ASA IKEv2 RA VPN con clientes VPN de Windows 7 o Android y configuración de autenticación de certificados

Contenido

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) versión 9.7.1 y posteriores para permitir que los clientes VPN nativos de Windows 7 y Android (red privada virtual) establezcan una conexión VPN RA (acceso remoto) con el uso de Internet Key Exchange Protocol (IKEv2) y Certificates como método de autenticación.

Colaboración de David Rivera y Cesar Lopez Zamarripa, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autoridad de certificación (CA)
- Public Key Infrastructure (PKI)
- VPN RA con IKEv2 en ASA
- Cliente VPN incorporado de Windows 7
- Cliente VPN nativo de Android

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CISCO1921/K9 - 15.5(3)M4a como servidor IOS CA
- ASA5506X - 9.7(1) como cabecera VPN
- Windows 7 como equipo cliente
- Galaxy J5 - Android 6.0.1 como cliente móvil

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Overview

Estos son los pasos para configurar los clientes VPN nativos de Windows 7 y Android para conectarse a una cabecera ASA:

Configurar autoridad de certificados

La CA permite incrustar el uso de clave extendida (EKU) requerido en el certificado. Para la cabecera ASA, se requiere certificado Server Auth EKU, mientras que el certificado del cliente necesita Client Auth EKU.

Se puede utilizar una variedad de servidores CA, como:

- servidor CA de Cisco IOS
- servidor OpenSSL CA
- servidor CA de Microsoft
- 3rd CA de parte

El servidor de CA del IOS se utiliza para este ejemplo de configuración.

Esta sección describe la configuración básica para que un CISCO1921/K9 con la versión 15.5(3)M4a funcione como servidor de CA.

Paso 1. Asegúrese de que el dispositivo y la versión sean compatibles con el comando eku.

```
IOS-CA# show run | section crypto pki
crypto pki server <CA_Server>
  issuer-name <cn=calo_root,ou=TAC,o=cisco>
  grant auto
  eku server-auth client-auth
```

Paso 2. Habilite el servidor HTTP en el router.

```
IOS-CA(config)#ip http server
```

Paso 3. Genere un par de claves RSA exportable.

```
IOS-CA(config)# crypto key generate rsa modulus 2048 label <HeadEnd> exportable
The name for the keys will be: HeadEnd
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds)
```

Paso 4. Configure un punto de confianza.

```
IOS-CA(config)# crypto pki trustpoint <HeadEnd>
IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
IOS-CA(ca-trustpoint)#subject-name <cn=HeadEnd.david.com>
IOS-CA(ca-trustpoint)#revocation-check none
IOS-CA(ca-trustpoint)#rsakeypair <HeadEnd>
```

> **Nota:** La dirección IP para el comando enrollment es una de las direcciones IP configuradas del router para una interfaz accesible.

Paso 5. Autentique el punto de confianza (Obtener el certificado de CA).

```
IOS-CA(config)#crypto pki authenticate <HeadEnd>
Certificate has the following attributes:
       Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
      Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Paso 6. Inscriba el punto de confianza (obtenga el certificado de identidad).

```
IOS-CA(config)#crypto pki enroll <HeadEnd>
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco123
Re-enter password: cisco123
% The subject name in the certificate will include: cn=HeadEnd.david.com
% The subject name in the certificate will include: Connected_2_INET-B
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose HeadEnd' command will show the fingerprint.
*Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 0017C310 9F6084E8
63053228 B449794F
*Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: CFE22C7A B2855C4D
B4B2412B 57FC7106 1C5E7791
*Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Paso 7. Verifique los certificados.

```
IOS-CA#show crypto pki certificates verbose <HeadEnd>
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 05
  Certificate Usage: General Purpose
```

```
  Issuer:
    cn=calo_root
  Subject:
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
    cn=HeadEnd.david.com
  Validity Date:
    start date: 16:56:14 UTC Jul 16 2017
    end   date: 16:56:14 UTC Jul 16 2018
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 0017C310 9F6084E8 63053228 B449794F
  Fingerprint SHA1: CFE22C7A B2855C4D B4B2412B 57FC7106 1C5E7791
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: E9B3A080 779A76E7 8BE44F38 C3E4DEDF 18E75009
    X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
   Authority Info Access:
    Extended Key Usage:
        Client Auth
        Server Auth
  Associated Trustpoints: HeadEnd
  Key Label: HeadEnd

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=calo_root
  Subject:
    cn=calo_root
  Validity Date:
    start date: 13:24:35 UTC Jul 13 2017
    end   date: 13:24:35 UTC Jul 12 2020
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
  Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
    Authority Info Access:
  Associated Trustpoints: test HeadEnd CA_Server
```

