



Instrukcja instalacji certyfikatu VPN dla routera Cisco

Spis treści

Wstęp	2
Wymagania odnośnie wersji IOS dla routerów Cisco	2
Wstępna konfiguracja urządzenia Cisco Router	2
Generowanie pierwszej pary kluczy RSA (na potrzeby SSH).....	3
Generowanie kolejnej pary kluczy RSA (na potrzeby IKE-VPN).....	4
Instalacja certyfikatów Urzędów (CA) CC Signet i tworzenie wniosku o certyfikat	5
<i>Konfiguracja trustpoint'a dla głównego Urzędu - RootCA</i>	7
<i>Konfiguracja trustpoint'a dla pośredniego Urzędu PCA Klasa 2</i>	8
<i>Konfiguracja trustpoint'a dla końcowego Urzędu CA Klasa 2</i>	9
<i>Konfiguracja danych, które będą zawarte we wniosku o certyfikat</i>	10
Import certyfikatu Signet VPN do urządzenia.....	12
Zapisanie bieżącej konfiguracji routera	13

Wstęp

Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować router Cisco do zestawiania połączeń VPN z wykorzystaniem certyfikatów cyfrowych. Kolejne rozdziały pomogą Ci przejść przez wszystkie etapy generowania kluczy, tworzenia wniosku o certyfikat oraz instalacji certyfikatu. W efekcie będziesz mógł z łatwością zabezpieczyć swój router korzystając z certyfikatów wystawionych przez Centrum Certyfikacji Signet.

Wymagania odnośnie wersji IOS dla routerów Cisco

IOS powinien być z serii (feature set) **Advanced Security**

W przypadku konfigurowania wersji IOS za pomocą **Software Advisor** należy zaznaczyć przynajmniej następującą funkcjonalność (software features):

Certificate Enrollment Enhancements
Certificate Security Attribute-Based Access Control
Certification Authority Interoperability (CA)
IPSec Network Security

Powyższa funkcjonalność jest dostępna w niżej wymienionych wersjach IOS (minimum).

12.3T obecnie najnowszy z tej serii [Early Deployment] to 12.3(11)T2
12.3 obecnie najnowszy z tej serii [Limited Deployment] to 12.3(12)

Wstępna konfiguracja urządzenia Cisco Router

! Należy upewnić się, że router ma poprawnie ustawioną datę i godzinę, przed przystąpieniem do kolejnych czynności. Sugerujemy, aby urządzenie synchronizowało czas za pomocą protokołu NTP z wiarygodnym serwerem czasu (np. ntp.signet.pl).

! Do wygenerowania wniosku nie jest potrzebne bezpośrednie połączenie z Centrum Certyfikacji Signet. Cały proces odbywa się off-line.

! Import certyfikatów Urzędów oraz import certyfikatu dla urządzenia wymaga, aby router miał dostęp do listy certyfikatów unieważnionych (CRL).

1. Router powinien mieć poprawnie skonfigurowaną nazwę *hostname*. Nazwa ta znajdzie się we wniosku o certyfikat, a docelowo będzie zawarta w certyfikacie w polu CN jako pierwsza część nazwy domenowej.

```
router(config)# hostname cisco2600
```

- Router powinien mieć poprawnie skonfigurowaną nazwę domenową. Nazwa ta znajdzie się we wniosku o certyfikat, a docelowo będzie zawarta w certyfikacie w polu CN jako druga część nazwy domenowej.

```
cisco2600(config)# ip domain-name korporacja.pl
```

Taka konfiguracja spowoduje, że we wniosku o certyfikat w polu CN (Common Name) znajdzie się wartość cisco2600.korporacja.pl.

Generowanie pierwszej pary kluczy RSA (na potrzeby SSH)

Pierwsza para kluczy, którą wygenerujemy w routerze, będzie tylko na potrzeby SSH. Te same klucze nie powinny być wykorzystywane do IKE-VPN.

