Techniczny biuletyn zabezpieczeń IT
e-Nowości
CLICO

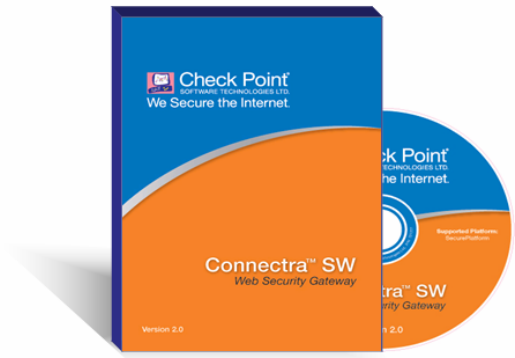
Konfiguracja urządzeń Connectra (SSL VPN) w zintegrowanym środowisku zarządzania Check Point SmartCenter

Technologia SSL VPN umożliwia pracownikom przebywającym poza siedzibą firmy oraz klientom i partnerom handlowym swobodny dostęp do aktualnych informacji, które są im potrzebne do prowadzenia biznesu. Odbywa się to za pomocą zwykłej przeglądarki Web (Microsoft IE, Netscape, Mozilla), tunelując ruch sieciowy w protokole https (SSL, TLS). Opracowane przez Check Point rozwiązanie Connectra łączy w sobie funkcjonalność portalu aplikacyjnego SSL VPN z rozbudowanymi mechanizmami bezpieczeństwa m.in. Intrusion Prevention System, Endpoint Security, Secure Browser. Techniczny opis rozwiązania i zasad jego konfiguracji można znaleźć w dokumencie: http://www.clico.pl/pdf/warsztaty_connectra.pdf

Firmy posiadające już zabezpieczenia Check Point (np. FireWall-1, VPN-1) mogą dokonać wdrożenia Connectra w istniejącym środowisku zarządzania Check Point SmartCenter. W takim przypadku naturalnym jest działanie Connectra nie jako oddzielnego urządzenia zabezpieczeń, ale jako dodatkowego modułu w istniejącym już systemie bezpieczeństwa. Daje to wiele korzyści, m.in. Connectra może korzystać z certyfikatów cyfrowych wydawanych przez urząd certyfikacji Check Point ICA, zdarzenia rejestrowane przez Connectra mogą być analizowane w odniesieniu do logów firewall.

- Connectra Appliance

- Connectra SW

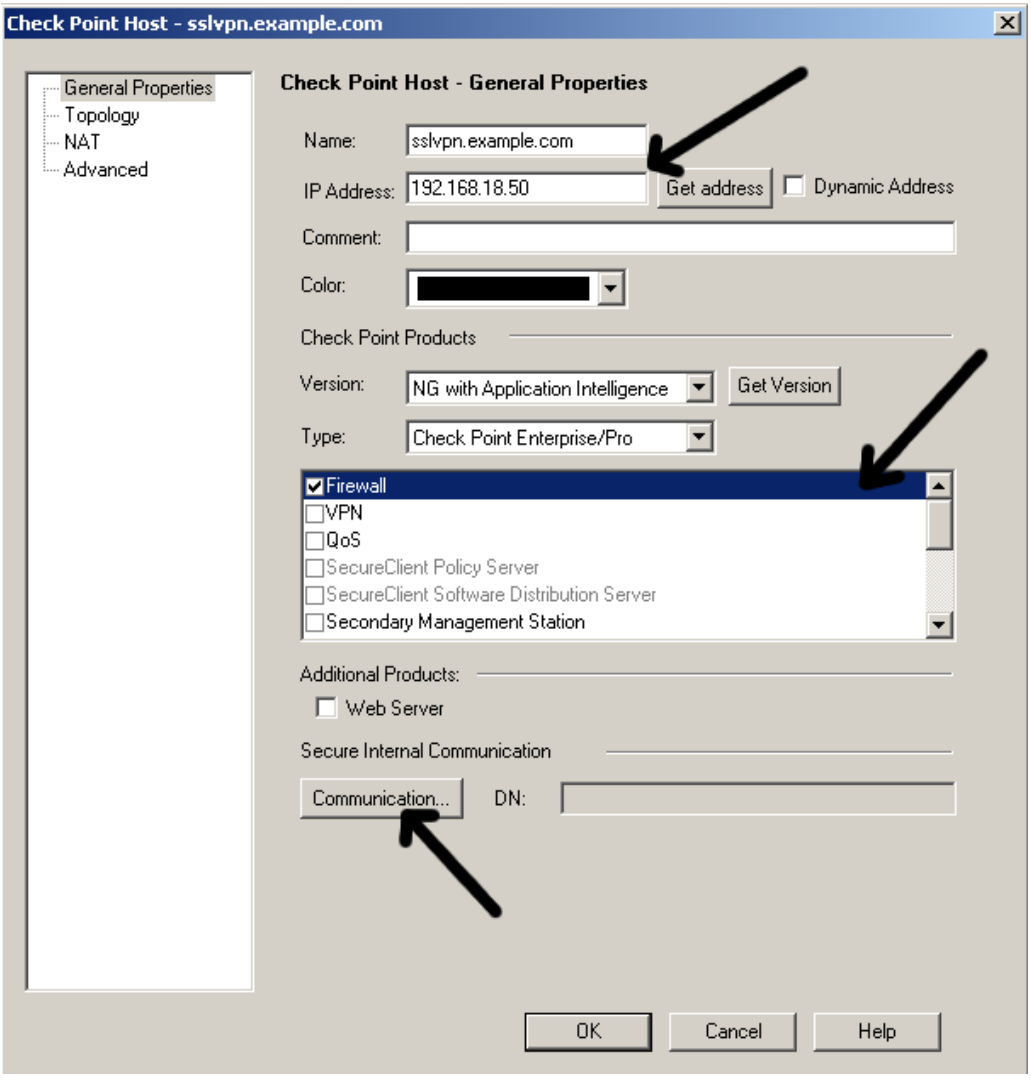


Connectra to pierwsze na rynku rozwiązanie SSL VPN, które jest dostępne jako dedykowane urządzenia Appliance oraz w wersji oprogramowania do instalacji na dowolnym sprzęcie. Zastosowanie własnego sprzętu zwiększa skalowalność rozwiązania oraz daje możliwość doboru platformy o odpowiedniej niezawodności i wydajność zgodnie z indywidualnymi preferencjami. Dostępność programowej wersji Connectra SW sprawia, że rozwiązanie to można łatwo przetestować przed podjęciem decyzji o jego zakupie i wdrożeniu.

