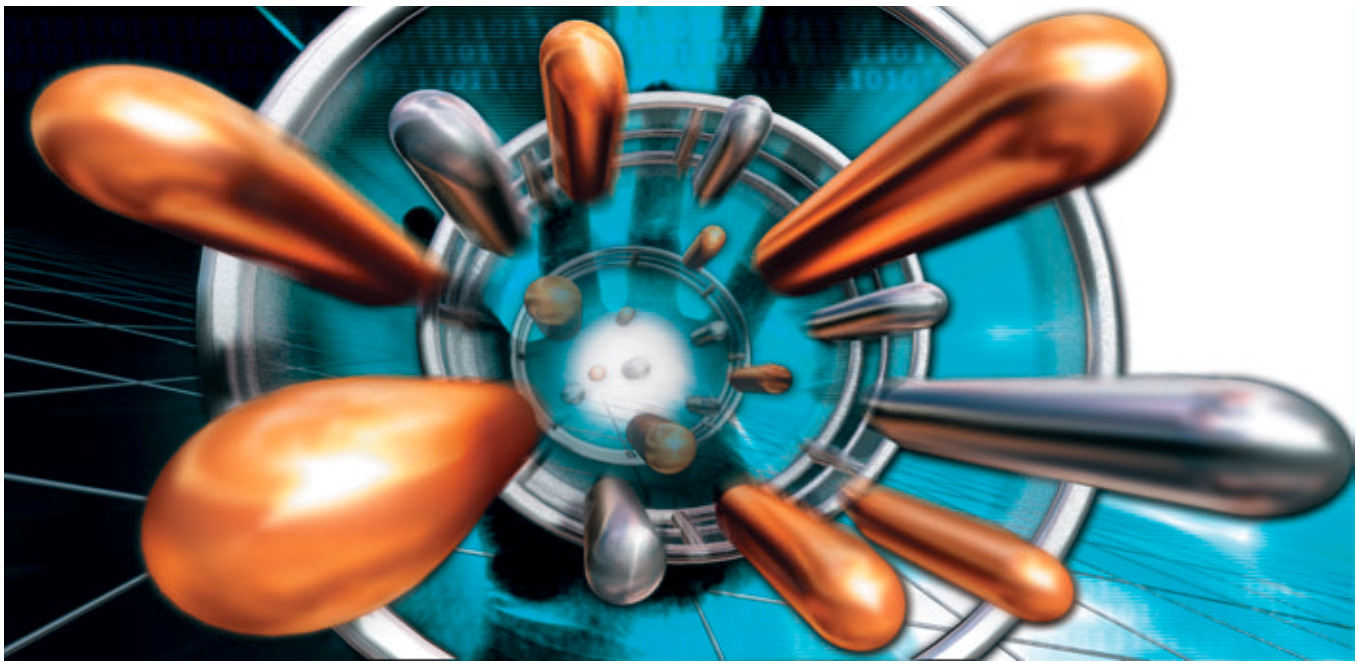


tomek siara

Tunelem do celu

Czy aby móc bezpiecznie przesyłać dane, trzeba wydawać pieniądze na kosztowne urządzenia dostępowe i dzierżawić linie telekomunikacyjne? Okazuje się, że powszechnie wykorzystywany Internet może służyć także do stworzenia prywatnej sieci.

Gdy administrator sieci komputerowej musi zapewnić w swojej firmie możliwość przekazywania danych między kilkoma oddziałami, wówczas ma do wyboru skonfigurowanie połączenia modemowego, wydzierżawienie osobnej linii telekomunikacyjnej lub zlecenie obsługi zdalnego dostępu zewnętrznej, specjalistycznej firmie. Pierwsze rozwiązane jest tanie, ale tylko w przypadku lokalnych połączeń. Kiedy filie są rozproszone po całym kraju, wówczas koszty połączeń telefonicznych mogą uczynić taką komunikację nieopłacalną. Pozostałe sposoby – mimo potencjalnie dużej szybkości i większej niezawodności – przy kilku lokalizacjach również mogą okazać się za drogie. Jeszcze gorzej jest w przypadku, kiedy firma ma wiele rozproszonych oddziałów, a pracownicy, którzy muszą mieć ciągły dostęp do korporacyjnej bazy danych, często podróżują. Wówczas mimo stałych łączy między oddziałami mobilni użytkownicy nadal zmuszeni są korzystać z drogich połączeń modemowych. Wówczas do wyboru jest rozwiązanie pośrednie, czyli wirtualna sieć prywatna (*Virtual Private Networking*, VPN). O technologii VPN warto pomyśleć nie tylko wtedy, gdy pracownicy firmy są często w podróży lub wykonują swoje zadania w domu, ale także kiedy wielu rozproszonym oddziałom trzeba zapewnić dostęp do zasobów wewnętrznej sieci korporacyjnej (intranetu).

Prywatny Internet?

VPN łączy dwa składniki jednej sieci komputerowej za pośrednictwem innej sieci. Technologię tę stworzono z myślą o wykorzystaniu istniejącej infrastruktury Internetu do bezpiecznego przesyłania poufnych informacji. Wiele firm (np. Intel lub Cisco) oferuje dedykowane urządzenia, jednak są one dość drogie w stosunku do alternatywnych rozwiązań programowych. Dzięki specjalnie zaprojektowanym protokołom możemy tworzyć sieci VPN na bazie systemów takich jak Windows, Linuks czy UNIX. Dlatego też użytkując któryś z tych systemów, nie musimy ponosić dodatkowych kosztów związanych z instalacją i konfiguracją sieci VPN. W przypadku Linuksa możemy skorzystać z pakietu Free SWAN, a na innych systemach uniksowych skonfigurować odpowiednio protokół IPSec. Z kolei w Windows zaimplementowano protokół PPTP (patrz: ramka „Protokoły tunelujące").