W kolejnym kroku wygenerujemy oddzielne klucze tylko na potrzeby IKE-VPN.

Klucze na potrzeby SSH nie powinny być usuwane z routera, nawet gdy SSH nie będzie wykorzystywany.

UWAGA: Usunięcie tej pary kluczy w przyszłości, może spowodować problemy podczas korzystania z innych kluczy (np. na potrzeby IKE-VPN).

Procedura wygląda następująco:

Po zalogowaniu się na urządzenie Cisco router i przejściu w tryb konfiguracji, wykonujemy poniższą komendę:

```
cisco2600(config)# crypto key generate rsa general-keys label ssh
```

Nazwa *ssh* w powyższej komendzie jest przykładowa i w docelowej konfiguracji może być dowolna.

Poniżej podajemy długość klucza 1024 bity.

```
The name for the keys will be: ssh
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys ...[OK]
```

Generowanie kolejnej pary kluczy RSA (na potrzeby IKE-VPN)

W pierwszym kroku wygenerujemy parę kluczy RSA. Klucz prywatny będzie przechowywany w urządzeniu i w przypadku fizycznej awarii urządzenia nie będzie możliwości jego odzyskania.

Teoretycznie istnieje możliwość wygenerowania kluczy z możliwością późniejszego wyeksportowania klucza prywatnego, ale włączenie tej opcji znacznie obniża bezpieczeństwo systemu. Zainteresowanych użytkowników odsyłamy do dokumentacji Cisco na stronę <http://www.cisco.com>.

Poniższy opis opisuje generowanie pary kluczy, **BEZ** możliwości eksportu klucza prywatnego z urządzenia i jest to jedyna konfiguracja zalecana przez Centrum Certyfikacji Signet.

Procedura wygląda następująco:

Po zalogowaniu się na urządzenie Cisco router i przejściu w tryb konfiguracji, wykonujemy poniższą komendę:

```
cisco2600(config)# crypto key generate rsa general-keys label Signet2005
```

Powyższa komenda generuje parę kluczy RSA i przyporządkowuje tym kluczom etykietę **Signet2005**. Należy zwrócić uwagę, żeby nazwa tej etykiety była identyczna z tą, którą podamy w późniejszej konfiguracji podczas edycji danych zawartych we wniosku (p. *Konfiguracja danych, które będą zawarte we wniosku o certyfikat*).

Po wykonaniu tej komendy router zwróci komunikat:

```
The name for the keys will be: Signet2005  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

Należy podać długość klucza - **1024**. Podanie innej długości klucza spowoduje, że wniosek o certyfikat zostanie odrzucony.

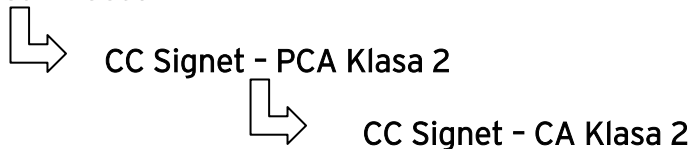
Po wybraniu długości klucza, pojawi się komunikat informujący o procesie generowania kluczy RSA:

