18.01.2023r.

Porównanie rozwiązań VPN pod kątem bezpieczeństwa

Szczepan Markowski

Projekt z przedmiotu „Zarządzanie infrastrukturą teleinformatyczną”

Streszczenie – Wirtualna Sieć Prywatna jest szerokim spektrum problemów i rozwiązań, określających bezpieczne konceptualne połączenie między punktami. W niniejszym projekcie podjęto próbę przybliżenia pojęcia VPN-u oraz przeglądu i analizy obecnych rozwiązań i wybranie najlepszego z dostępnych.

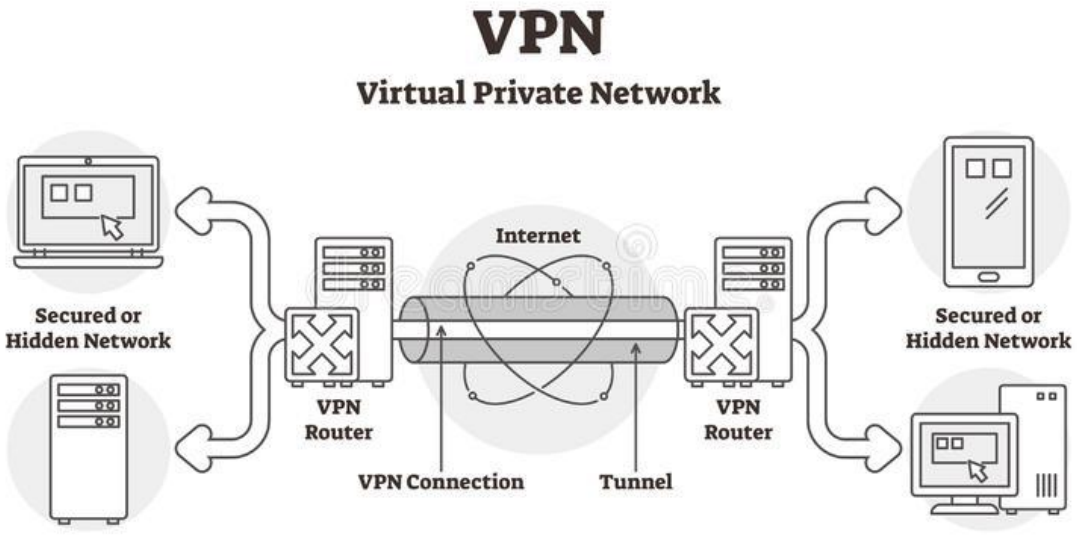
Spis treści

VPN

VPN (z angielskiego Virtual Private Network) jest to rodzaj sieci prywatnej opierający się o mechanizm tworzenia tunelu, a dokładniej bezpiecznego połączenia między nadawcą, a odbiorcą. Te tunele powstają przy użyciu niezabezpieczonych sieci publicznych takich jak Internet. VPN pozwala użytkownikom na uzyskanie bezpiecznego połączenia przy użyciu tych niezabezpieczonych sieci publicznych, tworząc wirtualny tunel, znaczy to, że w rzeczywistości nie ma nigdzie prawdziwego tunelu, tylko istnieje struktura logiczna pozwalająca na korzystanie z owych sieci publicznych na stworzenie takiego niematerialnego połączenia między dwoma punktami. Głównym celem VPN jest utworzenie bezpiecznych połączeń, lecz struktura VPN niesie za sobą także, obniżenie kosztów dedykowanych linii telekomunikacyjnych oraz zwiększenie możliwości pracy zdalnej przez ludzi na całym świecie, poprzez łączenie się takim tunelem bezpośrednio do firmy z drugiego końca świata. Możliwość pracy zdalnej jest zawdzięczana poprzez specyficzną budowę VPN głównie skupiającą się na budowie punkt-punkt.

Schemat działania

Schemat działania VPN jest banalnie prosty do zrozumienia nawet dla przeciętnego użytkownika Internetu. Użytkownik łączy się na swoim komputerze z klientem VPN, ta trasa nie jest w żaden sposób chroniona, ponieważ wszystko dzieje się na jednej maszynie. Następnie klient VPN tworzy trasę pomiędzy użytkownikiem, a serwerem. Warto wziąć pod uwagę, że użytkownik jak i serwer posiadają aplikację kliencką VPN. Ta trasa między tymi dwoma klientami jest zabezpieczana, np. przy użyciu szyfru blokowego, obecnie najczęściej używanym jest symetryczny szyfr blokowy AES256. Zaszyfrowane dane przemieszczają się wirtualnie stworzonym tunelem między klientami, w ten sposób, możliwe jest wykorzystanie sieci publicznej, ponieważ proces szyfrowania wykonywany na początku połączenia, uniemożliwia podglądanie danych przemieszczających się w publicznej sieci. Po dotarciu do klienta serwera dane są deszyfrowane, a następnie odczytywane przez punktu docelowy. Taki schemat działania jest zamieszczony na poniższym rysunku.