Zasady integracji Connectra z systemem zarządzania SCS

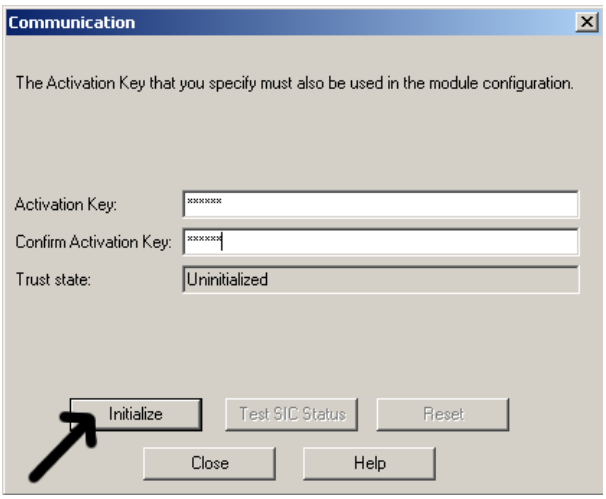
System Connectra w wersji 2.0 umożliwia integrację z innymi modułami firmy Check Point z wykorzystaniem mechanizmu zaimplementowanego w wersji NG, a mianowicie *Secure Internal Communication (**SIC**)*. Zestawienie połączenia SIC odbywa się z użyciem certyfikatów cyfrowych, generowanych przez *Internal CA*, które jest wbudowane w SmartCenter. Komunikacja jest zabezpieczona kryptograficznie przez protokół SSL. Dzięki zestawieniu SIC, moduły systemu zabezpieczeń mogą się komunikować ze sobą, a administratorzy wykorzystując narzędzia z rodziny SmartView mogą uzyskać zintegrowany obraz systemu bezpieczeństwa.

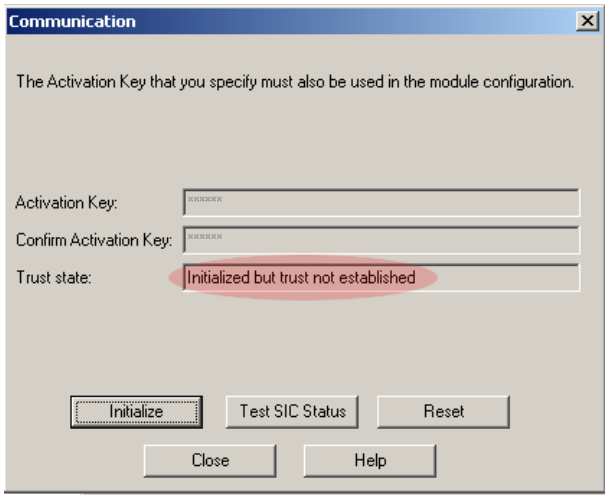
W celu zestawienia połączenia typu SIC w pierwszej kolejności zapewnić należy komunikację sieciową pomiędzy systemem Connectra i serwerem SmartCenter. Następnie przy pomocy narzędzia SmartDashboard należy stworzyć obiekt typu *Check Point Host*, nadając mu nazwę, podając adres IP oraz wybierając *Firewall*, jako zainstalowany moduł.



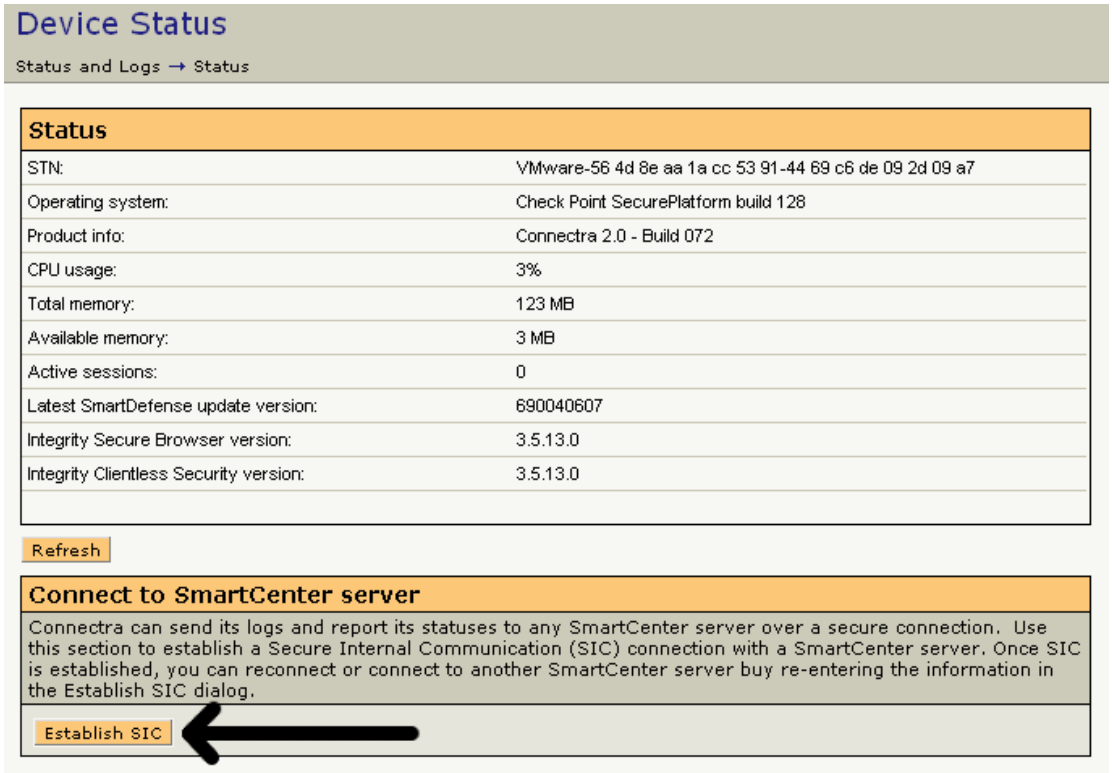
© 2005 CLICO Sp. z o.o. Wszelkie prawa zastrzeżone

Następnie należy nacisnąć przycisk *Communicaton...* Zostanie wtedy wyświetlone okno, w którym należy wpisać kod, służący do zestawienia połączenia i uwierzytelnienia stron podczas generowaniu certyfikatów. Po naciśnięciu *Initialize* proces zestawiania zostanie zainicjalizowany, lecz samo połączenie nie zostanie utworzone.



