# Czym jest wirtualna sieć prywatna

Virtual Private Network – rozwiązanie pierwotnie wykorzystywane przez duże organizacje, w celu zapewnienia pracownikom dostępu do informacji znajdujących się w firmowej sieci prywatnej. Stosowane w celu zapewnienia integralności (modyfikowanie), a także poufności (szyfrowanie) przesyłanych danych. Standardowym przykładem może być pracownik zdalny, który musi korzystać z zasobów znajdujących się w prywatnej sieci firmowej, jednak transfer danych odbywa się poprzez sieć Internet.

Obecnie jest to technologia wykorzystywana bardzo często poprzez użytkowników prywatnych, którzy cenią sobie prywatność, chcą uniknąć śledzenia przez rządy lub korporacje. Zastosowanie sieci VPN pozwala także uniknąć ograniczeń związanych z dostępnością pewnych licencji jedynie dla adresów IP z wybranych geolokalizacji.

Popularnym zastosowaniem dla VPN jest także unikanie NAT. Jest to przydatne, kiedy chcemy w danej sieci sterować bezpośrednio wybraną maszyną, unikając tym samym wielu przekierowań.

TUTAJ MOŻNA ZAPROPONOWAĆ PYTANIE: JAKIE SĄ PRZYKŁADY OBCHODZENIA GEOLOKALIZACJI ZA POMOCĄ VPN

ODPOWIEDŹ: WEŹMY PRZYKŁAD SERIALU, KTÓRY NA PLATFORMIE INTERNETOWEJ DOSTĘPNY JEST TYLKO Z LICENCJĄ DLA USA. KORZYSTAJĄC Z SERWERA VPN ZLOKALIZOWANEGO W STANACH, UKRYWAMY NASZE IP I PRZEZ ODBIORCĘ WIDZIANI JESTEŚMY JAKO UŻYTKOWNIK Z IP ODPOWIADAJĄCYM DOZWOLONEJ GEOLOKALIZACJI. DZIĘKI TEMU MOŻEMY KORZYSTAĆ Z DOSTĘPNYCH TYLKO TAM TREŚCI.

INNY PRZYKŁAD ODPOWIEDZI: POZWALA TO OSZCZĘDZIĆ PIENIĄDZE, PONIEWAŻ CZĘSTO CENY LOTÓW, HOTELI, WYCIECZEK, ITP. UZALEŻNIONE SĄ OD GEOLOKALIZACJI UŻYTKOWNIKA. KORZYSTAJĄC Z IP ROŻNYCH KRAJÓW MOŻEMY CENY PORÓWNYWAĆ, A TAKŻE WYBIERAĆ NAJATRAKCYJNIEJSZE

# Jak to działa

Klient VPN zainstalowany na komputerze/laptopie/smartfonie w momencie uruchomienia tworzy tzw. tunel VPN, prowadzący do serwera (może on znajdować się gdziekolwiek na świecie), z którego dopiero "wchodzi się" do internetu pod zmienionym IP. Urządzenia używające tego samego serwera mają niejako to samo wejście do sieci, więc dostawca internetu ani program szpiegujący nie mają żadnej możliwości sprawdzenia, co dana osoba dalej robi. Tworzy się wówczas wirtualna sieć prywatna. Tunel sprawia, że wysyłane pakiety są szyfrowane w locie i nawet jeśli ktokolwiek by je przejął - nie będzie mieć z nich żadnego pożytku. Bez odpowiednich metod deszyfracji są to wyłącznie nic nie mówiące dane.

## Szyfrowanie za pomocą klucza publicznego

Współczesne implementacje sieci dysponują wieloma mechanizmami, które pozwalają zapewnić bardzo wysoki poziom bezpieczeństwa.   
Wydawać by się mogło, że hasło i odpowiednie szyfrowanie to elementy wystarczające. Jednakże można wyróżnić trzy filary:

* Uwierzytelnianie
* Autoryzacja
* Szyfrowanie

Ich wykorzystanie w uproszczeniu wygląda tak:

KLIENT łączy się do SERWERA i przedstawia swój podpisany przez Certificate Authority (centrum certyfikacji) certyfikat, SERWER weryfikuje jego poprawność za pomocą certyfikatu CA.

