Co to jest VPN?

Jak działa?

Do czego służy?

VPN – Virtual Private Network

Jak sama nazwa wskazuje VPN to prywatna sieć „wirtualna”. Wirtualna oznacza w tym przypadku przeciwieństwo słowa fizyczna, a co za tym idzie-**nie istnieją żadne kable, które umożliwiają połączenia wewnątrz niej.**

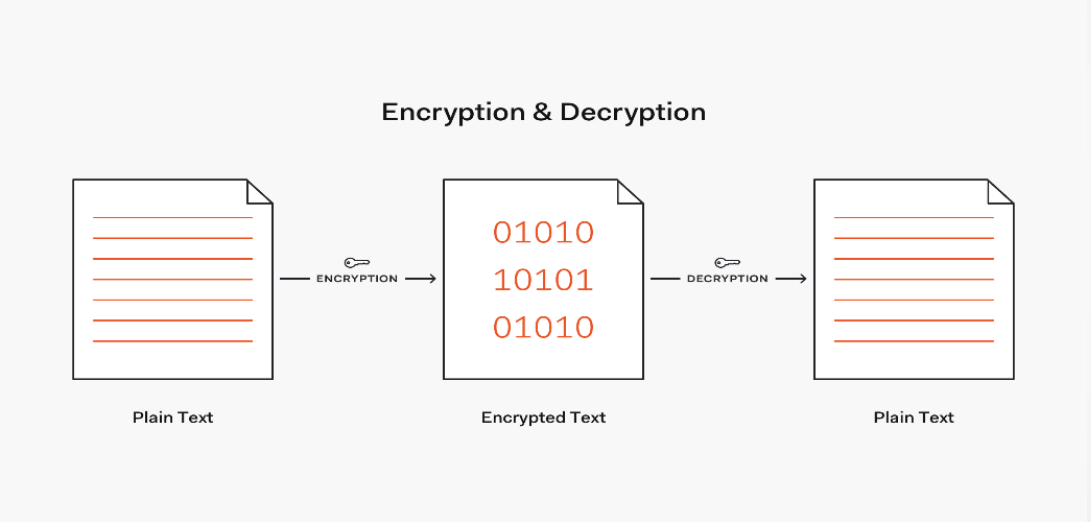
VPN łączy dwa punkty w sieci za pomocą wirtualnego połączenia, realizowanego np. przez sieć rozległą (choćby internet). Sieci połączone w ten sposób będą zachowywać się tak jakby były połączone fizycznie kablem, a ruch między nimi będzie przekazywany wirtualnym tunelem.

Normalnie podczas łączenia się z jakąkolwiek stroną, wysyłanych jest wiele pakietów z komputera, które mają dotrzeć do serwera na jakim strona stoi.
Tunelowanie wychwytuje wszystkie te pakiety, szyfruje i każdorazowo umieszcza w nowym pakiecie. Można to porównać do stworzenia pliku archiwum (zip, rar, 7z). Następnie serwer odpakowuje sobie te pakiety. Każdy kto przechwyci je w trakcie, otrzyma zaszyfrowane dane i nie będzie łatwo w stanie ocenić co chcieliście zrobić.

Biorąc pod uwagę publiczne sieci Wi-Fi (na przykład w kawiarni lub na lotnisku), zazwyczaj łączymy się z nimi bez zastanowienia. Niestety nie wiemy, kto ma dostęp do danych przesyłanych przez łącza tego typu.
Nie wiadomo kto może mieć dostęp do naszych haseł, danych konta bankowego, numerów kart kredytowych i wszystkich innych prywatnych danych przesyłanych w trakcie każdego połączenia z Internetem.

Po włączeniu usługi VPN, wszystkie dane są przesyłane przez **zaszyfrowany tunel**, który uniemożliwia dostęp do danych osobowych osobom niepowołanym. Oznacza to, że nawet gdyby cyberprzestępca przechwycił dane użytkownika, nie będzie w stanie ich odszyfrować.