```
% Generating 1024 bit RSA keys ...[OK]
```

Instalacja certyfikatów Urzędów (CA) CC Signet i tworzenie wniosku o certyfikat

Certyfikat dla VPN będzie wystawiony z Urzędu *CC Signet - CA Klasa 2*, który jest trzecim urzędem w hierarchii, która wygląda następująco:

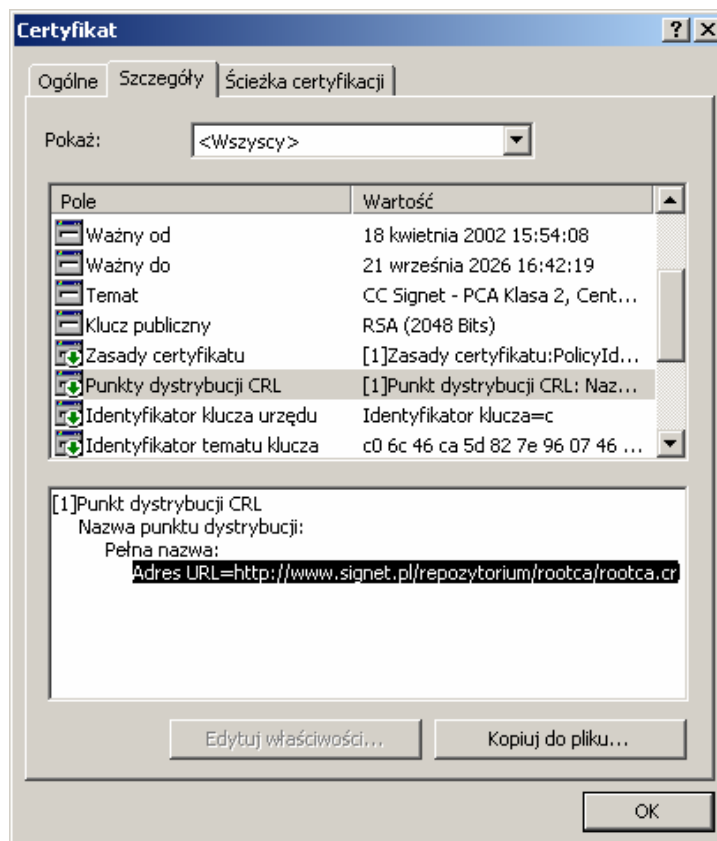
CC Signet - RootCA



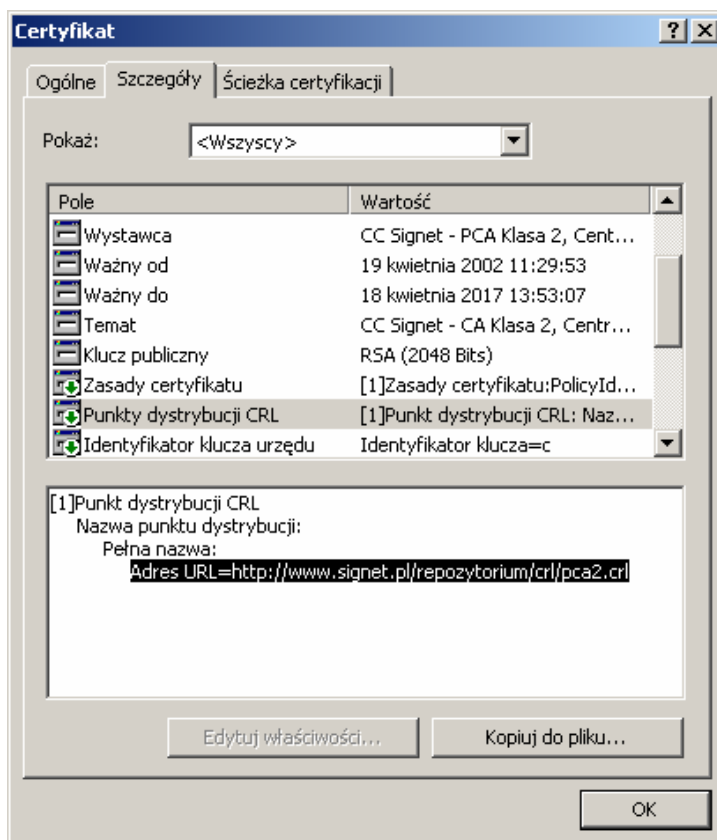
Warunkiem poprawnego funkcjonowania certyfikatu dla urządzenia jest zainstalowanie certyfikatów wszystkich urzędów w hierarchii. Poniżej znajduje się szczegółowy opis (krok po kroku), w jaki sposób poprawnie skonfigurować urządzenie.

W momencie instalowania certyfikatów Urzędów **PCA Klasa 2** i **CA Klasa 2** niezbędne jest, aby urządzenie posiadało dostęp do aktualnej listy certyfikatów unieważnionych (CRL).

Podczas importu certyfikatu urządzenie sprawdza pole **CDP** (Punkt dystrybucji CRL) w certyfikacie, które w przypadku Urzędu **PCA Klasa 2** wskazuje na URL o adresie <http://www.signet.pl/repozytorium/rootca/rootca.crl> i wygląda jak niżej.



W przypadku Urzędu CA Klasa 2 punkt CDP wskazuje na URL o adresie ***http://www.signet.pl/repozytorium/crl/pca2.crl***



Podczas importu tych certyfikatów urządzenie powinno mieć dostęp po protokole http do hosta www.signet.pl i konkretnych plików CRL jak zdefiniowano wyżej.

Jeżeli urządzenie nie ma bezpośredniego dostępu do Internetu i adres www.signet.pl jest nieosiągalny (np. gdy urządzenia są częścią prywatnej infrastruktury sieciowej odizolowanej od Internetu) należy zapewnić wewnątrz danej sieci dostęp do tych plików, z wykorzystaniem innych mechanizmów, jak np. serwer proxy lub wewnętrzny serwer WWW.

Taki serwer byłby odpowiedzialny za dystrybucję plików CRL wewnątrz prywatnej sieci.

W takim przypadku należy zapewnić odpowiednimi mechanizmami, zarówno replikację oryginalnych plików CRL bezpośrednio z repozytorium Centrum Certyfikacji Signet (www.signet.pl) i serwować te pliki wszystkim urządzeniom w prywatnej sieci, zachowując oryginalną strukturę katalogów, nazw plików jak również to, żeby urządzenia w przypadku połączenia z www.signet.pl nawiązywały faktycznie połączenie z wewnętrznym serwerem WWW (modyfikacja DNS lub hosts).