Działanie VPN polega na odpowiednim przetworzeniu danych, które mogą następnie zaszyfrowane podróżować w Internecie przez wirtualny kanał komunikacyjny. Protokół zapewniający transmisję nazywamy w tym przypadku protokołem tunelującym (*tunneling protocol*). Najogólniej mówiąc, zasada działania wirtualnego kanału polega na zestawieniu logicznego połączenia między komputerem użytkownika i serwerem. Obrazowo mówimy, że połączenie VPN to tunel biegnący przez Internet (lub inną sieć publiczną), pozwalający na bezpieczną pracę w taki sposób, jakby się miało bezpośrednie połączenie z siecią prywatną.

Zaleta VPN polega na tym, że aby bezpiecznie komunikować się z dowolnym miejscem na Ziemi, wystarczy ustanowić połączenie z lokalnym dostawcą usług internetowych (ISP – *Internet Service Provider*). W Polsce możemy skorzystać np. z numeru dostępowego TP SA (0202122). Dzięki globalnemu zasięgowi Sieci użytkownik oddalony od firmy o setki kilometrów może pracować na swoim komputerze, tak jakby był on połączony bezpośrednio z wewnętrzną siecią, i mieć dostęp do zasobów korporacyjnych. Podobnie mogą komunikować się z centralą firmy biura regionalne, oddziały i filie. Taka konfiguracja sprawia, że nie trzeba się martwić o wysokie koszty połączeń telefonicznych ani o to, skąd możliwe będzie komunikowanie się. Z perspektywy użytkownika VPN zapewnia połączenie z punktu do punktu (*point-to-point*), a rodzaj i infrastruktura wykorzystywanej do przesyłania danych sieci publicznej nie mają znaczenia. Dane wędrują przez sieć, tak jakby przesyłane były przez dedykowaną linię prywatną, stąd nazwa – wirtualna sieć prywatna.

W najczęściej spotykanych przypadkach serwer VPN zezwala pojedynczemu komputerowi na dostęp do zasobów swoich lub

Protokoły tunelujące

Aby można było stworzyć wirtualny tunel, obydwie strony (serwer i klient) muszą używać tego samego protokołu tunelującego (*tunneling protocol*). Rozróżniamy protokoły warstwy 2. lub 3. (*Layer 2* lub *Layer 3*). Podział ten odpowiada modelowi odniesienia OSI (*Open Systems Interconnection Reference Model*, patrz: CHIP 11/1999, s. 108) opracowanemu przez międzynarodową organizację standaryzacyjną ISO (*International Standards Organisation*). Protokoły warstwy 2. są skojarzone z warstwą łącza danych (*data-link*) i używają ramek (*frames*) jako jednostki wymiany. Przykładami protokołów warstwy 2. są: protokół **PPTP** (*Point-to-Point Tunneling Protocol*), **L2TP** (*Layer 2 Tunneling Protocol*) oraz **L2F** (*Layer 2 Forwarding*). Wszystkie wykorzystują ramki PPP do enkapsulacji pakietów wysyłanych przez sieć pośredniczącą. Stworzenie tunelu opartego na protokole warstwy 2. przypomina zwykłą sesję. Obydwie strony muszą być gotowe do nawiązania połączenia oraz muszą wynegocjować konfigurację jego parametrów przypisania adresów, szyfrowania oraz kompresji. W większości przypadków dane transmitowane tunelem są przesyłane protokołem wykorzystującym datagramy. Jako mechanizm zarządzania tunelem używany jest dodatkowy protokół sterujący (*control protocol*).

L2F jest protokołem transmisyjnym zaproponowanym przez Cisco, który pozwala na przesyłanie pakietów PPP między sprzętowymi routerami. W rozwiązaniu tym za utrzymanie tunelu między dwiema lokalizacjami odpowiedzialne są te urządzenia, a stworzony w ten sposób tunel ma charakter obligatoryjny (*compulsory tunnel*, patrz: tekst).

Protokół L2TP w swoim założeniu łączy zalety rozwiązań PPTP (patrz: ramka „Meandry PPTP“) i L2F. Pozwala on na transport ramek PPP, ale nie tylko przez sieci IP, lecz również X. 25, Frame Relay lub ATM (*Asynchronous Transfer Mode*). W przypadku użycia nagłówka protokołu IP wykorzystuje się go do tunelowania danych przez Internet. Jednak dzięki swoim rozszerzonym możliwościom można go używać bezpośrednio w połączeniach WAN (np. Frame Relay) bez użycia warstwy transportowej IP. L2TP w sieci IP używa datagramów UDP (*User Datagram Protocol*) i komunikatów sterujących L2TP do utrzymania tunelu.

