PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1081 — 2005
Nowoczesne technologie informacyjne w zarządzaniu

Ryszard Nikodem

BEZPIECZEŃSTWO POŁĄCZEŃ W ROZLEGŁYCH SIECIACH KOMPUTEROWYCH

1. Wprowadzenie

Realizację bezpiecznych połączeń w rozległych sieciach komputerowych zapewniają przede wszystkim wirtualne sieci prywatne, stosowane do łączenia odległych sieci lokalnych – są wtedy alternatywą budowania przez firmę własnej infrastruktury połączeń bądź dzierżawienia łączy stałych od dostawcy usług telekomunikacyjnych. Innym obszarem zastosowania tych sieci jest realizacja połączeń między siecią firmową a komputerami zdalnych użytkowników, którzy z dowolnego miejsca, korzystając z dowolnego rodzaju łącza, mogą połączyć się z serwerami sieci firmowej. Uzupełnieniem wspomnianych rozwiązań – stosowanym obecnie coraz częściej i na pewno godnym rozważenia – są usługi terminalowe i serwery aplikacyjne.

Wirtualne sieci prywatne z jednej strony są rozwiązaniem stosunkowo niedrogim, z drugiej strony udostępniają mechanizmy gwarantujące bezpieczeństwo zarówno transmisji danych, jak i zasobów. Nic zatem dziwnego, że coraz więcej użytkowników decyduje się na używanie tej technologii [Nikodem 2003]. Z kolei rozwiązania terminalowe pozwalają zdalnie udostępnić praktycznie każdą aplikację, upraszczają zarządzanie i ułatwiają zabezpieczenie aplikacji, dobrze integrując się z systemami uwierzytelniania.

W artykule omówiono wybrane zagadnienia związane z bezpieczeństwem połączeń w rozległych sieciach komputerowych. W kolejnych punktach dokonano przeglądu technologii stosowanych w wirtualnych sieciach prywatnych oraz wskazano zasady bezpiecznego korzystania z tych sieci. W punkcie 4 przedstawiono dodatkowe rozwiązania w zakresie zdalnego dostępu do sieci firmowych, w ostatnim zaś dokonano podsumowania rozważań.

2. Technologie IPSec i SSL VPN

Wirtualna sieć prywatna (VPN – *virtual private network*) to wydzielona część przepustowości sieci publicznej, logicznie odseparowana od reszty sieci i dostępna dla określonej grupy użytkowników. Wirtualne kanały są ustalane wyłącznie na czas transmisji między węzłami sieci stanowiącymi routery. Informacja – w zaszyfrowanej postaci – jest najczęściej przesyłana z sieci lokalnych lub pojedynczych komputerów, przy wykorzystaniu łączy i usług dostawców Internetu (ISP – *internet service provider*). W celu realizacji bezpiecznego połączenia sieci VPN stosują jeden z trzech protokołów: L2TP (Layer 2 Tunneling Protocol), IPSec lub SSL/TLS. Pierwszy z wymienionych, używany w połączeniach modemowych, stosowany jest coraz rzadziej. W tej sytuacji dominującą pozycję zajmuje protokół IPSec, ale protokół SSL/TSL cieszy się rosnącą popularnością.

Najczęściej sieci VPN są zarządzane przez oprogramowanie powstające w ramach projektów klasy *open source*. Jednak stwierdzenie, że są to sieci darmowe (oczywiście poza opłatami za użytkowanie łączy), może być mylące. Samo oprogramowanie rozprowadzane na licencji GNU GPL (General Public License) jest wprawdzie bezpłatne, lecz wdrożenie tych systemów może wymagać znacznych nakładów, większych niż w przypadku rozwiązań komercyjnych.

W dużych sieciach korporacyjnych wydajną sieć VPN można zrealizować, wykorzystując rozwiązania sprzętowe. Często funkcja VPN jest oferowana jako dodatkowa w sprzętowej zaporze sieciowej (*firewall*) lub w bramie sieci bezprzewodowej.

Protokół IPSec (IP Security) to w zasadzie nie jeden, ale grupa współpracujących protokołów komunikacyjnych i kryptograficznych, dostępnych obecnie dla każdego systemu operacyjnego i uważanych powszechnie za najbezpieczniejsze narzędzie tworzenia wirtualnych sieci prywatnych.