Jest to powszechnie stosowana praktyka i nie obniża ona poziomu bezpieczeństwa, gdyż lista certyfikatów unieważnionych (CRL) jest podpisana elektronicznie przez Urząd generujący taką listę i jakakolwiek nieautoryzowana modyfikacja CRL,

Konfiguracja danych, które będą zawarte we wniosku o certyfikat.

Wniosek o certyfikat zawiera klucz publiczny oraz dane opisowe urządzenia zawierające obowiązkowo przynajmniej:

1. **Adres IP urządzenia i/lub**
2. **Pełną nazwę domenową**

Jeżeli wniosek nie będzie zawierał żadnego z powyższych punktów, zostanie odrzucony jako błędny.

Wniosek powinien zawierać dane zgodnie z załączoną listą urządzeń. Wnioski, w których dane różnią się od podanych w dostarczonej liście, zostaną odrzucone jako błędne.

Adresem IP powinien być docelowy adres **IP interfejsu**, który będzie terminował kanał VPN (do którego będzie przypisana crypto map-a). Zamieszczenie adresu IP we wniosku (i docelowo w certyfikacie) jest opcjonalne. W większości przypadków wystarczy zdefiniowanie pełnej nazwy domenowej.

Pozostałe dane opisowe urządzenia, które mogą zostać zdefiniowane to:

CN (Common Name)
OU (Organizational Unit)
O (Organization)
C (Country)
E (Email)
i numer seryjny urządzenia.

Pole **CN** powinno zawierać pełną nazwę domenową (sugerowane) lub adres IP. Wpisanie innych wartości we wniosku do pola CN spowoduje odrzucenie wniosku jak błędny.

Pola **OU** i **O** powinny zawierać dane jednostki organizacyjnej i organizacji, która jest właścicielem urządzenia i która wnioskuje o certyfikat.

W polu **C (Country)** wymagany jest dwuliterowy kod kraju (PL).

W polu **E (Email)** powinien znaleźć się adres e-mail administratora urządzenia (osoby wnioskującej o certyfikat). Adres ten będzie weryfikowany podczas procesu rejestracji (generowania certyfikatu) i późniejszego odnowienia lub unieważnienia certyfikatu.

Wniosek o certyfikat zostanie automatycznie podpisany elektronicznie za pomocą wcześniej wygenerowanego klucza prywatnego, co jest gwarancją prawdziwości danych zawartych we wniosku.

Poniższa komenda konfiguruje dane, które będą zawarte we wniosku o certyfikat.