Rysunek. 1 – Schemat działa wirtualnej sieci prywatnej

Motywy powstania

Głównym motywem budowania sieci VPN jest aspekt finansowy. Obecnie istnieje bardzo rozległa i efektywna infrastruktura telekomunikacyjna. Co za tym idzie tworzenie nowej infrastruktury między dwoma miejscami, aby zapewnić bezpieczne połączenie pomiędzy punktami jest bardzo kosztowne. Dlatego wraz z progresywną idea wirtualizacji usług czy struktur, stworzenie wirtualnej sieci przy wykorzystaniu obecnie istniejących infrastruktur, dobrze wpasowuje się w tą ideę. Oprócz aspektu finansowego, motyw wprowadzenia relatywnie bezpiecznego połączenia odegrał ważną rolę podczas tworzenia VPN. Zapotrzebowanie na zdalny dostęp do pracy horrendalnie się zwiększyło za sprawą pandemii wirusa COVID-19 w 2020r. Już na tamtą chwilę od ponad 20 lat model technologii wirtualnej sieci prywatnej istniał i prężnie się rozwijał, lecz to globalny lockdown spowodował, że firmy szerzej zainteresowały się rynkiem zdalnego dostępu do miejsca pracy dla swoich pracowników. Aby mogli oni wykonywać swoją prace z domu, nie narażając siebie i innych na zarażenie. Możliwość dostępu do serwera firmy z odległego miejsca niosła by za sobą ryzyko wprowadzenia złośliwego oprogramowania, dlatego bezpieczeństwo danych przenoszonych od użytkownika do serwera jest tak ważną częścią powstania sieci VPN-owych.

Rodzaje struktur VPN

Istnieją różne rodzaje struktur VPN, w tym:

- Site-to-Site: struktura oparta o łączenie ze sobą oddzielnych sieci lokalnych (LAN). Pozwala to użytkownikom na dostęp do zasobów sieciowych w obu sieciach, jest to najbardziej zbliżone do imitacji fizycznego połączenia między sieciami.
- Remote Access: struktura, który skupia się na umożliwieniu użytkownikom zdalnego dostępu do sieci lokalnej (LAN), z dowolnego miejsca na ziemi. Użytkownicy mogą skorzystać z zasobów sieciowych danej siedzi jakby byli do niej podłączeni. Dzieje się to przy pomocy wykorzystanie specjalnego klienta VPN.
- Mobile: struktura bardzo zbliżona do struktury Remote Access, tylko w tym przypadku urządzeniem końcowym użytkownika jest urządzenie mobilne takie jak smartphone. Użytkownik jest w stanie skorzystać z dostępnych zasobów sieciowych, do których się łączy.

Bezpieczeństwo VPN

Bezpieczeństwo VPN opiera się o 3 główne założenia: poufność, uwierzytelnienie oraz integralność. Poufność odpowiada za zapewnienie ochrony dostępu do transportowanych danych. Jest to osiągalne za sprawą użycia algorytmów szyfrujących, w momencie kiedy dane zostają przechwycone przy pomocy aplikacji umożliwiającej podglądanie lub przechwytywanie pakietów. Osoba, której udało by się przechwycić takie dane nie powinna mieć możliwości skorzystania z nich, ponieważ będą one zaszyfrowane i tylko osoby posiadające klucze deszyfrujące są w stanie odczytać zawartość tych pakietów danych. Uwierzytelnienie jest zapewniane poprzez uniemożliwienie nieautoryzowanym użytkownikom dostęp do użytkownika VPN, poprzez zastosowanie np. certyfikatów cyfrowych lub wielopoziomowego uwierzytelniania np. hasło + odcisk palca + klucz u2f . Integralność jest zapewniana poprzez sprawdzanie czy podczas transmisji danych, nie zostały one przejęte i zmodyfikowane czy podmienione. Odpowiadają za to algorytmy wykrywające zmiany między wychodzącą a przychodzącą wiadomościom.

Rozwiązania VPN

Rozwiązania VPN można podzielić na dwie główne kategorie: protokoły komunikacyjne i aplikacje połączeniowe.

Protokoły komunikacyjne są zbiorem reguł i zasad pozwalającym na nawiązanie łączności pomiędzy dwoma urządzeniami komunikacyjnymi, aby rozpocząć proces wymiany danych. Do tej kategorii należą takie protokoły jak IPsec, SSL/TLS, PPTP czy L2TP.

Aplikacje połączeniowe natomiast są bardziej złożonymi tworami, ponieważ składają się z zestawu protokołów, który często jest bardziej złożony, także pozwala na zapewnienie większego bezpieczeństwa i obecnie jest uznawany za podstawowe

rozwiązanie do nawiązywania połączeń VPN. Posiada także otoczkę software-ową pozwalającej na samodzielne działanie. Jest to zapewniane przy pomocy terminala lub graficznego interfejsu.