Protokoły warstwy 3. odpowiadają warstwie sieciowej w modelu OSI (*Network layer*) i posługują się pakietami (*packets*). Do warstwy 3. należy protokół **IP-over-IP** oraz **IPSec Tunnel Mode** (*IP Security Protocol*). Protokoły te szyfrują i kompresują oryginalne pakiety IP i dopisują do nich jeszcze jeden (tym razem jawny) nagłówek IP. Ponieważ protokół funkcjonuje w warstwie sieciowej, technika ta zakłada, że wszelkie parametry konfiguracyjne oraz proces uwierzytelniania są przeprowadzane przez wyższe warstwy (np. aplikacji). Z tego powodu nie występują tutaj problemy zarządzania parametrami tunelu, autoryzacji użytkowników oraz przypisywania adresów.

całej sieci lokalnej, w której się znajduje. Oprócz takiego bezpośredniego połączenia możliwe jest również stworzenie VPN między routerami. W taki sposób można zapewnić dostęp ze wszystkich i do wszystkich komputerów będących w odległych sieciach lokalnych.

W przypadku stacji roboczej (klienta) i serwera z zainstalowanym oprogramowaniem umożliwiającym połączenie mówimy o tzw. tunelu dobrowolnym (*voluntary tunnel*), który jest tworzony na żądanie klienta. Dedykowane routery mają natomiast fabrycznie zaimplementowaną możliwość zestawiania tzw. tunelu obligatoryjnego lub inaczej obowiązkowego (*compulsory tunnel*). Różnica między tymi rodzajami połączenia polega na tym, że w drugim tunelu nie występuje rola klienta i serwera, jego parametry są z góry określone, a użytkownicy w ogóle nie muszą o nim wiedzieć. Wykorzystywane tam protokoły są na ogół inne niż w przypadku rozwiązań programowych.

Zapuszkowane pakiety

Jak już wiemy, tunelowanie polega na wykorzystaniu istniejącej publicznej infrastruktury sieciowej do przesyłania danych z jednej prywatnej sieci do drugiej. Jednak jak się dzieje to, że informacje mogą bezpiecznie przemieszczać się przez Sieć, tak jakby były przesyłane w lokalnej sieci? Działanie VPN przestanie być dla nas tajemnicą, jeśli przyjrzymy się bliżej pracy protokołów sieciowych.

Aby strumień danych (*payload*) mógł być przekazywany między komputerami, najpierw oprogramowanie protokołu musi podzielić go na części. Podzielone dane są odpowiednio formowane i zaopatrywane m.in. w informacje o tym, skąd pochodzą, dokąd są adresowane i jaka jest ich kolejność. W taki sposób powstają pakiety (*packets*, np. IP, IPX lub NetBEUI). Następnie, aby umożliwić podróż pakietów przez fizyczne łącze, system zaopatruje je w dodatkowe niezbędne informacje, nadając im postać tzw. ramek (*frames*, np. Ethernet).

W sieciach lokalnych często używany jest protokół IP, ale ponieważ stosuje się tu adresy prywatne, nasze pakiety nie mogą być przesyłane w Internecie. Może się również zdarzyć, że inny wykorzystywany przez nas protokół (np. NetBEUI) nie jest trasowalny. Dlatego zamiast wysyłać pakiety w oryginalnej postaci protokół tunelujący enkapsuluje (obudowuje) je w pakiety-kapsułki mogące poruszać się w sieci pośredniczącej (np. Internecie). Takie „opakowane” ramki dają się porównać do samochodów załadowanych na pociąg i wyjeżdżających z fabryki. Podróż danych przez tunel przypomina transport tych pojazdów do punktu dystrybucji, gdzie zostaną one rozładowane i skąd rozjadą się „o własnych siłach”. Po drodze nikt nie może jednak z nich skorzystać.

Na tunelowanie składa się kilka procesów. Są to: enkapsulacja (w naszym przykładzie jest to odpowiednik załadunku samochodu na wagon kolejowy), transmisja (podróż do punktu rozładunku) oraz proces odwrotny do enkapsulacji (czyli rozładunek lub wyjmowanie z kapsułek). Ogólnie mówiąc, proces enkapsulacji polega na dopisaniu odpowiednich nagłówków do oryginalnych pakietów (patrz: ramka „Połączenie PPTP”). Logiczna droga, jaką pokonują enkapsulowane pakiety, zwana jest tunelem. Po dotarciu do punktu przeznaczenia oryginalne ramki są „oczyszczane” z dodatkowego nagłówka i przekazywane do miejsca przeznaczenia.

Czy to może być bezpieczne?

Zdalny dostęp do zasobów sieci lokalnej powinien być zapewniony z dowolnego miejsca oraz musi gwarantować ochronę prywatności i integralności danych w trakcie ich wędrówki przez Internet. Dlatego do podstawowych wymagań spełnianych przez połączenie VPN należą: autoryzacja użytkowników, przypisywanie adresów, szyfrowanie danych, zarządzanie kluczami szyfrującymi oraz możliwość zastosowania dowolnego protokołu sieciowego. Sieci VPN oparte na protokołach PPTP lub L2TP spełniają wszystkie powyższe wymagania. Inne rozwiązania, takie jak np. IPSec, nie zawierają wszystkich wymienionych mechanizmów i dlatego mogą być stosowane tylko w specyficznych sytuacjach.

