Uniwersytet Mikołaja Kopernika
w Toruniu
Wydział Fizyki, Astronomii i Informatyki Stosowanej

Sebastian Janusz Wasilewski

Zarządzanie certyfikatami w systemie OpenVPN

Praca inżynierska napisana
pod kierunkiem
dra hab. Jacka Kobusa

Toruń 2005

dziękuję mojemu promotorowi
za poświęcony czas
i udzieloną pomoc.

Spis treści

1 Wstęp **3**

2 Zarys technologii VPN **4**

3 Niebezpieczeństwa sieci komputerowych **6**
3.1 Podsłuchiwanie 6
3.2 Podszywanie 7
3.3 Publicznie dostępne usługi 8

4 System OpenVPN **9**

5 Systemu OpenVPN – przykład zastosowania **12**

6 Zarządzanie systemem OpenVPN **16**
6.1 Założenia projektu 16
6.2 Implementacja 16
6.2.1 Dodawanie użytkowników 17
6.2.2 Blokowanie dostępu 20
6.2.3 Przeglądanie listy użytkowników 20
6.2.4 Regeneracja certyfikatów 20
6.2.5 Nadzór nad ruchem sieciowym 20
6.2.6 Nadzór nad połączeniami do openvpn 22
6.2.7 Powiadamianie użytkownika o zdarzeniach 23
6.3 Struktura katalogowa projektu 23
6.4 Instalacja 25

7 Podsumowanie **27**

Dodatek 1 **30**
addcert.pl 30
create_packages.pl 31
CrondExpireCheck.pl 32
delnewcert.pl 32
ReadStatusDaemon.pl 33
refreshcert.pl 34
revokecert.pl 36
sendinfo.pl 37
set_IP.pl 38
showactivity.pl 38
showlogins.pl 40
showstats.pl 41

showusers.pl 43

Dodatek 2 **45**
Biblioteka LaOH.pm 45

Dodatek 3 **49**
Konfiguracja serwera OpenVPN 49
Konfiguracja klienta OpenVPN 49

Dodatek 4 **51**
Konfiguracja systemu netfilter 51

Dodatek 5 **52**
main.conf 52

Dodatek 6 **55**
Konfiguracja ulogd 55
Konfiguracja logrotate dla ulogd 55

Dodatek 7 **56**
Podstawowa konfiguracja mechanizmów certyfikacji SSL 56

Dodatek 8 **59**
Szablony konfiguracji klienta 59

1 Wstęp

Dynamiczny rozwój Internetu w ostatniej dekadzie spowodował wzrost znaczenia problemów bezpieczeństwa transmisji danych i ochrony systemów komputerowych. Z zasad funkcjonowania sieci Internet wynika, że każdy przyłączony do niej komputer jest traktowany równorzędnie, co oznacza, że bezpieczeństwo systemu może zostać naruszone z dowolnego miejsca na świecie o dowolnej porze. Dodatkowo globalizacja oraz spadek cen połączeń internetowych spowodowały, że duże firmy, organizacje oraz instytucje naukowe i edukacyjne stanęły przed koniecznością łączenia swoich, niekiedy bardzo odległych oddziałów. Stąd wynika waga problemu bezpiecznego przesyłania danych pomiędzy komputerami oraz sieciami i stąd bierze się również konieczność opracowywania sposobów zapewniających bezpieczną wymianę danych pomiędzy tymi oddziałami. Jeszcze do niedawna główne problemy bezpieczeństwa sieciowego miały związek z powszechnym stosowaniem protokołów takich jak TELNET czy FTP, które przesyłają dane w sposób jawny. W ostatnich latach coraz częściej używa się nowych protokołów, np. SSH lub SFTP zapewniających poufność. Dla zapewnienia bezpiecznego łączenia lokalnych sieci komputerowych poprzez sieć Internet, a także umożliwienia poszczególnym użytkownikom nieskrępowanego dostępu do zasobów sieci lokalnych, opracowano technologię wirtualnych sieci prywatnych. Dzięki temu możliwa jest identyfikacja użytkowników i zapewnienie poufności w dostępie do prywatnych danych.

W celu ochrony lokalnej sieci oraz umożliwienia pracownikom Wydziału Fizyki, Astronomii i Informatyki Stosowanej UMK możliwości bezpiecznej pracy spoza Wydziału uruchomiony został serwer do obsługi połączeń w ramach wirtualnej sieci prywatnej. Celem pracy była budowa narzędzi wspomagających zarządzanie tym serwerem. Jej rezultatem jest opracowanie systemu LaOH (*Lazy admin's OpenVPN Helper*), który pozwala automatyzować takie zadania administracyjne jak: tworzenie/odwoływanie certyfikatów użytkowników, przygotowywanie plików konfiguracyjnych dla użytkowników, nadzór nad połączeniami. Na system ten składa się szereg skryptów napisanych w języku Perl.

Plan niniejszej pracy jest następujący. W pierwszej części dokumentu została ogólnie opisana technologia wirtualnej sieci prywatnej (rozdz. 2) oraz podstawowe niebezpieczeństwa sieci komputerowych (rozdz. 3). W dalszej części pracy został omówiony system OpenVPN (rozdz. 4) wraz z przykładowym jego zastosowaniem (rozdz. 5). Rozdz. 6 oraz dodatki zostały poświęcone opisowi systemu LaOH oraz jego implementacji i konfiguracji.