Obie te kategorie potocznie nazywane są protokołami, ponieważ obie grupy korzystają ze zbioru reguł w celu nawiązania połączenia do przesyłania danych.

Serwisy VPN

Serwisy VPN na przestrzeni ostatnich lat zyskują bardzo dużą popularność, co za tym idzie rynek VPN stale się powiększa. Największymi graczami obecnie są 3 firmy: NordVPN, Surfshark oraz ExpressVPN. Te 3 firmy działają na większości platform i korzystają głównie z aplikacji połączeniowych takich jak OpenVPN oraz WireGuard, o których będzie więcej w sekcji Protokoły. Lecz nie są to jedyne rozwiązania, z których korzystają, ponieważ w zależności od okoliczności czy miejsca, w którym się znajduje, potrzeby ulegają zmianie. Dlatego oferują oni różne rozwiązania, aby jak najbardziej dogodzić klientowi. Tak samo jak protokoły pracują razem, aby spełnić swoje zadanie najlepiej jak się da.

Protokoły

Protokoły VPN są zestawami reguł oraz standardów używanych do tworzenia i obsługi połączeń VPN. Głównym zadaniem protokołów jest komunikacja między użytkownikiem a serwerem VPN oraz ustanowienie bezpiecznego połączenia między użytkownikiem a serwerem, z którego użytkownik chce skorzystać. Istnieje wiele protokołów VPN, różnią się one między sobą pod wieloma względami, np. algorytmem szyfrującym, ogólnym bezpieczeństwem, prostotą konfiguracji, potencjalną prędkością, stabilnością czy zastosowanie.

AES256

Protokoły oprócz PPTP korzystają z algorytmu szyfrującego AES256, dlatego warto jest zapoznać się z nim trochę dokładniej. AES został w 2001 uznany za nowy standard kryptograficzny ubiegając 3DES-a. Sam proces działania jest prosty, algorytm wykorzystuje klucz o długości 256 bit, dzieli dane na bloki o długości 128 bitów i szyfruje je przy pomocy różnych działań matematycznych, wykonuje 14 rund takich działań gdzie za każdym razem dodaje jeden klucz rundy i powtarza ten proces, te 14 razy. Złamanie takiego klucza metodą brute-force zajęło by 2.73 * 10^61 lat. Natomiast algorytm AES na przestrzeni ostatnich 20 lat został poddany wielu próbom ataku, jednak były to klucze AES128, które były najbardziej zbliżone do próby sukcesu. Lecz

na dzień 08.01.2023r. nie ma doniesień o powodzeniu ataku na algorytm AES256, co pozwala go uznać za bezpieczny.

Najpopularniejsze protokoły

Obecnie dostępnych jest wiele protokołów VPN do użytku. Często spotykanym zjawiskiem jest łączenie protokołów dla lepszej wydajności czy zwiększenia bezpieczeństwa, dlatego można spotkać się z takimi połączeniami jak np. IKEv2/IPsec .Poniżej znajdują się niektóre z tych popularniejszych czy najciekawszych ze wszystkich obecnych:

- PPTP
- IKEv2/IPsec
- OpenVPN
- WireGuard

PPTP

Point to Point Tunneling Protocol – protokół komunikacyjny pozwalający na tworzenie sieci prywatnych z wykorzystaniem technologii tunelowania. Jest to pierwszy protokół VPN został użyty pierwszy raz już w 1996 przez pracownika Microsoft. Ostatecznie został wydany w 1999 roku przez firmy Microsoft, 3Com, obecną Nokie oraz innych. Protokół ten zagościł w sieci na dobre, ponieważ tunel PPTP jest tworzony i lokowany na porcie TCP o numerze 1723. PPTP korzysta z połączenia TCP, które inicjuje i zarządza tunelem GRE (Generic Routing Encapsulation) jest to dodatkowy protokół tunelowania wymyślony przez Cisco w roku 1994. Tunel GRE jest używany to przenoszenia enkapsulowanego pakietu PPP, co pozwala temu pakietowi zawrzeć np. IP czy IPX, ale właśnie to połączenie razem tworzy protokół zwany PPTP.

Specyfikacja

Algorytm szyfrujący – PPTP korzysta z MPPE (Microsoft Point-to-Point Encryption) jest to protokół Microsoftu, który szyfruje pakiety PPP oraz PPTP kluczami od 40-bit do 128-bit. W obecnych czasach długość tych kluczy uznawana jest za mało bezpieczną.

Bezpieczeństwo – Bezpieczeństwo protokołu można sprawdzić poprzez 3 warianty poufność, integralność oraz uwierzytelnienie:

- Poufność – Poufność jest zapewniana poprzez algorytmy szyfrujące dane w tym przypadku algorytm MPPE, wykorzystujący 128 bitowy klucz.
- Integralność - Integralność protokołu PPTP opiera się o mechanizm kontroli poprawności danych zwanego PPP (Point-to-Point Protocol), znajduje się on w

warstwie drugiej modelu ISO/OSI (warstwa łącza danych). PPP sprawdza integralność danych na parę sposobów jak np. szumy kontrolne czy numery sekwencyjne. Jeśli podczas przesyłania danych między urządzeniem a serwerem wystąpi błąd PPP to wykryje i wyśle żądanie o ponownej transmisji danych, aby naprawić powstałe błędy.