Zdalny komputer nawiązuje połączenie przez łącza sieci rozległej (np. Internetu) z bramą IPSec VPN, po czym inicjuje procedurę wymiany kluczy. Po pomyślnym uwierzytelnieniu następuje utworzenie bezpiecznego tunelu VPN, w którym może być zrealizowanych szereg transmisji.

Siec IPSecVPN pracuje w jednym z dwóch następujących trybów:

- **tunelowania**, stosowanym w przypadku, gdy połączenie z obu stron obsługują bramki VPN, a utworzony tunel pozwala komunikować się urządzeniom, które nie obsługują protokołu IPSec; szyfrowane są zawartości pola danych pakietu, bez szyfrowania nagłówka; trasa pakietu w sieci nie ulega zmianie, gdyż adres miejsca przeznaczenia pakietu pozostaje w formie jawnej;
- **transportowym**, realizowanym wyłącznie pomiędzy komputerami bądź urządzeniami obsługującymi protokół IPSec; szyfrowana jest cała zawartość pakietu, w tym pola adresu źródłowego i docelowego; zaszyfrowany pakiet podlega kompresji i jest umieszczany w polu danych nowego pakietu (zwanego „kopertą"), którego adres docelowy przyjmuje wartość adresu IP routera

sieci, w której jest zlokalizowany komputer przeznaczenia; rozszyfrowania danych dokonuje router i komputer docelowy.

Uzupełnienie protokołu IPSec stanowią trzy mechanizmy zabezpieczające: AH, ESP i IKE. Dwa pierwsze są wykorzystywane odpowiednio do kodowania treści pakietów i uwierzytelniania ich pochodzenia, trzeci – do negocjowania parametrów połączenia, w tym także używanych w trakcie połączenia kluczy szyfrujących [Koziński 2002].

Mechanizm AH (Authentication Header) zapewnia uwierzytelnienie integralności i pochodzenia danych. Pierwsze uzyskuje się dzięki sumie kontrolnej generowanej na podstawie kodu identyfikacyjnego wiadomości, drugie – w wyniku umieszczenia sekretnego, współdzielonego klucza w danych przeznaczonych do identyfikowania.

Zadaniem mechanizmu ESP (Encapsulating Security Payload) jest szyfrowanie danych, jednocześnie – jako opcja – może być realizowane uwierzytelnienie integralności i pochodzenia danych, zatem pełni on te same funkcje, które wykonuje mechanizm AH. Do szyfrowania mechanizm ESP stosuje symetryczny współdzielony klucz, tj. ten sam klucz wykorzystywany przy szyfrowaniu i deszyfrowaniu danych.

Istotnym zadaniem w sieciach działających zgodnie z protokołem IPSec jest identyfikacja komputerów, urządzeń i użytkowników uczestniczących w komunikacji. Aby transmisja była bezpieczna, niezbędna jest wymiana kluczy. Protokół IPSec dopuszcza dwa sposoby zarządzania wymianą kluczy – ręczny lub z wykorzystaniem mechanizmu IKE.

Negocjowanie parametrów przez mechanizm IKE (Internet Key Exchange) odbywa się przy użyciu protokołu transportowego UDP i dotyczy utworzenia tzw. SA (Security Associations) – bezpiecznych powiązań definiujących własności połączeń. Bezpieczne powiązania są tworzone w drugiej fazie negocjacji. Strony udostępniają sobie klucze publiczne, przy czym osobna para kluczy jest niezbędna dla każdego kierunku transmisji (bowiem połączenia IPSec są jednokierunkowe). Osobno dla każdego powiązania SA są ustalane parametry, m.in. okres ważności kluczy, rodzaj algorytmu szyfrowania (domyślnie algorytm 3DES), rodzaj algorytmu uwierzytelniającego (MD5 lub SHA).

Wśród najpopularniejszych i najbardziej zaawansowanych implementacji sieci IPSec VPN należy wymienić działające w środowisku Linux projekt FreeS/WAN (Secure Wide Area Network), oferujący silną kryptografię, oraz będący jego kontynuacją projekt OpenSwan, prostszy w implementacji od swego poprzednika, zwiększający też jego funkcjonalność, m.in. o funkcję NAT Traversal, niezbędną w sieciach wykorzystujących prywatne pule adresów oraz – do translacji adresów – mechanizm NAT (Network Address Translation).

