

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

VPN – Virtual Private Network

Użycie certyfikatów niekwalifikowanych
w sieciach VPN

wersja 1.1

Spis treści

1. CO TO JEST VPN I DO CZEGO SŁUŻY.....	3
2. RODZAJE SIECI VPN.....	3
3. ZALETY STOSOWANIA SIECI IPSEC VPN.....	3
4. METODY UWIERZYTELNIANIA.....	4
5. CERTYFIKATY CYFROWE.....	4
5.1. ZASTOSOWANIE CERTYFIKATÓW CYFROWYCH.....	5
5.2. SPOSÓB UZYSKANIA CERTYFIKATU DLA URZĄDZEŃ VPN	5
5.3. ZALETY STOSOWANIA CERTYFIKATÓW	5
5.4. URZĄDZENIA WSPIERAJĄCE CERTYFIKATY CYFROWE.....	6

1. Co to jest VPN i do czego służy

Skrót VPN (z ang. Virtual Private Network) oznacza Wirtualną Sieć Prywatną, zwaną potocznie „siecią VPN”. Sieci VPN pozwalają w sposób bezpieczny łączyć ze sobą sieci i komputery z wykorzystaniem niezaufanego i niebezpiecznego medium, jakim jest np. Internet, linie dzierżawione czy łącza radiowe. Transmisja pomiędzy poszczególnymi sieciami i komputerami odbywa się poprzez szyfrowane i zabezpieczone wieloma mechanizmami wirtualne „tunele”.

2. Rodzaje sieci VPN

Jest wiele rodzajów sieci VPN różniących się sposobem realizacji transmisji, stosowanymi mechanizmami zapewniającymi bezpieczeństwo i cechami funkcjonalnymi.

Wśród nich wyróżniamy:

- 1) oparte na protokole IPsec,
 - a) sieci typu **site-to-site** łączące ze sobą w sposób bezpieczny dwie lub więcej sieci; „tunele” pomiędzy tymi sieciami najczęściej są zakończone na dedykowanych urządzeniach takich jak routery z funkcją VPN, firewalle lub koncentratory VPN; nie wymagają instalacji żadnego oprogramowania na komputerach;
 - b) sieci typu **remote-access** lub **client-to-site** łączące w sposób bezpieczny pojedyncze komputery z sieciami; wymagają instalacji na komputerach specjalnego oprogramowania typu VPN Klient;
- 2) oparte na protokole SSL – najczęściej typu remote-access, nie wymagają instalacji specjalnego oprogramowania na komputerze, za to mają mniejszą funkcjonalność niż sieci VPN oparte na protokole IPsec,
- 3) oparte na innych protokołach / technologiach, np. L2TP.

3. Zalety stosowania sieci IPsec VPN

- zapewnienie poufności poprzez szyfrowanie danych silnymi algorytmami kryptograficznymi,
- zapewnienie integralności poprzez uniemożliwienie modyfikacji danych w trakcie transmisji,
- uwierzytelnianie stron poprzez zapewnienie, że nikt nie podszył się pod żadną ze stron,
- zapewnienie niezaprzeczalności, które oznacza, że strony nie mogą zaprzeczyć, że nie wysłały danej informacji, o ile informacja ta była podpisana kluczem prywatnym i podpis został poprawnie zweryfikowany.

4. Metody uwierzytelniania

Zanim zostanie zestawiony wirtualny „tunel” VPN, obie strony muszą się wzajemnie uwierzytelnić, aby mieć pewność, że urządzenie po drugiej stronie tunelu jest tym, za kogo się podaje.

Istnieją trzy metody uwierzytelniania:

- **hasło statyczne, klucze współdzielone (pre-shared key):** W trakcie przygotowywania do pracy urządzenia klucz wpisuje się bezpośrednio do pliku konfiguracyjnego. Metody tej nie poleca się z uwagi na łatwość popełnienia pomyłki w trakcie konfiguracji, możliwość podszycia się trzeciej strony w przypadku kompromitacji klucza a także z przyczyn administracyjnych (problematyczne jest zarządzanie połączeniami w obrębie kilku czy kilkunastu urządzeń)
- **klucze publiczne RSA:** Na każdym z urządzeń biorących udział w połączeniu generowana jest para kluczy: prywatny-publiczny. Klucze publiczne należy następnie wymienić ze wszystkimi uczestnikami połączenia. W procesie tym bierze udział człowiek, który musi „ręcznie” dokonać wymiany kluczy. Rozwiązanie to jest praktycznie nieskalowalne, przy większej liczbie urządzeń konieczne jest dokonanie $N*(N-1)$ wymiany kluczy, co jest czasochłonne. Dodatkowo w przypadku kompromitacji jednego z urządzeń należy wykasować stare i wgrać nowe klucze na pozostałych urządzeniach.
- **certyfikaty cyfrowe:** (ze względu na swoją strukturę stanowią najbardziej zaufany mechanizm uwierzytelniania, możliwe jest zautomatyzowanie procesu ich wymiany w przypadku kompromitacji jednej ze stron. Ta metoda uwierzytelniania cechuje się również skalowalnością. Przy „N” stronach biorących udział w połączeniu konieczne jest „N” uwierzytelnień i „N” certyfikatów)

