Wykorzystanie protokołu SCEP do zarządzania certyfikatami cyfrowymi w systemie zabezpieczeń Check Point NGX

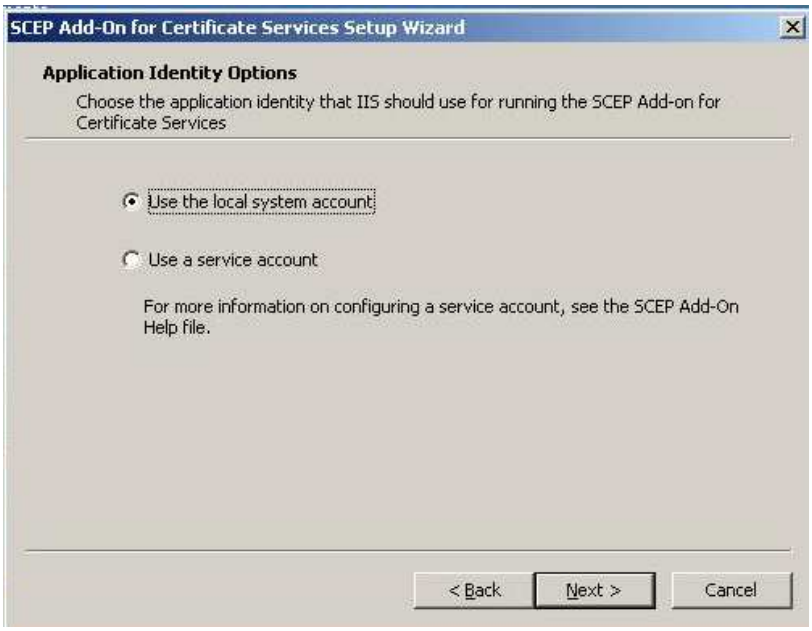
1. Wstęp

Protokół SCEP (*Simple Certificate Enrollment Protocol*) został zaprojektowany przez czołowego dostawcę certyfikatów, firmę Verisign. Ponieważ SCEP okazał się bardzo wygodnym narzędziem, jest obecnie zaimplementowany w produktach czołowych dostawców systemów bezpieczeństwa oraz wspierany przez wiele rozwiązań CA. Przedstawiony zostanie sposób generowania certyfikatów z użyciem serwera CA dostarczanego wraz z systemem Microsoft Windows 2003 Enterprise Edition.

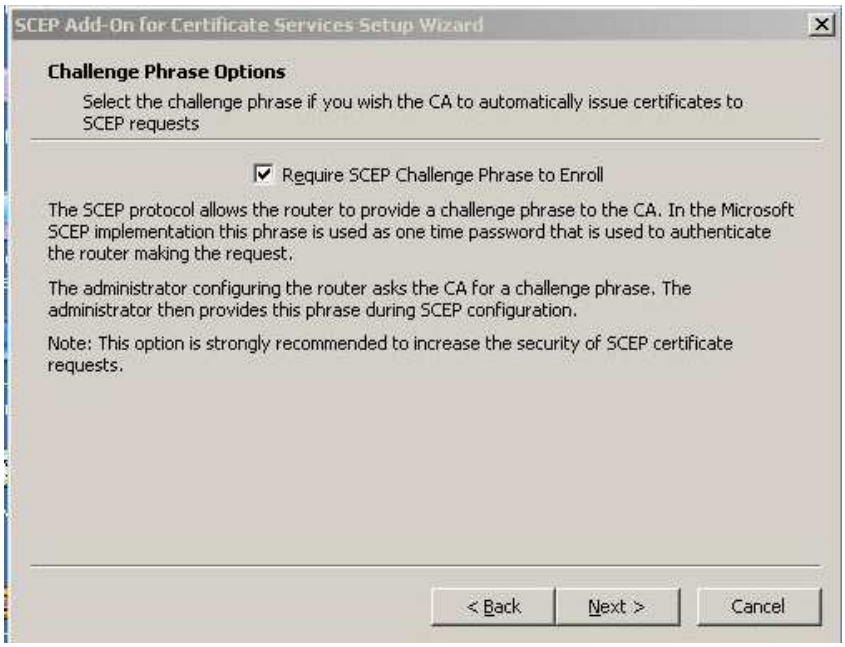
2. Konfiguracja serwera CA

Domyślna instalacja serwera CA w systemie Windows nie zawiera narzędzi SCEP, ale dostępna jest odpowiednia przystawka do pobrania ze strony firmy Microsoft. Po ściągnięciu i uruchomieniu oprogramowania instalacyjnego “kreator” pomaga przeprowadzić instalację.