Autoryzacja użytkowników zapewnia, że z połączenia VPN skorzystają wyłącznie uprawnieni ludzie, mający swój identyfikator i znający odpowiednie hasło. Dzięki identyfikacji możliwa jest inspekcja, czyli śledzenie i zapis tego, kto, kiedy i jakie informacje odczytuje. Zarządzanie adresowaniem pozwala na przypisywanie klientom adresów IP z prywatnej puli oraz gwarantuje, że adresy te nie zostaną ujawnione. Dzięki szyfrowaniu dane podróżujące przez Internet są nieczytelne dla pozostałych użytkowników, a mechanizmy zarządzania kluczami szyfrującymi dbają o częstą wymianę używanych przez serwer i klienta kodów. Największą zaletą połączenia VPN jest to, że przez wirtualny kanał można przekazywać pakiety lub datagramy dowolnych, używanych w prywatnej sieci protokołów transmisyjnych.

Na nic podsłuch

Zapewnienie bezpieczeństwa jest podstawowym wymogiem połączenia VPN. Gdyby tunelowane pakiety nie były w żaden sposób ▸ 182

chronione, wówczas każdy mógłby przechwycić transportowane dane i wykorzystać je. Nie byłoby to zgodne z ideą prywatnej sieci. Dlatego aby zapewnić poufność i bezpieczeństwo danych, nadawca dodatkowo musi je zaszyfrować. Deszyfrowanie po stronie odbiorcy możliwe jest tylko wtedy, gdy obie strony znają wspólny, tajny klucz. Dzięki temu zawartość przechwyconych w Internecie pakietów jest nieczytelna dla osób postronnych. Najważniejszym czynnikiem wpływającym na stopień bezpieczeństwa VPN, jest oprócz jakości algorytmu utajniania długość użytego klucza. Do złamania szyfru można używać różnych technik, jednak im dłuższy klucz, tym większej wymagają one mocy obliczeniowej. Z tego powodu dobrze jest używać możliwie najdłuższego klucza. Drugim czynnikiem wpływającym na skuteczność szyfrowania jest ilość przesyłanych danych. Okazuje się bowiem, że im więcej danych jest szyfrowanych za pomocą tego samego klucza, tym łatwiej jest go złamać. Dlatego w połączeniu VPN ma miejsce częsta zmiana klucza w czasie transmisji.

Dla przykładu: w implementacji Microsoftu każdy pakiet jest szyfrowany innym kluczem. System Windows NT korzysta z mechanizmów utajniających Microsoft Point-to-Point Encryption (MPPE), które używają szyfru strumieniowego RC4. Dopuszczalna długość użytego tu klucza (40 lub 128 bitów) jest domyślnie negocjowana między klientem i serwerem w trakcie ustanawiania połączenia, a wymianę klucza zapewnia algorytm RSA. Można jednak wymusić, że serwer będzie wymagał zawsze najlepszego szyfrowania i wówczas klient, który nie obsługuje 128-bitowego szyfrowania nie nawiąże połączenia. W mechanizmie MPPE każdy pakiet otrzymuje w nagłówku kolejny numer, a klucz szyfrujący zmienia się dla kolejnych pakietów w zależności od tego numeru. Dlatego też deszyfrowanie pakietów jest niezależne od kolejności ich dotarcia. Jeśli pakiety zostaną zagubione lub dotrą zbyt późno, to i tak odczytując ich numer, system może dobrać odpowiednią wartość klucza.

Sposoby autoryzacji PPP

Metoda autoryzacji **PAP** (*Password Authentication Protocol*) oparta jest na prostym schemacie wymiany niezaszyfrowanych informacji. Serwer dostępowy żąda nazwy użytkownika i hasła, a klient wysyła mu je w jawnej postaci. Ten sposób autoryzacji nie jest oczywiście bezpieczny, ponieważ każdy może przechwycić w sieci przekazywane dane i użyć ich do dostępu. Dlatego PAP nie chroni przed żadnymi atakami, jeżeli hasło nie będzie w żaden sposób zabezpieczone.

CHAP (*Challenge-Handshake Authentication Protocol*) jest mechanizmem autoryzacji wykorzystującym szyfrowanie i zabezpieczającym przed wysłaniem nieutajnionego hasła. Serwer dostępowy wysyła do klienta komunikat-wezwanie (*challenge*), który składa się z identyfikatora sesji (*session ID*) oraz losowego ciągu znaków. Klient używa algorytmu MD5 w celu wygenerowania wartości skrótu (patrz: CHIP 10/2000, s. 190) na podstawie identyfikatora sesji, dostarczonego ciągu znaków oraz hasła. Wygenerowaną wartość wraz z niezaszyfrowaną nazwą użytkownika klient odsyła (*response*) do serwera. Serwer zna prawdziwe hasło, identyfikator sesji oraz wysłany ciąg znaków i dlatego może powtórzyć obliczenie wartości skrótu i porównać wynik z informacjami nadesłanymi przez klienta. Dzięki temu mechanizmowi nie jest możliwe podszycie się pod uprawnionego klienta i wysłanie w celu autoryzacji przechwyconych wcześniej, oryginalnych informacji, ponieważ przy każdej próbie autoryzacji serwer generuje nowy ciąg znaków. Dodatkowo metoda CHAP skutecznie zapobiega przejęciu sesji, gdyż w trakcie trwania połączenia w nieprzewidywalnych odstępach czasu serwer wysyła ponowne wezwania do klienta. Nie znając hasła, nieupoważniony klient nie może prawidłowo odpowiedzieć i wówczas serwer decyduje o rozłączeniu.

