Wprowadzenie do technologii VPN

Sieci komputerowe są powszechnie wykorzystywane do realizacji transakcji handlowych i prowadzenia działalności gospodarczej. Ich zaletą jest błyskawiczny dostęp do ludzi, którzy potrzebują informacji. Problem polega jednak na tym, że informacje o strategicznym znaczeniu dla firmy są narażone na zagrożenia związane z bezpieczeństwem. W rezultacie sieć zaufana i bezpieczna, która jest cały czas do dyspozycji firmy to konieczność. Taka sieć daje wiele możliwości ważnych z punktu widzenia konkurencyjności oraz wpływa na polepszenie jakości procesów biznesowych w firmie. Coraz częściej, w celu podwyższenia swojej skuteczności na rynku i efektywności pracy, firmy polegają na bezpiecznej poczcie elektronicznej, wymianie dokumentów elektronicznych, sieciach intranetowych, sieciach ekstranetowych oraz wirtualnych sieciach prywatnych **VPN** (*ang. virtual private network*).

W dzisiejszym globalnym środowisku biznesowym, firmom zależy na zaufaniu do partnerów handlowych i przekonaniu, że jest zachowana prywatność ich informacji. Utrzymanie bezpieczeństwa rozległej infrastruktury sieciowej odbywa się najczęściej za pomocą VPN. Pierwszym powszechnie stosowanym rodzajem tej technologii jest tzw. **zaufany VPN** (*ang. trusted VPN*). Zaufany VPN to łącze uzyskane od operatora telekomunikacyjnego z zapewnieniem, że dane w nich przesyłane są odpowiednio chronione. Przykładem zaufanego VPN są łącza dzierżawione ATM i Frame Relay. Bezpieczeństwo tego rozwiązania bazuje na zaufaniu do operatora telekomunikacyjnego. Z technicznego punktu widzenia firma nie ma gwarancji, że urządzenia w sieci operatora, przez które przesyłane są ich dane nie zostaną przejęte przez osoby nieupoważnione np. hakerów czy niezadowolonych pracowników.

Drugim rodzajem jest **bezpieczny VPN** *(ang. secure VPN)*, w którym transmisja danych odbywa się poprzez łącza publiczne, a do jej ochrony stosuje się techniki kryptograficzne. Firma wykorzystując bezpieczny VPN sama decyduje, jakie środki ochrony należy zastosować. Bezpieczny VPN posiada jeszcze jedną istotną zaletę. Jego koszt utrzymania jest znacznie niższy od łączy dzierżawionych. Należy jednak zwrócić uwagę na fakt, że bezpieczny VPN realizowany jest poprzez łącza publiczne, gdzie operatorzy nie mają możliwości zagwarantowania na całej drodze transmisji danych stałych parametrów sieci (QoS[1]). Nie dla wszystkich aplikacji można więc wykorzystywać ten rodzaj VPN. Dla aplikacji wrażliwych na opóźnienia transmisji danych i przepustowość łącza stosuje się tzw. **hybrydowy VPN** (*ang. hybrid VPN*), który realizowany jest poprzez łącza dzierżawione, odpowiednio zabezpieczone za pomocą technik kryptograficznych.

Zastosowanie technik kryptograficznych w sieciach VPN wymaga właściwego zaplanowania zabezpieczeń, wdrożenia odpowiednio dobranych środków ochrony oraz w trakcie eksploatacji utrzymania ich poprawnego stanu.