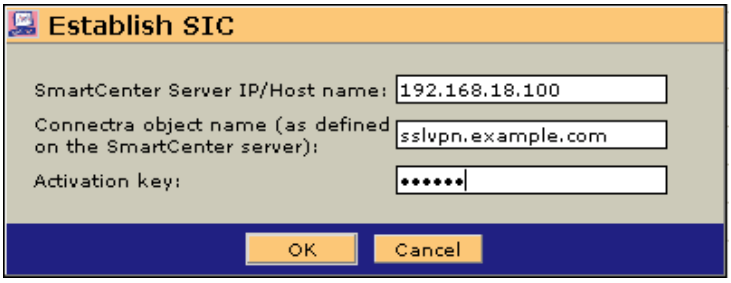


W portalu administracyjnym systemu Connectra, zestawienie połączenia za pomocą *SIC* dokonuje się w menu *Status*. Należy nacisnąć przycisk *Establish SIC*.

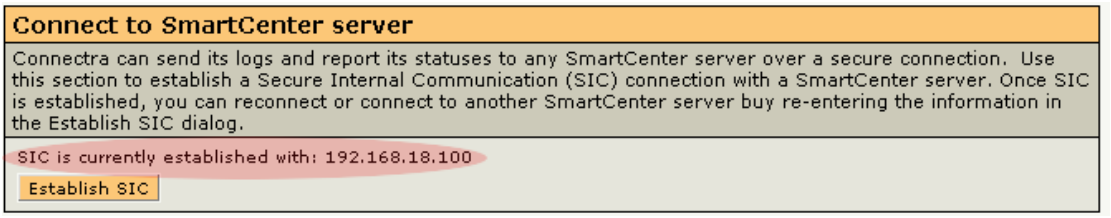


© 2005 CLICO Sp. z o.o. Wszelkie prawa zastrzeżone

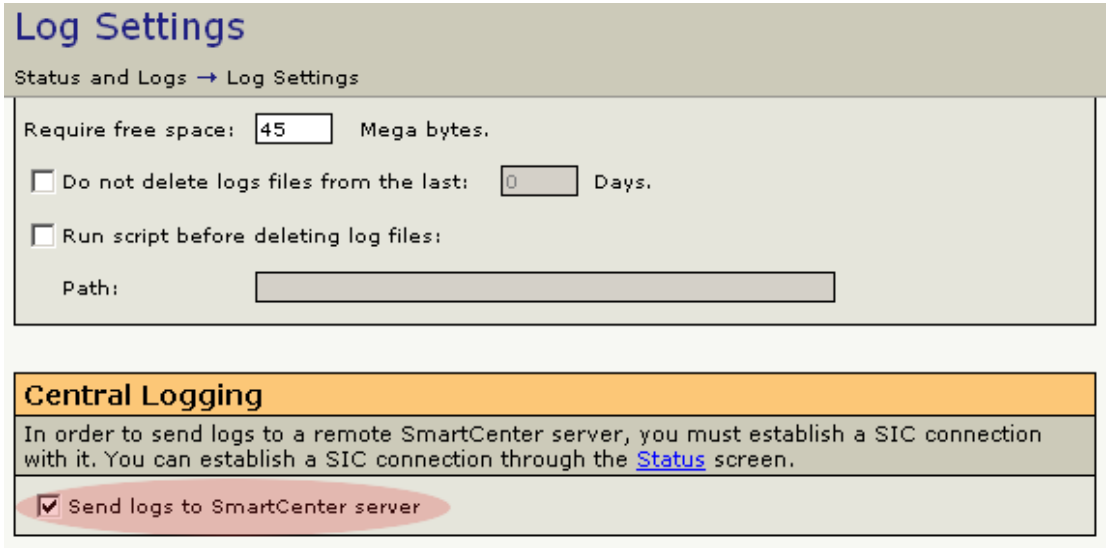
W kolejnym kroku otworzy się okienko, w którym należy wpisać adres IP SmartCenter Servera, nazwę obiektu Connectra, tak jak została zdefiniowana przy pomocy SmartDashboard oraz kod, który został wprowadzany przy inicjalizacji obiektu.



Po zatwierdzeniu wprowadzonych danych, po kilku chwilach komunikacja powinna zostać nawiązana, a na stronie statusu wyświetlona informacja o zestawieniu połączenia z serwerem.