MS-CHAP (*Microsoft CHAP*) różni się od poprzedniego rozwiązania tym, że użyty algorytm to MD4. Ponadto klient w odpowiedzi na wezwanie serwera odsyła nazwę użytkownika wraz z wartością skrótu, obliczoną na podstawie dostarczonego przez serwer identyfikatora sesji i losowego ciągu znaków oraz skrótu hasła. Podnosi to bezpieczeństwo, ponieważ serwer nie przechowuje hasła użytkownika, a jedynie jego wartość skrótu.

Uwierzytelnianie VPN może być zrealizowane również przez inne protokoły, takie jak **EAP** (*Extensible Authentication Protocol*) lub **SPAP** (*Shiva PAP*).

Na początku był modem

Protokoły tunelujące warstwy 2. bazują na standardzie PPP (*Point-to-Point Protocol*), który został zaprojektowany w celu przesyłania danych za pośrednictwem modemowych lub dedykowanych połączeń z punktu do punktu. Protokół, o którym mowa, enkapsuluje pakiety IP, IPX lub NetBEUI w ramki PPP, a następnie transmituje je przez ustanowione połączenie komutowane. Przykładem wykorzystania protokołu PPP jest połączenie modemowe z numerem dostępowym do Internetu TP SA. W trakcie ustanawiania sesji odbywają się cztery fazy negocjacji, które muszą zakończyć się sukcesem, aby dane mogły być przesyłane (patrz: ramka „Połączenie PPP").

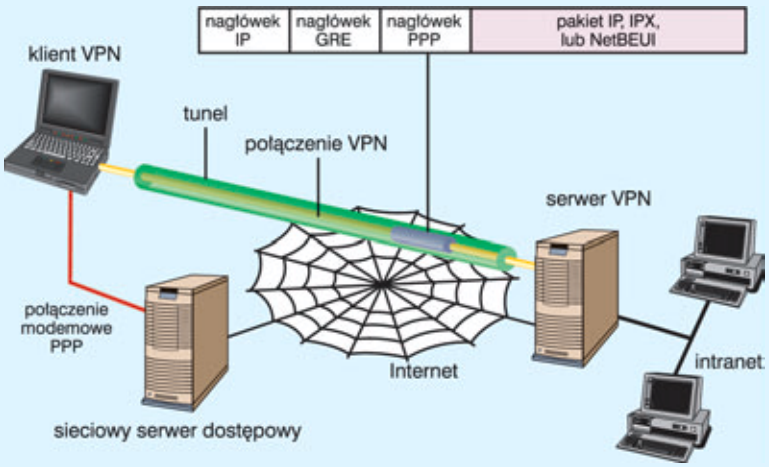
W kapsułkach do celu

Przykładem protokołu warstwy 2. zaimplementowanym przez Microsoft w systemie Windows jest protokół PPTP. Jest on odpowiedzialny za umieszczanie ramek protokołu PPP w datagramach IP (*Internet Protocol*) w celu transmisji przez sieć, jaką jest Internet. PPTP zapewnia utworzenie, utrzymanie i zamknięcie tunelu. Aby możliwa była wymiana pakietów, musi istnieć połączenie IP pomiędzy klientem i serwerem PPTP.

Po otrzymaniu danych sieciowy serwer dostępowy (*Network Access Server*, NAS) dostawcy ISP odrzuca ramkę PPP i zastępuje ją inną, właściwą dla używanej dalej sieci. W celu odczytania przesyłanych danych serwer lub klient PPTP musi kolejno przetworzyć i odrzucić ramkę łącza danych, nagłówek IP, nagłówki GRE i PPP, a następnie zdekompresować i rozszyfrować uzyskaną w ten sposób porcję danych oraz przekazać

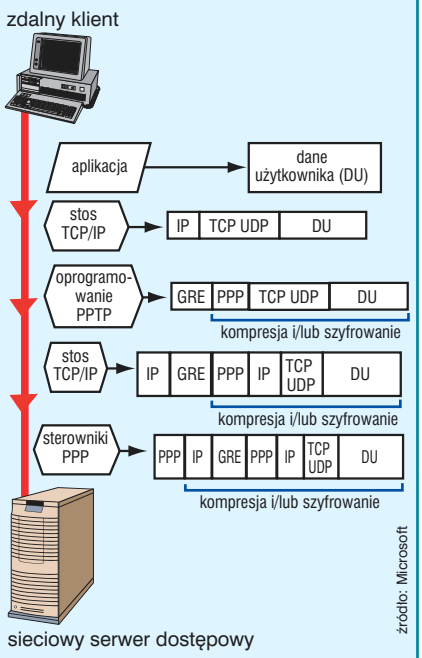
185

Składniki połączenia VPN



W połączeniu VPN dane z prywatnej sieci podróżują do serwera wirtualnym tunelem. W rzeczywistości najpierw pakiety są przesyłane od klienta do sieciowego serwera dostępowego, skąd są przekazywane do Sieci, a dopiero później do serwera VPN.