[1] QoS – Quality of Service

1. Algorytmy kryptograficzne stosowane w sieciach komputerowych

Zabezpieczenie informacji przesyłanych zarówno w sieciach prywatnych jak i publicznych (np. Internet) najczęściej odbywa się z wykorzystaniem odpowiednich technik kryptograficznych. Przed wysłaniem do sieci pakiety poddawane są operacji szyfrowania oraz innym dodatkowym przekształceniom zapewniającym ich:

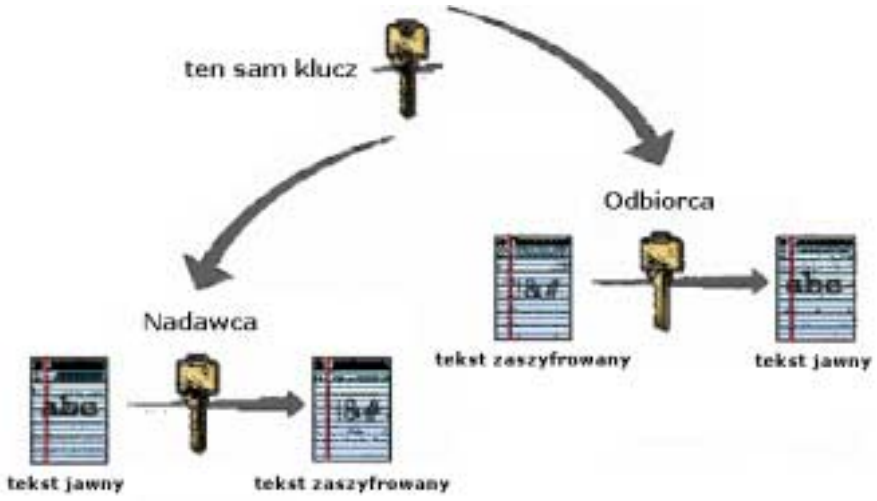
- poufność danych (*ang. data confidentiality*),
- integralność danych (*ang. data integrity*),
- uwierzytelnianie źródła danych (*ang. data origin authentication*),
- niezaprzeczalność (*ang. non-repudiation*).

Do podstawowych algorytmów i technik kryptograficznych stosowanych w sieciach komputerowych można zaliczyć szyfry symetryczne (np. DES), szyfry asymetryczne (np. RSA), algorytm Diffiego-Hellmana, funkcje haszujące (np. MD5) oraz podpisy i certyfikaty cyfrowe (X.509). Ochrona transmitowanych informacji odbywa się za pomocą sprzętowych lub programowych szyfratorów. W systemach o podwyższonych wymaganiach bezpieczeństwa najczęściej stosuje się bardziej niezawodne i łatwiejsze w instalacji szyfratory sprzętowe. W zastosowaniach rządowych i wojskowych urządzenia te muszą posiadać odpowiedniej klasy certyfikaty bezpieczeństwa. W instytucjach komercyjnych, z uwagi na niższą cenę i większą elastyczność z reguły stosuje się szyfratory programowe, często zintegrowane z innymi zabezpieczeniami sieci (np. Firewall).

Szyfry symetryczne

Tradycyjne algorytmy kryptograficzne, określane mianem systemów szyfrowych z kluczem tajnym (*pot. szyfry symetryczne*), zakładają użycie identycznego klucza do szyfrowania i deszyfrowania. Jest oczywiste, iż wartość tego klucza musi być utrzymywana w ścisłej tajemnicy (patrz rysunek 1). Ogólnie, algorytmy szyfrujące kluczem tajnym można podzielić na:

- szyfry blokowe - blok szyfrogramu jest funkcją tylko jednego bloku wiadomości (np. AES, DES, 3DES, IDEA, RC2, RC5, SAFER),
- szyfry strumieniowe - blok szyfrogramu jest funkcją wszystkich poprzedzających wiadomości (np. RC4, A5).