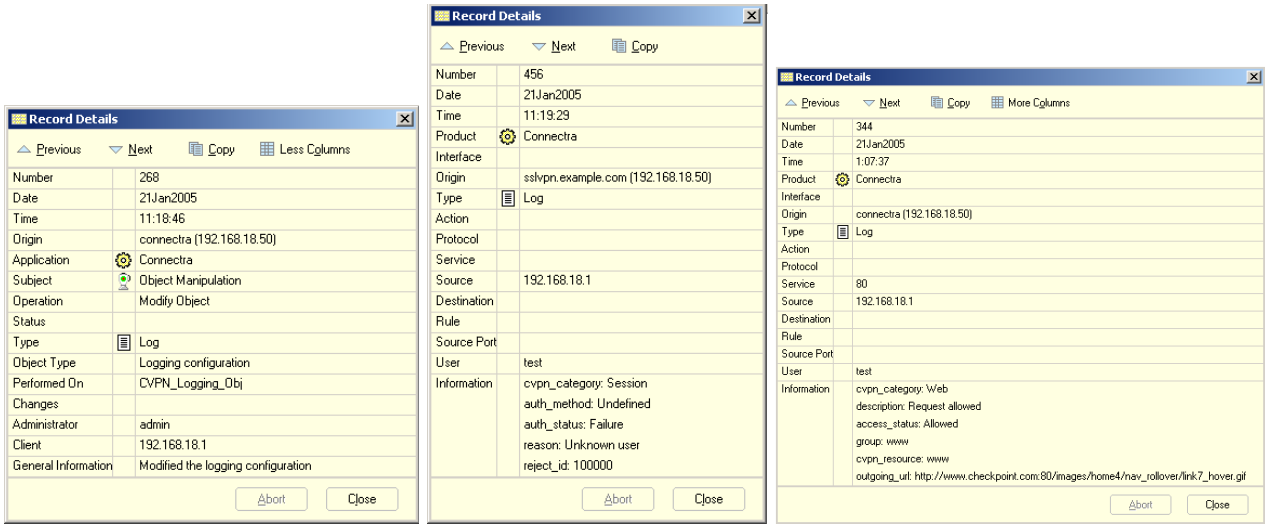


Pozostało skonfigurownie centralnego logowania. W menu *Status->Log Settings* należy zaznaczyć *Send logs to SmartCenter server*.



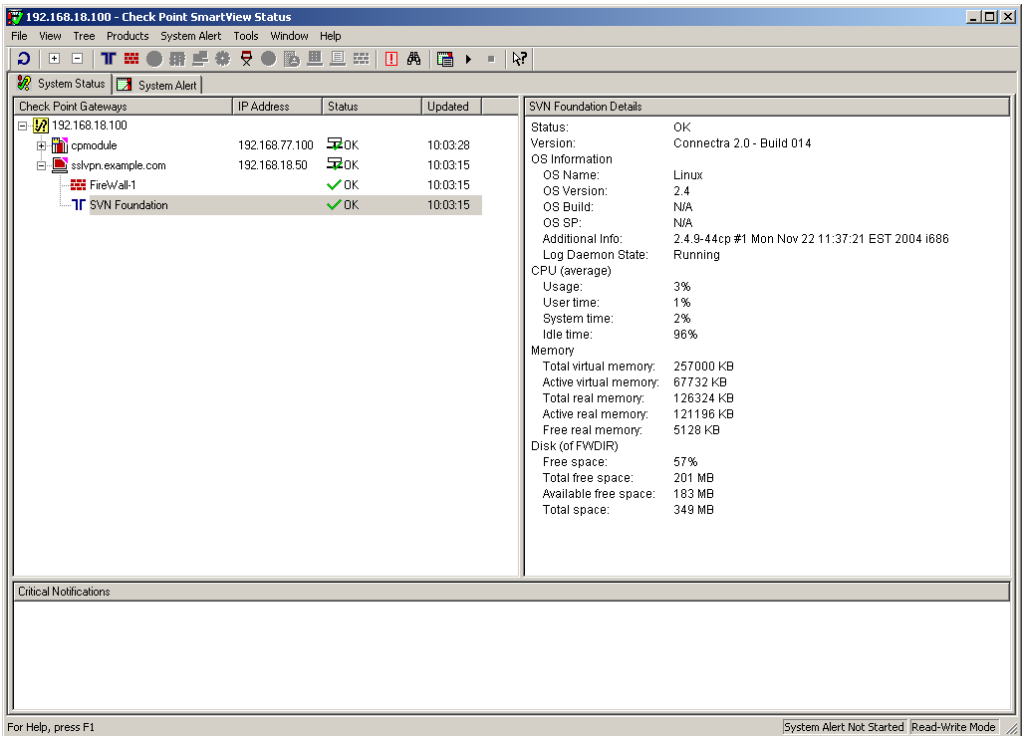
© 2005 CLICO Sp. z o.o. Wszelkie prawa zastrzeżone

Wszystkie logi, zarówno te związane z dostępem do zasobów, jak i audytem działań adminstracyjnych będą wysyłane do centralnego serwera logów.



Do późniejszej obróbki i korelacji logów może być użyty moduł SmartView Reporter lub inne narzędzie, certyfikowane w ramach aliansu OPSEC.

Status systemu Connectra można sprawdzić za pomocą oprogramowania SmartView Status. W ramach elementu *SVN Foundation* można sprawdzić takie parametry, jak dostępna pamięć, wolne miejsce na dysku, czy obciążenie procesora.



© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

Wykorzystanie certyfikatów generowanych przez ICA

Za pomocą Check Point ICA można wygenerować certyfikaty, które będą służyły zarówno do uwierzytelnienia portalu, jak i użytkowników. Aby wygenerować certyfikat dla portalu, należy we właściwościach obiektu Connectra w programie SmartDashboard zaznaczyć kwadracik VPN. Wtedy automatycznie zostanie wygenerowany certyfikat o nazwie *defaultCert*. Taki certyfikat należy następnie wyeksportować do formatu PKCS12. W tym celu należy zalogować się do systemu, na którym jest zainstalowany SmartCenter Server i z linii komend wydać polecenie:

vpn export_p12 -obj sslvpn.example.com -cert defaultCert -file sslvpn.cert -passwd abc123

Plik z wyeksportowanym certyfikatem należy przekopiować do komputera, na którym dostępne są narzędzia do obróbki plików kryptograficznych, na przykład ***openssl***. Z pliku PKCS12 należy wydobyć certyfikat i klucz prywatny. Za pomocą ***openssl*** wykonuje się to w sposób następujący:

[root@fedora1 root]# openssl pkcs12 -in sslvpn.cert -nocerts -out sslvpn_key.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase: ****
Verifying - Enter PEM pass phrase: ****
A[root@fedora1 root]# openssl pkcs12 -in sslvpn.cert -nokeys -out sslvpn_cert.pem
Enter Import Password: ****
MAC verified OK
[root@fedora1 root]#

