ZESPÓŁ LABORATORIÓW TELEINFORMATYKI TRANSPORTU

ZAKŁAD INŻYNIERII TRANSPORTU LOTNICZEGO
I TELEINFORMATYKI (ITLIT)

Politechnika Warszawska | Wydział Transportu

LABORATORIUM ZITLIT

INSTRUKCJA DO ĆWICZENIA NR 6

Bezpieczeństwo wymiany danych w sieciach VPN

Warszawa 2023

1. Cel i zakres ćwiczenia

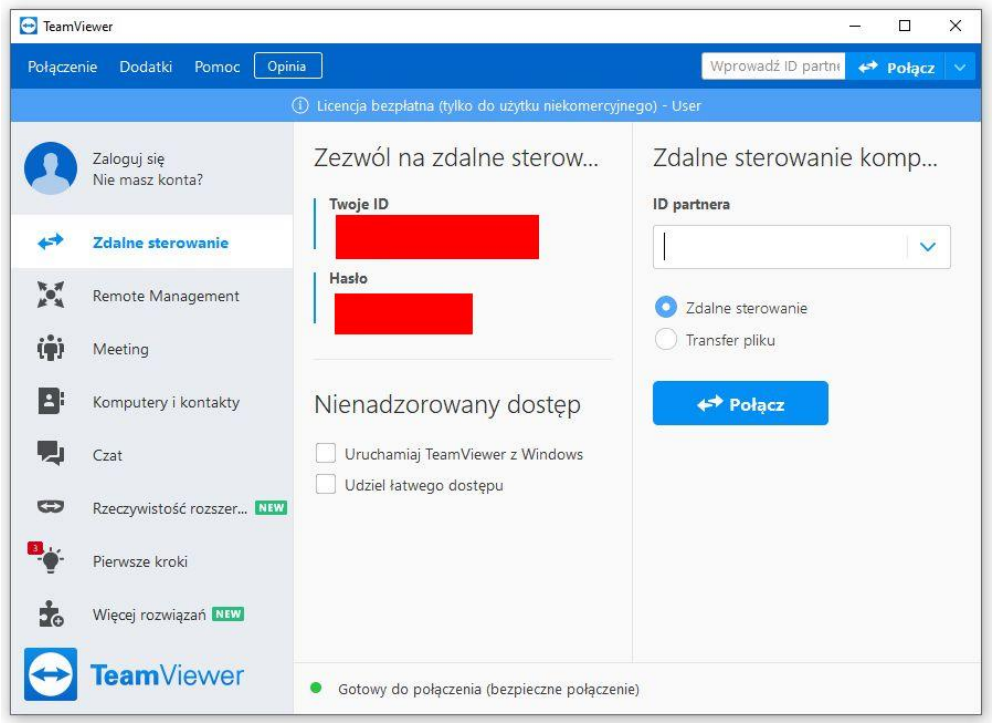
Celem ćwiczenia jest ocena możliwości wykorzystania sieci VPN dla zachowania prywatności w sieci Internet oraz zwiększenia bezpieczeństwa podczas pracy zdalnej.

2. Wykaz wykorzystanych przyrządów

- komputer PC z systemem Windows 10 lub innym,
- program *ProtonVPN* (rys. 2.1),
- wyszukiwarka *DuckDuckGo* (rys. 2.2),
- program *TeamViewer* (rys. 2.3).

Rys. 2.1 Program ProtonVPN

Rys. 2.2 Wyszukiwarka DuckDuckGo



Rys. 2.3 Program TeamViewer

3. Wprowadzenie

3.1 Sieci VPN

Kiedy odwiedzasz w Internecie ulubione strony i portale, robisz zakupy w sklepie online, sprawdzasz swoje dane, czy grasz w gry, można pójść za Tobą i sprawdzić kim jesteś, gdzie się pojawiasz, jakie strony odwiedzasz. I jeśli komuś na tym zależy — znajdzie Cię bez problemu! Nawet zapuka do drzwi Twojego własnego domu!

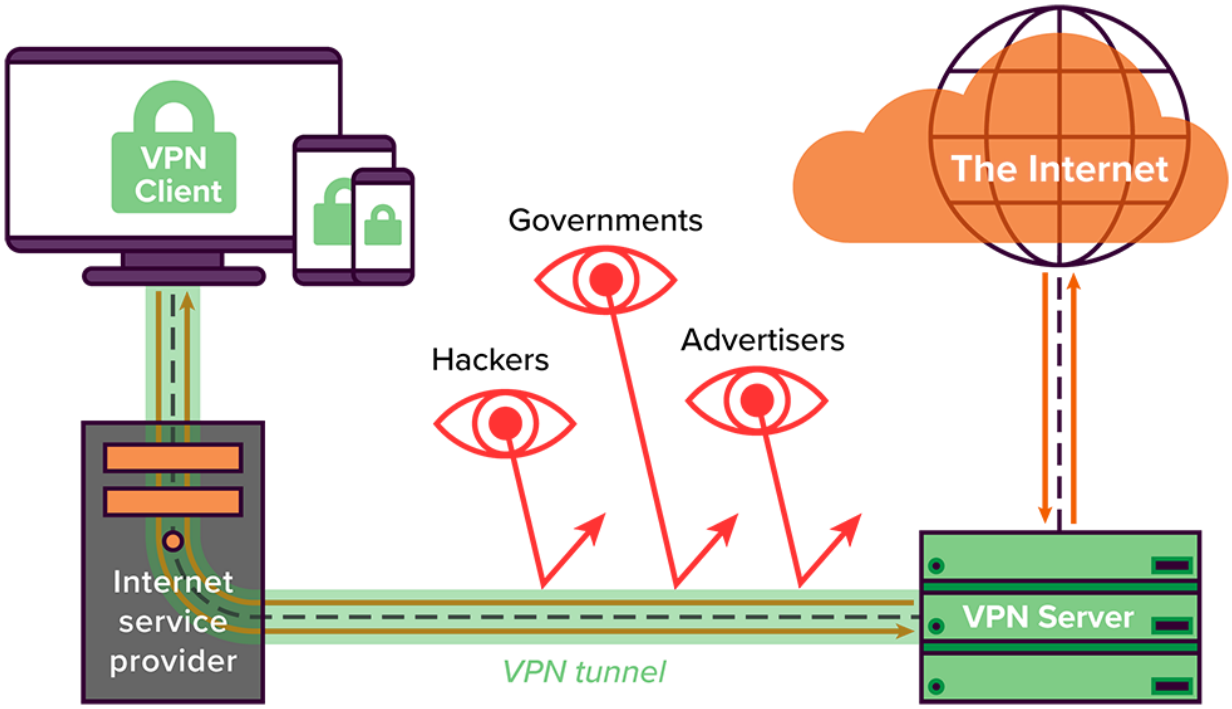
VPN, a dokładnie Virtual Private Network, to wirtualna sieć prywatna, która pozwala na połączenie dwóch sieci lub użytkownika z siecią, w sposób szyfrowany i bezpieczny. VPN zapewnia wyższy poziom ochrony i prywatności podczas surfowania po Internecie. Dzięki niej, możesz przeglądać Internet zupełnie anonimowo, jakbyś miał na sobie pelerynkę niewidkę! Nikt Cię nie zauważy, nikt Cię nie namierzy i nie wyśledzi. Ale jak działa VPN? W jaki sposób może to osiągnąć?

3.2 Jak działa VPN?

Najprościej mówiąc, VPN tworzy bezpieczne połączenie, przekierowując ruch przez wyspecjalizowane serwery, ukrywając Twoją aktywność w sieci. Dokonuje tego sposobem, który nazywamy tunelowaniem. Jeśli chcesz spacerować po cyberprzestrzeni pozostając niezauważonym, koniecznie włącz VPN, zanim połączysz się z Internetem. Wtedy Twoje połączenie nastąpi poprzez zabezpieczony i szyfrowany tunel, a Twoja lokalizacja będzie zamaskowana i chroniona przez sieć VPN. Jest to nie tylko doskonały sposób na przeglądanie stron zabezpieczonych blokadą regionalną, ale także ochrona podczas korzystania z darmowych, publicznych hotspotów Wi-Fi.

Włączając VPN, łączysz się z routerem Twojego dostawcy usługi, który chroni Twój własny router i ukrywa Twój prawdziwy adres IP, który jest w Internecie jak odcisk Twojego palca! Łącząc się z siecią za pomocą VPN, jedynym widocznym źródłem połączenia, jest po prostu któryś z routerów dostawcy VPN, a tych jest wiele… Dla cyberprzestępców, pozostajesz więc niemożliwym do namierzenia i do zidentyfikowania celem.

VPN szyfruje każdy Twój krok, który stawiasz online. Szyfruje wszystko, co przeglądasz, co wysyłasz i co odbierasz. Jak działa szyfrowanie? Polega ono na zamianie czytelnego tekstu na nieczytelny kod. Rodzajów szyfrowania jest kilka i choć każdy z nich, ma swoje plusy i minusy, to każdy zapewnia skuteczne zniekształcenie danych tak, aby nikt nie mógł ich wykorzystać.