Protokół SSL (Secure Sockets Layer) używany od lat w celu zwiększenia bezpieczeństwa transakcji w Internecie, znalazł także zastosowanie przy budowie wirtualnych sieci prywatnych. Protokół SSL w wersji 3 lub nowszy TSL (Transport

Layer Security) w wersji 1 stanowią podstawę przy zestawianiu połączenia VPN w trzech następujących etapach (por. [Ryłko 2005]):

- ustalenie między stronami parametrów sesji, takich jak rodzaj szyfru, długość klucza, sposób kompresji,
- wzajemna autoryzacja serwera i klienta oraz ustanowienie klucza sesyjnego (SSL/TSL Handshake Protocol),
- transmisja szyfrowana.

Do budowy sieci VPN opartych na protokole SSL/TSL można wykorzystać takie oprogramowanie, jak OpenVPN, SSL-Explorer lub Yavipin.

Pakiet OpenVPN charakteryzuje się łatwą obsługą i rozbudowanymi możliwościami konfiguracyjnymi. Wymaga zainstalowania także pakietu OpenSSL do generowania par certyfikatów przy nawiązywaniu połączeń. Dostępne są wersje pakietu dla takich systemów operacyjnych, jak Linux, Windows, OpenBSD, FreeBSD, NetBSD oraz Solaris.

Oparty na Javie, pakiet SSL-Explorer do budowania bezpiecznych połączeń, wykorzystuje protokół SSL z kluczem o długości 128 bitów. Można go zintegrować z bazą użytkowników MS Active Directory. Nie wymaga instalacji oprogramowania klienckiego – wystarczy przeglądarka internetowa. Dostępne są wersje dla systemu Windows oraz Linux (Red Hat).

Pakiet Yavipin (Yet another VPN) działa w środowisku Linuksa i służy do połączeń między dwoma węzłami. Przesyłane pakiety są szyfrowane algorytmem Blowfish i uwierzytelniane, a klucze sesyjne często zmieniane i kasowane z pamięci. Podobnie jak pierwszy z omawianych pakietów, Yavipin wymaga instalacji pakietu OpenSSL.

Trochę inny obszar zastosowań ma pakiet VPNMonitor. Jest to oprogramowanie napisane w Javie i służące do monitorowania ruchu pakietów w sieci VPN. Może być używane do obserwowania zarówno sieci IPSec, jak i SSL. Dodatkowo umożliwia wizualizację ruchu pakietów między węzłami sieci.

Użytkownik ma zatem duży wybór w zakresie wirtualnych sieci prywatnych. Czy są to jednak rozwiązania gwarantujące bezpieczne połączenia?

3. Wirtualne sieci prywatne – czy rzeczywiście bezpieczne?

Na tak postawione pytanie odpowiedź brzmi: i tak, i nie.

Sieci VPN są bezpieczne w tym sensie, że dostarczają mechanizmy i narzędzia do budowy połączeń w dużym stopniu bezpiecznych, wszakże pod warunkiem, że będą także właściwie stosowane. Praktyka pokazuje, że często jest inaczej. W cytowanym w artykule [Krawczyk 2005] ostatnim raporcie firmy NTA Monitor, na podstawie trzyletnich testów, stwierdzono, że działające sieci VPN w ponad 90% nie są bezpieczne. Mamy zatem paradoks – wirtualna sieć prywatna, powszechnie postrzegana jako całkowicie odporna na ataki, okazała się najsłabszym ogniwem w zabezpieczeniach sieciowych.

Jakie działania wymienia się jako te, które mogą zwiększyć bezpieczeństwo sieci VPN? Zwłaszcza dwa obszary są w tym zakresie szczególnie ważne:
- stosowane oprogramowanie i sprzęt VPN,
- administrowanie siecią VPN.

Nawet renomowani producenci **oprogramowania i urządzeń sieciowych** popełniają błędy ułatwiające włamanie do sieci VPN. Przykładem może być inna postać komunikatu błędu w sytuacji, gdy wprowadzono niepoprawny identyfikator (login), a inna – gdy wprowadzono poprawny identyfikator użytkownika, lecz niepoprawne hasło. Niektóre implementacje protokołu IKE działają w taki właśnie sposób, ułatwiając zadanie włamywaczom.