- Uwierzytelnienie – Uwierzytelnienie protokołu PPTP w głównej mierze opiera się o protokół MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) lub EAP-MS-CHAP v2 (Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2). Te protokoły są oparte o hasła uwierzytelniające, lecz Microsoft nie zaleca z korzystania z tylko takiego zabezpieczenia i radzi zhermetyzować tunele PPTP. Cały protokół opiera się o wygenerowanie żądania połączenia z serwerem VPN, otrzymania unikalnego identyfikatora użytkownika i hasła, użycie tych danych do wygenerowania odpowiedzi na wyzwanie handshaku, a ostatecznie serwer sprawdza czy odpowiedź użytkownika jest poprawna i jeśli jest akceptuje połączenie, jeśli nie połączenie jest odrzucane.

Prostota konfiguracji – Konfiguracja PPTP jest banalnie prosta głównie przez wzgląd na to, że każdy Windows począwszy od Windowsa 98 posiada już wgrany ten protokół w system. Sama konfiguracja przebiega bardzo szybko (około 5 minut), jest wiele poradników na Internecie oraz cały proces konfiguracji może odbywać się przez GUI.

Potencjalna prędkość – Sam protokół nie wpływa bezpośrednio na prędkość transmisji danych, lecz pośrednio wpływ. Jest to przez proces szyfrowania, który w tym protokole jest relatywnie prosty, dlatego ten protokół jest jednym z najszybszych. Korzysta on z niskopoziomowego szyfrowania co nie zmienia zbytnio oferowanej prędkości transmisji oferowanej przez dostawcę Internetu.

Stabilność – PPTP jest starym protokołem dlatego jest dosyć stabilny i dobrze sobie radzi podczas stabilnego łącza, lecz gdy łącze jest niestabilne pojawiają się problemy.

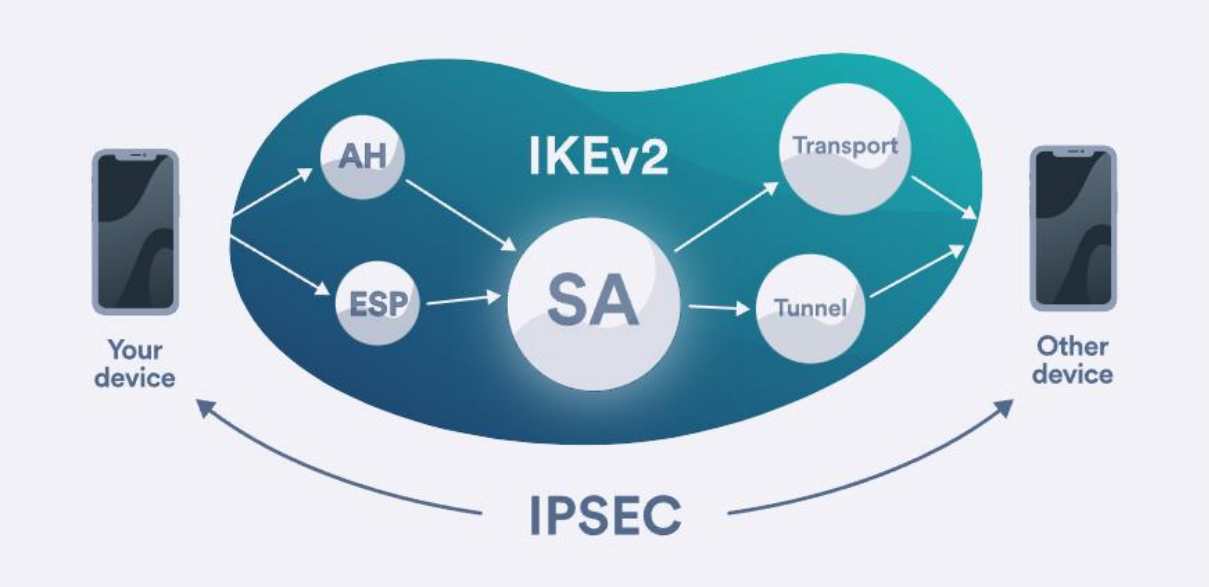
Zastosowanie – Protokół PPTP najlepiej się sprawuje podczas używania niezawodnej sieci, gdzie liczy się prędkość dostępu do danych i gdzie bezpieczeństwo nie jest tak ważne, ponieważ od 2012 według Microsoftu ten protokół nie spełnia wymogów określania go jako bezpieczny protokół VPN.