SERWER przedstawia swój podpisany przez CA certyfikat a KLIENT go weryfikuje na podstawie certyfikatu CA.

SERWER szyfruje transmisję do KLIENTA za pomocą publicznego klucza KLIENTA, a KLIENT za pomocą swojego prywatnego go odszyfrowuje

KLIENT szyfruje transmisję do SERWERA za pomocą publicznego klucza SERWERA, a SERWER za pomocą swojego prywatnego go odszyfrowuje

SERWER za pomocą swojego prywatnego klucza podpisuje (zapewnia integralność i pewność pochodzenia) dane do KLIENTA, a KLIENT weryfikuje to za pomocą publicznego klucza SERWERA

KLIENT za pomocą swojego prywatnego klucza podpisuje dane do SERWERA, a SERWER weryfikuje to za pomocą publicznego klucza KLIENTA

Istnieje jeszcze opcjonalny krok polegający na sprawdzeniu czy certyfikat partnera transmisji nie został odwołany (ang. revoke) i robi się to za pomocą weryfikacji list CRL, które udostępnia CA na stronie WWW.

Procedura zapewnia, że uczestnik transmisji jest tym za kogo się podaje oraz że transmisja została zaszyfrowana i zabezpieczona przed modyfikacją przez osoby trzecie.

## Remote Access VPN

Klient takiego połączenia to pojedynczy użytkownik komputera, który łączy się z siecią prywatną ze zdalnej lokalizacji. Serwer sieci VPN zapewnia dostęp do zasobów sieci, do której jest podłączony. Pakiety wysyłane przez połączenie VPN pochodzą od klienta sieci VPN.

Klient sieci VPN uwierzytelnia się na serwerze sieci VPN i, w celu wzajemnego uwierzytelnienia, serwer VPN uwierzytelnia się na kliencie VPN.

## Site-to-site VPN

Połączenie to łączy dwie części sieci prywatnej (tej samej, lub różnych). Pozwala to na przykład na organizację połączeń routowanych z oddzielnymi biurami lub z innymi organizacjami przez Internet. Routowane połączenie VPN w Internecie działa logicznie jako dedykowane łącze Wide Area Network (WAN).

Serwer sieci VPN zapewnia routowane połączenie z siecią, do której jest podłączony serwer sieci VPN. W przypadku połączenia VPN typu site-to-site pakiety wysyłane z dowolnego routera przez połączenie VPN zwykle nie pochodzą z routerów. Router wywołujący (klient VPN) uwierzytelnia się na routerze odpowiadającym (serwerze VPN), a w celu wzajemnego uwierzytelnienia router odpowiadający uwierzytelnia się na routerze wywołującym.

# Wady i zalety

# Protokoły

L2TP – nie szyfruje ruchu, pozwala jedynie na jego kapsułkowanie, przy zastosowaniu szyfrowania np. w warstwie wyższej, jest wydajnym rozwiązaniem.

OpenVPN – pozwala na wyłączenie szyfrowania, autoryzacji, uwierzytelnienia i jedynie kapsułkowanie jak L2TP. Dzięki takiemu rozwiązaniu można np. fizycznie wydzielić fragment sieci czy zastosować szyfrowanie w warstwie wyższej.

# Statystyki użytkowania

Zgodnie z danymi Global Web Index, w użyciu VPN przodują Tajlandia, Indonezja czy Chiny, gdzie z VPN korzysta około 20% użytkowników Internetu. W Europie, USA czy Australii widać znacznie mniejsze zainteresowanie tą technologią. Tam z VPN korzysta zaledwie 4 – 6 % użytkowników sieci.

W każdym z krajów można jednak zauważyć, że 20 – 30 % użytkowników VPN, to osoby chcące utrzymać anonimowość w sieci. Najmniejsze zainteresowanie anonimowością występuje w Ameryce południowej, natomiast największe w południowej Azji.