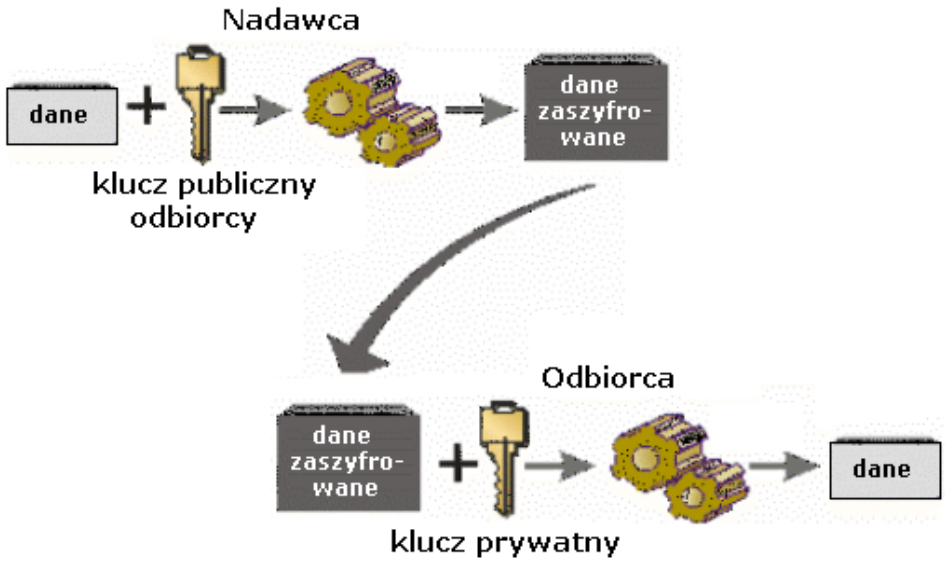


Rys 1) Zasada działania szyfru symetrycznego

Wartość algorytmu szyfrującego zależy od jego odporności na krypto-analizę, a w szczególności tzw. atak brutalny. Atak brutalny (*ang. brute force attack*) ma na celu wyznaczenie formy jawnej informacji na podstawie kryptogramu oraz pewnego jawnego fragmentu wiadomości, bez znajomości klucza szyfrowania. Atak polega na sprawdzaniu całej przestrzeni klucza, a jego powodzenie zależy w głównej mierze od długości klucza przyjętego dla określonego algorytmu szyfrowania.

Szyfry asymetryczne

W odniesieniu do środowiska sieci komputerowych stosowanie systemów szyfrowych klucza tajnego jest uciążliwe z uwagi na konieczność ciągłego utajniania kluczy szyfrowania. Jak do tej pory nie wynaleziono środka transportu, poprzez który można by było sprawnie przekazywać tajny klucz pomiędzy nadawcą i odbiorcą informacji. Propozycją rozwiązania tego problemu są systemy szyfrowe z kluczem jawnym (*pot. szyfry asymetryczne*), które pozwalają na prowadzenie szyfrowania danych bez konieczności wcześniejszej wymiany tajnych informacji. Systemy szyfrowe klucza jawnego zakładają, iż każda ze stron uczestniczących w procesie szyfrowania/deszyfrowania informacji jest wyposażona w parę matematycznie zależnych kluczy: klucz prywatny (tajny) i klucz publiczny (jawny). Dane zaszyfrowane jednym z tych kluczy mogą być rozszyfrowane wyłącznie przy użyciu odpowiadającego mu drugiego klucza (patrz rysunek 2). Przyjęte jest, iż klucz prywatny podlega ścisłej ochronie i nigdy nie opuszcza maszyny swojego właściciela w odróżnieniu od klucza publicznego, który może być rozprowadzany publicznie. Do najbardziej rozpowszechnionych szyfrów asymetrycznych można zaliczyć algorytm RSA (1978, Ronald Rivest, Adi Shamir, Leonard Adleman) oraz algorytmy oparte na krzywych eliptycznych.