Po przeczytaniu i zaakceptowaniu licencji pojawi się okno do wyboru konta.

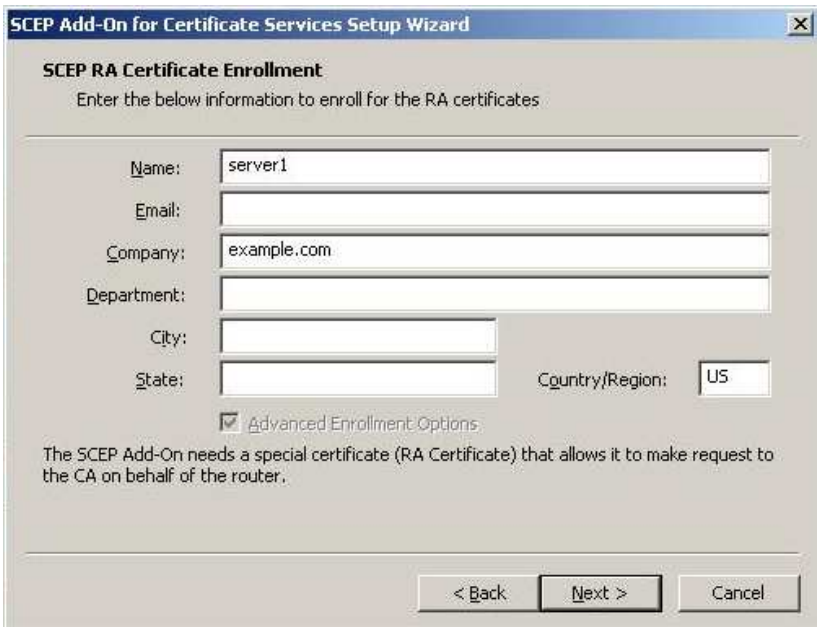


Należy wskazać konto w systemie, z którego oprogramowanie będzie korzystało. Może to być lokalne konto systemowe lub specjalne konto z odpowiednio zdefiniowanymi uprawnieniami.

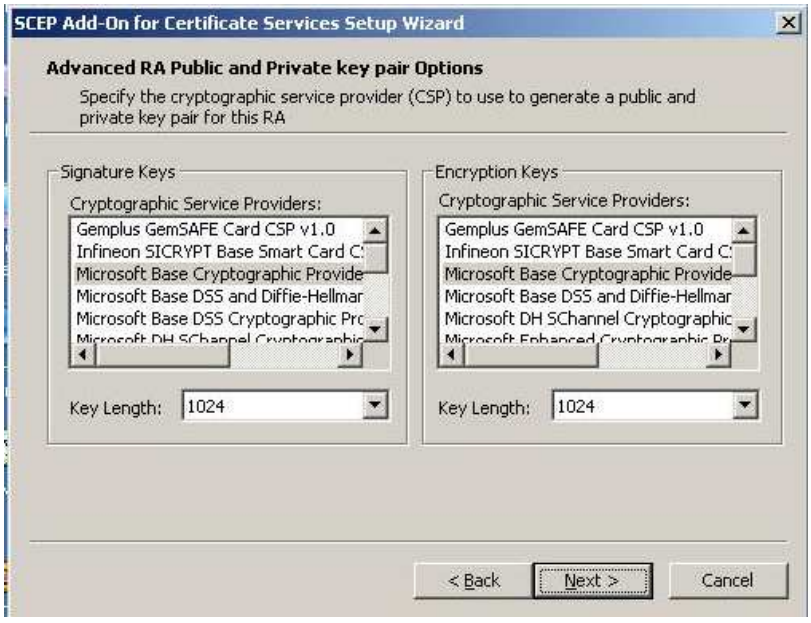


Następnie należy wybrać, czy do wydawania certyfikatu będzie używane hasło jednorazowe. Dokonuje się tego przez zaznaczenie *Require SCEP Challenge Phrase to Enroll*.

Należy również podać informacje o agencie obsługującym wydawanie certyfikatów.



Należy wybrać opcje związane z kluczami do podpisu i szyfrowania.