Inną przyczyną pogorszenia bezpieczeństwa są wprowadzone przez producentów rozszerzenia protokołu IPSec, które umożliwiają rejestrację całych sesji IKE i łamanie ich *off-line*.

Z kolei winą producentów routerów jest brak – dostępnej we wszystkich systemach operacyjnych – prostej funkcji blokowania konta po przekroczeniu określonej liczby nieuprawnionych prób zalogowania się. Z punktu widzenia ochrony przed tzw. atakiem słownikowym (czyli próbą złamania hasła za pomocą tysięcy prób logowania się w krótkim czasie), błędem w routerach jest brak opóźnienia po błędnym uwierzytelnieniu. Tego typu drobne zabezpieczenie uczyniłoby atak słownikowy praktycznie nieskutecznym.

Wśród postulatów adresowanych do **administratora sieci VPN,** mających polepszyć bezpieczeństwo, warto pamiętać o następujących [Krawczyk 2005]:
- wyłączyć „agresywny" tryb IKE (w ten sposób uniemożliwi się rejestrację sesji IKE),
- włączyć na routerze najsilniejsze z dostępnych szyfrowań (standardem jest 3DES z kluczem długości 168/192 bity, nowsze rozwiązanie to szyfr AES z kluczem od 128 do 256 bitów),
- wprowadzić reguły wymuszające minimalną długość hasła (co znacznie wydłuży czas złamania hasła, wręcz uczyni to niemożliwym w sensownym czasie),
- rozważyć zakup klientów VPN obsługujących uwierzytelnienie jednorazowymi hasłami generowanymi przez tokeny sprzętowe,
- chronić system przed końmi trojańskimi i ograniczyć użytkownikom możliwość modyfikacji konfiguracji.

Dopiero wszystkie wymienione czynności i szereg innych, stosowane łącznie i konsekwentnie, sprawią, że wirtualne sieci prywatne będą bezpieczne.

4. Zdalny dostęp metodami alternatywnymi

Ze względu na strukturę połączeń rozróżnia się rozwiązania typu sieć–sieć (*LAN-to-LAN*) oraz klient–sieć (*client-to-LAN*). Sieć wirtualna typu **sieć–sieć** służy do połączenia dwóch lub więcej lokalnych sieci komputerowych i znajduje

zastosowanie zarówno w modelu intranetowym (łączonych jest wiele oddziałów jednej firmy), jak i ekstranetowym (w bezpieczny sposób są łączone sieci różnych, niezależnych i współpracujących ze sobą partnerów handlowych i kontrahentów). Z kolei sieć wirtualna typu **klient–sieć** łączy użytkownika z siecią lokalną i zapewnia bezpieczną, szyfrowaną komunikację pomiędzy serwerem VPN (ukrytym zazwyczaj za firmowym firewallem) i komputerem użytkownika, który uzyskuje dostęp do sieci firmowej z dowolnej sieci obsługującej protokół internetowy IP.

W drugiej z wymienionych struktur, nazywanej też **zdalnym dostępem**, uzupełnieniem sieci VPN są:
- usługi terminalowe,
- serwery aplikacyjne.

W rozwiązaniach tych tunel VPN służy do nawiązania połączenia (często w tym celu stosuje się wspomniany już pakiet OpenVPN, ze względu na obsługę wielu platform i odporność na zrywanie połączenia), po czym zdalną sesją zarządza serwer terminalowy – np. Microsoft Terminal Services lub Jetro CockpIT (w środowisku Windows), podobne rozwiązania dla otoczenia Linuksa czy wieloplatformowa Tarantella – lub serwer aplikacyjny.

Usługi terminalowe pozwalają uruchamiać na serwerze sesje klienta z równoczesnym przekierowaniem ekranu, klawiatury, myszki i drukarek do zdalnego użytkownika. Uzyskuje się w ten sposób scentralizowany dostęp do praktycznie dowolnej aplikacji firmowej. Jednocześnie jest to rozwiązanie niewymagające pod względem pasma transmisji – w typowych zastosowaniach wystarcza 20-25 Kb/s dla jednego użytkownika [Marciniak 2005].