Paso 8. Exporte el punto de confianza de HeadEnd al terminal en formato PKCS12 para obtener el certificado de identidad. El certificado de CA y la clave privada se agregan en un solo archivo.

```
IOS-CA(config)#crypto pki export
```

<cisco123>
Exported pkcs12 follows:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH
BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz
Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB
3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj
v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV
ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu
niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3
vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz
EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+
Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2
bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F
bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam
RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b
eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg
VbYsR+51XfQEH5xu88E5EUPWZ86YdUSlbD8ky6WOn0M1O4K6rNDLkgwXcxw3CaZ8
zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8
C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc
+OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN
Ua0MbDEa8T5Le4dCigaA+t1QxQOPGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O
lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw
9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h
9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC
77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2
zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7LOlCeUcVDM8aQfy
HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X
2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE
RE6m7O8RiPSD2RjjamCmmmnH5dK5wxF7YlIeK/+ZVrfwLecEPRl+eVw0isM/JN/a
WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs
yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR
4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhGO88voq8MMGXEe/q+DIjaVE1htYu
k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWXlXfgrfLEH0utwHTyr3J2vQk5CD37
ZAfsF6zxEvtU2t41J0e9OjWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y
BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg
ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm9OBsqd12lHurCCmHy7kM5pqf0MMlhH7
oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR
QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX1l
BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte
ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt
xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w
S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+
ik6bmxcnO0qdcHtt2HTbI+kYpken3YrFOh9Jnm9ZKT63gQSqQWL800ZVd4dAZceg
FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd
XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn
ISSzQjrkxoNwwOfn87O5fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy
FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/
Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ
jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9
TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp
3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn
cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir
pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX
AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp
kuauRzQ8/pwszaZuPh/5rE77z8zMut3+OE5CslB9npzNi0b0itaaRl13bBBml1xn
r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG
ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR
B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id
zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr
ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv
cJRb68aOyZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSFlM89Sn4

```
GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo
5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z
LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F
I8Ii8TA9MCEwCQYFKw4DAhoFAAQUjO/On/REYODupznP9SwYnFX92BYEFESx1MSa
ho3Cv1cZYM0TzZEzlsKdAgIEAA==
---End - This line not part of the pkcs12---

CRYPTO_PKI: Exported PKCS12 file successfully.
*Jul 17 15:46:49.706: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported.
```

Paso 9. Cree un punto de confianza vacío en el ASA.

```
ASA(config)# crypto ca trustpoint <HeadEnd>
DRIVERAP(config-ca-trustpoint)# exit
```