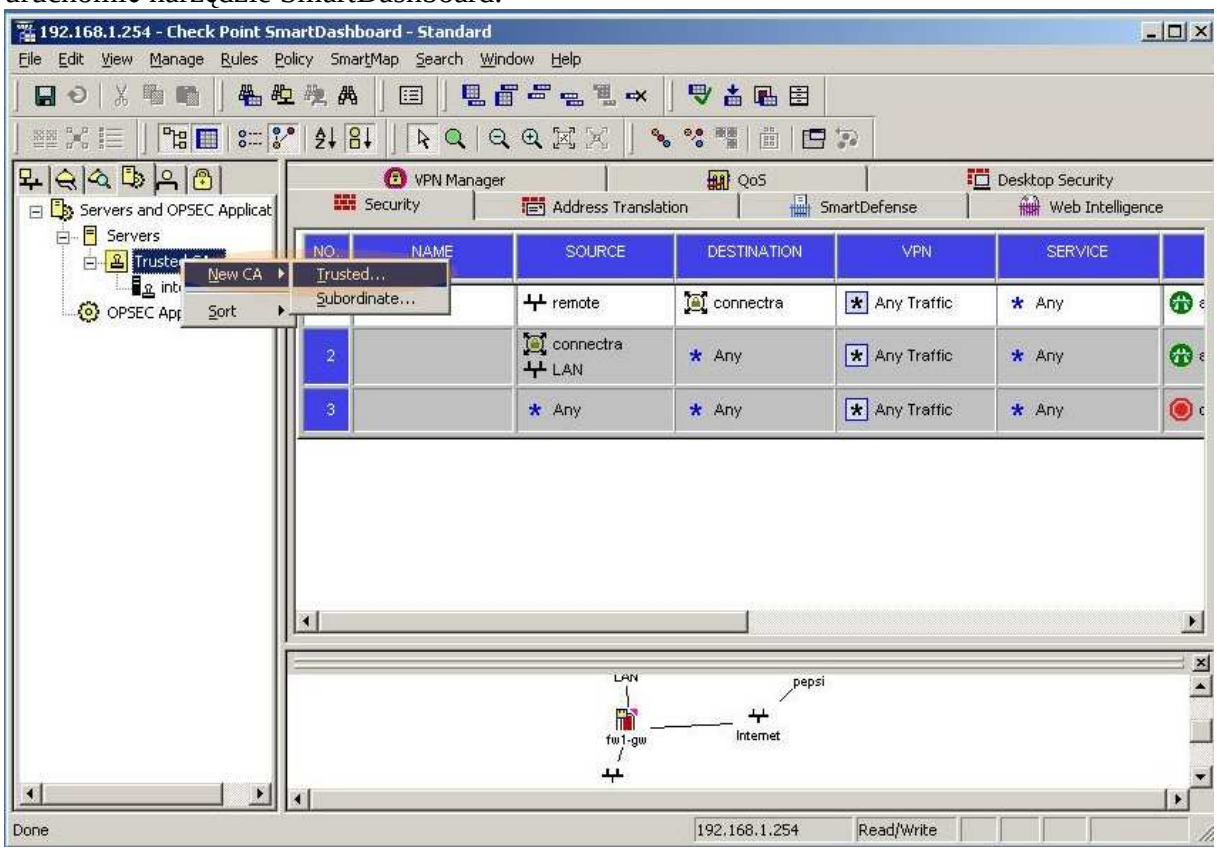


Z odpowiednich list wybiera się dostawców zarejestrowanych w systemie usług kryptograficznych.