Podsumowanie PPTP

Protokół PPTP jest prostym i szybkim protokołem, nie jest on już uznawany za bezpieczny ponieważ MPPE używa klucza 128 bitowego, a MS-CHAP v2, korzysta z funkcji haszującej SHA 1, która jest podatna na atak kolizyjny, czyli hasz z dwóch różnych wejść daje takie samo wyjście. Co za tym idzie np. w 2012 portal Linkedin, który korzystał z funkcji haszującej SHA 1, został zaatakowany i cały proces krakowania zajął niecałe 72 godziny. Obecnie obejście zabezpieczeń VPN korzystającego z protokołu PPTP zajmuje mniej niż 5 minut, tyle co jego konfiguracja.

IKEv2/IPsec

Ikev2/IPsec – jest to połączenie dwóch protokołów, Internet Key Exchange version 2, który jest protokołem wymiany kluczy szyfrujących, zajmuje się on automatycznym ustaleniem i negocjowaniem parametrów szyfrowania i uwierzytelnienia połączenia VPN. IKE korzysta z certyfikatu uwierzytelniania X.509 np. przy wymianie klucza jak w schemacie Diffiego-Hellmana, polegającego na stworzeniu klucza publicznego oraz prywatnego gdzie tylko połączenie tych dwóch kluczy uwierzytelnia przesłane dane. Internet Protocol Security, jest drugim protokołem w tej parze, który zajmuje się głównie uwierzytelnieniem i szyfrowaniem pakietów danych, dlatego w połączeniu z IKEv2, tworzą bardzo dobrą parę. IPsec znajduje się w 3 warstwie modelu ISO/OSI (warstwa sieci), gdzie głównie opiera swoje działanie o użycie szyfrowania kryptograficznego do zapewnienia bezpiecznego połączenia przy komunikacji sieci IP. Wspiera on wszystkie 3 główne cechy bezpieczeństwa jak poufność, integralność oraz uwierzytelnienie.



Rysunek 2. Zobrazowanie połączenia przy użyciu protokołu IKEv2/IPsec

Obraz jest własnością Surfshark B.V.

Specyfikacja

Algorytm szyfrujący – Głównym algorytmem szyfrującym w protokole IKEv2/IPsec jest AES (Advanced Encryption Standard), który został przyjęty za standard w roku 2001. Długość klucza wacha się od 128 do 256 bit. Z czego w tym protokole używany jest 256 bitowy klucz posiadający 14 rund.

Bezpieczeństwo – Bezpieczeństwo protokołu można sprawdzić poprzez 3 warianty poufność, integralność oraz uwierzytelnienie:

- Poufność – Poufność zapewnia część IKEv2 korzystająca z algorytmu AES256.
- Integralność – Integralność tego protokołu opiera się różne mechanizmy kontroli poprawności danych, przy pomocy HMAC-SHA-256, który jest wykorzystywany w protokole IPsec. Kody HMAC opierają się na funkcji skrótu SHA. Kod taki może być wygenerowany tylko przez osobę posiadającą tajny klucz i jest on niezależny od kluczy szyfrujących dane. Następnie tylko osoba znająca ten tajny klucz jest w stanie zweryfikować autentyczność tych danych.
- Uwierzytelnienie – Uwierzytelnienie opiera się o protokół EAP, który jest wspierany od drugiej wersji IKE. Schemat działania prezentuje się następująco: Na początku użytkownik wysyła żądanie połączenia z serwerem VPN, następnie VPN wysyła wyzwanie z identyfikatorem użytkownika i hasła, podobnie jak w przypadku protokołu MPPE w PPTP. Następnie użytkownik używa hasła i algorytmu do wygenerowania odpowiedzi i wysyła odpowiedź. Serwer VPN ją sprawdza i akceptuje lub odrzuca, jeśli odpowiedź zostanie zaakceptowana to użytkownik otrzymuje propozycje parametrów szyfrowania i uwierzytelnienia dla stworzenia nowego połączenia. Użytkownik może zaakceptować taką propozycję i nawiązać bezpieczne połączenia. W tym momencie po nawiązaniu połączenia protokół IKEv2 korzysta z protokołu IPsec do szyfrowania danych i uwierzytelnienia urządzeń w procesie bezpiecznej wymiany danych pomiędzy stornami.

Prostota konfiguracji – Konfiguracja samego IKEv2/IPsec jest sama w sobie trudna, lecz w wykorzystaniu jej do połączenia VPN wydaje się w miarę prosta, ponieważ te protokoły są wbudowane w system od wersji Windows 7 do Windowsa 10. Systemy operacyjne Linux niestety nie są wspierane przez ten protokół, a na samym Windowsie są lepsze alternatywy

Potencjalna prędkość – Potencjalna prędkość protokołu IKE została zwiększona podczas stworzenia drugie wersji tego protokołu jak i poprzez zastosowanie IPsec SA, który zmniejszył opóźnienie połączenia jak i przyczynił się do zwiększenia szybkości połącznia

Stabilność – Protokoły te utrzymują bardzo dobrą stabilność połączenia poprzez automatyczna przełączanie między różnymi sieciami, aby komfort korzystania był jak największy. Przy użyciu stabilnych i niezawodnych łącz internetowych, stabilność tych protokołów jest na bardzo wysokim poziomie.