Paso 10. Importe el archivo PKCS12.

```
ASA(config)#crypto ca import <HeadEnd> pkcs12 <cisco123>
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEgguGMIILgjCCC34GCSqGSIb3DQEH
BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz
Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB
3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj
v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV
ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu
niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3
vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz
EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+
Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2
bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F
bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam
RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b
eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg
VbYsR+51XfQEH5xu88E5EUPWZ86YdUSlbD8ky6WOn0M1O4K6rNDLkgwXcxw3CaZ8
zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8
C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc
+OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN
Ua0MbDEa8T5Le4dCigaA+t1QxQOPGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O
lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw
9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h
9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC
77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2
zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7LOlCeUcVDM8aQfy
HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X
2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE
RE6m7O8RiPSD2RjjamCmmmnH5dK5wxF7YlIeK/+ZVrfwLecEPRl+eVw0isM/JN/a
WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs
yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR
4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhGO88voq8MMGXEe/q+DIjaVE1htYu
k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWXlXfgrfLEH0utwHTyr3J2vQk5CD37
ZAfsF6zxEvtU2t41J0e9OjWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y
BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAi1rYDqyIjhgdme56tVV0Vg
ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm9OBsqd12lHurCCmHy7kM5pqf0MMlhH7
oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR
QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX1l
BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte
ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt
xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w
S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royTOuYm0d+
ik6bmxcnO0qdcHtt2HTbI+kYpken3YrFOh9Jnm9ZKT63gQSqQWL800ZVd4dAZceg
FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9gnMgMJmikP2ghgOAd
```

```
XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn
ISSzQjrkxoNwwOfn87O5fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy
FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/
Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ
jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9
TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp
3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZS0SjsLmn
cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir
pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX
AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp
kuauRzQ8/pwszaZuPh/5rE77z8zMut3+OE5CslB9npzNi0b0itaaRl13bBBml1xn
r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG
ecside21F6CcWO5ywABBxDYQXM1P9qkC/2bkPkEJ0jBI5P5L1+Yqb8hTlone/InR
B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id
zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr
ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv
cJRb68aOyZvVBU0yoLbox84QKLHIsA92pplS7VFrAWP65wrhs4XOf4YSFlM89Sn4
GD/yEsGVJzwGrxgCNnOZkLIKsFbIOjp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo
5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z
LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F
I8Ii8TA9MCEwCQYFKw4DAhoFAAQUjO/On/REYODupznP9SwYnFX92BYEFESx1MSa
ho3Cv1cZYM0TzZEzlsKdAgIEAA==
quit
INFO: Import PKCS12 operation completed successfully
```

Paso 11. Verifique la información del certificado.

```
ASA(config)#show crypto ca certificates <HeadEnd>
CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: MD5 with RSA Encryption
  Issuer Name:
    cn=calo_root
  Subject Name:
    cn=calo_root
  Validity Date:
    start date: 13:24:35 UTC Jul 13 2017
    end   date: 13:24:35 UTC Jul 12 2020
  Storage: config
  Associated Trustpoints: test HeadEnd
Certificate
  Status: Available
  Certificate Serial Number: 05
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=calo_root
  Subject Name:
    hostname=Connected_2_INET-B
    cn=HeadEnd.david.com
  Validity Date:
    start date: 16:56:14 UTC Jul 16 2017
    end   date: 16:56:14 UTC Jul 16 2018
  Storage: config
  Associated Trustpoints: HeadEnd
```

Generar un certificado de cliente

Paso 1. Genere un par de claves RSA exportable.

```
IOS-CA(config)# crypto key generate rsa modulus 2048 label <Win7_PC> exportable
The name for the keys will be: Win7_PC
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 5 seconds
```

Paso 2. Configure un punto de confianza.

```
IOS-CA(config)# crypto pki trustpoint <Win7_PC>
IOS-CA(ca-trustpoint)#enrollment url http://10.201.180.230:80
IOS-CA(ca-trustpoint)#subject-name <cn=Win7_PC.david.com>
IOS-CA(ca-trustpoint)#revocation-check none
IOS-CA(ca-trustpoint)#rsakeypair <Win7_PC>
```

Paso 3. Autentique el punto de confianza configurado (Obtener el certificado de CA).

```
IOS-CA(config)#crypto pki authenticate <Win7_PC>
Certificate has the following attributes:
       Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
      Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

Paso 4. Inscriba el punto de confianza autenticado (obtenga el certificado de identidad).

```
IOS-CA(config)#crypto pki enroll <Win7_PC>
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco123
Re-enter password: cisco123
% The subject name in the certificate will include: cn=Win7_PC.david.com
% The subject name in the certificate will include: Connected_2_INET-B
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Win7_PC' command will show the fingerprint.
*Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 9153E537 11C16FAE
B03F7A38 775DBB92
*Jul 17 15:21:11.343: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 3BC4AC98 91067707
BB6BBBFB ABD97796 F7FB3DD1
*Jul 17 15:21:15.675: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Paso 5. Verifique la información de los certificados.

```
IOS-CA#show crypto pki certificates verbose <Win7_PC>
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 03
  Certificate Usage: General Purpose
  Issuer:
    cn=calo_root
  Subject:
    Name: Connected_2_INET-B
    hostname=Connected_2_INET-B
```

```
    cn=Win7_PC.david.com
  Validity Date:
    start date: 13:29:51 UTC Jul 13 2017
    end   date: 13:29:51 UTC Jul 13 2018
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 9153E537 11C16FAE B03F7A38 775DBB92
  Fingerprint SHA1: 3BC4AC98 91067707 BB6BBBFB ABD97796 F7FB3DD1
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: F37266AE 61F64BD9 3E9FA80C 77455F21 5BEB870D
    X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
    Authority Info Access:
    Extended Key Usage:
        Client Auth
        Server Auth
  Associated Trustpoints: Win7_PC
  Key Label: Win7_PC
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=calo_root
  Subject:
    cn=calo_root
  Validity Date:
    start date: 13:24:35 UTC Jul 13 2017
    end   date: 13:24:35 UTC Jul 12 2020
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: DA4502F4 CEFB4F08 AAA3179B 70019185
  Fingerprint SHA1: A887F6DB 0656C7E2 857749F3 EA3D7176 8920F52F
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: B5EEEEB9 31B9A06C CBD9893C 0E318810 5CA657E6
    Authority Info Access:
  Associated Trustpoints: test HeadEnd Win7_PC CA_Server
```