```
cisco2600(config)# crypto ca trustpoint Signet2005
cisco2600(ca-trustpoint)# subject-name CN=cisco2600.korporacja.pl,
OU=Dzial IT, O=Korporacja Sp. z o.o., C=PL, E=adminiator@korporacja.pl
cisco2600(ca-trustpoint)# usage ike
cisco2600(ca-trustpoint)# rsakeypair Signet2005 1024 1024
```

Uwaga! Nie używamy polskich znaków

Przykładowe użycie komendy **subject-name** spowoduje ustawienie następujących wartości do wniosku o certyfikat:

```
CN=cisco2600.korporacja.pl
OU=Dzial IT
O=Korporacja Sp. z o.o.
C=PL
E=adminiator@korporacja.pl
```

Pole **CN (Common Name)** powinno zawierać albo pełną nazwę domenową (p. Wstępna konfiguracja urządzenia), albo adres IP. W naszym przykładzie pole CN zawiera nazwę domenową, która znajdzie się w certyfikacie.

Uwaga! Pole CN może zawierać tylko pełną nazwę domenową, lub adres IP. Jeżeli we wniosku o certyfikat (PKCS#10) znajdzie się inna wartość niż adres IP lub nazwa domenowa, wniosek zostanie odrzucony.

Pole **OU (Organizational Unit)** powinno zawierać nazwę jednostki organizacyjnej w danej firmie, która będzie umieszczona w certyfikacie (np. Dział IT).

Pole **O (Organization)** powinno zawierać nazwę firmy (np. Korporacja Sp. z o.o.).

Pole **C (Country)** powinno zawierać dwuliterowy kod kraju. W przykładzie C=PL.

Pole **E (e-mail)** powinno zawierać adres e-mail administratora danego urządzenia. Adres e-mail będzie umieszczony w certyfikacie.

1. Jeżeli chcemy, aby w certyfikacie znajdował się adres IP urządzenia, wykonujemy dodatkowo następującą komendę

```
cisco2600(ca-trustpoint)# ip-address fastethernet0/0
```

Komenda **ip-address fastethernet0/0** spowoduje, że do wniosku o certyfikat zostanie dołączony adres IP interfejsu FastEthernet0/0. **Interfejs musi być poprawnie skonfigurowany i aktywny (up).**

Jeżeli kanał VPN będzie terminowany na innym interfejsie (np. FastEthernet0/1), komenda powinna wyglądać tak: **ip-address fastethernet0/1**

Użycie adresu IP w certyfikacie może spowodować ograniczenie funkcjonalności do jednego interfejsu.

Po skonfigurowaniu urządzenia jak w powyższym opisie, dajemy komendę **exit** (wychodząc z konfiguracji trustpointa).

```
cisco2600(ca-trustpoint)# exit  
cisco2600(config)#
```

Następnie wykonujemy komendę, która ostatecznie wygeneruje wniosek o certyfikat w formacie **PKCS#10**, z wcześniej skonfigurowanymi wartościami.

```
cisco2651(config)# crypto ca enroll Signet2005  
% Start certificate enrollment ..  
  