5. Certyfikaty cyfrowe

Przez „certyfikat” rozumiemy dane podpisane cyfrowo przez tzw. „zaufaną trzecią stronę”. Dane, o których mowa zawierają zazwyczaj następujące informacje:

- Klucz publiczny właściciela certyfikatu.
- Nazwę zwyczajową (np. imię i nazwisko, pseudonim, etc.)
- Nazwę organizacji.
- Jednostkę organizacyjną.
- Zakres stosowania (podpisywanie, szyfrowanie, autoryzacji dostępu itp.)
- Czas, w jakim certyfikat jest ważny.
- Informacje o wystawcy certyfikatów.
- Sposób weryfikacji certyfikatu (np. adres, pod którym można znaleźć listy CRL).
- Adres, pod którym znajduje się polityka certyfikacji, jaką zastosowano przy wydawaniu tego

certyfikatu.

Struktura certyfikatu nie jest sztywna i w zależności od potrzeb można umieszczać w niej dodatkowe pola, wykraczające poza definicję standardu.

5.1. Zastosowanie certyfikatów cyfrowych

W rozwiązaniach dla sieci VPN certyfikat stanowi element uwierzytelniający każdą ze stron biorących udział w połączeniu. Dzięki temu rozwiązaniu podszycie się pod jedną ze stron biorących udział w połączeniu jest wysoce nieprawdopodobne.

5.2. Sposób uzyskania certyfikatu dla urządzeń VPN

Ogólny zarys czynności, które należy wykonać, by urządzenia służące do zestawienia połączeń VPN mogły autoryzować się przy użyciu certyfikatów przedstawione są w kolejnych krokach:

- 1) Przy użyciu urządzenia generowana jest para kluczy RSA (tj. klucz publiczny i klucz prywatny),
- 2) Urządzenie generuje zbiór danych w standardzie PKCS10, który zawiera jego dane identyfikacyjne oraz publiczny klucz RSA,
- 3) Klucz publiczny jest przekazywany do urzędu certyfikacji (za pośrednictwem stosowanego formularza),
- 4) Urząd certyfikacji po zweryfikowaniu pliku PKCS10 podpisuje go swoim kluczem prywatnym RSA (wystawia certyfikat),
- 5) Urządzenie pobiera wystawiony certyfikat cyfrowy, jak również listę CRL i certyfikat urzędu z danego urzędu certyfikacji.

5.3. Zalety stosowania certyfikatów

- uwierzytelniają strony biorące udział w połączeniu,
- zapewniają poufność danych,
- zapewniają integralność danych,
- zapewniają niezaprzeczalność danych.

Niektórzy z producentów urządzeń z zaimplementowaną funkcjonalnością VPN pozwalają na dodatkową kontrolę uwierzytelnianych poprzez certyfikat stron połączeń. Możliwe jest ograniczenie zestawienia sesji jedynie dla połączeń uwierzytelnionych certyfikatem pochodzącym od konkretnego dostawcy. Ponadto można weryfikować (wymusić) istnienie określonych pól certyfikatu, zawierających odpowiednie wartości. Dzięki tak rozbudowanym mechanizmom uwierzytelniania certyfikaty w zastosowaniach VPN stanowią najsilniejsze ogniwo, na podstawie którego dopuszcza się bądź odrzuca połączenia zdalne, inicjowane przez drugą stronę, która chce nawiązać bezpieczne połączenie siecią zdalną.

Istotną zaletą jest też skalowalność rozwiązań opartych na certyfikatach. Żaden inny mechanizm nie daje takiej łatwości w uaktualnianiu mechanizmów uwierzytelniania, jaką zapewniają certyfikaty. Urządzenia, które w pełni wspierają oferowane standardy w praktyce samodzielnie pobierają nowe certyfikaty, jeśli poprzednie zostały wycofane np. poprzez listę CRL. Dzięki istnieniu „zaufanej trzeciej strony” ich podrobienie jest wysoce nieprawdopodobne. Stanowią wygodną metodę zabezpieczenia sieci dla administratorów, którzy zarządzają złożoną infrastrukturą sieci.

W przypadku połączeń typu „remote - access” oprócz łatwości zarządzania użytkownicy są autoryzowani przy użyciu silnych mechanizmów uwierzytelniania, przy jednoczesnym zachowaniu skalowalności rozwiązania.

5.4. Urządzenia wspierające certyfikaty cyfrowe

- routery CISCO
- koncentratory VPN CISCO
- routery Juniper serii M
- urządzenia serii NetScreen
- firewalle rodziny CheckPoint
- inne urządzenia

Od strony sprzętu, na którym dokonana zostanie implementacja bezpiecznego uwierzytelnienia połączeń VPN przy użyciu certyfikatów wymagane jest jedynie, aby wspierały one ścieżki certyfikacji. Wymóg ten jest niezbędny z uwagi na sposób realizacji wystawienia certyfikatu dla urządzenia (zgodnego z ogólnie przyjętym standardem).