Szyfrowanie



Każde połączenie VPN jest odpowiednio szyfrowane, właśnie dzięki temu nie można podsłuchać naszego ruchu sieciowego.
Najlepsze serwery korzystają z nowoczesnych zabezpieczeń, których nie da się złamać. Dobrym przykładem jest opisywany dalej serwer OpenVPN, który korzysta z szyfrowania AES-256-CBC. Jest to symetryczny szyfr blokowy o długości klucza 256 bit, z systemem CBC (Cipher Block Chaining), co oznacza, że każda wiadomość jest zależna od poprzedniej. Szyfrowanie tego typu jest wykorzystywane między innymi przez agencję NSA do ochrony ściśle tajnych dokumentów. Uważa się, że jest nie do złamania.

Rodzaje protokołów

Protokoły sieci VPN to inaczej protokoły komunikacyjne z określonymi regułami i zasadami, które mają pozwolić na bezpieczne połączenia pomiędzy dwoma punktami. Oto najpopularniejsze protokoły sieci VPN:

- **PPTP-** Jeśli korzystamy z tego typu protokołu, powinniśmy jak najszybciej przestać. Ma on kilka zalet, ale brak bezpieczeństwa całkowicie przekreśla jego przydatność, a Microsoft odradza jego używanie. Niestety, nadal jest stosowany przez wiele firm i użytkowników nieświadomych potencjalnego zagrożenia.

- **L2TP/IPSec -** Jest to hybryda dwóch protokołów, samo L2TP pozwala tylko na utworzenie tunelu komunikacyjnego i przesyłanie danych. Za bezpieczeństwo odpowiedzialny jest protokół IPSec, który uwierzytelnia i szyfruje połączenia. Zapewniał wysokie bezpieczeństwo, jednak po ujawnieniu przez Edwarda Snowdena informacji o NSA można przyjąć, że protokół IPSec nie zapewnia wcale tak wysokiej ochrony i może być złamany przez służby specjalne.

Zalety IPSec:

- zapewnienie poufności poprzez szyfrowanie danych silnymi algorytmami kryptograficznymi,
- zapewnienie integralności poprzez uniemożliwienie modyfikacji danych w trakcie transmisji,
- uwierzytelnianie stron poprzez zapewnienie, że nikt nie podszył się pod żadną ze stron,
- zapewnienie niezaprzeczalności, które oznacza, że strony nie mogą zaprzeczyć, że nie wysłały danej informacji, o ile informacja ta była podpisana kluczem prywatnym i podpis został poprawnie zweryfikowany.

- **OpenVPN -** Hybryda różnych protokołów, która zapewnia najwyższy stopień ochrony. Nie ma żadnych doniesień, które sugerowałyby złamanie jej zabezpieczeń. Wykorzystuje bibliotekę OpenSSL i protokoły SSLv3 oraz TLSv1. Pozwala to na korzystanie z najlepszych form szyfrowania połączenia i zabezpieczania sesji. Można też łączyć się za pomocą dowolnego portu, dzięki czemu unikniemy wykrycia, że korzystamy z połączenia z siecią VPN.

Zalety:

- otwarty kod źródłowy,
- najwyższy poziom bezpieczeństwa,
- szerokie możliwości konfiguracji

Wady:

- wymaga instalacji specjalnej aplikacji,
- konfiguracja może sprawić trudność początkującym użytkownikom