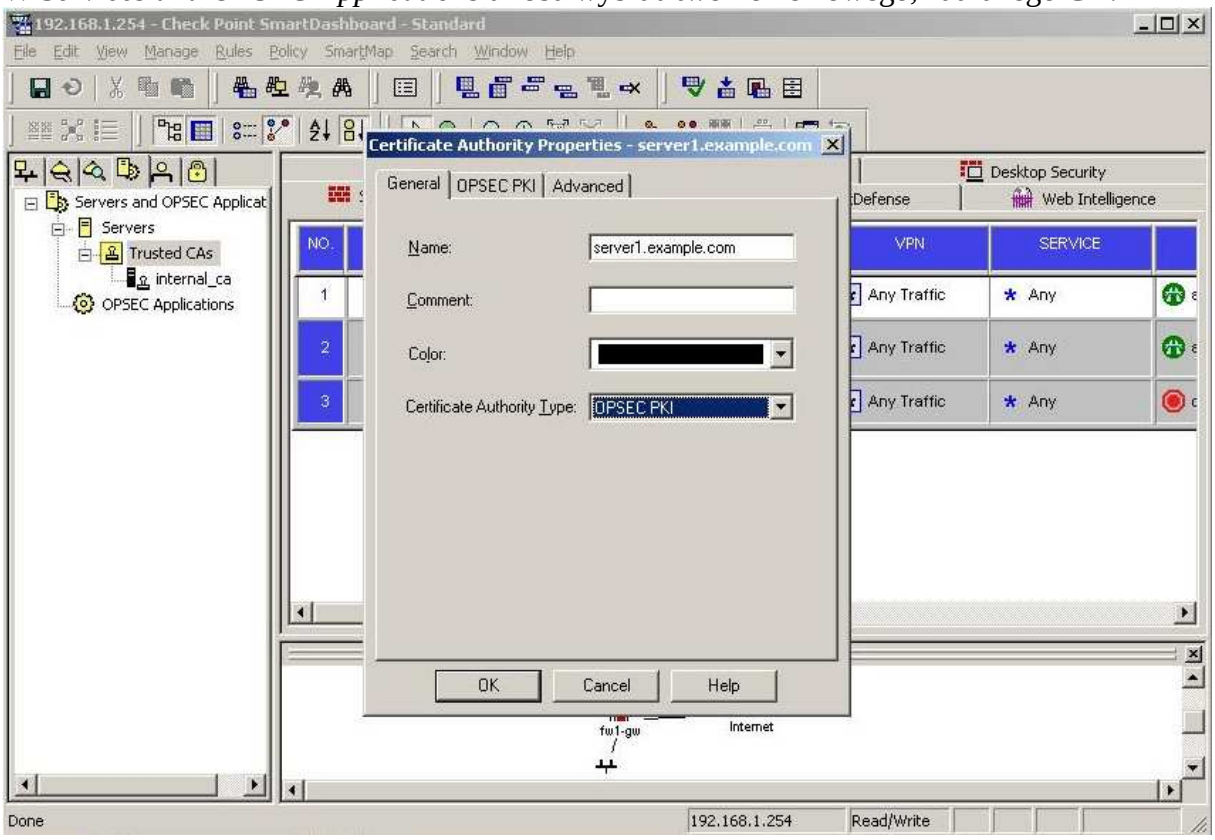
Na tym kończy się prawidłowo wykonana procedura instalacji przystawki protokołu SCEP w systemie Windows 2003 Server.

3. Konfiguracja zewnętrznego CA w systemie Check Point

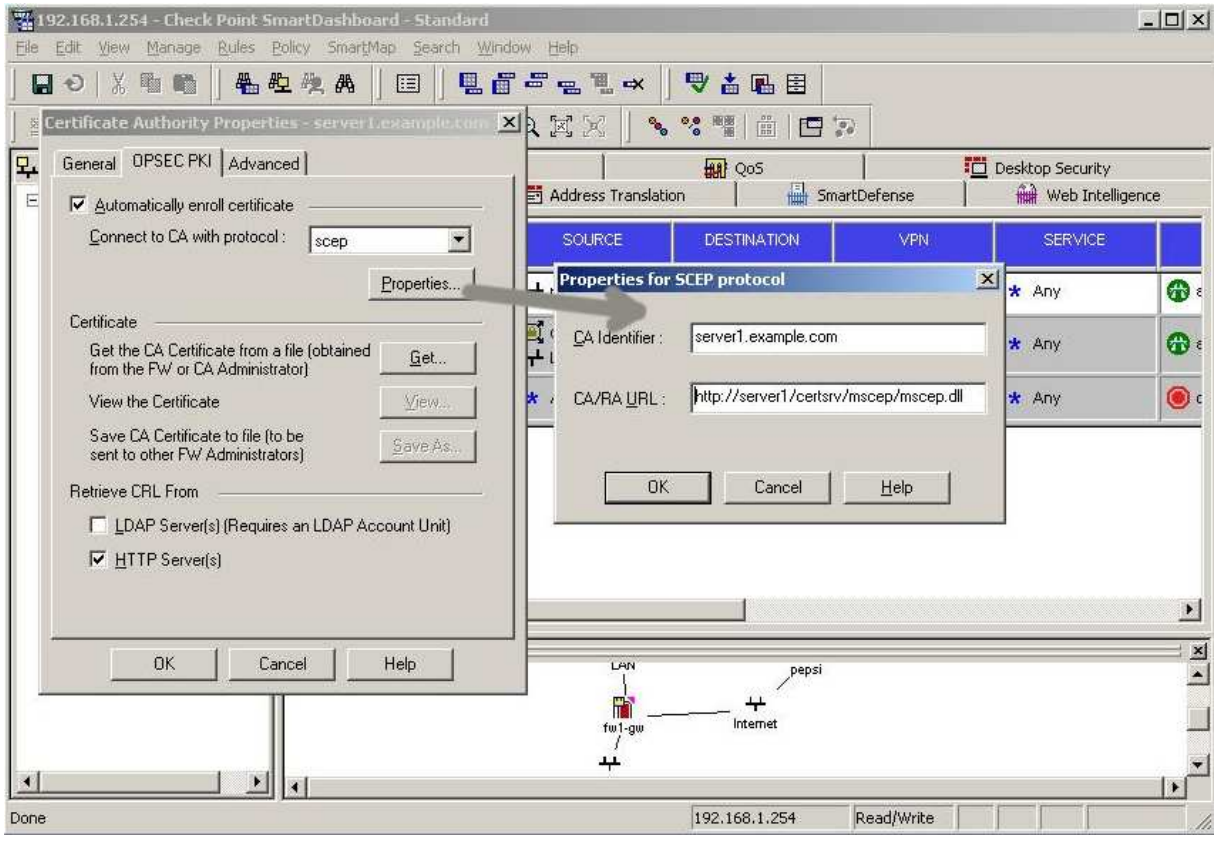
W oprogramowaniu do zarządzania systemem bezpieczeństwa firmy Check Point należy uruchomić narzędzie SmartDashboard.