W Polsce, aż 26% użytkowników VPN, korzysta z tej sieci chcąc zachować anonimowość.

# Prawo a VPN

Czy używanie VPN jest zgodne z prawem?

Zleży to od kraju.

Nielegalne jest to w:

* Chiny - Dostawcy sieci VPN mogą nadal działać, jeśli uzyskają licencję od rządu, ale warunki, na jakie muszą się zgodzić po prostu wypaczają cały sens stosowania tej usługi.
* Irak - aby śledzić i powstrzymać ISIS, zabronił używania VPN
* Zjednoczone Emiraty Arabskie - może kosztować Cię bardzo wysoką grzywę (nawet do dwóch milionów złotych).   
   - Główna motywacja tego zakazu = usługi VOIP (‘odbierają’ zysk firmom telekomunikacyjnym)
* Turcja - aby uniemożliwić korzystanie z mediów społecznościowych
* Białoruś - w 2015 r. idąc w ślady zablokowano korzystanie z usług Tor i VPN. Dostawcy usług internetowych są zobowiązani do sprawdzania dziennie aktualizowanej listy zabronionych usług publikowanych przez agencje rządowe.
* Oman - aktywnie zakazuje i cenzuruje media, w tym internet i zabrania używania VPN.
* Iran – VPN można używać tylko gdy pochodzą od usługodawców mających licencję wydaną przez rząd, co pośrednio sprzeciwia się istocie samej sieci VPN.
* Rosja - rząd rosyjski uchwalił prawo zabraniające korzystania z VPN.
* Korea Północna – reżim
* Mjanma (dawniej Birma)
* Wietnam

# VPN i VNC – brzmi podobnie ale…

Nazwy VNC (Virtual Network Computing) i VPN (Virtual Private Network) mogą brzmieć podobnie, ale w rzeczywistości są zupełnie inne.

Technologia VNC jest używana do zdalnego podglądu i sterowania innymi maszynami za pośrednictwem połączenia sieciowego.   
Jest ona niezwykle przydatna przy korzystaniu z pulpitu zdalnego spoza biura lub z innej części domu. Jest to również dobre narzędzie dla administratorów do zdalnego rozwiązywania problemów z komputerami w sieci.

Typowe zastosowania VNC:

* Pracownicy zdalni
* Procesy ciągłości działania biznesowego (BCP)
* Zdalna pomoc techniczna

wady VNC:

* VNC wykorzystuje nadmierną przepustowość łącza
* Działają wolno
* Zmniejszona użyteczność aplikacji

różnice między VNC a VPN:

* VNC jest zazwyczaj używany do kontrolowania komputerów z innego komputera za pomocą połączenia sieciowego.
* Sieć VPN umożliwi dowolnej aplikacji na Twoim komputerze dostęp do Internetu za pośrednictwem bezpiecznego i szyfrowanego połączenia. Ukryje również Twoją tożsamość, zmieniając Twój adres IP i dając Ci dostęp do mnóstwa ograniczonych w różny sposób witryn. Sieć VPN to popularna implementacja oprogramowania, która umożliwia użytkownikom podłączenie komputerów do sieci. Udostępnia ona bardziej zaawansowane pojęcia, takie jak protokoły tunelowania. Jest to świetny sposób na zbudowanie sieci prywatnej w oparciu o większą publiczną, taką jak Internet.
* VNC pozwala kontrolować komputer zdalny, zazwyczaj przez VPN.

VNC jest świetny dla firm lub osób, które chcą uzyskać dostęp do zdalnego komputera, ale VPN jest lepszy dla tych, którzy również chcą szyfrować pliki i zabezpieczyć swoje dane.

IP Security zapewnia:

* uwierzytelnianie pochodzenia danych
* sprawdzenie integralności danych
* poufność danych
* ochronę odpowiedzi – uniemożliwienie przechwycenia datagramów
* automatyczne zarządzanie kluczami szyfrującymi – umożliwia konfigurację dużych sieci bez lub przy niewielkim udziale użytkownika,