**Korzyści z zastosowania mechanizmu i protokołu bezpiecznej komunikacji VPN versus HTTPS**

**VPN:**

Wirtualna sieć prywatna lub VPN to technologia, która zmienia adres IP i tworzy bezpieczny wirtualny tunel między naszym urządzeniem a serwerem VPN.

Wszystkie informacje, które przechodzą przez ten tunel, są zaszyfrowane, więc nie można ich wyświetlić ani przejąć.

Kiedy łączysz się z VPN, nie tylko szyfruje ruch Twojej przeglądarki, ale także szyfruje wszystkie inne rodzaje ruchu internetowego przychodzącego z i do naszego urządzenia.

Dlatego wszystkie dane, które przesyłamy przez Internet, są ukryte przed dostawcą usług internetowych i innymi osobami trzecimi.

Ludzie używają usług VPN, aby chronić poufne informacje w Internecie i omijać ograniczenia cenzury narzucane przez niektóre kraje i usługi.

W większości przypadków VPN są instalowane ręcznie przez użytkowników.

**HTTPS vs VPN:**

Jeśli naprawdę zależy na prywatności i bezpieczeństwie w Internecie, powinniśmy używać ich obu.

1. Protokół HTTPS musi być włączony w przeglądarce i odwiedzanej witrynie internetowej (nie musimy konfigurować go ręcznie w przeglądarce, ponieważ wszystkie nowoczesne przeglądarki obsługują protokół HTTPS). Klient VPN musi zostać ręcznie zainstalowany przez użytkownika.
2. HTTPS szyfruje ruch internetowy między przeglądarką a serwerem odwiedzanej witryny. Wirtualna sieć prywatna szyfruje cały ruch między urządzeniem a serwerem VPN (Internetem).
3. VPN zmienia nasz adres IP, maskuje naszą cyfrową tożsamość, szyfruje ruch internetowy i pozwala ominąć ograniczenia cenzury. HTTPS nie robi żadnej z tych rzeczy. VPN pozwala wybrać nową lokalizację geograficzną (która jest świetna do uzyskiwania dostępu do zablokowanych treści).
4. HTTPS zapewnia nieco słabsze szyfrowanie niż VPN i jest bardziej narażony na określone typy ataków hakerów. Jednak HTTPS szyfruje dane przeglądarki od punktu końcowego do odwiedzanej witryny, chroniąc w ten sposób połączenie przed ukierunkowanymi atakami MITM, manipulacją DNS i próbami phishingu. HTTPS szyfruje tylko to, co jest wysyłane przez przeglądarkę do serwera i z powrotem, i tylko wtedy, gdy jest włączone w odwiedzanych witrynach.
5. Sieci VPN na ogół używają bardziej zaawansowanych metod szyfrowania. Chociaż każde szyfrowanie jest lepsze niż żadne
6. Podczas korzystania z VPN prędkość połączenia internetowego może być niestabilna. Częstym powodem jest odległość od fizycznej lokalizacji do zdalnego serwera, z którym chcemy się połączyć.

**Korzyści z jednoczesnego zastosowania komunikacji VPN i HTTPS.**

Niestety, wszystkie poufne informacje, które wprowadzamy na niezabezpieczonej stronie internetowej, mogą być nadal monitorowane i kradzione, nawet jeśli przekierowujemy swój ruch przez VPN.

Ale to nie jest wada VPN, tak po prostu działają technologie HTTPS i VPN.

Chodzi o to, że HTTPS zapewnia szyfrowanie od końca do końca między punktem końcowym (wyjściowym serwerem internetowym) a witryną, do której uzyskujesz dostęp.

Sieć VPN szyfruje przesyłany ruch do punktu końcowego, którym jest sam serwer VPN.

Jednak w drodze z tego punktu końcowego do docelowej witryny internetowej ktoś może przechwycić nasze poufne dane, chyba że odwiedzana witryna internetowa jest zabezpieczona przez HTTPS.

**Dlatego ważne jest, aby jednocześnie używać HTTPS i VPN.** W końcu nie ma bitwy zwanej HTTPS vs VPN. Istnieje raczej synergia między nimi.