Zastosowanie – Ten zestaw protokołów najlepiej się sprawdza w przypadku połączeń mobilnych, ponieważ jest w stanie szybko i automatycznie przełączać się między różnymi sieciami, co pozwala zwiększyć komfort korzystania z połączenia VPN.

Podsumowanie IKEv2/IPsec

Zestawienie tych dwóch protokołów przyniosło bardzo dużych zmian, ponieważ IPsec narażony był na ataki zalewania DDoS (Distributed Denial of Service), gdzie protokół IKEv2 pomógł je zminimalizować, a IPsec przysłużył się do zmniejszenia opóźnienia

podczas połączenia. Obecnie nie było żadnych ataków na ten zestaw protokołów, dlatego są one uznawane za bezpieczne.

OpenVPN

OpenVPN jest to oprogramowanie skupiające się na stworzeniu bezpiecznego połączenia VPN typu punkt-punkt. Tworzenie bezpiecznych połączeń tunelowych odbywa się przy użyciu biblioteki OpenSSL oraz protokołów SSL/TLS. OpenVPN np. w porównaniu do IKEv2/IPsec nie korzysta z protokołu IPsec jako pośrednika przy połączeniu. Rozwiązanie OpenVPN jest dostępne dla serwerów jak i klientów. Cały kod implementacji zawiera się w 400 000 linijek kodu głównie napisanych w języku C, aby jakkolwiek zwiększyć efektywność poprzez wykorzystanie niskopoziomowego języka programowania, w porównaniu do WireGuarda posiadającego 4000 linijek kodu. OpenVPN posiada graficzny interfejs oraz jest dostępny na wszystkich możliwych platformach.

Specyfikacja

Algorytm szyfrujący – Algorytm szyfrujący opiera się o biblioteki OpenSSL, która opiera się o implementację protokołu SSL korzystającą z algorytmu szyfrującego jakim jest AES256. Dodatkowo można wybrać dwa tryby szyfrowania CBC (Cipher Block Chaining) lub GCM (Galois/Counter Mode) polegające na szyfrowaniu bloków danych. GCM stał się głównym trybem szyfrowania na serwerach korzystających z OpenVPN, ponieważ łączy on szyfrowanie wraz z uwierzytelnieniem. Nadal jednak wspierany jest tryb CBC korzystający ze skrótów haszów korzystający z uwierzytelniania pakietów przy użyciu SHA1 HMAC.

Bezpieczeństwo – Bezpieczeństwo protokołu można sprawdzić poprzez 3 warianty poufność, integralność oraz uwierzytelnienie:

- Poufność – Poufność opiera się na szyfrowaniu danych algorytmem AES256, uniemożliwiającym odszyfrowanie danych przez niepożądane osoby.
- Integralność – Integralność zapewniana jest poprzez wykorzystanie tls-auth opierającego się na dodawaniu dodatkowych podpisów HMAC przy każdym wyzwaniu handshaku pakietów SLL/TLS. Takie rozwiązanie chroni przez atakami typu DoS, zalewanie portów, zalewanie bufora, nadsłuchiwaniem portów, czy przechwyceniem handshaku.
- Uwierzytelnienie – Uwierzytelnienie tego protokołu polega na wieloetapowym uwierzytelnienia osoby korzystającej. Zaczynając od lokalnego uwierzytelnienia korzystającego z haszu hasła (SHA256) wraz z użyciem PSK (pre-shared key), czyli użyciu kluczy haszujących pozwalających na stworzenie takich haszy, ich wymianę oraz potwierdzenie swoich tożsamości. Następnie można dodatkowo skorzystać z zewnętrznego uwierzytelnienia na serwerze, przy użyciu systemów takich jak PAM, LDAP, RADIUS czy SAML. Wszystko

przy wykorzystaniu certyfikatów uwierzytelniających. Najpierw jednak wymagane jest skonfigurowanie takiej formy uwierzytelnienia na serwerze przez administratora.

Prostota konfiguracji – Konfiguracja na poziomie klienckim jest banalnie prosta, wystarczy pobrać aplikacje OpenVPN CONNECT, a następnie załadować plik .OVPN, pozwalający na skorzystanie z bezpiecznego połączenia tunelowego. Natomiast konfiguracja na poziomie serwera jest nieco bardziej skomplikowana

Potencjalna prędkość – Prędkość tego protokołu jest zadziwiająco szybka, biorąc pod uwagę, ilość kodu w implementacji. Oczywiście sama prędkość będzie w górnej mierze zależna od transferu oferowanego przez dostawcę Internetu jak i serwera.