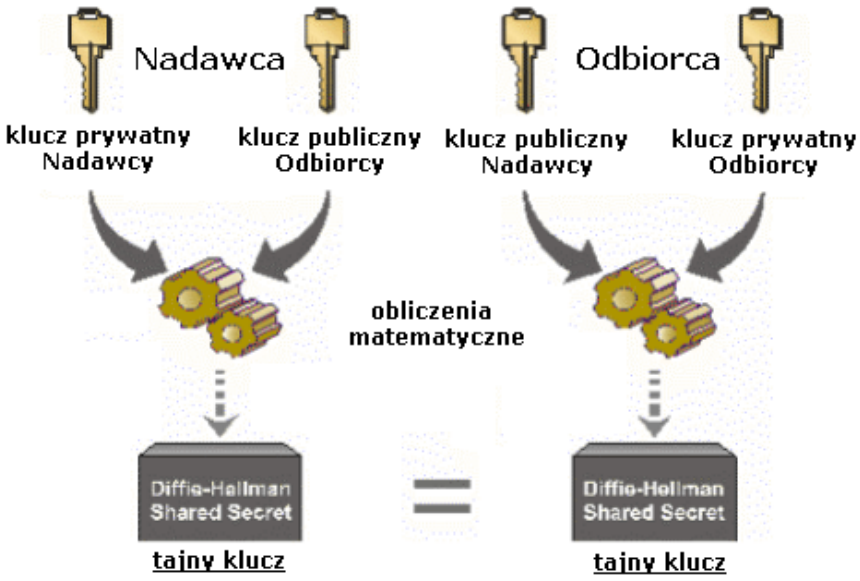


Rys 2) Zasada działania szyfru asymetrycznego

Jedną z poważnych wad, jaką można zarzucić szyfrom asymetrycznym jest mała szybkość działania (np. szybkość RSA w porównaniu do DES jest ok. 1000 razy mniejsza). Aby zaradzić tej sytuacji, większość popularnych systemów ochrony danych używa RSA wyłącznie do szyfrowania klucza sesji, wykorzystywanego do szyfrowania właściwych informacji przy pomocy algorytmu z kluczem tajnym np. DES (tzn. stosuje się kombinacje szyfrów asymetrycznych i symetrycznych).

Algorytm Diffiego-Hellmana

Bardzo wartościowym rozwiązaniem należącym do grupy krypto-systemów klucza publicznego jest algorytm Diffiego-Hellmana. Nazwa algorytmu pochodzi od nazwisk jego twórców Whitfielda Diffie i Martina Hellmana. Zasadniczo, algorytm Diffiego-Hellmana nie może być bezpośrednio wykorzystany do szyfrowania danych. Algorytm umożliwia, aby nadawca i odbiorca informacji mogli wyznaczyć jeden, tajny klucz szyfrowania bez konieczności wcześniejszej wymiany jakichkolwiek poufnych informacji.