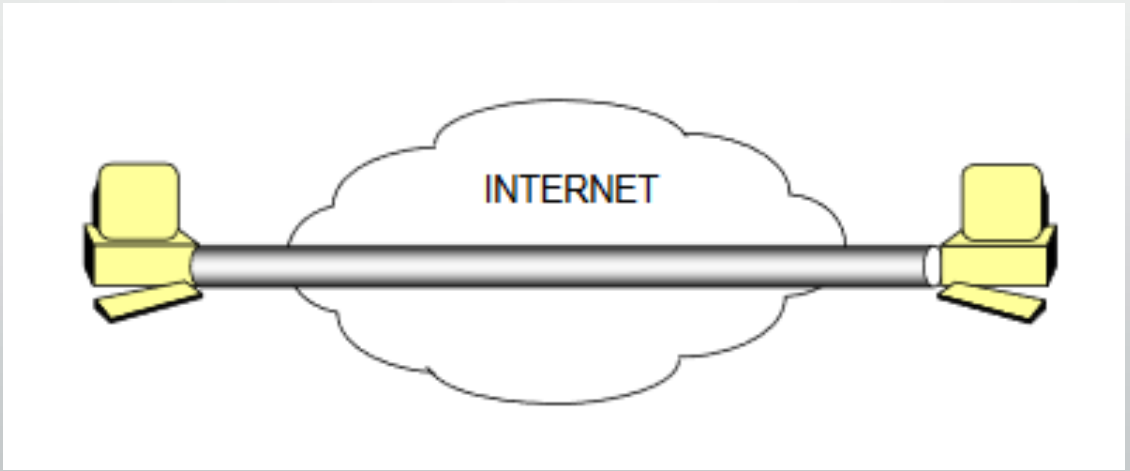
- **IKEv2/IPSec** (ang. Internet key exchange version 2) to protokół tunelowania opracowany przez Microsoft i Cisco, stosowany zazwyczaj w połączeniu z szyfrowaniem IPSec. Ma on liczne zalety, łącznie z możliwością automatycznego przywracania połączenia VPN w razie rozłączenia z Internetem. Jest on bardzo odporny na zmianę sieci, dzięki czemu jest bardzo przydatny dla użytkowników telefonów często przełączających się pomiędzy domową siecią Wi-Fi, a łączami mobilnymi lub pomiędzy hotspotami.

  Protokół IKEv2/IPSec nie jest niestety jeszcze tak powszechny, ale jego popularność rośnie dzięki **szybkości, bezpieczeństwu i elastyczności** tego systemu.

- **SSTP** (ang. Secure Socket Tunneling Protocol) jest przydatny jako alternatywne rozwiązanie zamiast standardowych protokołów w miejscach, gdzie stosowanie VPN jest utrudnione, ponieważ umożliwia **ominięcie większości zapór sieciowych**. SSTP działa podobnie do OpenVPN, ale w przeciwieństwie do OpenVPN stanowi własność firmy Microsoft, co oznacza, że nie podlega niezależnym audytom. Ze względu na powiązania firmy Microsoft z NSA (Agencją Bezpieczeństwa Narodowego USA) w przyszłości można mieć pewne wątpliwości co do wiarygodności tej normy.

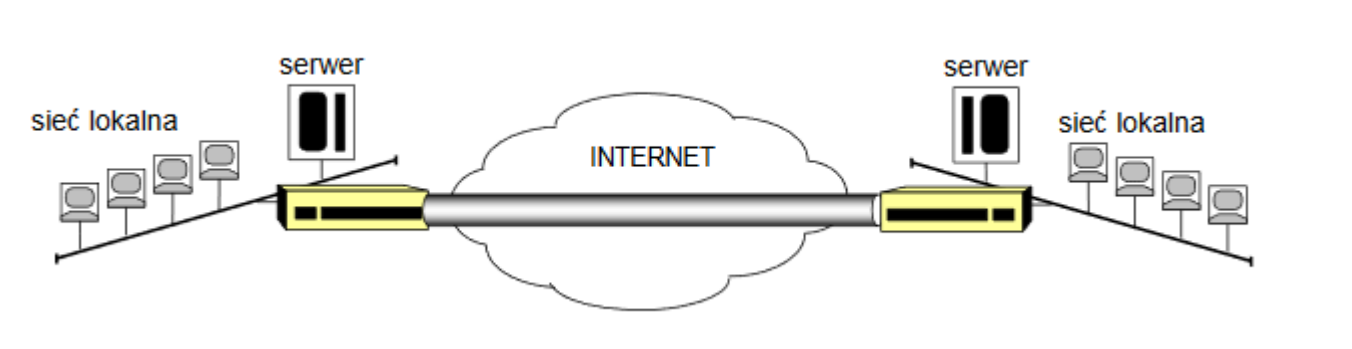
Konfiguracja host-to-host

Najprostszy rodzaj konfiguracji. Mamy dwa pojedyncze stanowiska które są wyposażone w odpowiednie oprogramowanie lub karty sieciowe, które umożliwiają szyfrowanie i deszyfrowanie wysyłanych danych pomiędzy dwoma jednostkami