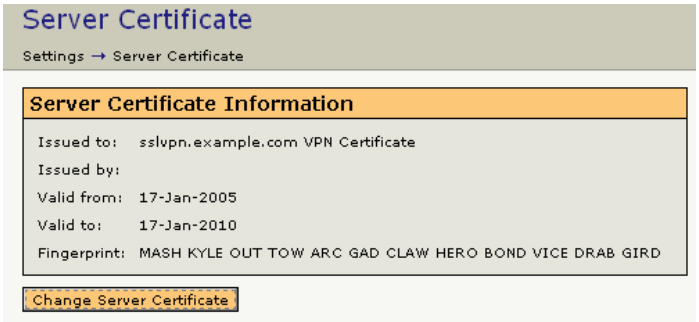
Następnie w pliku **sslvpn_cert.pem** należy usunąć pierwszy certyfikat (ICA), za pomocą na przykład edytora tekstowego. Plik z kluczem prywatnym **sslvpn_key.pem** oraz certyfikatem **sslvpn_cert.pem** należy przekopiować na komputer, gdzie jest zainstalowana przeglądarka do zarządzania portalem.

© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

Z menu należy wybrać *Settings -> Server Certificate*, a następnie *Change Server Certificate*.

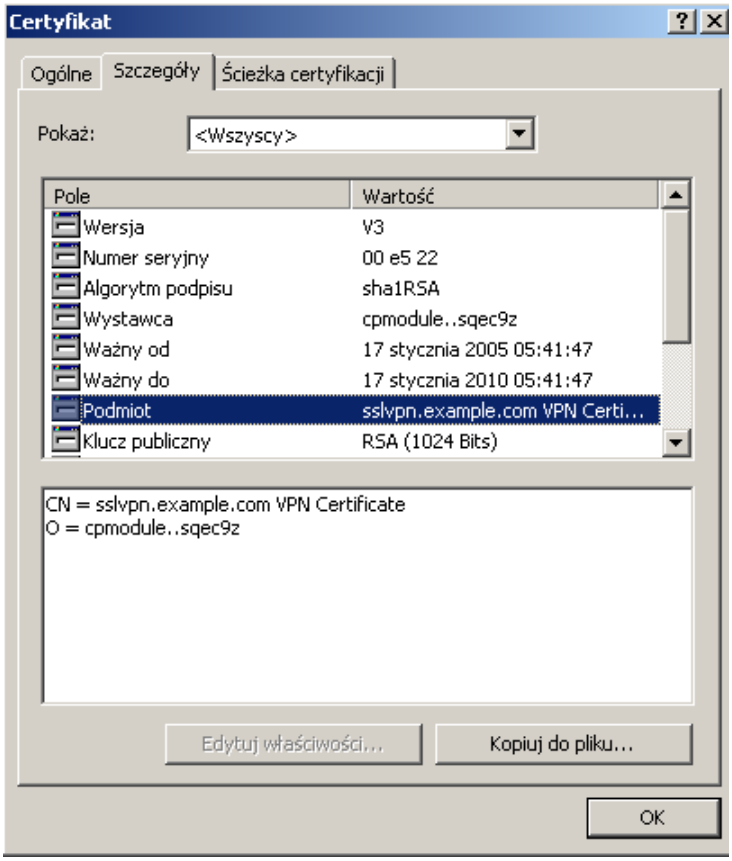
W następnym kroku należy podać lokalizację plików z certyfikatem i kluczem, oraz wprowadzić hasło, które było użyte przy wydobywaniu kluczy z pliku PKCS12.

Po prawidłowym zainstalowaniu system informuje o tym, wyświetlając aktualne dane dotyczące certyfikatu.



© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

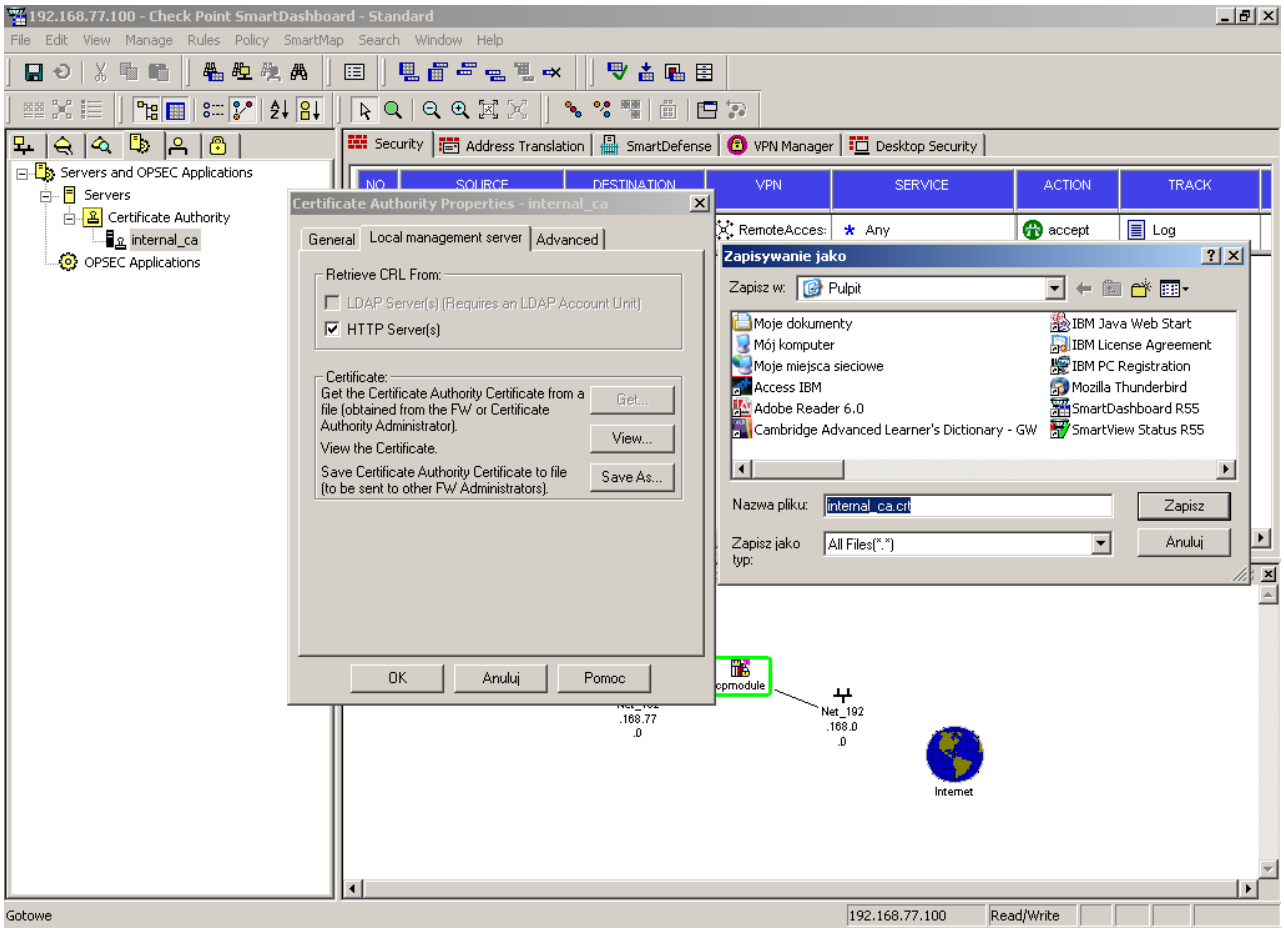
Portal przy logowaniu się do niego, będzie się przedstawiał nowym certyfikatem.



© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

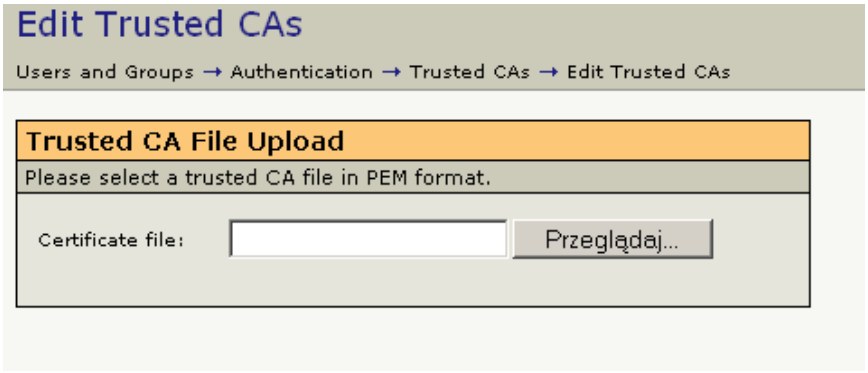
Uwierzytelnienie użytkowników za pomocą certyfikatów oraz kart inteligentnych

Użytkownicy, logując się do portalu mogą wykorzystywać certyfikaty cyfrowe, w celu potwierdzenia swojej tożsamości. Certyfikaty mogą być przechowywane w plikach, lub urządzeniach kryptograficznych (karty inteligentne, Security Chip-y). Aby uruchomić uwierzytelnianie w oparciu o certyfikaty potrzebny jest certyfikat urzędu, który będzie wystawiał certyfikaty dla użytkowników. Może to być dowolny system CA (wspierane są tylko te z aliansu OPSEC). W naszym przypadku będzie to ICA SmartCenter serwera. Certyfikat ICA można uzyskać przy pomocy SmartDashboard.

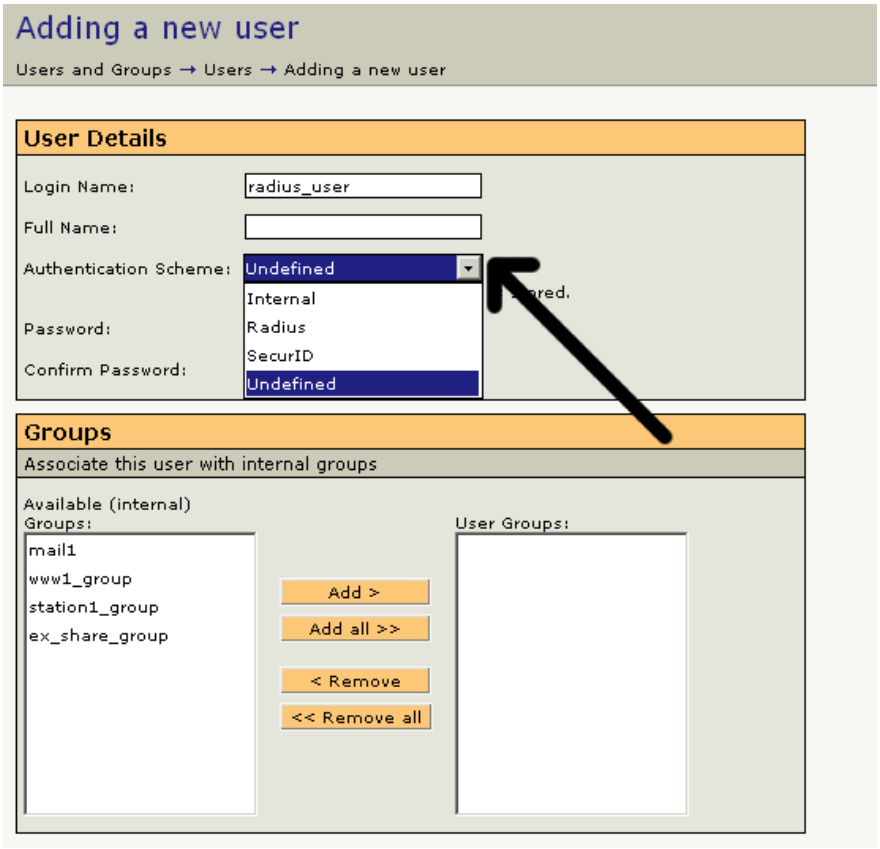


© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

Po zapisaniu certyfikatu do pliku należy go zaimportować za pomocą portalu administracyjnego do Connectry. W tym celu należy wybrać z menu ***Users and Groups*** -> ***Authentication*** -> ***Trusted CA***.