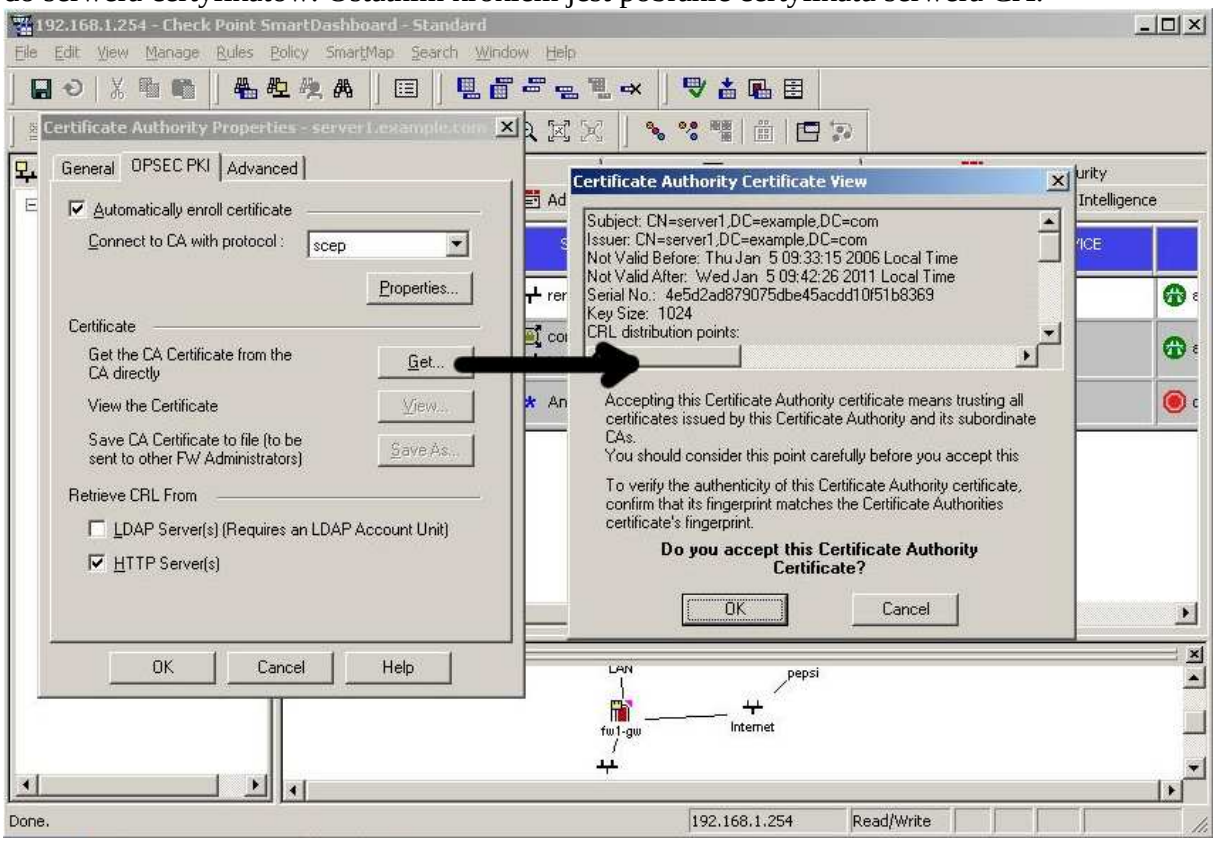
W *Services and OPSEC Applications* trzeba wybrać tworzenie nowego, zaufanego CA.