Większość dostawców VPN oferuje również dodatkowe zabezpieczenia, jakimi są własne systemy Domain Name System. DNS to system identyfikacji nazw, który jest czymś w rodzaju internetowej książki telefonicznej. Taki spis zawiera tekstowe adresy URL i powiązane z nimi odpowiednie adresy IP. Wystarczy podać samą nazwę strony, zamiast ciągu cyfr. Cyberprzestępcy mogą obserwować DNS i śledzić Twoją aktywność. Jednak system sieci VPN, używając dodatkowego szyfrowania, może skutecznie zablokować i te działania.

3.3 Co można zrobić z VPN?

VPN ukrywa przed innymi użytkownikami, którzy aktualnie korzystają z tej samej sieci, wszystko to, co robisz. Dzięki temu, możesz swobodnie korzystać ze swojej poczty, a nawet sprawdzać stan konta, bez obawy o wyciek danych.

Na pewno wiesz, że nie poleca się korzystania bez ochrony, z publicznych połączeń Wi-Fi, które dla hakerów i cyberprzestępców, są niczym wesołe miasteczko z niezliczoną ilością atrakcji! Tam, wyjątkowo łatwo można nas wyśledzić, jednak dzięki VPN, takie działania stają się niemożliwe. Również, kiedy ściągasz jakiekolwiek pliki, jesteś narażony na atak wielu złośliwych programów szpiegujących – nie z usługą VPN! VPN sprawi, że malware, nie mogąc Cię namierzyć – totalnie zgłupieje!

3.4 Dlaczego potrzebujesz sieci VPN?

W tej chwili, kiedy wiesz już jak działa sieć VPN, pytanie, czy w ogóle jej potrzebujesz, jest zupełnie zbędne. Odpowiedź jest tylko jedna i klarowna! Oczywiście, że jej potrzebujesz! Co więcej, jest Ci niezbędna! Sieci VPN są obecnie wyjątkowo potrzebne! Zgodnie z niedawną zmianą przepisów i postanowieniem Federalnej Komisji Łączności, Twój dostawca Internetu może obecnie, całkowicie swobodnie udostępniać Twoje dane osobowe, Twoją lokalizację, historię przeglądania stron i wszystkie inne informacje, które na Twój temat posiada. Sieć VPN, która uniemożliwia śledzenie Twoich działań, zagwarantuje Ci całkowitą prywatność, nawet względem Twojego dostawcy Internetu! Korzyści, wynikające z używania VPN są ogromne i każdego dnia tylko przybierają na sile.

3.5 Protokoły VPN

PPTP VPN

Skrót PPTP VPN oznacza Tunneling Protocol Point-to-Point. Podobnie jak wskazuje jego nazwa, PPTP VPN tworzy tunel i przechwytuje wysyłane dane. Dość długa nazwa dla najczęściej używanego rodzaju VPN. PPTP VPN jest wykorzystywany przez użytkowników zdalnych, aby podłączyć się do sieci VPN z wykorzystaniem dotychczasowego połączenia internetowego. Jest to przydatny protokół VPN zarówno dla użytkowników biznesowych, jak i użytkowników domowych. Aby uzyskać dostęp do sieci VPN użytkownicy logują się do VPN za pośrednictwem atestowanego hasła. PPTP VPN jest idealny do użytku osobistego i biznesowego, ponieważ nie wymaga zakupu i instalacji dodatkowego sprzętu, a funkcje zazwyczaj oferowane jako niedrogie dodatkowe

oprogramowanie. PPTP VPN to najpowszechniej stosowany protokół także ze względu na kompatybilność z systemami Windows, Mac i Linux.

Chociaż wydaje się, że PPTP VPN ma wiele zalet, to są także wady tej sieci VPN. Wadą korzystania z PPTP VPN jest to, że nie zapewnia on szyfrowania, którego zazwyczaj chcemy korzystając z VPN. Inną wadą jest to, że opiera się na protokołach PPP lub Point to Point Protocol w celu wdrożenia środków bezpieczeństwa.

Site-to-Site VPN

VPN typu Site-to-Site jest również nazywany VPNem typu Router-to-Router i jest stosowany głównie w zastosowaniach korporacyjnych. Fakt, że wiele firm ma swoje biura zlokalizowane zarówno w kraju jak i za granicą powoduje, że VPN Site-to-Site służy do podłączenia do głównej sieci lokalnych sieci wielu biur. Ten system znany jest również jako VPN oparty o Intranet. Odwrotne rozwiązanie jest również możliwe przy użyciu Site-to-Site VPN. Firmy wykorzystują taki rodzaj VPN, aby połączyć się z innymi firmami w ten sam sposób, co jest klasyfikowane jako Extranet VPN. W prostych słowach Site-to-Site VPN pozwala zbudować wirtualny most, który łączy sieci w różnych miejscach w celu podłączenia ich do internetu i utrzymania bezpiecznej i prywatnej komunikacji między tymi sieciami.

Podobny do tego z PPTP VPN, VPN Site-to-Site działa na rzecz stworzenia bezpiecznej sieci. Jednak brak jest dedykowanej linii w użyciu, pozwalając różnym lokalizacjom w obrębie firmy, jak już wspomniano, utworzyć połączenie VPN. Ponadto w odróżnieniu od PPTP, routing, szyfrowanie i deszyfrowanie odbywa się przez router sprzętowy lub oprogramowanie na obu końcach.

L2TP VPN

L2TP oznacza Layer to Tunneling Protocol, który został opracowany przez firmę Microsoft i Cisco. VPN L2TP to VPNy, które zwykle wykorzystują także inny protokół bezpieczeństwa VPN do stworzenia bardziej bezpiecznego połączenia VPN. L2TP VPN tworzy tunel pomiędzy dwoma punktami połączeń L2TP VPN, a inny protokół taki, jak IPsec szyfruje dane i koncentruje się na zapewnieniu komunikacji między tunelami.

L2TP jest podobne do PPTP. Podobieństwa istnieją pod względem braku szyfrowania i tego, że oba opierają się na protokole PPP. Zaczynają się różnić w odniesieniu do poufności danych i ich integralności. L2TP VPN zapewniają obie opcje, podczas gdy PPTP VPN.

IPsec

IPsec jest skrótem od Internet Protocol Security. IPsec VPN to protokół używany w celu zabezpieczenia komunikacji internetowej w sieci IP. Tunel jest skonfigurowany w zdalnym miejscu tak, by umożliwić Ci dostęp do serwera centralnego. IPSec działa w celu zabezpieczenia komunikacji protokołu internetowego poprzez sprawdzenie każdej sesji i indywidualnie szyfruje pakiety danych w całym połączeniu. Istnieją dwa tryby, w których działa IPsec VPN. Są to Tryb transportu i Tryb tunelowania. Oba tryby służą do ochrony transferu danych pomiędzy dwoma różnymi sieciami. W trybie transportu komunikat w pakiecie danych jest szyfrowany. W trybie tunelowym, cały pakiet danych jest szyfrowany. Jedną z zalet korzystania z IPSec jest to, że można także stosować go w dodatku do innych protokołów bezpieczeństwa w celu zapewnienia silniejszego systemu bezpieczeństwa.

Mimo, że jest to wartościowa technologia VPN, to ma jednak wielką wadę polegającą na tym, że wykorzystanie tego protokołu jest czasochłonne i wymaga czasochłonnej instalacji klienta, która musi nastąpić przed rozpoczęciem użytkowania.

SSL oraz TLS

SSL to skrót od Secure Sockets Layer, a TLS to skrót od Transport Layer Security. Oba funkcjonują jako jeden protokół. Oba są wykorzystywane do budowy połączenia VPN. Jest to połączenie sieci VPN, w którym przeglądarka służy jako klient, a użytkownik jest ograniczony do specyficznych zastosowań, zamiast korzystać z całej sieci. SSL i TLS protokoły wykorzystywane głównie przez internetowe witryny handlowe i usługodawców. SSL i TSL VPN zapewniają Ci bezpieczne sesje z przeglądarki na komputerze do serwera aplikacji. To dlatego, że przeglądarki internetowe potrafią łatwo włączyć obsługę SSL i nie wymagają praktycznie żadnego działania ze strony użytkownika. Przeglądarki internetowe są już zintegrowane z SSL i TSL. Połączenia SSL mają ciąg https na początku adresu URL zamiast http.

MPLS VPN

Multi-Protocol Label Switching lub VPN MPLS to najlepsze wykorzystanie do połączeń typu Site-to-Site. Jest to przede wszystkim spowodowane faktem, że MPLS to najbardziej elastyczne i wygodne rozwiązanie. MPLS to standardowa baza zasobów, która służy do przyspieszenia rozkładu pakietów w sieci dla wielu protokołów. VPN MPLS to systemy, które są dostrojone przez ISP. VPN dostrojony przez ISP ma miejsce wtedy,, gdy dwie lub więcej stron są

połączone tworząc sieć VPN przy użyciu tego samego ISP. Jednak największą wadą użycia MPLS VPN jest fakt, że sieć nie jest tak łatwa do skonfigurowania w porównaniu z innymi VPN. Nie jest to również łatwa sieć do modyfikacji. Zatem VPN MPLS są zwykle droższe.