Jak powstaje pakiet PPTP



Transport pakietów przez sieć polega na dopisywaniu do nich odpowiednich nagłówków w kolejnych etapach. Najpierw aplikacja kliencka generuje dane przeznaczone do wysłania (na rysunku: Dane Użytkownika, DU). Wówczas używany w sieci prywatnej protokół sieciowy (na przykładzie TCP/IP) zaopatruje je w odpowiednie nagłówki, tworząc pakiety. W kolejnym etapie oprogramowanie PPTP szyfruje i/lub kompresuje je, a następnie dopisuje do nich nagłówek PPP. Do powstałej w ten sposób ramki PPP dopisywany jest kolejny nagłówek, tym razem GRE (protokół GRE zaprojektowano w celu stworzenia powszechnego, łatwego i szybkiego mechanizmu enkapsulacji danych przesyłanych przez sieci IP i nadano mu numer 47). Tak przygotowany pakiet GRE jest następnie przekazywany pod kontrolę stosu TCP/IP i otrzymuje nagłówek IP zawierający informacje o internetowych adresach: docelowym serwera i źródłowym klienta PPTP. Na koniec datagram IP jest dodatkowo umieszczany w ramce warstwy łącza danych, której format określa architektura warstwy fizycznej. W przypadku klienta i zwykłego modemu lub karty ISDN jest to ramka PPP. Po jej otrzymaniu sieciowy serwer dostępowy (Network Access Server, NAS) dostawcy ISP odrzuca ramkę PPP i zastępuje ją inną, właściwą dla używanej dalej sieci.

Połączenie PPP

W pierwszej fazie ustanowienia połączenia (*link establishment*) PPP wykorzystuje protokół LCP (*Link Control Protocol*) w celu zarządzania fizycznym połączeniem (nawiązanie, utrzymanie, zakończenie). W fazie tej protokół dokonuje wyboru sposobu autoryzacji (patrz: ramka „Sposoby autoryzacji PPP") oraz ustala, czy strony będą używały kompresji i szyfrowania. Ostateczny wybór algorytmów oraz inne szczegóły są jednak precyzowane w ostatniej fazie.

Kolejny etap to autoryzacja użytkownika (*User Authentication*). W tej fazie komputer klienta prezentuje serwerowi informacje o użytkowniku. Specjalne metody bezpiecznej autoryzacji wykluczają możliwość ataków opierających się na wysłaniu przechwyconych wcześniej pakietów (*replay attack*) lub przejęciu kontroli nad ustanowionym już połączeniem (*client impersonation*). Atak pierwszego rodzaju polega na podszyciu się pod prawdziwego klienta i wysyłaniu przechwyconych w trakcie oryginalnej autoryzacji pakietów w odpowiedzi na żądania serwera. W przypadku drugiego rodzaju ataku haker czeka do momentu zakończenia autoryzacji, a następnie przechwytuje parametry połączenia, odłącza uprawnionego użytkownika i przejmuje kontrolę nad połączeniem. Większość implementacji PPP ogranicza się do dwóch lub trzech metod autoryzacji. W przypadku Windows mogą to być metody PAP, CHAP lub MS-CHAP.

Po dokonaniu autoryzacji następuje sprawdzenie warunków połączenia zwrotnego (*PPP Callback Control*). Jest to faza opcjonalna, która wykorzystuje protokół CBCP (*Callback Control Protocol*). Jeżeli zarówno serwer z modemem dostępowym, jak i klient są w taki sposób skonfigurowane, to w tym momencie wymuszane jest rozłączenie i serwer łączy się za pomocą zdefiniowanego wcześniej numeru telefonicznego z klientem. Pozwala to na zachowanie jeszcze większego bezpieczeństwa, ponieważ w ten sposób możliwe jest połączenie wyłącznie z określonym miejscem.

Na koniec w czwartej fazie (*Invoking Network Layer Protocol*) PPP inicjuje sterujące protokoły kontrolne (*control protocols*) warstwy sieciowej w celu skonfigurowania parametrów uzgodnionych w fazie pierwszej. Dla przykładu: protokół IPCP (*IP Control Protocol*) przypisuje dynamiczny adres IP klientowi, a protokół kontroli kompresji CCP (*Compression Control Protocol*) negocjuje warunki kompresji i szyfrowania. W systemie Windows odpowiedzialne są za to odpowiednio mechanizm MPPC (*Microsoft Point-to-Point Compression*) i MPPE (*Microsoft Point-to-Point Encryption*). Po zakończeniu wszystkich etapów negocjacji PPP rozpoczyna przekazywanie danych w obydwu kierunkach. Do każdego wysyłanego pakietu dopisuje się nagłówek PPP, który jest odrzucany przez system odbiorcy. Jeśli kompresja danych została wynegocjowana w fazie 1. i skonfigurowana w fazie 4., wówczas dane są dodatkowo kompresowane przed wysłaniem. Podobnie jest w przypadku szyfrowania.

ją dalej. Uwierzytelnianie, które odbywa się podczas tworzenia połączenia VPN opartego na PPTP, korzysta z tych samych mechanizmów co uwierzytelnianie połączeń PPP. Mogą to być w szczególności metody CHAP lub PAP.

W intranecie i w Internecie

Dzięki uniwersalności rozwiązania VPN stosuje się je zarówno do łączenia pojedynczych komputerów, jak i całych sieci. Typowe połączenie VPN może działać i za pośrednictwem Internetu, i wewnątrz prywatnej sieci lokalnej. Dzięki obecności serwera podłączonego do Internetu użytkownik komputera wyposażonego w modem może się połączyć z oddaloną o setki kilometrów siecią korporacyjną, płacąc jedynie za lokalne połączenie telefoniczne. Po uzyskaniu dostępu do Internetu klient inicjuje połączenie z serwerem w swojej firmie, a następnie uzyskuje dostęp do zasobów intranetu. W przypadku połączenia dwóch sieci lokalnych odpowiednio skonfigurowane routery przekazują pomiędzy sobą dane przez kanał VPN.