W polu nazwa należy wpisać najlepiej FQDN serwera CA, a w polu typ pozostawić *OPSEC PKI*.



W zakładce *OPSEC PKI* trzeba wybrać opcję automatycznego wydawania certyfikatów, protokół SCEP, a następnie go skonfigurować. W okienku należy wpisać identyfikator serwera CA oraz URL prowadzący aplikacji wystawiającej certyfikaty. W naszym przypadku jest to URL http://server1/certsrv/mscep/mscep.dll – link ten można uzyskać podłączając się do serwera certyfikatów. Ostatnim krokiem jest pobranie certyfikatu serwera CA.

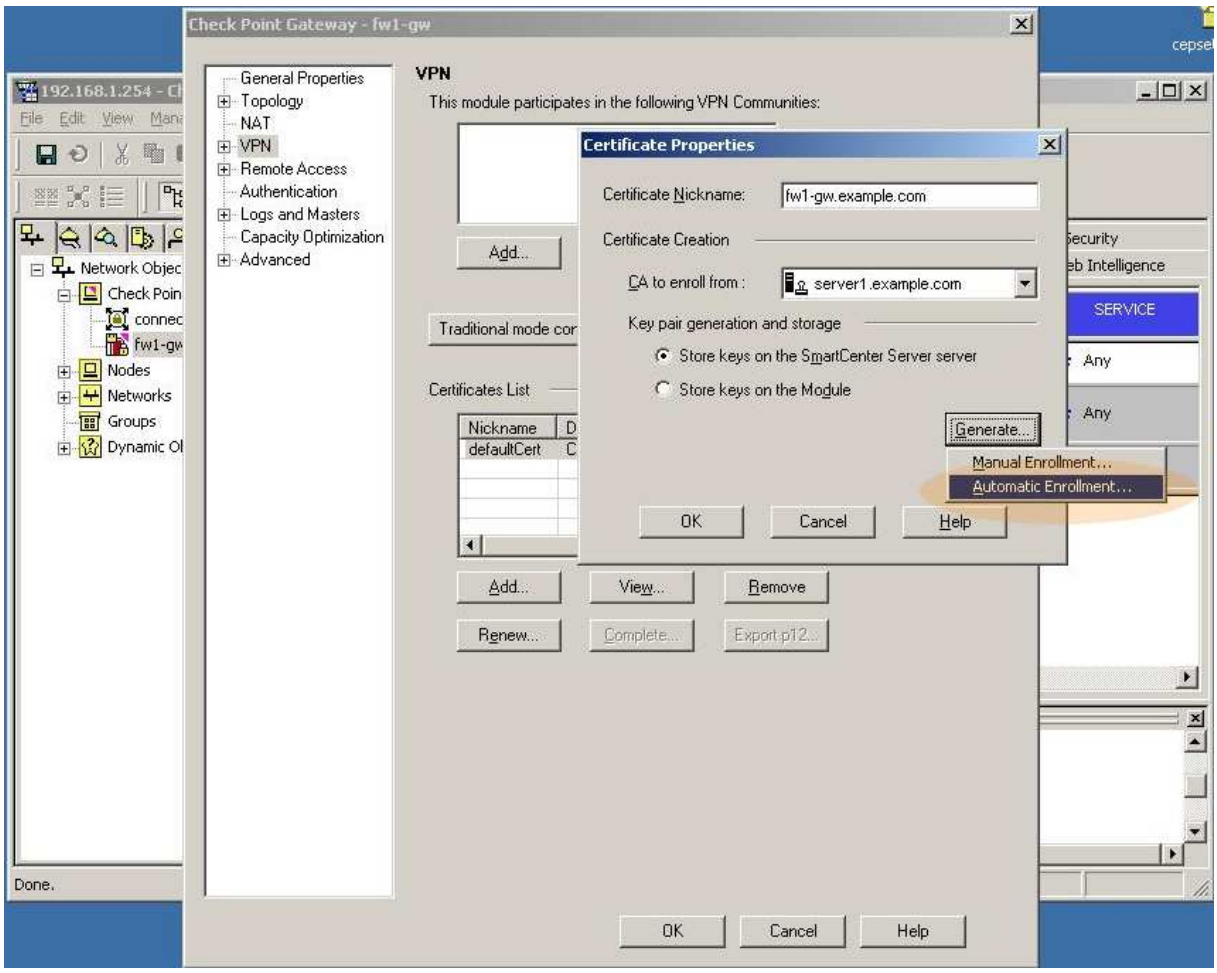


Po zaakceptowaniu certyfikatu w systemie Check Point zostanie zarejestrowany nowy zewnętrzny serwer certyfikatów.