VPN hybrydowy

VPN hybrydowy łączy w sobie zarówno MPLS oraz protokół IP Sec lub VPN oparty o IPsec. Ale te dwa typy sieci VPN są stosowane oddzielnie w różnych lokalizacjach. Jednak możliwe jest stosowanie ich obu w tym samym miejscu. Robi się to z zamiarem wykorzystania VPN IPsec, jako kopii zapasowej dla MPLS VPN.

IPsec VPN to VPN, który wymaga trochę sprzętu po stronie klienta, jak wspomniano wcześniej. Urządzenie to zazwyczaj ma postać routera lub uniwersalnego urządzenia zabezpieczającego. Za pomocą routera lub uniwersalnego urządzenia zabezpieczającego dane są szyfrowane, tworząc tunel VPN, jak omówiono powyżej. Z kolei VPN MPLS są wykorzystywane przez operatora, za pomocą urządzeń w jego sieci.

W celu połączenia tych dwóch sieci VPN ustanowiona zostaje brama w celu wyeliminowania tunelu IPSec na jednej stronie i przekierowuje go do MPLS VPN na drugim końcu, przy jednoczesnym zachowaniu bezpieczeństwa VPN.

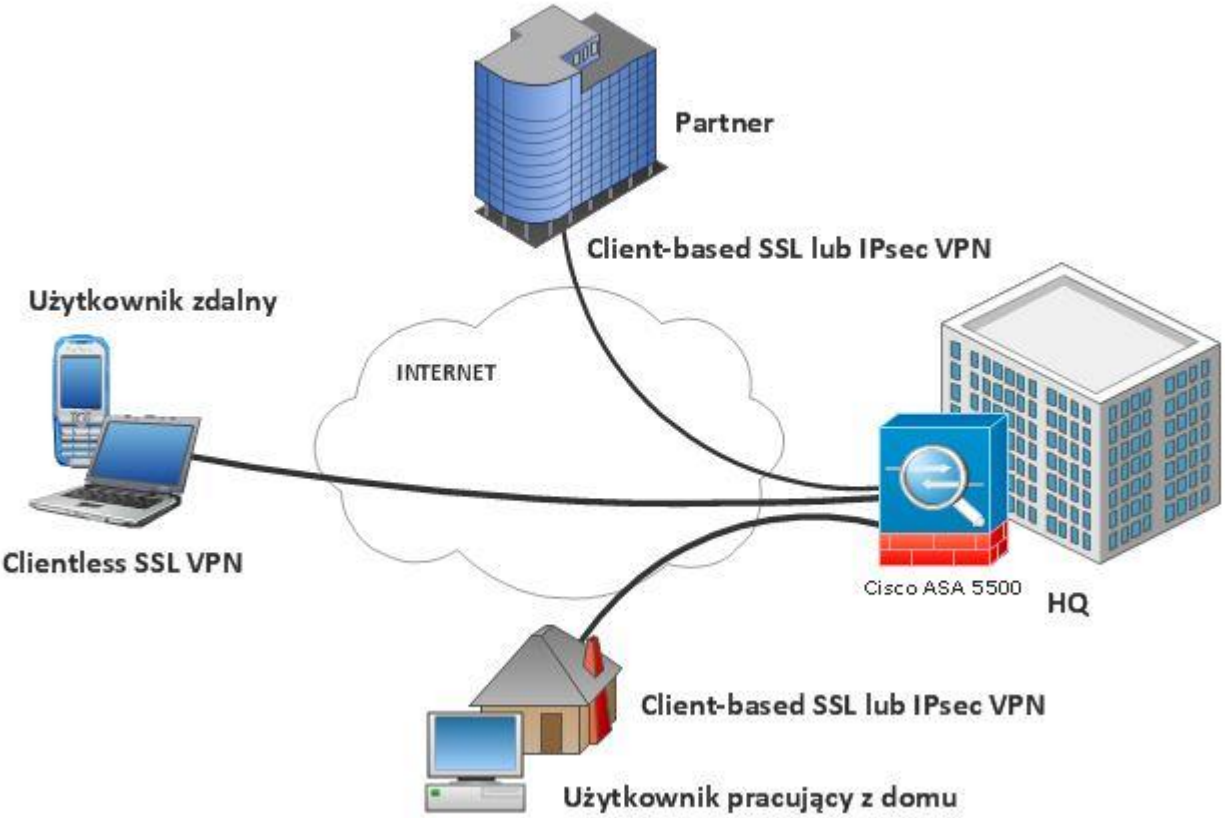
VPN hybrydowe są wykorzystywane przez firmy głównie dlatego, że używanie MPLS w swoich lokalizacjach nie byłoby najwłaściwszym wyborem. Istnieje ogromna ilość zalet, które posiada MPLS w porównaniu do publicznych połączeń internetowych, jednak koszt jest wysoki. Dlatego stosując hybrydowe VPN można uzyskać dostęp do centralnej lokalizacji z odległego miejsca. Hybrydowe VPN są ogólnie kosztowne jednak oferują większą elastyczność.

3.6 Typy sieci VPN

Istnieją dwa główne typy VPN:

1. **Remote Access VPN** – bezpieczne połączenie z siecią serwerów dostawcy VPN, które umożliwiają dalszy dostęp do publicznego Internetu; najczęściej używane przez: użytkowników domowych, małe i średnie firmy; łatwe w konfiguracji i utrzymaniu; typowe zastosowanie: dostęp do treści z ograniczeniami geograficznymi, bezpieczne połączenie z siecią biurową podczas podróży służbowych (nawet poprzez publiczne Wi-Fi).
2. **Site-to-Site VPN** (Router-to-Router VPN) – bezpieczne połączenie między sieciami prywatnymi danej organizacji (Intranet) lub między jej siecią prywatną a partnerami

zewnętrznymi (Extranet); najczęściej używane przez: duże podmioty (takie jak korporacje lub organizacje rządowe), wymagające konfiguracji i utrzymania, wymagają znacznych zasobów; typowe zastosowanie: korzystanie z centralnej sieci organizacji z innej lokalizacji geograficznej (może to być inne miasto, kraj, kontynent itp).



3.7 Metody uwierzytelnienia w sieci VPN

Zanim zostanie zestawiony wirtualny „tunel" VPN, obie strony musza się wzajemnie uwierzytelnić, aby mieć pewność, że urządzenie po drugiej stronie tunelu jest tym, za kogo się podaje.

Istnieją trzy metody uwierzytelniania:

1. hasło statyczne, klucze współdzielone (pre-shared key): W trakcie przygotowywania do pracy urządzenia klucz wpisuje się bezpośrednio do pliku konfiguracyjnego. Metody tej nie poleca się z uwagi na łatwość popełnienia pomyłki w trakcie konfiguracji, możliwość podszycia się trzeciej strony w przypadku kompromitacji klucza a także z

przyczyn administracyjnych (problematyczne jest zarzadzanie połączeniami w obrębie kilku czy kilkunastu urządzeń)

2. klucze publiczne RSA: Na każdym z urządzeń biorących udział w połączeniu generowana jest para kluczy: prywatny-publiczny. Klucze publiczne należy następnie wymienić ze wszystkimi uczestnikami połączenia. W procesie tym bierze udział człowiek, który musi „ręcznie" dokonać wymiany kluczy. Rozwiązanie to jest praktycznie nieskalowalne, przy większej liczbie urządzeń konieczne jest dokonanie N*(N-1) wymiany kluczy, co jest czasochłonne. Dodatkowo w przypadku kompromitacji jednego z urządzeń należy wykasować stare i wgrać nowe klucze na pozostałych urządzeniach.
3. certyfikaty cyfrowe: (ze względu na swoja strukturę stanowią najbardziej zaufany mechanizm uwierzytelniania, możliwe jest zautomatyzowanie procesu ich wymiany w przypadku kompromitacji jednej ze stron. Ta metoda uwierzytelniania cechuje się również skalowalnością. Przy „N" stronach biorących udział w połączeniu konieczne jest „N" uwierzytelnień i „N" certyfikatów)

3.8 Certyfikaty cyfrowe

Przez „certyfikat" rozumiemy dane podpisane cyfrowo przez tzw. „zaufaną trzecią stronę". Dane, o których mowa zawierają zazwyczaj następujące informacje:

- Klucz publiczny właściciela certyfikatu.
- Nazwę zwyczajowa (np. imię i nazwisko, pseudonim, etc.)
- Nazwę organizacji.
- Jednostkę organizacyjna.
- Zakres stosowania (podpisywanie, szyfrowanie, autoryzacji dostępu itp.)
- Czas, w jakim certyfikat jest ważny.
- Informacje o wystawcy certyfikatów.
- Sposób weryfikacji certyfikatu (np. adres, pod którym można znaleźć listy CRL).
- Adres, pod którym znajduje się polityka certyfikacji, jaka zastosowano przy wydawaniu tego certyfikatu.

Struktura certyfikatu nie jest sztywna i w zależności od potrzeb można umieszczać w niej dodatkowe pola, wykraczające poza definicje standardu.

