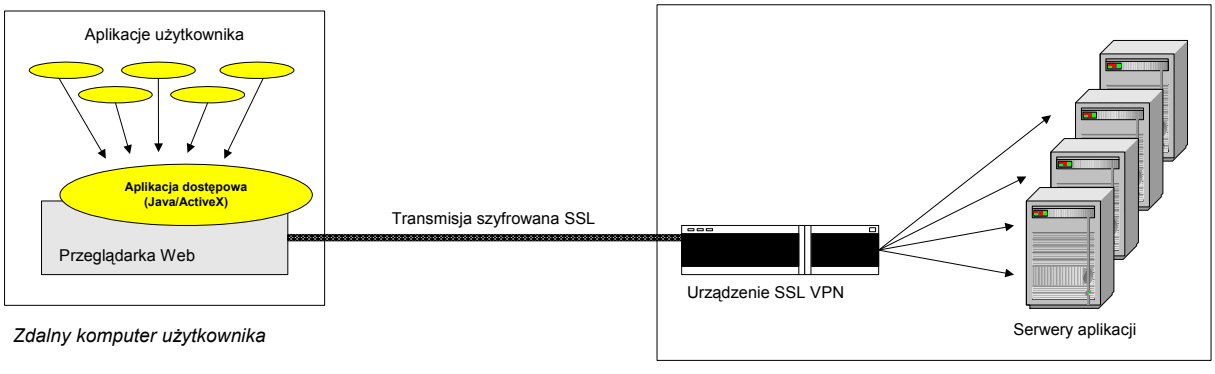
SSL VPN – nowy standard sieci VPN

IPSec jest ogólnie przyjętym standardem i najczęściej stosowaną technologią sieci VPN. W niektórych zastosowaniach posiada jednak istotne ograniczenia (np. zdalny dostęp użytkowników). Alternatywną do IPSec technologią VPN jest SSL. Podstawową zaletą SSL jest dostępność sieci VPN ze zwykłego komputera PC, na którym nie ma potrzeby instalowania i konfigurowania dodatkowego oprogramowania. Technologia SSL VPN opiera się na zasadzie wykorzystania mechanizmów szyfrowania i uwierzytelniania transmisji danych zawartych w przeglądarkach Web.

Użytkownicy mogą za pomocą zwykłej przeglądarki Web (np. MS Internet Explorer, Netscape) korzystać z usług systemu informatycznego firmy. SSL VPN jest szczególnie dogodnym sposobem dostępu do sieci firmowej dla pracowników będących w podróży, którzy w hotelach, na lotniskach, czy salach konferencyjnych mają do dyspozycji tylko pre-konfigurowane stacje dostępowe do Internetu. SSL VPN posiada oczywiste zalety i w wielu zastosowaniach jest lepszym rozwiązaniem od IPSec. Planując wdrożenie sieci VPN należy jednak zdawać sobie sprawę, że SSL nie jest tak uniwersalnym rozwiązaniem jak IPSec (tzn. nie wszystkie aplikacje są wspierane). SSL VPN stwarza także dodatkowe wymagania bezpieczeństwa.

Dostępne na rynku rozwiązania SSL VPN znacząco różnią się w zakresie obsługiwanych aplikacji oraz dostępnych mechanizmów bezpieczeństwa. Wg badań wykonanych przez niezależne instytucje najbardziej uniwersalne i zaawansowane technicznie rozwiązanie SSL VPN to NetScreen Secure Access (m.in. raport Gartner z kwietnia 2003, raport Network Computing z listopada 2003, raport Network World z stycznia 2004). Przedstawione w dalszej części opracowania informacje nt. technologii SSL VPN dotyczą tego rozwiązania.



Zasada funkcjonowania sieci SSL VPN

Wykorzystując protokół SSL można w naturalny sposób zapewnić dostęp do intranetowych aplikacji HTTP. W technologii Web można łatwo zaimplementować emulatory terminali Telnet/SSH. Niektóre aplikacje posiadają możliwości ochrony transmisji danych poprzez SSL (np. aplikacje klienta poczty mogą komunikować się z urządzeniem dostępowym SSL VPN za pomocą protokołów POP-over-SSL, IMAP-over-SSL oraz SMTP-over-SSL). Większość aplikacji systemu informatycznego do komunikacji sieciowej nie wykorzystuje jednak protokołu HTTP. Ich obsługa w rozwiązaniach SSL VPN wymaga załadowania na komputer użytkownika aplikacji Java lub ActiveX, które przekierowują ruch sieciowy do urządzenia dostępowego SSL VPN (patrz rysunek).

Komunikacja aplikacji użytkowników z serwerami w sieci wewnętrznej firmy jest tunelowana za pomocą protokołu SSL. Odbywa się to zwykle z zaangażowaniem serwisu rozwiązywania nazw DNS. Klient aplikacji w odpowiedzi DNS o adres IP docelowego serwera otrzymuje lokalny adres komputera. Połączenie aplikacji do lokalnego komputera jest następnie w sposób zabezpieczony kryptograficznie tunelowane do urządzenia SSL VPN i stamtąd uzyskuje dostęp do serwera w sieci wewnętrznej firmy. Dobrej klasy rozwiązania SSL VPN potrafią rozwiązywać nazwy DNS bez konieczności modyfikowania lokalnej konfiguracji DNS.

Mając na uwadze łatwość dostępu do sieci SSL VPN należy wdrożyć stosowne środki bezpieczeństwa. Systemy SSL VPN oferują w tym zakresie szereg mechanizmów zabezpieczeń, m.in.:

- wiarygodne uwierzytelnianie tożsamości użytkowników (np. RADIUS, SecureID),
- kontrola dostępu użytkowników do określonych aplikacji systemu informatycznego,
- weryfikacja stanu bezpieczeństwa zdalnego komputera (np. aktualna wersja skanera antywirusowego, uruchomione zabezpieczenia Personal Firewall),
- usuwanie danych aplikacji z komputera po zakończeniu pracy użytkownika (np. usuwanie zapisów w pamięci Cache przeglądarki Web),
- rejestrowanie i raportowania zdarzeń.

Systemy SSL VPN wymagają opracowania projektu i wdrożenia, które uwzględnia specyficzne dla tego rozwiązania aspekty bezpieczeństwa. Istotne w tym przypadku jest zagrożenie utraty poufności danych firmy. Wynika ono przede wszystkim z faktu, że użytkownicy mogą korzystać z komputerów niekontrolowanych przez administratorów firmy. Przeglądarka Web domyślnie zapisuje dane w pamięci Cache, które mogą być później odczytane przez innych użytkowników. Na komputerach może być także zainstalowane oprogramowanie rejestrujące dane odczytywane przez przeglądarkę Web i wprowadzane przez użytkowników (np. key logger). Potencjalnie może zdarzyć się także sytuacja gdzie użytkownik korzystający np. z komputera w kawiarence internetowej pozostawi otwarte sesje aplikacji. Stosowaną zwykle praktyką we wdrożeniach SSL VPN jest dostęp do ważnych aplikacji systemu informatycznego tylko z komputerów należących do firmy, po wcześniejszej weryfikacji ich stanu zabezpieczenia.