W wielu firmach dane z niektórych działów są często tak bardzo poufne, iż pozostali pracownicy nie powinni mieć do nich dostępu. W takich przypadkach stosuje się fizyczne oddzielenie sieci danego departamentu od reszty intranetu. Chroni to dane, utrudnia jednak komunikację i przesyłanie pozostałych informacji. Zastosowanie wirtualnej sieci prywatnej eliminuje ten problem, gdyż dzięki niej oddzielony wcześniej segment może być fizycznie połączony z całą siecią za pośrednictwem serwera VPN. Komputer ten nie pozwala na bezpośrednie przekazywanie informacji pomiędzy sieciami, umożliwia jednak uprawnionym użytkownikom dostęp do chronionej części za pośrednictwem szyfrowanego połączenia. Dla osób, które nie mają odpowiednich uprawnień, oddzielony segment jest po prostu niedostępny.

Dmuchanie na zimne?

Praktycznie we wszystkich firmach dostęp do Internetu zapewniony jest za pośrednictwem specjalnego serwera lub routera pełniącego funkcję tzw. zapory ogniowej (*firewall*). Jej zadaniem jest filtrowanie pakietów i pilnowanie dostępu do lokalnych zasobów. Krótko mówiąc, firewall decyduje o tym jaki rodzaj komunikacji zachodzi między siecią lokalną i Internetem. Filtrowanie pakietów pozwala na precyzyjne określenie, które usługi sieciowe mogą być dostarczane z zewnątrz, i odgrywa kluczową rolę w bezpieczeństwie sieci wewnętrznej. W przypadku zastosowania serwera VPN razem z zaporą ogniową stosuje się dwa podejścia. Serwer VPN może znajdować się przed firewallem i mieć bezpośrednie połączenie z Internetem lub może znajdować się między siecią lokalną a firewallem.

Jeżeli zdecydujemy się na postawienie serwera VPN przed zaporą ogniową, to powinniśmy ▸ 186

Meandry PPTP

O zwykłej karcie sieciowej często mówi się, że jest ona sprzętowym (fizycznym) interfejsem, ponieważ pełni w systemie rolę urządzenia odpowiedzialnego za przekazywanie pakietów do warstwy fizycznej sieci. W trakcie nawiązywania połączenia VPN zarówno na serwerze, jak i na stacji roboczej tworzony jest tzw. wirtualny interfejs. Nie odpowiada on żadnemu konkretnemu urządzeniu, ale z punktu widzenia komunikacji sieciowej zachowuje się jak karta Dial-Up czy sieciowa. Po ustanowieniu tunelu tworzy on wirtualne połączenie typu point-to-point. Interfejs klienta ma przyporządkowany adres IP – tak samo jak normalna karta sieciowa. Przypisywaniem adresów zajmuje się serwer. Domyślnie powinny one być uzyskiwane za pomocą usługi DHCP (*Dynamic Host Configuration Protocol*), jednak możliwe jest również skonfigurowanie stałych adresów. Serwer VPN ma zazwyczaj dwa fizyczne interfejsy sieciowe: jeden podłączony do sieci zewnętrznej (np. Internet), a drugi do prywatnej sieci lokalnej. W przypadku połączeń VPN dla każdego klienta tworzony jest osobny wirtualny interfejs.

Aby możliwe było przekazywanie danych pomiędzy klientami, trzeba skonfigurować przekazywanie ruchu IP dla wszystkich interfejsów. Jednakże zezwolenie na trasowanie (*routing*) pomiędzy fizycznymi interfejsami spowoduje, że serwer będzie bez przeszkód przekazywał wszystkie pakiety z sieci publicznej do prywatnej. Aby ochronić sieć lokalną przed dostępem z zewnątrz, należy skonfigurować tzw. filtrowanie PPTP. Zapewni to przekazywanie danych przez serwer tylko pomiędzy klientami VPN i siecią wewnętrzną oraz wykluczy możliwość nieautoryzowanego dostępu z zewnątrz.

Filtrowanie pakietów polega na określeniu, jakie informacje mogą być przekazywane do i z chronionej sieci. Dla interfejsu internetowego serwera musimy zezwolić na dopuszczanie pakietów na porcie TCP numer 1723 (pozwoli to na przekazywanie wiadomości sterujących tunelem od klienta) oraz protokołu IP GRE numer 47 (co umożliwi przekazywanie tunelowanych danych). Aby zapewnić ruch pakietów kontrolnych do klienta, należy również zezwolić na wysyłanie pakietów od serwera, wychodzących z portu 1723, by jednak możliwe było tunelowanie danych w tym kierunku, trzeba umożliwić także wychodzenie pakietów protokołu IP GRE.

Kiedy wirtualny interfejs klienta otrzyma właściwy adres IP jednocześnie musi nastąpić zmiana w jego tablicy routingu. Adres domyślnej bramy powinien być ustalony w taki sposób, aby dane wędrowały przez bezpieczne połączenie zamiast bezpośrednio przez sieć pośredniczącą. W przypadku Windows w trakcie ustanawiania połączenia serwer przypisuje adres zdalnemu klientowi, a jego system zmienia domyślną ścieżkę routingu, tak aby wszystkie dane wysyłane były przez nowo utworzony wirtualny interfejs.