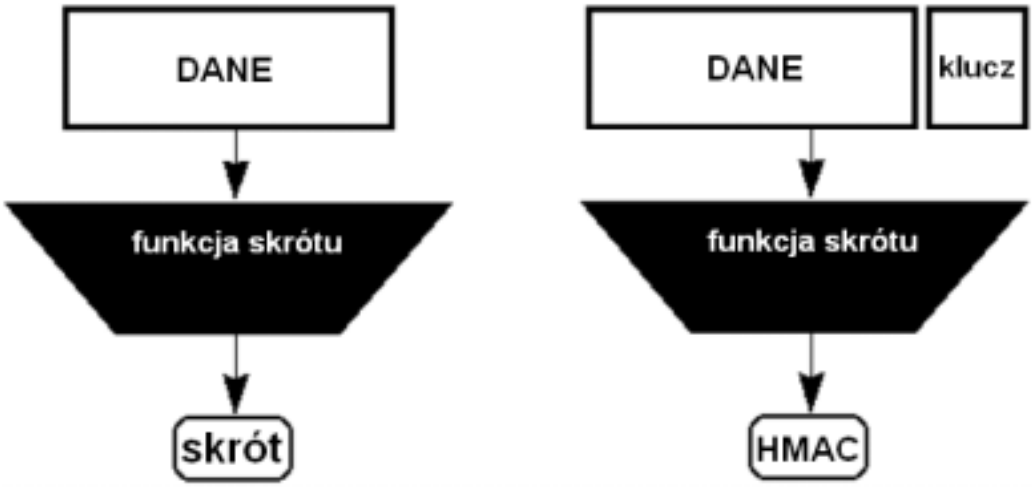


Rys 3) Zasada działania algorytmu Diffiego-Hellmana

Klucz wyznaczony algorytmem Diffiego-Hellmana może być później wykorzystany do szyfrowania danych przy pomocy któregoś z systemów szyfrowych klucza tajnego (np. DES, IDEA, RC4). Obok RSA, algorytm Diffiego-Hellmana jest najpopularniejszym krypto-systemem klucza publicznego wykorzystywanym w sieci Internet.

Funkcje haszujące i HMAC

W przypadku przesyłania ważnych dokumentów za pośrednictwem sieci komputerowej, istotną rolę odgrywa kwestia potwierdzania integralności otrzymywanych informacji (tzn. odbiorca chciałby być pewny, że dane nie zostały zmodyfikowane w czasie transmisji). Zapewnienie integralności przesyłanych informacji uzyskuje się najczęściej poprzez utworzenie tzw. skrótu komunikatu (*ang. message digest*) przy pomocy odpowiedniego algorytmu matematycznego.



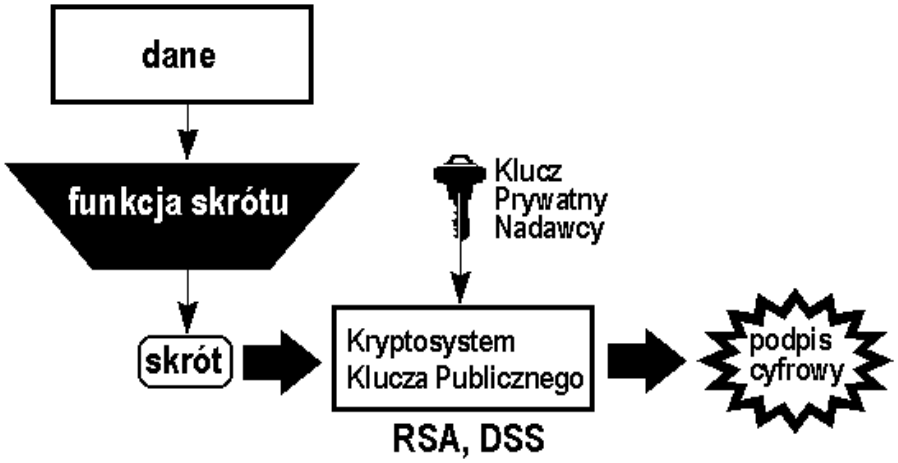
Rys 4) Zasada działania funkcji haszującej i HMAC

Algorytmy takie określane są mianem jednokierunkowych funkcji skrótu z uwagi na swoje właściwości. Obliczenie skrótu wiadomości sprowadza się do podania tej wiadomości jako argumentu jednokierunkowej funkcji skrótu. Termin jednokierunkowa oznacza, że nie powinno być możliwości wyznaczenia treści wiadomości na podstawie jej skrótu. Jednokierunkowe funkcje skrótu określane są także jako funkcje haszujące z uwagi na dodatkowe wymaganie, które zakłada, iż prawdopodobieństwo znalezienia dwóch różnych wiadomości mających takie same skróty jest bardzo małe. Wśród najbardziej rozpowszechnionych funkcji można wyróżnić MD2 i MD5 opracowane przez Ronalda Rivesta oraz tzw. bezpieczny algorytm haszujący SHA i SHA-1 (*ang. secure hash algorithm*) zaproponowany przez amerykański Narodowy Instytut Standardów i Technologii wraz z Narodową Agencją Bezpieczeństwa USA.