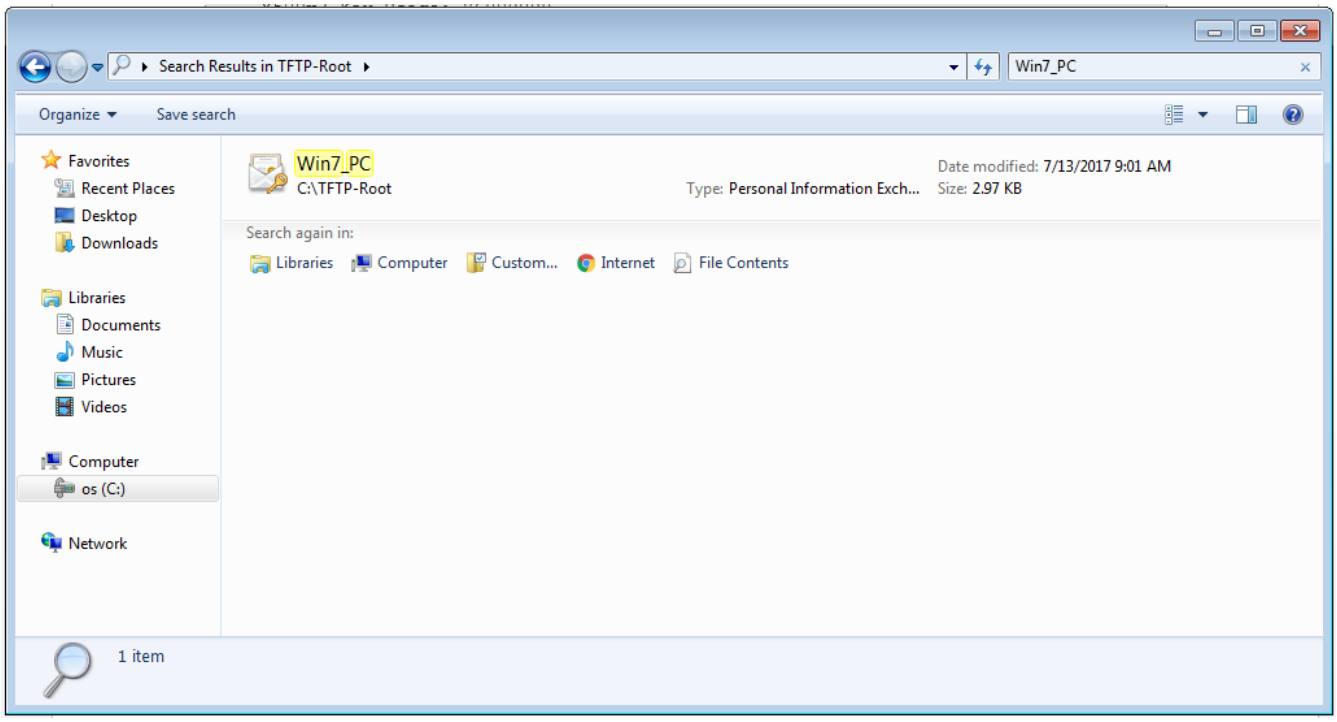
Instalación del certificado de identidad en el equipo cliente de Windows 7

Paso 1. Exporte el punto de confianza Win7_PC con nombre a un servidor FTP/TFTP (instalado en su equipo Windows 7) en formato PKCS12 (.p12) para obtener el certificado de identidad, el certificado CA y la clave privada en un solo archivo.

