyrekcja Autostrady Pakietów informuje: ciężarówki VPN nie są niewidzialne, nie potrafią przejeżdżać przez za niskie wiadukty i nadal podlegają zasadom ruchu. Kierownik złożył odwołanie od wszystkich trzech punktów.