Zalety rozwiązań terminalowych to m.in. znacznie prostsza (niż w systemach rozproszonych) aktualizacja aplikacji, ułatwienia w śledzeniu pracy użytkowników, wykorzystaniu licencji, monitorowaniu wydajności, zarządzaniu uprawnieniami do zasobów. W porównaniu z typowymi sieciami VPN nie występują konflikty adresów IP. Utrzymywanie scentralizowanych danych ułatwia ich zabezpieczenie i stosowanie spójnych reguł bezpieczeństwa.

Serwery terminalowe to rozwiązanie znane od dawna, także z tzw. połączeń wdzwanianych (modemowych), które znalazło obecnie nowe zastosowanie. Natomiast nowym podejściem jest zdalny dostęp do **serwera aplikacyjnego**. W tym rozwiązaniu zestawiane połączenie obsługuje szyfrowaną wymianę danych między komputerem-klientem a usługą (aplikacją) sieciową. Przykładem najpopularniejszego serwera aplikacyjnego do zdalnego dostępu jest komercyjny Nokia SAS (Secure Access System). Pakiet ten działa ze wszystkimi przeglądarkami, ruch między klientem i serwerem przenoszony jest w sesjach HTTP, nie występują zatem problemy z translacją adresów NAT. Ponieważ połączenia są zestawiane za pośrednictwem działającego w sieci publicznej brokera, klient i serwer mogą być bez problemu zlokalizowani za zaporami sieciowymi *firewall*.

5. Zakończenie

Trzeba pamiętać, że wirtualne sieci prywatne działają w sieciach publicznych, są zatem bardziej niż sieci korporacyjne narażone na atak z zewnątrz. Niezbędne jest więc zastosowanie mocnych metod autoryzacji i uwierzytelniania, a także innych mechanizmów chroniących najcenniejsze dane przedsiębiorstwa.

Błędem często popełnianym przez użytkowników wirtualnych sieci prywatnych jest przeświadczenie, że technologia VPN sama w sobie wystarczy do bezpiecznej komunikacji i ochrony zasobów. Przy wdrożeniu VPN powinno się opracować szczegółowe procedury postępowania w sytuacjach zagrożenia oraz przygotować i zmodyfikować dotychczasową lub wdrożyć nową politykę bezpieczeństwa, określić minimalne standardy bezpieczeństwa i opracować procedury ich wdrożenia i kontroli.

Obszarem, w którym wirtualne sieci prywatne powinny znaleźć w najbliższej przyszłości szerokie zastosowanie, wydają się lokalne sieci bezprzewodowe (WLAN – Wireless Local Area Network). Stosowany w tych sieciach, i będący jednym z elementów standardu 802.11, protokół WEP (Wired Equivalence Protocol) jest powszechnie krytykowany, ponieważ nie gwarantuje oczekiwanej poufności transmisji. Realizowana w sieciach WLAN transmisja radiowa jest narażona na podsłuchanie przez każdego intruza znajdującego się w zasięgu nadającej bezprzewodowej karty sieciowej lub punktu dostępowego. Metody uwierzytelniania stron nawiązujących połączenie oraz szyfrowania pakietów, opracowane i przetestowane w sieciach VPN, mogą być wykorzystane do zwiększenia bezpieczeństwa sieci bezprzewodowych.

Literatura

Koziński M., *Tunel zamknięty na klucz (bezpieczne połączenie przy użyciu protokołu IPSec)*, „PC Kurier" 2002 nr 1.

Krawczyk P., *Dziura w tunelu*, „Computerworld" 2005 nr 8.

Marciniak M., *Tunel w budowie*, „Computerworld" 2005 nr 10.

Nikodem R., *Bezpieczeństwo transmisji danych w wirtualnych sieciach prywatnych*, [w:] *Informatyka narzędziem zarządzania w XXI wieku*, red. J. Kisielnicki, Wyd. Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, Warszawa 2003.

Rylko K., *VPN za darmo*, „NetWorld" 2005 nr 3.

CONNECTION SECURITY IN WIDE AREA NETWORKS

Summary

The article concerns secure connections in VPN (Virtual Private Network). In order to improve network secutiry, protocols such as IPSec and SSL are applied. A network, built from proper components and well managed, is really secure. Other methods, as terminal services and application servers, are also mentioned.

Dr inż. Ryszard Nikodem jest starszym wykładowcą w Katedrze Teorii Informatyki Akademii Ekonomicznej we Wrocławiu

e-mail: Ryszard.Nikodem@ae.wroc.pl