Stabilność – Stabilność jest na bardzo dobrym poziomie, ponieważ aplikacja ciągle jest pod ścisłym nadzorem, posiada ona ogromną społeczność, która jest w stanie informować na bieżąco o błędach jakie napotkali. Nie można zapomnieć, że nadal jest to aplikacja, dlatego zawsze istnieje szansa na wystąpienie jakiegoś błędu, lecz pożytkując się dokumentacją z oficjalnej strony OpenVPN, można skorzystać ze stabilnej wersji aplikacji wraz z konfiguracją nastawioną głównie na stabilność działania.

Zastosowanie – Zastosowanie tego protokołu jest wszechstronne. Wspiera on większość platform, jest prosty w konfiguracji, posiada graficzny interfejs. Jest to znakomita aplikacja spełniająca rolę protokołu do połączeń VPN.

WireGuard

WireGuard klasyfikuje się jakoś pomiędzy aplikacją połączeniową, a protokołem komunikacyjnym, ponieważ jest to protokół komunikacyjny sam w sobie, ale posiada także oprogramowanie typu open-source. Używa podejścia z książki „The State-of-the-Art Cryptography Techniques for Secure Data Transmission” Bhanu Chander (Pondicherry University, India). Jest to oprogramowanie między platformowe. Wydane w 2015 roku, a w 2020 roku, gdzie zapotrzebowanie na bezpieczną zdalną komunikacją sięgało zenitu, ukazała się wersja na systemy operacyjne Linux. WireGuard skupia się na prostocie co niesie za sobą wysoką wydajność, minimalne pole ataku oraz prostotę użytkowania.

Specyfikacja

Algorytm szyfrujący – WireGuard w porównaniu do obecnej konkurencji jaką jest OpenVPN, który korzysta z AES256, WireGuard korzysta z ChaCha20, który jest znacznie szybszym algorytmem szyfrującym ponieważ, jest symetrycznym algorytmem, tzn. potrzeba tylko jednego klucza do szyfrowania i deszyfrowania. Głównym wyborem algorytmu ChaCha20 jest lepsza wydajność oraz fakt, że procesory typu ARM jak np. na urządzeniach mobilnych, czy nowe macbooki, posiadają jeszcze

lepszą jakość, ponieważ procesory typu x86, które są od dawna produkowane i głównie znajdują się w komputerach stacjonarnych wspierają zbiór instrukcji przeznaczony dla algorytmu AES.

Bezpieczeństwo – Bezpieczeństwo protokołu można sprawdzić poprzez 3 warianty poufność, integralność oraz uwierzytelnienie:

- Poufność – Poufność jest zapewniana poprzez szyfrowanie danych wysyłanych podczas transmisji danych przy użyciu takich algorytmów jak ChaCha20. Ten algorytm jest bardzo skuteczny, wydajny jak i oferuję duże bezpieczeństwo danych.
- Integralność – Integralność w tym przypadku, również się opiera o skróty haszy przy pomocy HMAC, jednak warto nadmienić ze integralność nie jest tutaj priorytetem tak samo jak przy OpenVPN, gdzie wszystkie adresy IP są trzymane w bazie danych przez co wszystko powierzamy firmie zewnętrznej.
- Uwierzytelnienie – Uwierzytelnianie odbywa się poprzez parę kluczy, prywatny oraz publiczny. Gdzie klucz publiczny jest w posiadaniu serwera, a klucz prywatny u użytkownika, dlatego te klucze nie powinny nigdy być transportowane razem. Do tego serwer posiada także certyfikat roota, czyli jak użytkownik chce się połączyć z serwerem to jest weryfikowany ten certyfikat i taki użytkownik może nawiązać połączenie, serwer posiada także bazę wszystkich klientów jako peery, które są identyfikowane jako klucze publiczne oraz posiada własny klucz prywatny do nawiązywania połączenia. Gdzie użytkownik posiada tylko klucz prywatny i wie że jest jednym peerem w bazie serwera.

Prostota konfiguracji – Konfiguracja jest bardzo prosta, na Linuxie jest już od 2020 automatycznie zaimplementowana w systemie, natomiast na Windowsie czy innych systemach operacyjnych wystarczy pobrać i zainstalować klienta co zajmuje nie więcej niż 10 minut.

Potencjalna prędkość – Prędkość jest dla tego protokołu priorytetem, dlatego jest ona na najwyższym poziomie, krótka implementacja kodu w języku C, jak i wy korzystanie symetrycznego algorytmu szyfrującego niesie za sobą, bardzo wydajne doznanie, co przoduje względem konkurencji.

Stabilność – Stabilność jest podobna lub lepsza od protokołu OpenVPN, co już jest imponujące. Jest to poprzez zastosowanie, bardzo prostej struktury wykorzystania punktów końcowych do połączenia, wraz z możliwością zmiany połączenia bez straty ciągłości połączenia.

Zastosowanie – Jest to bardzo uniwersalne narzędzie, które niesie za sobą jakość i bezpieczeństwo w parze, bardzo dobrze sprawdza się przy komputerach stacjonarnych i przoduje przy jednostkach mobilnych opartych o procesory ARM.