% The subject name in the certificate will include:  
CN=cisco2600.korporacja.pl,OU=Dzial IT,O=Korporacja Sp. z  
o.o.,C=PL,E=adminiator@korporacja.pl  
% The fully-qualified domain name in the certificate will be:  
cisco2600.korporacja.pl  
% The subject name in the certificate will include: cisco2600.korporacja.pl  
Display Certificate Request to terminal? [yes/no]: yes  
Certificate Request follows:  
  
MIICFzCCAYACAQAwbUxJjAkBgkqhkiG9w0BCQEF3NlYmFzdGhhbi5kc2F0d2FA  
dHBpLnBsmQswCQYDVQQGEwJQTDEOMAwGA1UEChMFMRmlybWExETAPBgNVBAsTCER6  
aWFsIElUMQ4wDAYDVQQDEwVDaXNjbzFLMA8GA1UEBRMIQjUwMDRDQUEwFwYJKoZI  
hvcNAQkIEwoxMC4zLjEuMjAwMB8GCSqGSIb3DQEJAhYSY2l2Y28yNjUxLmZpcmlh  
LnBsmIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8yAOQwA8YKCLCrKF9YhcI  
u+QHaRyNLWjmGPjqvL6jCT5s9DEBW4Ij90Sqw6r1A2RtLEPeQRvUL7bFYhWngkhf  
OmhtRRxjlimuyyp9oeD5Jl9dnhEpOY7ak6x2172KMxo0snufb/qKLWzgc2NzuIH  
JQjnIg8N80nWkoZ+ebK98wIDAQABOCEwHwYJKoZIhvcNAQkOMRIwEDAObgNVHQ8B  
Af8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEAM/mzCHiSP9Ksit6bHanOLAGRfUai  
VBlWGFg1MAG4/sMGP6d6Sp8t7MzJDN2Sr2kmev6V/MS9vFG1sWpKG2aPlptUmcUF  
ZgIsNtyej9CAyGEQ2h01xzBXOAJNirMO+EyEFbtD6spoOxCPsrVen3PKcbMmyKEZ  
m6QfT5R4tT6jric=  
  
---End - This line not part of the certificate request---  
  
Redisplay enrollment request? [yes/no]: no
```

Tak wygenerowany wniosek kopiujemy i zapisujemy do pliku tekstowego.

W ten sposób wygenerowany wniosek o certyfikat należy wkleić na stronie Centrum Certyfikacji Signet podczas procesu pozyskiwania certyfikatu dla VPN.

Ostatnim krokiem będzie import certyfikatu.

Import certyfikatu Signet VPN do urządzenia

Po uzyskaniu certyfikatu, ostatnim krokiem będzie jego instalacja w routerze.

W tym celu wykonujemy komendę:

```
cisco2600(config)# crypto ca import Signet2005 certificate
```

Po wykonaniu komendy pojawi się komunikat mówiący o tym, żeby wkleić certyfikat w formacie **base 64 (PEM)**.

```
% The fully-qualified domain name in the certificate will be:
cisco2600.korporacja.pl

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
```

Należy zwrócić uwagę, aby wkleić zawartość certyfikatu wraz z liniami

-----BEGIN CERTIFICATE----- oraz -----END CERTIFICATE----- ,

tak jak w przykładzie poniżej:

```
-----BEGIN CERTIFICATE-----
MIIFsDCCBJigAwIBAgIKF1O+TAAAAAANjANBgkqhkiG9w0BAQUFADBjMRMwEQYK
CZImiZPyLQGGRYDbGFuMRQwEgYKcZImiZPyLQGBGRYEc3dpcjEcmBoGA1UEAxMT
V2luZG93cyAyMDAzIFNlcnZlcjAeFw0wNDEyMjExNDQ3MDdaFw0wNjE5MjExNDQ3
MDDaMGgxChAJBgNVBAYTA1BMMQ4wDAYDVQQKEWVGAxJtYTERMA8GA1UECxMIRHpp
YWwgSVQxZDjAMBgNVBAMTBUNpc2NvMSYwJAYJKoZIhvcNAQkBFhdzZWJhc3RpdjY4
ZlJhdHdhQHRwaS5wBDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAvmGdKMAP
GCGiwyhfwIXCLVkb2kcjS1o5hj46ry+owk+bPQxAVuCI/dEqluq9QNkbSxD3kEb
6ii8GYHNjc7iByUI5yIPdfNjlpKGfnmyvfMCAwEAaOCav0wggL5MAsGA1UdDwQE
AwIFoDAdBgNVHQ4EFgQUdTw4DxJJC7wtSI8XmFxmNMZVdVlIwHwYDVR0jBBgwFoAU
2D/HnzBNqSptYcM6ctwKArT1h1IwggEZBgNVHR8EggEQMIIBDDCCAQigggEEoIIB
AIAvGxkYXA6Ly8vQ049V2luZG93cyUyMDIwMDMlMjBTZXJ2ZXIsQ049ZGVsbC1z
ZWIsQ049Q0RQLENOPVB1YmxpYyUyMETleSUyMFNlcnZpY2VzLENOPVN1cnZpY2Vz
LENOPUNvbmZpZ3VyYXRpb24sREM9c3dpcixEQz1sYW4/Y2VydG1maWNhdGVsZXZv
Y2F0aW9uTG1zdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50
hj9odHRwOi8vZGVsbC1zZWluc3dpcjE5sYW4vQ2VydEVucm9sbC9XaW5kb3dzJTlw
MjAwMyUyMFNlcnZlcjE5jcmwggEnBggrBgEFBQcBAQSCARKwggEVMIGzBggrBgEF
BQcwAoaBpmxkYXA6Ly8vQ049V2luZG93cyUyMDIwMDMlMjBTZXJ2ZXIsQ049QU1B
LENOPVB1YmxpYyUyMETleSUyMFNlcnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZp
Z3VyYXRpb24sREM9c3dpcixEQz1sYW4/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVj
dENsYXNzPWNlcnRpb25BdXRpb25BdXRpb25BdXRpb25BdXRpb25BdXRpb25BdXRpb25
Ly9kZWxsLXNlYi5zd2lyLmXhbi9DZXJ0RW5yb2xsL2RlbGwgc2ViLnN3aXIubGFu
X1dpbmRvd3MlMjAyMDAzJTiwU2VydMvYmNydDA/BgkrBgEAYI3FAIEMh4wAEKA
UABTAEUQAQWBJAG4AdABLAHIAbQBLAQQAaQBhAHQAZQBPAZAgBsAgkAbgBlMAwG
A1UdEwEB/wQCMAAwEwYDVR01BAwwCgYIKwYBBQUIAgIwDQYJKoZIhvcNAQEFBQAD
ggEBAEkG3zwM1DCMvvy6Ydu+pWSHSXBeyT3TNaFb6ZSbAkVEg4qoxSgMV8A2Ra
XqSEReHtBAULq/85Fvmom8Xzfv9/uYmE9cpkYrNuwlwpOFy79Neg9lrkEqQfWRV
NvHpsnSgHayzH/CAUD33liPuQytDSSeyDXDpXNtZ8Zph201tle3mMYn8g7Kknmt
SIqW3BRX8OgvsQhLPhQe8RqQ2W+W+P4QNHiv7XgR7fbHrmS+1KQhnANSCT18XtEj
5kz6M6QHJfKHDSkYNMKfY0euRJ779XNFmjU0+fSAFbf0HKtQwpvxcm8RRP7GrPMc
MQguTXVJkw90Xg2HkQEicqsF0dg=
-----END CERTIFICATE-----
```

Uwaga! Nie należy wklejać powyższego przykładu!

Zapisanie bieżącej konfiguracji routera

Ostatnim krokiem będzie zapisanie bieżącej konfiguracji i restart routera.

Konfigurację zapisujemy komendą **wr mem** (jak poniżej):

```
cisco2600# wr mem
Building configuration...

Feb 16 11:50:35.064: %SYS-5-CONFIG_I: Configured from console by console[OK]
```