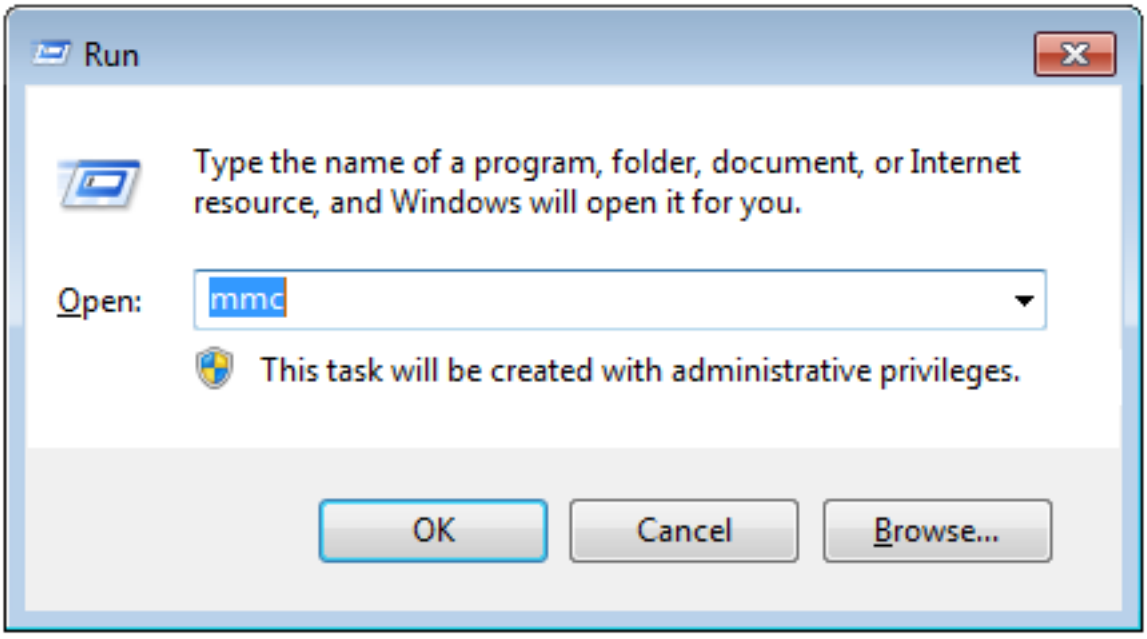
```
IOS-CA(config)#crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password
<cisco123>
Address or name of remote host [10.152.206.175]?
Destination filename [Win7_PC.p12]?
```

```
!Writing pkcs12 file to tftp://10.152.206.175/Win7_PC.p12
!
CRYPTO_PKI: Exported PKCS12 file successfully.
*Jul 17 16:29:20.310: %PKI-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully Exported.
```