Zastosowanie certyfikatów cyfrowych

W rozwiązaniach dla sieci VPN certyfikat stanowi element uwierzytelniający każdą ze stron biorących udział w połączeniu. Dzięki temu rozwiązaniu podszycie się pod jedna ze stron biorących udział w połączeniu jest wysoce nieprawdopodobne.

Sposób uzyskania certyfikatu dla urządzeń VPN

Ogólny zarys czynności, które należy wykonać, by urządzenia służące do zestawienia połączeń VPN mogły autoryzować się przy użyciu certyfikatów przedstawione są w kolejnych krokach:

1. Przy użyciu urządzenia generowana jest para kluczy RSA (tj. klucz publiczny i klucz prywatny),
2. Urządzenie generuje zbiór danych w standardzie PKCS10, który zawiera jego dane identyfikacyjne oraz publiczny klucz RSA,
3. Klucz publiczny jest przekazywany do urzędu certyfikacji (za pośrednictwem stosowanego formularza),
4. Urząd certyfikacji po zweryfikowaniu pliku PKCS10 podpisuje go swoim kluczem prywatnym RSA (wystawia certyfikat),
5. Urządzenie pobiera wystawiony certyfikat cyfrowy, jak również listę CRL i certyfikat urzędu z danego urzędu certyfikacji.

4. Oprogramowanie

Efektywne korzystanie z sieci VPN zależy nie tylko od jej funkcjonalności, wykupionego planu lub konfiguracji na określonym urządzeniu. Oprócz kwestii niematerialnych, ważne są również aspekty techniczne, dzięki którym używanie VPN będzie nie tylko skuteczne, ale również proste.

Każda sieć VPN powinna zostać odpowiednio skonfigurowana na urządzeniu, na którym ma działać. Niezależnie czy jest to komputer stacjonarny, telefon, telewizor, router czy laptop, uruchomienie VPN wymagać będzie pobrania odpowiedniego programu, jego instalacji oraz

dokonania potrzebnych ustawień. Program VPN to nic innego jak aplikacja, udostępniona przez dostawcę usługi, za pośrednictwem której możesz sterować swoją siecią VPN.

Pobranie i instalacja programu do VPN jest bardzo prosta i niczym nie różni się od pobrania i instalacji innego programu, jak chociażby popularnego komunikatora Skype lub Viber. Ze strony dostawcy sieci VPN należy ściągnąć odpowiednią aplikację, a później postępować według wskazówek.

Kluczem do sukcesu jest wybór właściwego programu – na każde urządzenie powinieneś pobrać inny. VPN client (client = program) ściśle współpracuje z systemem operacyjnym danego urządzenia, dlatego ważny jest nie tylko rodzaj sprzętu, ale przede wszystkim jego główne oprogramowanie. Na każdy system operacyjny dostępny jest inny program do VPN, dlatego jeśli masz Windowsa, wybierz program VPN dla Windows, jeśli MacOS (na sprzętach Apple – Macbookach, iMac, Mac Mini, Mac Pro), to VPN dla MacOS, jeśli Linuxa, to VPN dla Linuxa, jeśli Androida, to VPN dla Androida, jeśli iOS na iPhone lub iPadOS na iPadzie, to VPN dla iPhona i iPada, itd. Opcja VPN download jest w standardzie u niemal każdego dostawcy usług VPN.

Na rynku dostępne są darmowe programy VPN i płatne abonamenty. Różnice między nimi dotyczą nie tylko zakresu usługi i obecności lub braku limitów, ale również funkcjonalności samego programu. Opcje darmowe zwykle są bardzo ograniczone. Większość dostawców VPN to dostawcy spoza Polski, dlatego niewiele bezpłatnych programów VPN jest dostępnych w języku polskim. Jeśli słabo znasz angielski, to będzie dla Ciebie duży problem. Obsługa takiego programu może też być utrudniona ze względu na poziom zaawansowania i skomplikowany interfejs – dostawcy rzadko dbają o przejrzystość. Dodatkowo zwróć uwagę także na samą jakość usług. Darmowe VPN wykorzystują mniej zaawansowane protokoły szyfrujące, dlatego poziom bezpieczeństwa i ochrony danych jest mniejszy, niż w przypadku usług płatnych, zapewniających dostęp do najlepszych protokołów bezpieczeństwa. Ponadto, niektóre z nich działają bardziej jak program do zmiany IP, niż jako pełnoprawny program VPN. Jeżeli dołożysz do tego małą, ograniczoną liczbę serwerów, limity transferu i przepustowości oraz fakt, że za dostęp do tych programów zapłacisz swoimi danymi osobowymi zamiast pieniędzmi, to “bezpłatne” opcje przestają być tak bardzo atrakcyjne.

Większą funkcjonalnością cechują się programy płatnych sieci VPN. Są łatwiejsze w obsłudze, bardziej intuicyjne i dopracowane. Niezależnie od stopnia zaawansowania poradzisz

sobie z ich instalacją i konfiguracją. Często otrzymasz też możliwość zmiany języka (nie zawsze na polski, ale na pewno inny niż angielski) oraz dostęp do tutoriali.

Programy płatne zapewniają:

- większe bezpieczeństwo,
- lepszą ochronę danych,
- bardziej zaawansowane protokoły bezpieczeństwa,
- możliwość wyboru serwerów z pełnej puli danego dostawcy,
- nieograniczoną przepustowość,
- nieograniczony transfer,
- możliwość dopasowania programu do własnych preferencji.

W porównaniu do opcji bezpłatnych, płatny VPN program zapewnia więc większą użyteczność, funkcjonalność i wydajność.

#	DOSTAWCA	CENA	FUNKCJE	OCENA	ZNIŻKA	WIĘCEJ
1	NordVPN	€2.97 ZA MIESIĄC	• 5100+ lokalizacji w 59 krajach • Windows, Mac, Linux, Android, iOS, Routrery • Max. 6 urządzeń • OpenVPN, PPTP, L2TP/IPSec • 30-dniowa gwarancja zwrotu	★★★★★	-68% Przy płatności na 2 lata z góry	Zobacz stronę Recenzja NordVPN
2	Surfshark®	€2.10 ZA MIESIĄC	• 3200+ serwerów w 65 krajach • Windows, Mac, Linux, Android, iOS, Routrery • Nieograniczona liczba urządzeń • OpenVPN, PPTP, L2TP/IPSec • 30-dniowa gwarancja zwrotu	★★★★★	-81% Przy płatności na 2 lata z góry	Zobacz stronę
3	PUREVPN	€2.96 ZA MIESIĄC	• 3200+ lokalizacji w 140+ krajach • Windows, Mac, Linux, Android, iOS, Routrery • Max. 10 urządzeń • OpenVPN, PPTP, L2TP/IPSec • 31-dniowa gwarancja zwrotu	★★★★★	-70% Przy płatności na 2 lata z góry	Zobacz stronę Recenzja PureVPN
4	ExpressVPN	$8.32 ZA MIESIĄC	• 160+ lokalizacji w 94+ krajach • Windows, Mac, Linux, Android, iOS, Routrery • Max. 3 urządzenia • OpenVPN, PPTP, L2TP/IPSec • 30-dniowa gwarancja zwrotu	★★★★★	-35% Przy płatności na rok z góry	Zobacz stronę Recenzja ExpressVPN
5	IPVANISH VPN	$3.75 ZA MIESIĄC	• 1500+ lokalizacji w 75+ krajach • Windows, Mac, Linux, Android, iOS, Routrery • ∞ urządzeń • OpenVPN, PPTP, L2TP/IPSec • 30-dniowa gwarancja zwrotu	★★★★½	-50% Przy płatności na rok z góry	Zobacz stronę Recenzja IPVanish

Programy darmowe:

- ProtonVPN https://protonvpn.com
- Windscribe https://windscribe.com
- TunnelBear https://www.tunnelbear.com
- Hide.me https://hide.me/en/
- HotspotShield https://www.hotspotshield.com
- Speedify https://speedify.com
- Opera https://www.opera.com/pl/

4.1 Program CyberGhost – płatny w pełnej wersji

Program łączy się z zewnętrznym serwerem VPN, szyfrując wszystkie wysyłane i pobierane za pośrednictwem naszego komputera dane. Praca z CyberGhost VPN odbywa się w dwóch etapach - najpierw nawiązywane jest połączenie przy użyciu 1024-bitowego szyfrowania SSL, a następnie wszelaki transfer danych odbywa się z wykorzystaniem 256-bitowego prywatnego klucza AES. Zapewnia to niemal 100-procentową ochronę przed podsłuchem, a także zabezpiecza przed odczytem naszego adresu IP na odwiedzanych stronach. Co najwyżej odczytany zostanie adres serwera VPN, z którym wcześniej się połączyliśmy.

Kluczowe cechy programu:

- niewielkie narzędzie do ochrony prywatności,
- umożliwia ukrywanie IP i anonimowe surfowanie w sieci,
- oferuje ochronę cyfrowej tożsamości,
- pozwala ominąć ograniczenia regionalne,
- umożliwia anonimowe korzystanie z sieci torrent,
- ochrona danych podczas korzystanie z publicznych sieci.