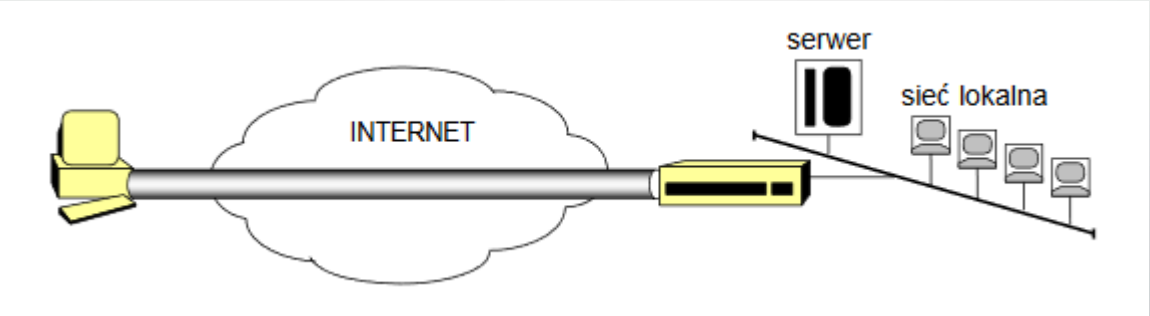
Konfiguracja net-to-net

Na końcach tunelu znajdują się urządzenia szyfrujące/routery ze specjalnymi kryptograficznymi modułami które szyfrują transmisję wychodzącą z sieci lokalnych. Wewnątrz sieci lokalnych, transmisje nie są szyfrowane.



Konfiguracja host-to-net

Na jednym końcu tunelu znajduje się pojedyncza jednostka. Ma ona dostęp do zasobów sieci lokalnej która łączy się z urządzeniem szyfrującym, znajdującym się po drugiej stronie sieci



Jak korzystać z VPN?

VPN to najlepsza opcja, aby pozostać prywatnym i bezpiecznym w sieci online. Aktualnie na rynku jest wielu dostawców (np. ExpressVPN, NordVPN, CyberGhost, Surfshark) którzy umożliwiają bezpieczne korzystanie z internetu. Wystarczy ściągnąć aplikacje od wybranego dostawcy. Po uiszczeniu odpowiedniej opłaty i skonfigurowaniu aplikacji, użytkownik danego systemu operacyjnego będzie chroniony przed wglądem do swojej prywatności. Najlepsi usługodawcy VPN współpracują z takimi aplikacjami i systemami jak: Windows, iOS, Android, MAC OS, Chrome, Firefox, Safari, Linux oraz Netflix. ExpressVPN jest aktualnie określany mianem najlepszego VPN (ma ponad 3000 serwerów w 95 państwach)

Dlaczego VPN jest przydatny?

W dobie dzisiejszego wirtualnego świata, który stał się codziennością, VPN jest przydatny ponieważ szyfruje dane przesyłane przez tunel w celu ochrony tożsamości użytkownika. VPN przekierowuje ruch internetowy do specjalnie skonfigurowanego serwera, ukrywa adres IP użytkownika i w sposób szczególny szyfruje wszystkie dane które są wysyłane i odbierane. Ewentualne przechwycenie danych przez cyberprzestępce niczym nie skutkuje, ponieważ nie będzie w stanie ich odszyfrować.

Reklamy które są wyświetlane na korzystanych przez nas stronach internetowych bądź wysyłane na nasze e-maile są skutkiem braku zabezpieczeń VPN. Dostawca usług ma wgląd do naszych danych i wykorzystuje je często bez naszej wiedzy. Gdy posiadamy zabezpieczenie VPN, dane użytkownika są szyfrowane i chroniony jest adres IP. Dostawca w takiej sytuacji nie ma możliwości gromadzenia metadanych użytkownika i historii co znacznie powiększa prywatność w sieci.

Dziękuję za uwagę