3. Generowanie certyfikatów dla bram VPN

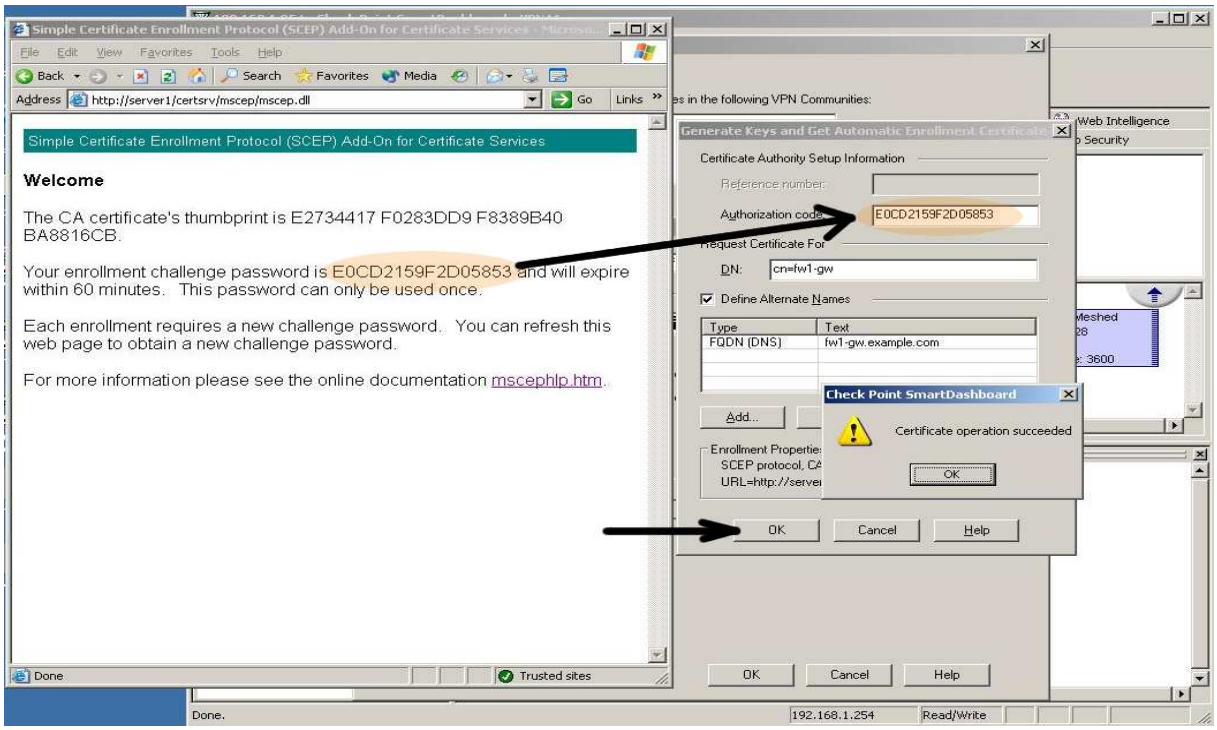
Oprogramowanie Check Point ma wbudowany serwer CA, który automatycznie wydaje certyfikat dla każdego systemu VPN zarządzanego przez dany SmartCenter Server. Może jednak zachodzić potrzeba wydania certyfikatu dla bramy VPN przez zewnętrzny serwer CA. Certyfikat można uzyskać generując odpowiednie zgłoszenie do urzędu certyfikacji i przekazać je w trybie *off-line* lub też zastosować protokół SCEP. Druga metoda jest oczywiście znacznie prostsza i wygodniejsza, albowiem wystarczy wykonać kilka prostych kroków i uzyskuje się certyfikat. Do generacji certyfikatów dla bram VPN służą odpowiednie narzędzia związane z obiektami VPN-1. Należy otworzyć właściwości obiektu Check Point

Gateway, dla którego ma być wygenerowany certyfikat, wybrać właściwości VPN, a następnie przycisk Add.