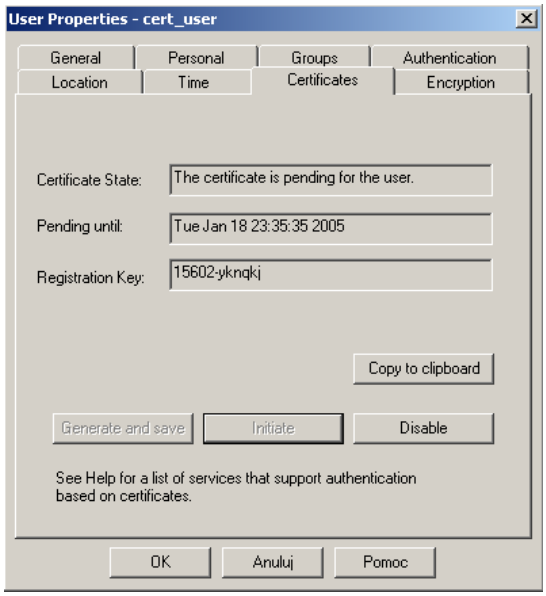


Po zainstalowaniu certyfikatu należy jeszcze zdefiniować użytkowników, którzy będą przedstawiać się certyfikatami cyfrowymi. Tacy użytkownicy powinni mieć wybrany schemat uwierzytelnienia ***Undefined***.

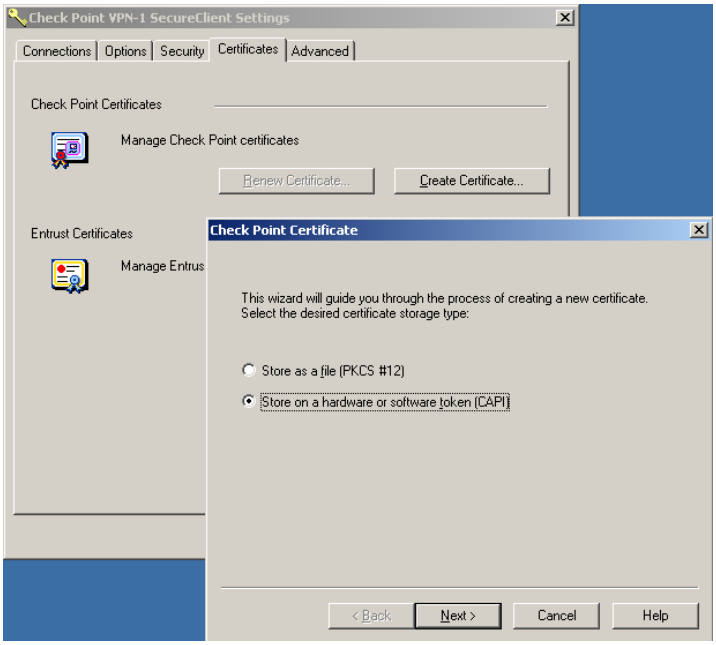


© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

W przypadku generowania certyfikatów z ICA dla użytkowników posługujących się kartami i oprogramowaniem ActivCard Gold, jedynym rozsądnym wyjściem jest użycie oprogramowania SecuRemote/SecureClient. W SmartDashboard preinicjalizuje się certyfikat dla konkretnego użytkownika, a następnie za pomocą SR/SC generuje certyfikat bezpośrednio na karcie.

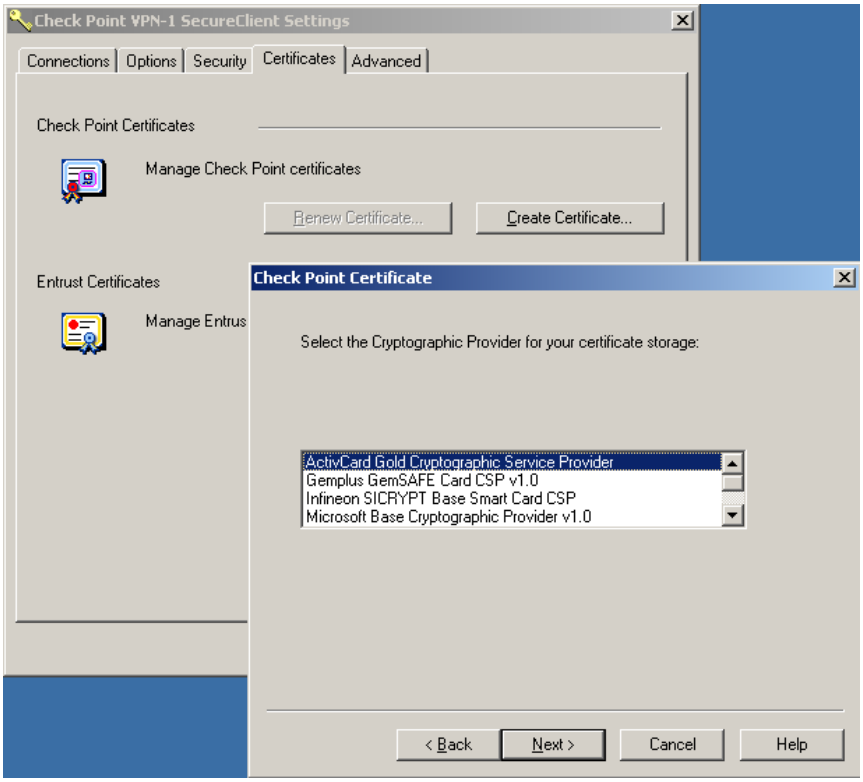


W tym celu w oprogramowaniu SR/SC wybiera się z menu ***Settings*** -> ***Certificates*** -> ***Checkpoint Certificates*** -> ***Create Certificate***