4.2 Program ProtonVPN - darmowy

Szwajcarski VPN stworzony przez entuzjastów bezpieczeństwa online to prawdopodobnie jeden z najlepszych bezpłatnych VPN. Dostępny jest również w płatnej wersji, choć funkcje darmowej są nadal imponujące. ProtonVPN wyposażony jest w protokoły OpenVPN oraz IKEv2. W połączeniu z szyfrowaniem AES-256, są one gwarancją tego, że żaden cyberprzestępca nie wykradnie Twoich haseł. Jeżeli chodzi o politykę zera logów, to ProtonVPN w stu procentach ją egzekwuje i na ich stronie można przeczytać, że firma nie zapisuje nigdzie poufnych danych na Twój temat. Wszelkie problemy i pytania związane z działaniem programu można kierować do supportu. Co prawda ProtonVPN nie oferuje live chatu, ale nie można narzekać na kontakt mailowy. Zwykle rzeczową odpowiedź dostajemy w mniej niż 20 godzin. Często zdarza się, że darmowy VPN przepuszcza DNS oraz Web-RTC. W Proton VPN nie ma o tym mowy. Działanie Netflixa poprzez ProtonVPN nie jest tak oczywiste, a na pewno nie jest to możliwe w darmowej wersji. Instalacja jak i konfiguracja programu jest banalna, a sam interfejs wygląd bardzo nowocześnie. Szybkość serwerów jak na darmowy VPN jest dobra. Lepszej prędkości możemy się spodziewać po zakupie pełnej wersji. Darmowa trwa 7 dni i możecie dzięki niej przetestować działanie programu. Dostępny na: Windows, Apple, Android, Linux

5. Sieci VPN na routerze

Chociaż większość ludzi instaluje VPN na swoim komputerze lub telefonie, to jednak wielu nie wie o tym, że można zainstalować VPN także i na routerze. Routery działają zazwyczaj na poziomie warstwy sieciowej, więc posiadanie sieci VPN zainstalowanej na routerze zapewnia zabezpieczenie dowolnego urządzenia w sieci, szyfrowany ruch i przekierowuje dodatkowo wszystkie urządzenia przez inny kraj. Jeśli chcesz korzystać z VPN na wielu urządzeniach, najlepszym rozwiązaniem może być po prostu zainstalowanie tej usługi na swoim routerze. Chociaż początkowo wymagane jest nieco więcej pracy, cały proces jest dość prosty.

Wystarczy wykonać trzy proste kroki: pierwszym z nich jest zarejestrowanie się w sieci VPN u renomowanego dostawcy usług. Drugim jest zainstalowanie oprogramowania sprzętowego (firmware) DD-WRT na routerze (tzw. flashowanie). Ostatnim krokiem jest skonfigurowanie klienta VPN na routerze gotowym do pracy z oprogramowaniem DD-WRT w celu połączenia się z usługą VPN.

Dlaczego warto ustawić VPN na routerze?

Skoro wiemy już jak korzystać z VPN, jak skonfigurować VPN i jak ustawić VPN na routerze, dowiedzmy się jeszcze, dlaczego warto to zrobić. Korzyści jest wiele. Sieć VPN na routerze pozwala nam:

1. Zmienić IP i ominąć blokady regionalne – Dzięki zmianie IP możesz uzyskać dostęp do stron, usług i materiałów, które są zablokowane w danym kraju. Wystarczy zmienić swoją lokalizację, aby z powodzeniem ominąć wszelkie blokady regionalne. Polska nie ma licencji na dostęp do interesujących Cię materiałów? Przekieruj sieć na kraj, który ją ma i oglądaj!
2. Zapewnić sobie bezpieczeństwo w sieci – Nie tylko sieci publiczne narażają nas na kradzież danych i cyberataki. Używając sieci domowej, również nie możemy czuć się do końca bezpieczni. Publiczna sieć Wi-Fi jest dla hakera wesołym miasteczkiem z bezproblemowym dostępem do wszystkich atrakcji – sama przyjemność! Zabezpieczenia sieci domowej bez dobrego antywirusa porównajmy do zadania na poziomie szkoły podstawowej – odrobina zachodu, ale wysiłek niewielki! Kradzież danych, które chronione są przez sieć VPN to natomiast próba rozszczepienia atomu przez humanistę! – rzecz tak trudna, że praktycznie niemożliwa!
3. Zapewnić sobie nieprzerwaną ochronę – Jeśli VPN szyfruje połączenie routera z internetem, to każde urządzenie połączone z routerem również jest automatycznie chronione. Zapewnia to bezpieczeństwo wszystkim urządzeniom jednocześnie i chroni też każde nowe urządzenie. Oznacza to, że nie tracimy ochrony nawet przy zmianie sprzętu.

5.1 Rejestracja u dostawcy usług VPN

Zanim zaczniesz, musisz jednak wykupić renomowaną usługę VPN. Router będzie podłączony do tej usługi po przygotowaniu go do pracy z oprogramowaniem DD-WRT. Potrzebujesz dobrej, godnej zaufania usługi VPN, tak samo, jak dobrego routera.

Powinieneś poszukać dostawcy VPN, którego warunki świadczenia usług pozwalają na instalację oprogramowania na routerze, a jednocześnie oferuje on nieograniczoną przepustowość bez ogólnego ograniczania pasma lub specyficznego dla różnych usług dławienia przepustowości, a także oferującego wiele węzłów wyjściowych w kraju, z którego chcesz się połączyć.

Po zakończeniu procesu rejestracji otrzymasz powitalną wiadomość e-mail od dostawcy swojej sieci VPN z dostępem do dedykowanego konta przy użyciu wybranej nazwy użytkownika i hasła. Na potrzeby tego przewodnika będziemy używać ExpressVPN.

5.2 DD-WRT

DD-WRT jest zasadniczo firmware dla routerów bezprzewodowych i punktów dostępowych. To oprogramowanie działa w systemach operacyjnych Linux i jest kompatybilne z innymi routerami. Głównym zadaniem firmware DD-WRT jest zastąpienie istniejącego firmware w routerze, które zostało stworzone przez producenta routera. To oprogramowanie jest w stanie dodać nowe funkcje, które nie były obecne do tej pory, a które zwiększają funkcjonalność routera.

DD-WRT obsługuje funkcje takie jak system dystrybucji IPv6, zaawansowany poziom Quality of Service, sterowanie mocą wyjściową i usługi oparte o demony. Istnieje również pewne wsparcie oprogramowania dla kart SD. Wiele firm już zaczęło wysyłać swoje routery z firmware DD-WRT, ale jest to dostosowana wersja firmware, która może spełnić potrzeby użytkownika.

5.3 Instalacja oprogramowania DD-WRT na Twoim routerze

Zainstalowanie DD-WRT na routerze pozwoli mu działać jako klient VPN, który umożliwi Ci połączenie z serwerem VPN za jego pośrednictwem. DD-WRT to alternatywne oprogramowanie open source odpowiednie dla szerokiej gamy routerów bezprzewodowych (WLAN) i punktów dostępu firm takich jak D-Link, TP-Link, Linksys, Netgear, Asus i innych. Został zaprojektowany jako ulepszony zamiennik oprogramowania fabrycznego (OEM), zapewniając jednocześnie wiele dodatkowych możliwości. Możesz myśleć o DD-WRT jako specjalnym oprogramowaniu, które obsługuje Twój router.

Oprogramowanie to umożliwia również konfigurację na nim usługi ExpressVPN. Bez wbudowanego oprogramowania DD-WRT niemożliwe jest skonfigurowanie usługi VPN na routerze. Aktualizacja firmware routera do DD-WRT znosi wiele ograniczeń wbudowanych w domyślne oprogramowanie układowe i przekształca Twój router w wydajne urządzenie klasy biznesowej z zaawansowanymi funkcjami, w tym obsługą OpenVPN (protokołu znanego z silnych algorytmów szyfrowania i szyfrów).

Jeśli Twój istniejący router nie jest fabrycznie wyposażony w DD-WRT, musisz zainstalować to oprogramowanie samemu w procesie zwanym flashowaniem. Jest to proste zadanie, ale może okazać się także bardzo trudne; wykonanie go niepoprawnie może w efekcie dać Ci

router, który nadaje się tylko do wyrzucenia. Należy pamiętać, że flashowanie routera za pomocą firmware innego producenta może spowodować unieważnienie gwarancji na urządzenie (jeśli jeszcze ona obowiązuje). Zapoznaj się z polityką gwarancyjną dotyczącą tego urządzenia. W zależności od specyfikacji sprzętowej routera może wystąpić również obniżenie prędkości Internetu podczas korzystania z połączenia VPN ze względu na niewielką moc procesora routera wymaganą do przetwarzania szyfrowania VPN. Przed rozpoczęciem procesu flashowania należy najpierw sprawdzić, czy dla danego routera dostępna jest odpowiednia wersja oprogramowania DD-WRT. Po drugie, należy także pamiętać o następujących wymaganych warunkach wstępnych przed aktualizacją firmware swojego routera:

1. Nie aktualizuj oprogramowania sprzętowego routera za pośrednictwem bezprzewodowego połączenia z Internetem, korzystaj wyłącznie z połączenia przewodowego.
2. Wykonaj twardy reset na routerze, zanim uaktualnisz oprogramowanie zgodnie z "procedurą 30/30/30".
3. O ile nie określono inaczej, użyj przeglądarki Internet Explorer, aby uzyskać dostęp do interfejsu administratora routera.