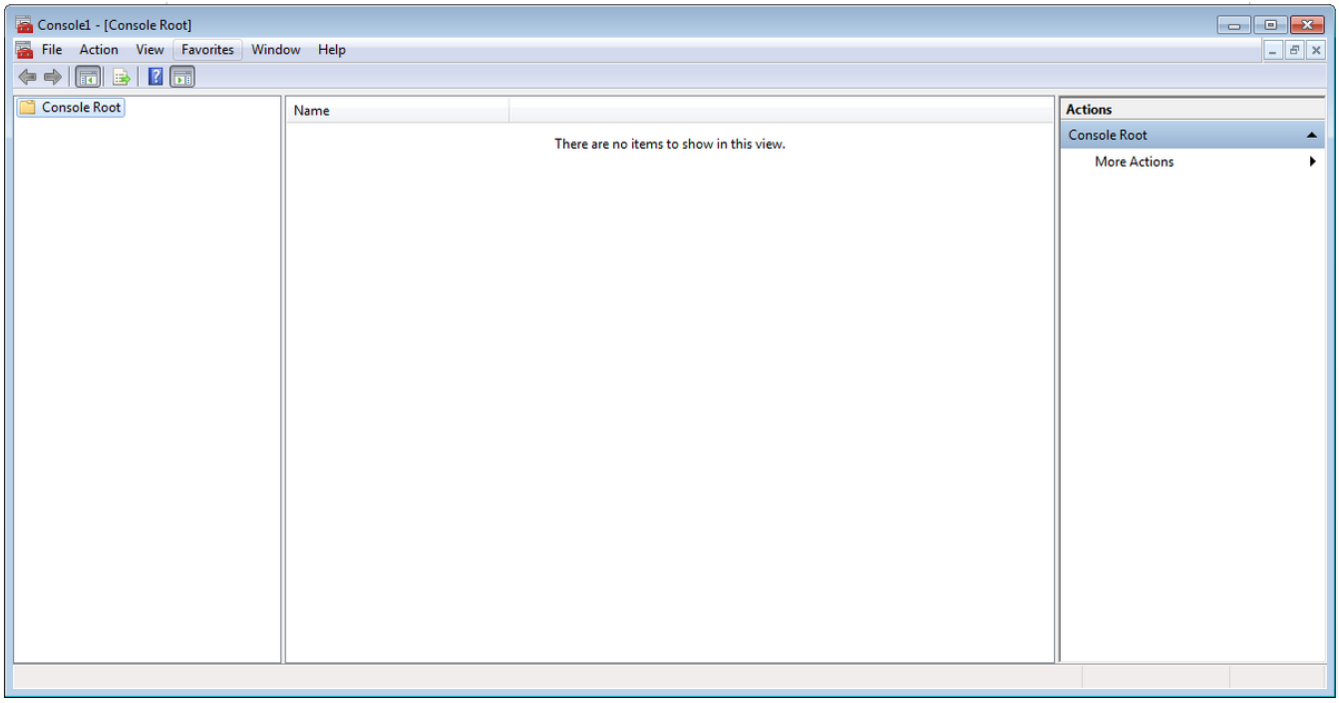
Así es como se ve el archivo exportado en un equipo cliente.



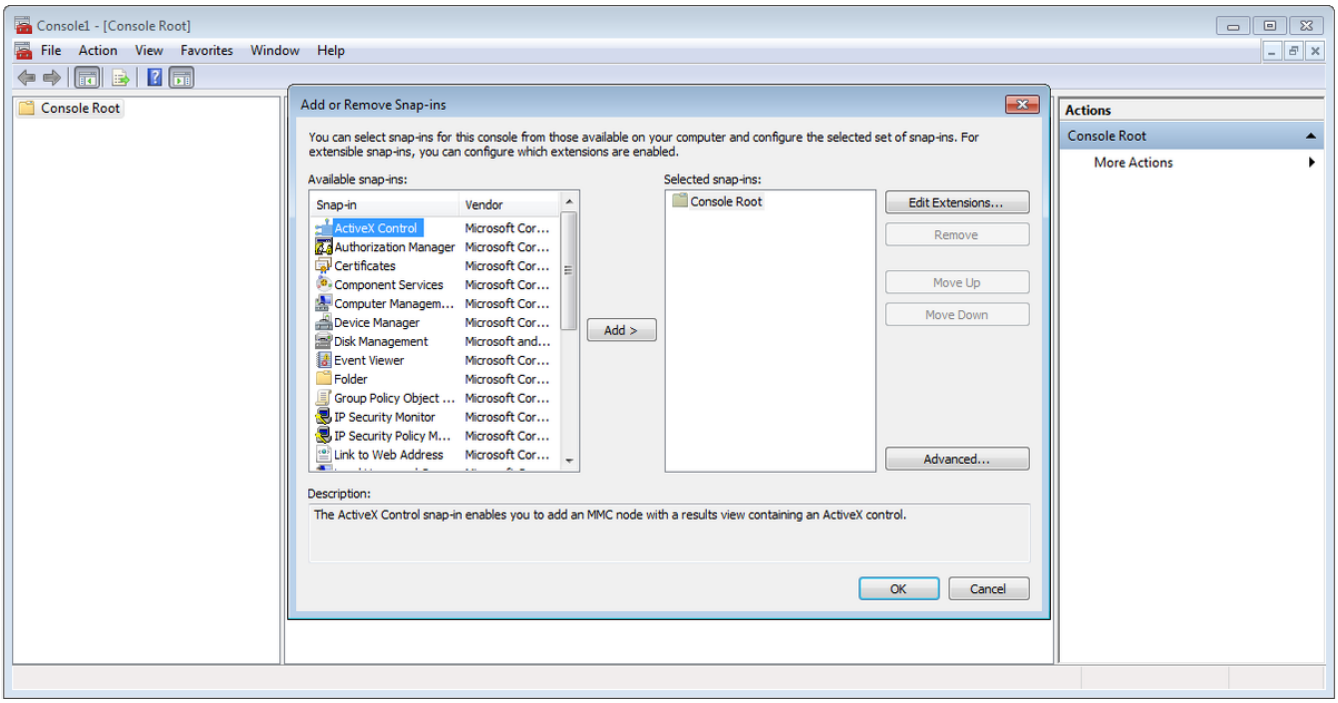
Paso 2. Presione **Ctrl + R** y escriba **mmc** para abrir Microsoft Management Console (MMC).