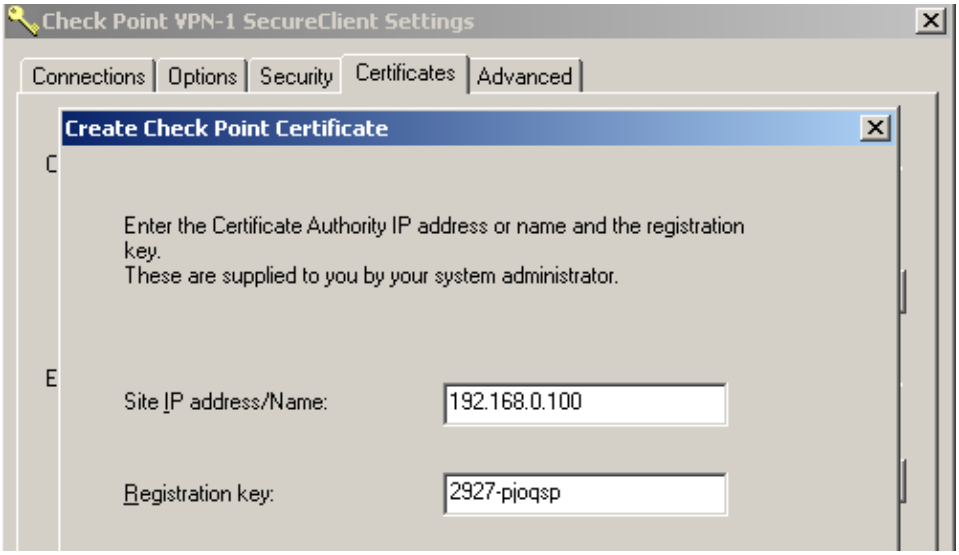


© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE

Certyfikat należy zapisać za pomocą CAPI, wybierając ActivCard Gold CSP.

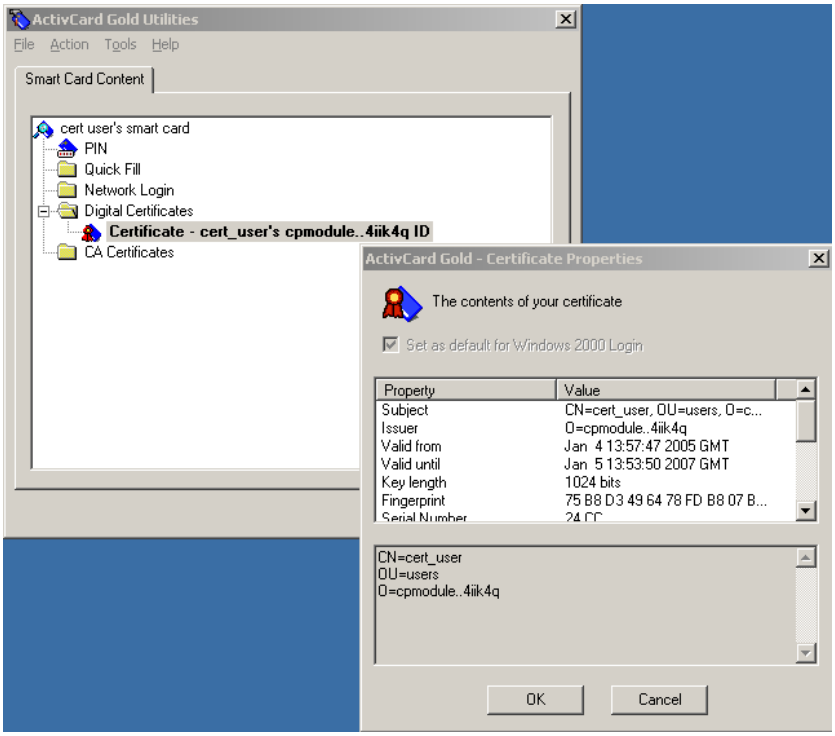


Następnie należy podać adres IP bramki VPN, na której został wygenerowany kod inicjujący certyfikat, oraz wpisać ten kod.

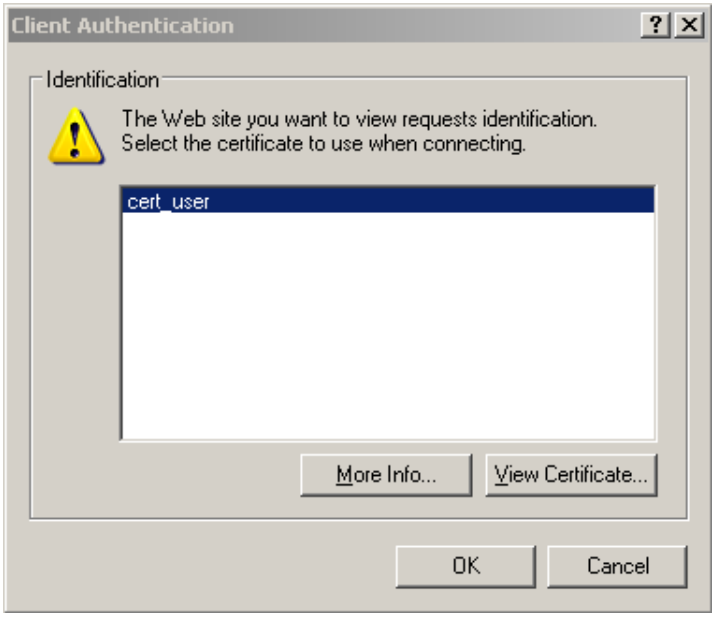


© 2005 CLICO Sp. z o.o. Wszelkie prawa zastrzeżone

Po kilku chwilach, potrzebnych do przeprowadzenia operacji kryptograficznych (generowanie kluczy, podpisy cyfrowe) na karcie zostanie umieszczony certyfikat.



W celu zalogowania się do portalu z użyciem certyfikatów, należy w opcjach logowania na stronie wybrać ***Certificate Sign In***, a następnie wybrać certyfikat z listy dostępnych.



Po podaniu PINu do karty sprawdzeniu poprawności certyfikatu użytkownik może rozpocząć pracę z portalem.

© 2005 CLICO SP. Z O.O. WSZELKIE PRAWA ZASTRZEŻONE