Procedura 3 x 30:

- 1×30 – naciśnij przycisk zasilania i trzymaj przez 30 sekund,
- 2×30 – odepnij router od zasilania na 30 sekund,
- 3×30 – ponownie przytrzymaj przycisk przez 30 sekund.

Po spełnieniu tych niezbędnych wymagań można rozpocząć proces instalacji oprogramowania DD-WRT. Jeśli nie lubisz instalować DD-WRT na routerze, możesz kupić gotowy (wstępnie zainstalowany) router gotowy do pracy z DD-WRT. Choć zazwyczaj są one droższe, niż zwykłe routery, to jednak firmy Buffalo Technology, Netgear, Asus i Linksys oferują wstępnie zainstalowane spersonalizowane wersje oprogramowania sprzętowego DD-WRT dla niektórych z routerów ze swojej oferty.

5.4 Konfiguracja klienta VPN na routerze DD-WRT

Po zakończeniu instalacji DD-WRT na routerze, następnym krokiem jest skonfigurowanie klienta OpenVPN na tym urządzeniu, aby umożliwić mu łączenie się z usługą VPN lub serwerem. Istnieją dwa możliwe sposoby osiągnięcia tego: metoda GUI i metoda skryptowa. W tym przewodniku użyjemy metody wykorzystującej interfejs GUI, która jest zalecana dla większości użytkowników. Wykonaj poniższe kroki, aby skonfigurować klienta VPN na routerze DD-WRT:

1. Przejdź do witryny dostawcy sieci VPN i zaloguj się do swojego konta VPN, aby pobrać pliki instalacyjne.
2. Kliknij odnośnik do plików konfiguracyjnych DD-WRT.OVPN. Na Twój komputer zostanie pobrany cały folder zawierający pełną listę lokalizacji serwerów ExpressVPN. Po pobraniu rozpakuj zawartość tego folderu.
3. Teraz otwórz interfejs administracyjny routera. Możesz to zrobić wpisując adres IP routera w pasku adresu swojej przeglądarki. Jeśli nie masz pewności co do tego adresu, zapoznaj się z dokumentacją routera w celu poznania jego domyślnego adresu IP.
4. Po pierwsze musisz skonfigurować ustawienia sieciowe, aby upewnić się, że Twój router DD-WRT może łączyć się z Internetem. Adres IP musi należeć do innej klasy sieci niż jakikolwiek inny router w Twojej sieci. Aby skonfigurować ustawienia sieciowe, przejdź do menu Setup -> Basic Setup, w opcji „WAN Connection Type" ustaw „Automatic Configuration – DHCP" i podaj routerowi DD-WRT stały lokalny adres IP w polu „Network Setup", jak pokazano na poniższej grafice. W sekcji Network Address Server Settings (DHCP) ustaw następujące adresy DNS ExpressVPN:
    - Static DNS 1 = 162.242.211.137
    - Static DNS 2 = 78.46.223.24
    - Static DNS 3 = 0.0.0.0 (domyślnie)
    - Use DNSMasq for DHCP = zaznaczone
    - Use DNSMasq for DNS = zaznaczone
    - DHCP-Authoritative = zaznaczone

Instrukcja: https://pl.vpnmentor.com/blog/jak-zainstalowac-vpn-na-swoim-routerze/

6. Przykładowe Routery DD-WRT

Routery, które są dostępne na rynku przeznaczone są dla zwykłego użytkownika, więc producenci starają się zapewnić, aby wszystko było proste, od podłączenia do skonfigurowania. Chociaż to jest dobre rozwiązanie patrząc na to z tego punktu widzenia, ale może też ograniczyć rzeczy, jakie można zrobić za pomocą takiego routera. Uzyskaj router, który ma fabrycznie zainstalowane firmware DD-WRT i odblokuj jego prawdziwy potencjał. Oto niektóre z najlepszych routerów DD-WRT, jakie można kupić.

Netgear Nighthawk R7000 – cena ok. 800,00

Jest to jeden z najlepszych routerów DD-WRT w swojej klasie. Dzięki wydajnemu procesorowi dostaniesz wysoką szybkość ponieważ może on szyfrować i odszyfrować ruch VPN bez żadnych przeszkód. anteny zapewniają mocny sygnał w całym domu. Kolejną cechą, która sprawia, że się on wyróżnia jest jego szybkość transferu 1900 Mbps i i łączność USB 3.0.

Asus RT-AC66U – cena ok. 450,00

Asus RT-AC66U ma najlepszy rozmiar pamięci Flash, co oznacza, że może obsługiwać najbardziej rozbudowane wersje DD-WRT. Wolniejszy procesor oznacza, że trzeba będzie pogodzić się z wolniejszą prędkością VPN. Jest to jeden z najlepszych routerów dla tych, którzy nie mogą sobie pozwolić na płacenie gigantycznej ceny za NetGear Nighthawk.

Netgear AC1450 – cena ok. 750,00

Wiele osób może nie uznać AC1450 za dobry router, patrząc na jego przystępną cenę. Ale nie pozwól, by cena Cię zmyliła. Ten router ma potężny procesor i taką samą ilość pamięci RAM i Flash, co niektórzy z jego drogich konkurentów. Jedynym minusem jest jego wewnętrzna antena, która ogranicza jego możliwości podczas transmisji bezprzewodowych dalekiego zasięgu.

Asus AC5300 DD-WRT FlashRouter – cena ok. 1300,00

Został zaprojektowany tylko w jednym celu: Stworzenia wspaniałej sieci dla gracza. Jest on po brzegi napakowany zaawansowanymi możliwościami optymalizacji gier, umożliwia dominującą wydajność Wi-Fi, solidną stabilność i najwyższy poziom bezpieczeństwa w Internecie. Utrzymany w temacie ROG interfejs Centrum Gry umożliwia łatwe sterowanie każdą z niesamowitych funkcji tego routera. Pulpit Gry w czasie rzeczywistym dostarcza Ci informacji o wszystkich Twoich urządzeniach i połączeniach, podczas gdy Game IPS (System Zapobiegania Włamaniom) i Game Boost to odpowiednio:

centrum dowodzenia bezpieczeństwem sieci i bardzo wydajna funkcja przyspieszania gier. Inne przydatne funkcje to obsługa Gamers Private Network® za pośrednictwem WTFast®, wykrywający zatory transferu Radar Wi-Fi. Mapa pingów Game Radar, która pokazuje Ci lokalizację najszybszych serwerów, a także VPN Fusion do jednoczesnej obsługi VPN równolegle do swojego połączenia internetowego.

Dla ochrony Twojej sieci ROG Rapture GT-AC5300 jest wyposażony w Game IPS (System Zapobiegania Włamaniom), najwyższej klasy system zapobiegania włamaniom zasilany przez technologię Trend Micro™. Chroni on Twoją sieć przed atakami i zagrożeniami zewnętrznymi, neutralizując je zanim zdążą dotrzeć do sieci lub urządzeń. Nawet jeśli oprogramowanie antywirusowe Twojego komputera nie jest aktywne – np. w celu obejścia blokady jakiejś gry, Game IPS nadal chroni sieć przed atakami i włamaniami, dzięki czemu masz spokój w czasie rozgrywki.

Jeśli masz już dość sytuacji, gdy sieć VPN spowalnia Twoją grę, ROG ma dla Ciebie rozwiązanie. ROG Rapture GT-AC5300 oferuje zabójczą funkcję o nazwie VPN Fusion, która pozwoli Ci na uruchomienie połączenia VPN oraz zwykłego połączenia internetowego — w tym samym czasie! Także nawet jeśli inni użytkownicy sieci potrzebują połączenia VPN, Ty nadal możesz cieszyć się grami w maksymalnej prędkości.

7. Uwagi praktyczne

Pod żadnym pozorem nie należy „upraszczać” zadania i próbować wykonywać pomiarów/obserwacji jednocześnie z kilku punktów instrukcji. Jest to najszybsza droga do pomyłki w identyfikacji przebiegów, co skutkuje odrzuceniem sprawozdania.

Pomimo, że w instrukcji zawsze używa się określeń typu „połącz”, „zestaw połączenie”, to jest bardzo prawdopodobne, że dane połączenia będzie już wykonane. Nie należy, więc automatycznie rozłączać tego, co jest połączone – najpierw sprawdzamy istniejące połączenia.

W nawiasach klamrowych {} podane są ustawienia podstawowych parametrów przyrządu pomiarowego – odnoszą się do przyrządu powołanego przed nawiasami.