Komputerom, które przed połączeniem z serwerem VPN muszą połączyć się przez modem z sieciowym serwerem dostępowym, przypisywane są dwa adresy. Pierwszy to internetowy adres IP, przydzielany w trakcie połączenia PPP przez dostawcę usług internetowych do karty Dial-Up. Drugi natomiast jest przydzielany przez serwer VPN do wirtualnego interfejsu PPTP. Najczęściej jest to adres z prywatnej podsieci wewnętrznej, ponieważ musi on być osiągalny przez komputery znajdujące się w intranecie.

Tunelowane dane są przesyłane między adresem przydzielonym przez serwer VPN a adresami komputerów znajdujących się w intranecie. Jednakże routery internetowe mogą przetwarzać jedynie pakiety z adresami publicznymi i przekazywać je do zewnętrznego interfejsu serwera VPN. Dlatego do oryginalnych pakietów dopisywany jest dodatkowy nagłówek IP, pozwalający na przekazywanie pakietu między adresem przydzielonym przez dostawcę usług internetowych i publicznym adresem serwera.

Aby móc otrzymywać dane z Internetu, system klienta PPP dodaje do tablicy routingu domyślną ścieżkę, wskazującą na interfejs Dial-Up połączony z Internetem. W rezultacie komputer może przekazywać datagramy do swojego dostawcy, skąd trafiają one do Internetu. Jest to najczęściej spotykany przypadek komputera domowego, który nie ma kart sieciowych. Dzięki temu wszystkie adresy internetowe są osiągalne poprzez router znajdujący się u dostawcy. Po ustanowieniu połączenia VPN tworzona jest nowa domyślna trasa routingu, wskazująca na wirtualny interfejs należący do tunelu. Poprzednia domyślna droga jest zachowywana z wyższą metryką. Dodanie nowej domyślnej trasy oznacza, że wszystkie internetowe lokalizacje poza adresem serwera VPN będą nieosiągalne.

skonfigurować odpowiednio filtrowanie pakietów na interfejsie internetowym, tak aby przepuszczał on tylko pakiety z i do kanału VPN. Po odszyfrowaniu pakietów serwer VPN przekaże je do firewalla, który pozwoli na ich transport do wewnętrznej sieci. Ponieważ ruch przychodzący z serwera VPN jest generowany tylko przez uwierzytelnionych klientów, filtrowanie na zaporze może być użyte do ochrony przed ich dostępem do niektórych specjalnych zasobów wewnętrznych. Z drugiej strony, ponieważ dowolny ruch z Internetu musi przejść przez serwer VPN, można w ten sposób ograniczyć dostęp do intranetowych usług FTP lub WWW tylko do użytkowników VPN.

Częściej spotykaną konfiguracją jest umieszczenie serwera VPN za zaporą ogniową w tzw. strefie zdemilitaryzowanej (DMZ – *demilitarized zone*). Strefa DMZ jest segmentem sieci IP chronionym przez zaporę, ale zawierającym zasoby dostępne dla użytkowników z Internetu (serwer FTP, WWW). W tym przypadku serwer VPN ma jedną kartę sieciową połączoną ze strefą DMZ, a drugą z intranetem. Przy takim rozwiązaniu omówione wcześniej filtry muszą być skonfigurowane dla zewnętrznego interfejsu firewalla. Dodatkowe filtry mogą zezwalać na dostęp do serwerów WWW, FTP lub innych. Ponieważ oprogramowanie firewalla nie używa algorytmów szyfrujących ani nie zna wykorzystanych przez VPN kluczy, może jedynie filtrować i przetwarzać zewnętrzne nagłówki tunelowanych pakietów. Oznacza to, że w rzeczywistości wirtualny tunel przebiega również przez zaporę. Nie osłabia to jednak bezpieczeństwa, gdyż połączenie VPN wymaga autoryzacji.

Drogi i bezdroża

Sieci VPN zapewniają bezpieczeństwo tym, którzy zdecydowali się odgrodzić ścianami tunelu od reszty cyberprzestrzeni. Chroni to przed różnymi zagrożeniami, jakie kryją się w Internecie. Zastosowanie programowych rozwiązań VPN zawartych w systemach Windows, Linux lub UNIX pozwala dziś na korzystanie z zalet opisanej technologii nie tylko dużym i bogatym firmom. Dlatego surfując na co dzień w Internecie, coraz częściej ocieramy się o takie witualne ściany. Obserwujemy obecnie także większe zainteresowanie ochroną danych. Coraz powszechniej stosowane szyfrowanie połączeń WWW czy chociażby osobiste firewalle (patrz: CHIP 12/2000, s. 228) to najprostsze przykłady. Dlatego sądzę, iż należy się spodziewać, że już niedługo wszyscy będziemy poruszali się w Sieci tunelami.

Adrian Borowski

INFO

Grupy dyskusyjne
Uwagi i komentarze do artykułu:
news://news.vogel.pl/chip.artykuly
Pytania techniczne:
news://news.vogel.pl/chip.internet

Internet
Free SWAN
http://www.freeswan.org/
Opis protokołów stosowanych w VPN
http://idm.internet.com/articles/200009/vpn.html
Artykuły na temat VPN-ów
http://intranets.about.com/compute/intranets/cs/vpn/
VPN FAQ
http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html