Podsumowanie

Jest to nowe rozwiązanie, które jest w stanie zrewolucjonizować bezpieczne połączenia VPN. Przez fakt istnienia na rynku 8 lat jest zawsze szansa, że gdzieś znajdzie się luka, która sprowadzi to rozwiązanie na dno, lecz nadal żadnej takiej nie było. Co tylko potwierdza wielkość tego rozwiązania.

Porównanie przedstawionych rozwiązań

Poniżej przedstawiona zostaje tabela porównawcza, powyżej prezentowanych rozwiązań VPN pod wszelakimi względami. Dokładny opis względów bezpieczeństwa znajduję się w specyfikacji danego protokołu podzielony na 3 najważniejsze czynniki takie jak poufność, integralność czy uwierzytelnianie. Wiele z tych kategorii posiada podobne rozwiązania technologiczne, dlatego w tabeli znajduję się ogólnikowe porównanie. Większość popularnych rozwiązań na dzień dzisiejszy tj. 08.01.2023. Nie posiada żadnych udanych ataków, ze względu na wykorzystanie algorytmów szyfrujących zawierających się w dzisiejszych standardach.

	Algorytm Szyfrujący	Bezpieczeństwo	Konfiguracja	Prędkość	Stabilność	Zastosowanie
PPTP	MPPE 128-bit	Niskie	Prosta	Szybka	Wysoka	Starsze urządzenia
IKEv2/IPsec	AES256 256-bit	Duże (brak zagrożeń na tę chwilę)	Prosta klient Trudna samemu	Szybka	Wysoka	Urządzenia mobilne
OpenVPN	AES256 256-bit	Duże (brak zagrożeń na tę chwilę)	Prosta klient Średnia serwer	Szybka	Wysoka	Różnorodne
WireGuard	ChaCha20 256-bit	Duże (brak zagrożeń na tę chwilę)	Prosta	Szybka	Bardzo Wysoka	Różnorodne

Podsumowanie

Podsumowując protokoły takie jak IKEv2/IPsec, OpenVPN, WireGuard są rozwiązaniami spełniającymi kryteria bezpieczeństwa na najwyższym poziomie. Ich zastosowanie jest wszelakie w większości konfiguracja nie zajmuje dłużej niż 5 minut. Według mojej opinii dwoma najlepszymi rozwiązaniami są OpenVPN oraz WireGuard, oferują one największe możliwości, niosąc za sobą proste interfejsy graficzne, które są w stanie zebrać rzeszę osób niezwiązanych z cyberbezpieczeństwem jak i fanatyków anonimowości w Internecie. Warto wspomnieć, że serwisy takie jak NordVPN oraz Surfshark wspierają rozwiązanie OpenVPN, jak i WireGuard, co potwierdza wybór tych dwóch rozwiązań jako jeden z lepszych na obecną chwilę.

Bibliografia

Library and Technology Services. EWFM Library, 8A East Packer Ave, Lehigh University, Bethlehem, PA 18015.[dostęp: 06.01.2023]. Dostęp w Internecie: https://lts.lehigh.edu/services/explanation/vpn-overview

Artykuł „What is a VPN?" Paul Ferguson, Geoff Huston. [dostęp 06.01.2023]. Dostęp w Internecie: https://uh.edu/tech/cisre/resources/ia-resources/_files/7033/Week7/vpn2.pdf

Atyukuł „Pointto Point Tunneling Protocol PPTP" aktualizowany [02 Jan 2023] [dostęp 06.01.2023]. Dostęp w Internecie: https://www.serverbrain.org/certificate-security-2003/pointtopoint-tunneling-protocol-pptp.html

Pomoc techniczna firmy Microsoft [dostęp 06.01.2023]. Dostęp w Internecie: https://support.microsoft.com/pl-pl/topic/wdra%C5%BCanie-uwierzytelniania-peap-ms-chap-v2-w-sieciach-microsoft-pptp-vpn-d5ca1ebe-d9ee-4379-fd3f-e7be05fa3ae2

Artykuł „Hacking any PPTP VPN in 3 Minutes" [Dostęp 06.01.2023]. Dostęp w Internecie: https://rfsp.blogspot.com/2016/11/hacking-any-pptp-vpn-in-3-minutes.html

Artykuły uzupełniające ze strony Wikipedia [Dostęp 07.01.2023]. Dostęp w Internecie: https://en.wikipedia.org/wiki/Virtual_private_network

Artykuł „IKEv2 VPN: the guide that answers all of your questions" na portalu Surfshark [Dostęp 08.01.2023]. Dostęp w Internecie: https://surfshark.com/blog/ikev2-vpn

Dokumentacja OpenVPN [Dostęp 08.01.2023]. Dostęp w Internecie: https://openvpn.net

Dokumentacja WireGuard [Dostęp 08.01.2023]. Dostęp w Internecie: https://www.wireguard.com