Dla uproszczenia i zwiększenia przejrzystości instrukcji wprowadzono poniższe symbole, które zostały wykorzystane w tekście.:

 zapisz przebieg na dysku,

 pytanie, na które odpowiedź musi znaleźć się w sprawozdaniu,

8. Realizacja zadania

Adres IP, lokalizacja i szybkość łącza

8.1 Wejdź na stronę https://www.speedtest.pl/ . Jaki jest Twój adres IP? Kto jest dostawcą usług internetowych? (Nie musisz podawać tych danych w sprawozdaniu, ale je zapisz).

8.2 Pozwól na automatyczny wybór serwera i uruchom test Twojego łącza internetowego klikając na *START*. Zapisz wyniki, robiąc zrzut ekranu. Jakie są wartości Ping oraz szybkości pobierania i wysyłania? Jak można je ocenić? Jak wyglądają na tle innych?

8.3 Wejdź na stronę https://www.ipfingerprints.com/ . Jak strona widzi Twój adres IP? Jakie informacje odczytuje? Czy są one poprawne?

8.4 Wejdź na stronę https://www.iplocation.net/ . Czy dane są takie same jak poprzednio? Czy ta strona widzi i „wie" więcej na Twój temat, coś nie tylko o lokalizacji, ale i używanym sprzęcie oraz jego konfiguracji? Jak działa geolokalizacja oparta na IP? Jak i do czego te dane mogą być wykorzystane?

8.5 Wejdź na stronę https://whatismyipaddress.com/ip-hostname i wklej w pole tekstowe swój adres IP. Jaka jest nazwa hosta?

Oprogramowanie ProtonVPN

8.6 Uruchom program *ProtonVPN*. Ponieważ wymaga on przy starcie logowania to możliwe, że jest on już uruchomiony przez prowadzącego.

8.7 Program, w panelu z lewej strony, ma dwie zakładki: *Kraje* i *Profile*. W wersji darmowej dostępne są tylko trzy kraje.

8.8 Klikając na dany kraj można rozwinąć listę serwerów w nim dostępnych. Połączenie z serwerem następuje po kliknięciu na klawisz *Połącz* obok nazwy serwera.

8.9 Wybierz kolejno trzy serwery z każdego z trzech dostępnych krajów. Zwracaj uwagę na obciążenie serwera – informacja jest dostępna obok jego numeru IP. Staraj się tak wybrać, aby znaleźć serwery mało, średnio i bardzo obciążone.

8.10 Kolejno połącz się z tymi serwerami. Dla każdego z serwera powtórz punkty od 8.1 do 8.2. Pamiętaj, by za każdym razem odświeżać strony. Zbierz wyniki pomiarów i wartości Ping

oraz szybkości pobierania i wysyłania w tabelce. Obok wartości wyraź zmianę w procentach. Co się zmieniło? Który parametr uległ największej a który najmniejszej zmianie? Co wpływa na te zmiany? Co i kiedy będzie największym problemem podczas korzystania z programu *CyberGhost*?

8.11 Dla każdego z serwera powtórz punkty od 8.3 do 8.5. W miarę możliwości zbierz wyniki w tabelce. Co się zmieniło? Co strony nadal wiedzą na Twój temat i o Twoim sprzęcie? Co udało się ukryć, a czego nie?

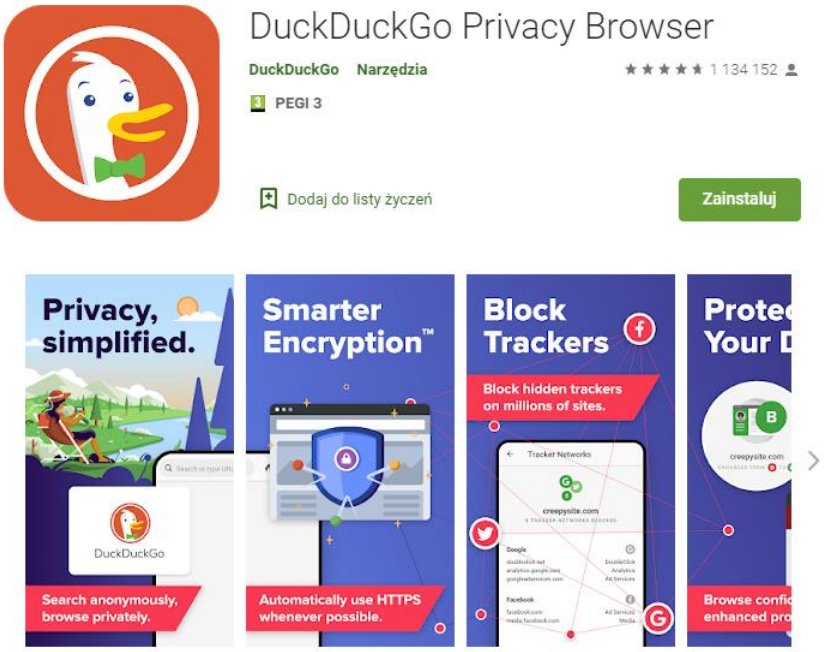
Przeglądarka DuckDuckGo

8.12 Wejdź na stronę https://duckduckgo.com/ . Czym wg twórców różni się *DuckDuckGo* od innych wyszukiwarek? Na co jest położony główny nacisk?

8.13 Sprawdź wyniki wyszukania w *Google* i *DuckDuckGo* dla kilku fraz o różnym stopniu popularności. Czy wyniki wyszukania są takie same czy różne?

Urządzenia mobilne – dla chętnych do wykonania w domu

8.14 Zainstaluj wyszukiwarkę *DuckDuckGo* na urządzeniu mobilnym.



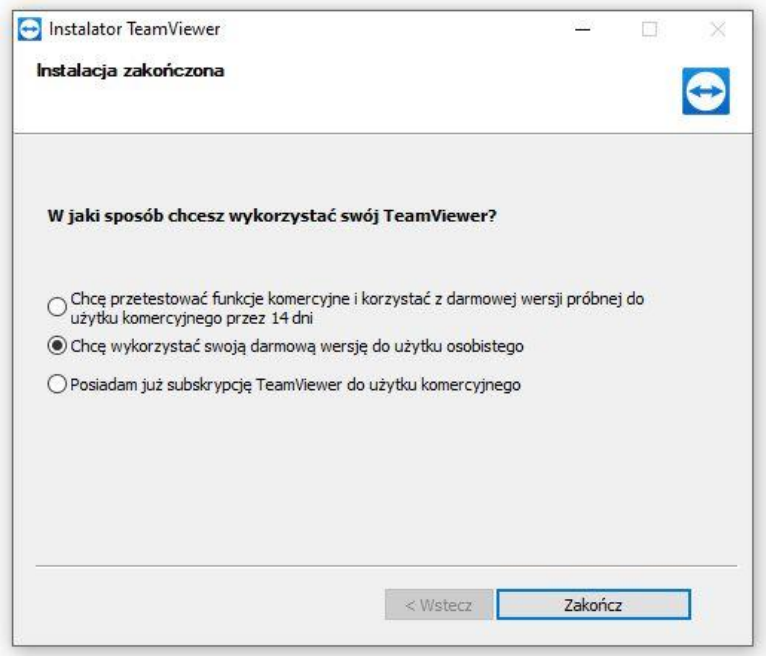
8.15 Sprawdź wyniki wyszukania w *Google* i *DuckDuckGo* dla kilku fraz o różnym stopniu popularności. Czy wyniki wyszukania są takie same czy różne? Czy korzystanie z *DuckDuckGo* jest dla Ciebie gorsze/trudniejsze/wolniejsze od korzystania z Google?

8.16 Wyszukaj dla swojego systemu darmowy program VPN, inny niż CyberGhost – program CyberGhost w wersji próbnej i darmowej nie pozwoli na korzystanie z jednego konta na więcej niż jednym urządzeniu bez wcześniejszego usunięcia tego urządzenia z listy.

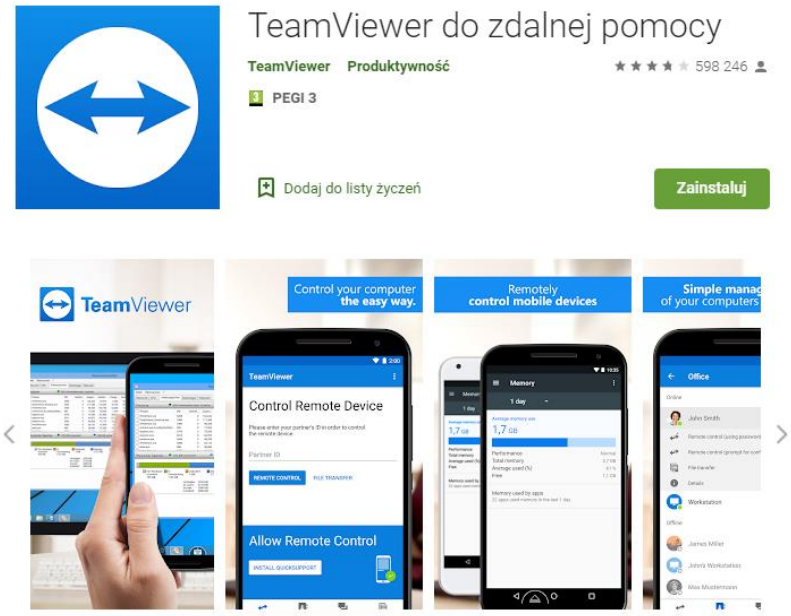
8.17 Powtórz punkty od 6.1 do 6.5 dwa razy – bez oraz z połączeniem VPN. Jeśli będzie możliwość wyboru serwera to wybierz teoretycznie „najlepszy", czyli najbliższy i najmniej obciążony. Zapisz wyniki w prostej tabelce i zmiany wartości Ping oraz szybkości pobierania i wysyłania wyraź w procentach. Co i jak się zmieniło? Czy urządzenie mobilne może być normalnie użytkowane czy też VPN w czymś przeszkadza? Czy darmowe programy VPN oferują to samo co programy płatne?