Wykorzystanie funkcji haszującej zapewnia integralność danych, nie daje jednak pewności, że dane zostały wysłane przez prawdziwego nadawcę. Potencjalnie intruz może, bowiem wysłać dane w imieniu innej osoby wraz z prawidłowym skrótem wiadomości. W celu zapewniania także autentyczności danych stosuje się operacje Hashing Message Authentication Code (HMAC). Polega ona na tym, że wiadomość wraz z tajnym kluczem poddawana jest funkcji haszującej (patrz rysunek 4). Tajny klucz HMAC, podobnie jak w szyfrach symetrycznych, znany jest tylko nadawcy i odbiorcy danych.

Podpisy cyfrowe

Analiza skrótu wiadomości pozwala wykryć, czy wiadomość w czasie transmisji została zmodyfikowana, jednak nie gwarantuje jej autentyczności (tzn. nie można jednoznacznie określić, przez kogo wiadomość została wysłana). Stosowanie operacji HMAC w aplikacjach sieciowych jest uciążliwe z uwagi na konieczność przekazywania tajnego klucza uwierzytelniania. Powszechnie wykorzystywaną techniką uwierzytelniania informacji jest tworzenie tzw. podpisów cyfrowych (*ang. digital signature*). Podpis cyfrowy może zostać wykonany poprzez zaszyfrowanie skrótu wiadomości za pomocą szyfru asymetrycznego z użyciem klucza prywatnego nadawcy (patrz rysunek 5). Jeżeli odbiorca będzie w stanie odszyfrować podpis cyfrowy za pomocą klucza publicznego nadawcy to może być pewny, że podpis cyfrowy został wykonany przez nadawcę i tym samym potwierdzić autentyczność otrzymanych informacji.



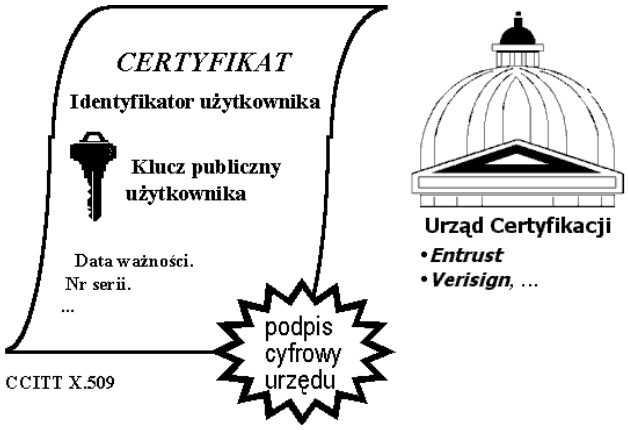
Rys 5) Proces tworzenia podpisu cyfrowego

Podpis cyfrowy może być wykonany za pomocą wspomnianego już systemu RSA lub algorytmu DSA (Digital Signature Algorithm), zaproponowanego przez Narodowy Instytut Standardów i Technologii USA jako standard tworzenia podpisów cyfrowych. Algorytm DSA znany jest także pod nazwą Digital Signature Standard (DSS).

Urzędy certyfikacji

Krypto-systemy klucza publicznego są niezawodne w małych środowiskach, gdzie nadawcy i odbiorcy mają do siebie zaufanie i mogą bezpośrednio wymieniać swoje klucze publiczne np. poprzez wymianę dyskietek. Zupełnie inna sytuacja występuje w dużych sieciach komputerowych, takich jak Internet, czy sieci korporacyjne i ekstranetowe. Powstaje wtedy problem, w jaki sposób upewnić się, iż uzyskany poprzez sieć klucz publiczny rzeczywiście należy do właściwej osoby. Łatwo wyobrazić sobie scenariusz, w którym intruz podmienia klucz publiczny określonego użytkownika, a następnie przechwytuje i swobodnie deszyfruje wiadomości kierowane do tego użytkownika.