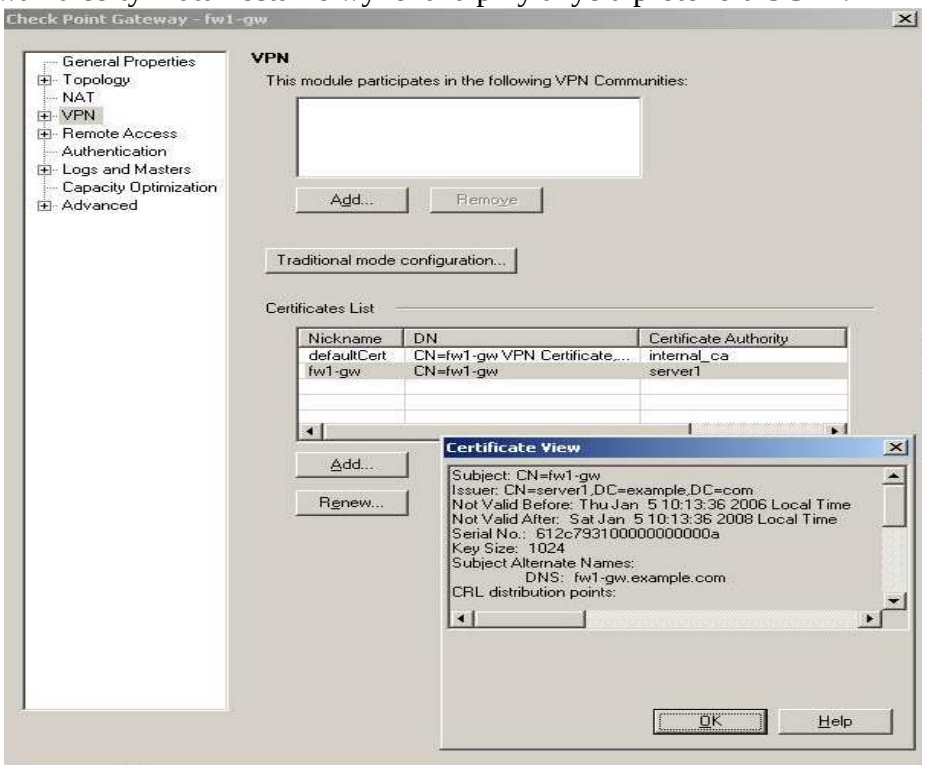


W okienku należy wpisać nazwę certyfikatu, pod jakim będzie rozpoznawany w systemie. Wybrana nazwa nie ma wpływu na funkcjonowanie systemu zabezpieczeń – służy tylko wygodzie. Jako nazwa certyfikatu została przykładowo wpisana nazwa domenowa. Następnie należy wybrać CA, z którego certyfikat ma być pozyskany. W tym przypadku jest to CA uprzednio zdefiniowane, ponieważ certyfikaty będą pozyskiwane za pomocą protokołu SCEP.

Dodatkowo można wskazać miejsce przechowywania kluczy. Klucze mogą zostać zapisane na serwerze zarządzającym lub na module Firewall/VPN. Następnie, po naciśnięciu Generate dostępne są dwie możliwości stworzenia certyfikatu – ręczna i automatyczna. Przy ręcznym generowaniu certyfikatu zostanie stworzone żądanie do CA, które można skopiować, a następnie wkleić w odpowiednim miejscu portalu zewnętrznego CA. W celu uzyskania certyfikatu przy pomocy protokołu SCEP należy wybrać metodę automatycznego generowania.



Otworzy się wtedy kolejne okienko, w którym należy podać DN generowanego certyfikatu. Można również określić alternatywne identyfikatory takie jak adres e-mail, adres IP czy FQDN. Należy podłączyć się również do serwera Microsoft CA otwierając stronę, która została wprowadzona jako link do CA w definicji serwera SCEP. W tym przypadku jest to link do strony http://server1/certsrv/mscep/mscep.dll, na której zostanie wyświetlony kod *challenge*, który należy przepisać do okna *Authorisation code*. Po naciśnięciu OK operacja generowania certyfikatu zostanie wykonana przy użyciu protokołu SCEP.



Po zamknięciu okienka można zweryfikować wystawiony certyfikat we właściwościach obiektu Check Point Gateway, wybierając VPN, następnie podświetlając certyfikat i naciskając View. Widać, że certyfikat został wystawiony przez zewnętrzny CA.

Marek Krauze,
CCSE+ NG, CCSE NGX