Zdalny dostęp – dla chętnych do wykonania w domu

8.18 Ze strony https://global.teamviewer.com/pl/do-pobrania/windows/ pobierz program *TeamViewer* w wersji odpowiedniej dla Twojego systemu operacyjnego. Zainstaluj program. Po uruchomieniu wybierz wersję testową.

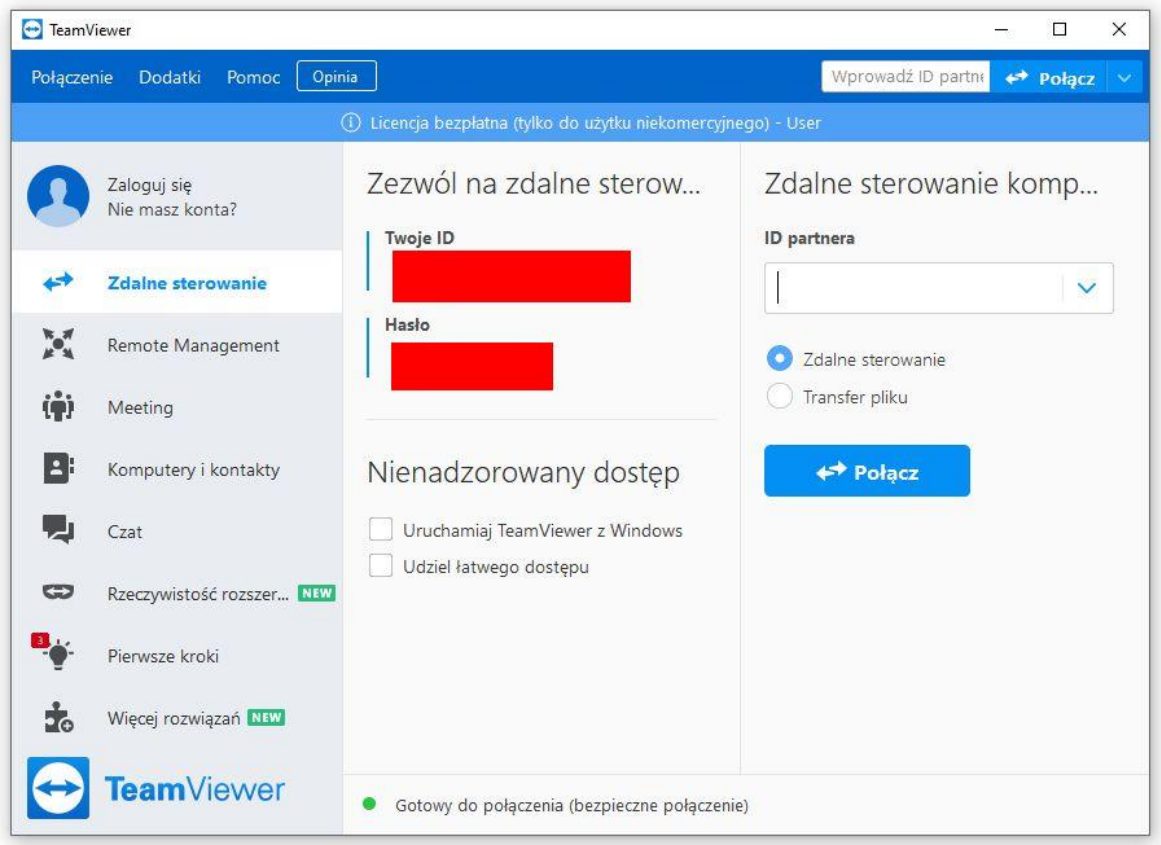


8.19 Zainstaluj program *TeamViewer* na drugim komputerze lub urządzeniu mobilnym – telefonie lub tablecie.



Uwaga!!! Jeśli nie masz drugiego urządzenia to możesz wykonać tę część zadania z drugą osobą z grupy. Wymaga to jednak całkowitego zaufania, ponieważ druga osoba uzyska nie tylko dostęp do Twojego identyfikatora i hasła TeamViewer, ale również do zasobów Twojego komputera.

8.20 Uruchom program *TeamViewer* i na obu urządzeniach wprowadź dane identyfikacyjne oraz hasło drugiego urządzenia.



8.21 Połącz oba urządzenia kolejno w dwóch trybach – *Zdalne sterowanie* i *Transfer pliku*. Co umożliwiają oba tryby? Czym się one różnią? Jaki jest komfort pracy na obu urządzeniach? Co najbardziej na niego wpływa?

Uwaga!!! Ewentualne zrzuty ekranów należy w zakresie zawartości Twojego urządzenia ograniczyć do minimum, bez ujawniania swoich danych.

Dobór routera VPN

8.22 Korzystając z popularnych stron sklepów, portali aukcyjnych i porównywark dokonaj przeglądu i zestawienia dostępnych routerów obsługujących VPN różnych producentów (np. TP-LINK, Asus, FRITZ!Box, Linksys, Teltonika, Synology). Zestawienie przeprowadź w trzech grupach cenowych:

- 200,00 – 350,00 PLN
- 350,00 – 650,00 PLN
- 650,00 – 1500,00 PLN

8.23 Nie zapisuj do sprawozdania wszystkich danych technicznych wszystkich routerów, jest ich zbyt dużo. Zwróć jednak na nie uwagę i staraj się je porównać, wychwytując róznice. Z czego wynika róznica w cenie pomiędzy poszczególnymi routerami? Czym one się różnią skoro wszystkie są „routeramiVPN”? Czy każdy router oferuje taki sam poziom komfortu użytkowania i bezpieczeństwa użytkownikowi VPN?

Konfiguracja routera VPN

8.24 Zapoznaj się z prezentowaną konfiguracją demonstarcyjnego routera. Wykonaj w trakcie kilka zrzutów ekranu do sprawozdania. Jaki to model routera? Jakie są jego możliwości i ograniczenia dla VPN?

8.25 Spośród routerów wybranych w p. 8.22 wybierz JEDEN wg następującej zależności: jeśli ostatnia cyfra Twojego numeru albumu/indeksu to 0, 1 lub 2 wybierz router z grupy cenowej 200-350, jeśli ostatnia cyfra to 3, 4, 5 lub 6 to wybierz router z grupy cenowej 350-650 a jeśli ostatnia cyfra to 7, 8 lub 9 to z grupy cenowej 650-1500.

8.26 Wyszukaj w Internecie instrukcję obsługi dla wybranego w p. 8.25 routera.

8.27 Korzystając z pobranej instrukcji oraz dostępnych w Internecie zrzutów dokonaj przykładowej konfiguracji wybranego routera. Czy oprócz routera będzie cos jeszcze potrzebne do uruchomienia VPN? Jeśli tak to co?

9. Wykonanie sprawozdania

Nie należy umieszczać w sprawozdaniu podstaw teoretycznych, ani opisów stanowiska laboratoryjnego.

Sprawozdanie musi zawierać wszystkie wyniki pomiarów/obserwacji oraz wszystkie zarejestrowane dane i zrzuty ekranu  prezentowane wg kolejności ich wykonania. Każdy tekst i obraz muszą być opatrzone numerem punktu instrukcji wg, którego zostały zarejestrowane. Muszą być opatrzone opisem, wyjaśniającym, co przedstawiają. W sprawozdaniu muszą się znaleźć odpowiedzi na wszystkie postawione w instrukcji pytania,  ponumerowane wg punktów, w których zostały postawione. Zarówno opisy, jak i odpowiedzi, mają być zwięzłe, ale przedstawione pełnymi zdaniami. Sprawozdanie musi się kończyć wnioskami z całego ćwiczenia.

10. Literatura

[1] Serafin M., Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone, Helion 2013,

[2] Zaręba P., Praktyczne projekty sieciowe. Opanuj sieci w praktyce, Helion 2019,

[3] https://blog.avast.com/pl/co-to-jest-vpn-i-jak-dziala

[4] https://bitdefender.pl/jak-dziala-siec-vpn/

[5] https://pl.vpnmentor.com/blog/rozne-rodzaje-vpnow-scenariusze-ich-uzytkowania/

[6] https://networkexpert.pl/baza-wiedzy/vpn-omowienie-roznych-typow-dostepu-zdalnego/

[7] https://www.forscope.pl/blog/czym-jest-vpn/

[8] http://www.neurosoft.edu.pl/zg/plugins/files/files/VPN.pdf

[9] https://topvpn.pl/program-do-vpn/