Skutecznym i efektywnym rozwiązaniem tego problemu są tzw. urzędy certyfikacji (*ang. certificate authority*). Mówiąc ogólnie, urząd certyfikacji jest to zaufana instytucja, która odpowiada za dystrybucję kluczy publicznych użytkowników.

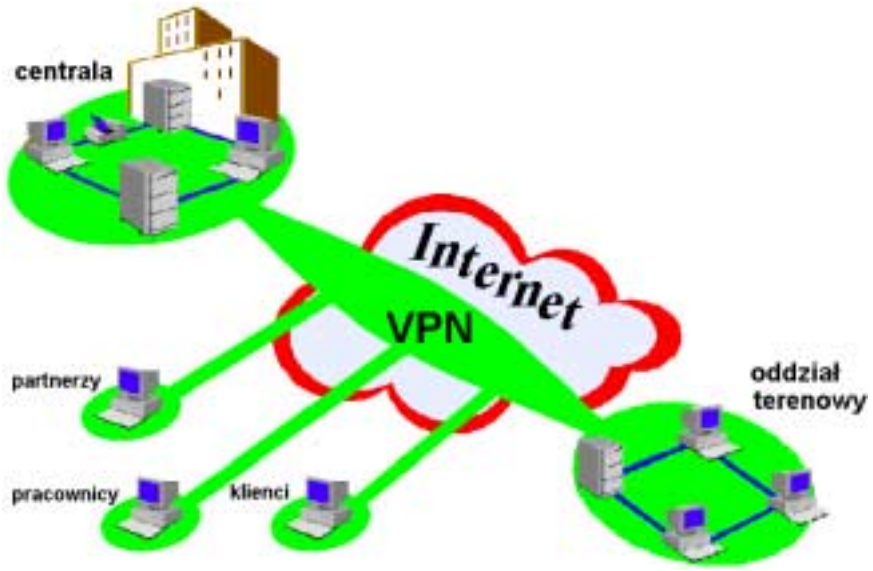


Rys 6) Podstawowe elementy certyfikatu cyfrowego

Użytkownik, aplikacja lub urządzenie, które zamierzają prowadzić szyfrowanie w systemie klucza publicznego najpierw powinni zarejestrować się w urzędzie certyfikacji oraz dostarczyć swoje klucze publiczne wraz z danymi identyfikacyjnymi. Dystrybucja kluczy odbywa się za pośrednictwem znormalizowanych dokumentów określanych jako certyfikaty cyfrowe (norma CCITT X.509). Rysunek 6 pokazuje podstawowe elementy tego dokumentu.

2. Koncepcja i zasady funkcjonowania sieci VPN

Koncepcja funkcjonowania sieci **VPN (*ang. virtual private network*)** polega na tworzeniu wydzielonych, logicznych kanałów transmisji danych w ramach sieci rozległej tak, aby dane przesyłane tymi kanałami zostały zabezpieczone w zakresie poufności, integralności i autentyczności (patrz rysunek 7). Zabezpieczenie danych w sieci VPN realizowane jest za pomocą technik kryptograficznych.

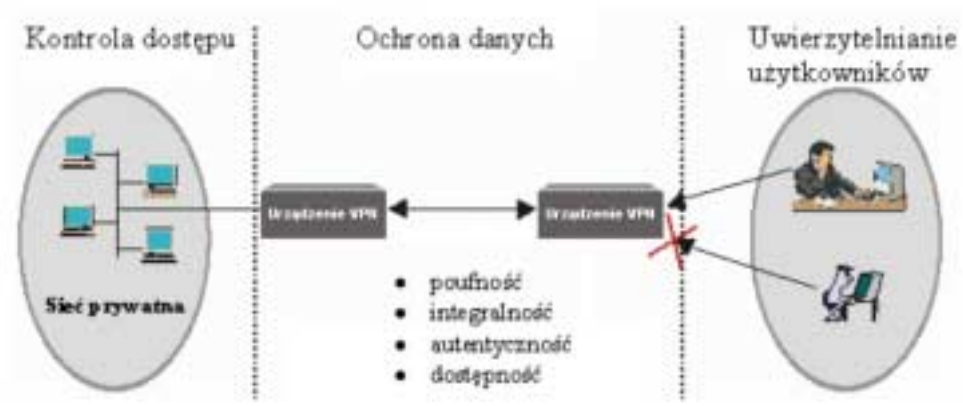


Rys 7) Koncepcja tworzenia sieci VPN

Wyróżnia się dwa podstawowe rodzaje VPN:

- **Site-Site** – wirtualna sieć prywatna pomiędzy odległymi sieciami LAN; kanały VPN otwierane są przez brzegowe urządzenia VPN,
- **Client-Site** – wirtualna sieć prywatna pomiędzy odległą stacją PC i siecią LAN; kanały VPN otwierane są przez program klienta VPN na stacji PC i brzegowe urządzenie, określane jako koncentrator VPN.

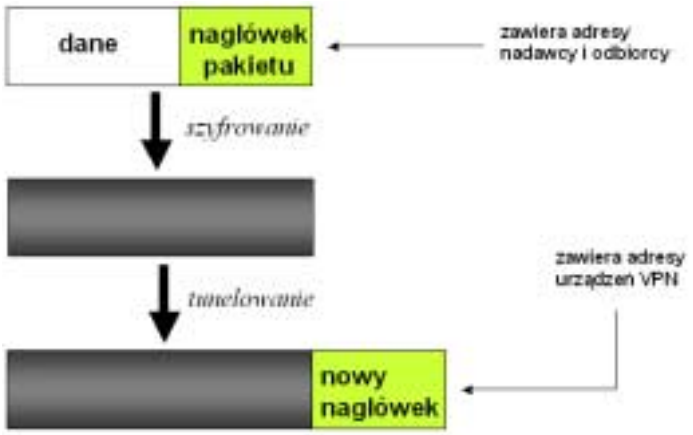
Sieci VPN typu Site-Site mogą być implementowane w dwóch topologiach – **Meshed VPN** oraz **Hub & Spoke**. W topologii Meshed VPN wszystkie urządzenia VPN zestawiają tunele bezpośrednio ze sobą. Jest ona najczęściej stosowana przy mniejszej liczbie tuneli VPN. W topologii Hub & Spoke występuje centralne urządzenie VPN, które pośredniczy w zestawianiu tuneli dla innych urządzeń. Przy dużej liczbie tuneli VPN nie jest bowiem efektywne, aby konfigurować i zestawiać bezpośrednie połączenia ze wszystkimi urządzeniami.



Rys 8) Funkcje zabezpieczeń realizowane w sieci VPN

Technicznie, klasyczna sieć VPN realizuje:

- szyfrowanie/uwierzytelnianie danych,
- kontrolę dostępu do sieci wirtualnej,
- uwierzytelnianie użytkowników (w sieci Client-Site),
- tunelowanie pakietów (opcjonalnie).



Rys 9) Tunelowanie pakietów w sieci VPN

Tunelowanie pakietów jest z punktu widzenia bezpieczeństwa ważną operacją wykonywaną w sieci VPN. Polega ono na szyfrowaniu całości oryginalnego pakietu i przesyłaniu go w nowym pakiecie pomiędzy urządzeniami brzegowymi VPN (patrz rysunek 9). Dzięki temu intruz przebywający na drodze VPN nie może odczytać informacji nt. prowadzonej komunikacji sieciowej pomiędzy użytkownikami i serwerami. Tunelowanie pakietów w wielu przypadkach usprawnia także konfigurację sieci (np. eliminuje potrzebę konfiguracji translacji adresów NAT).

Mariusz Stawowski