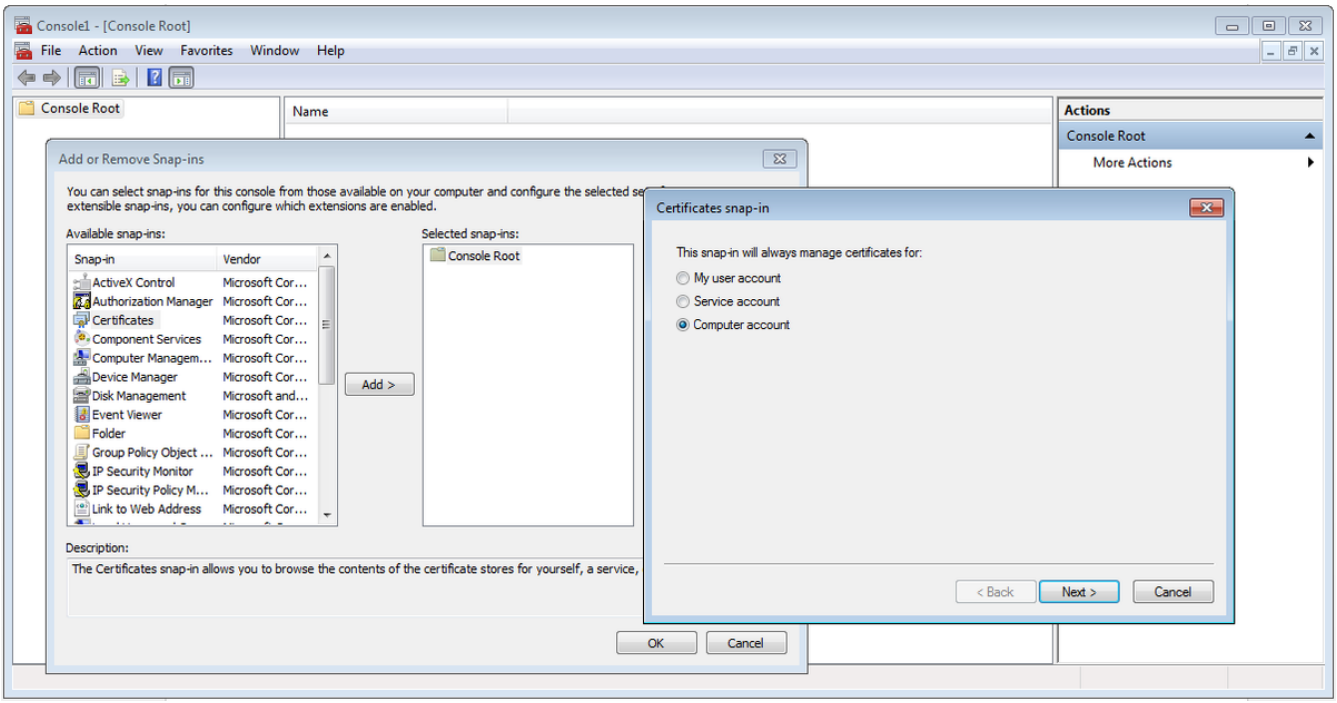
Paso 3. Seleccione **OK**.



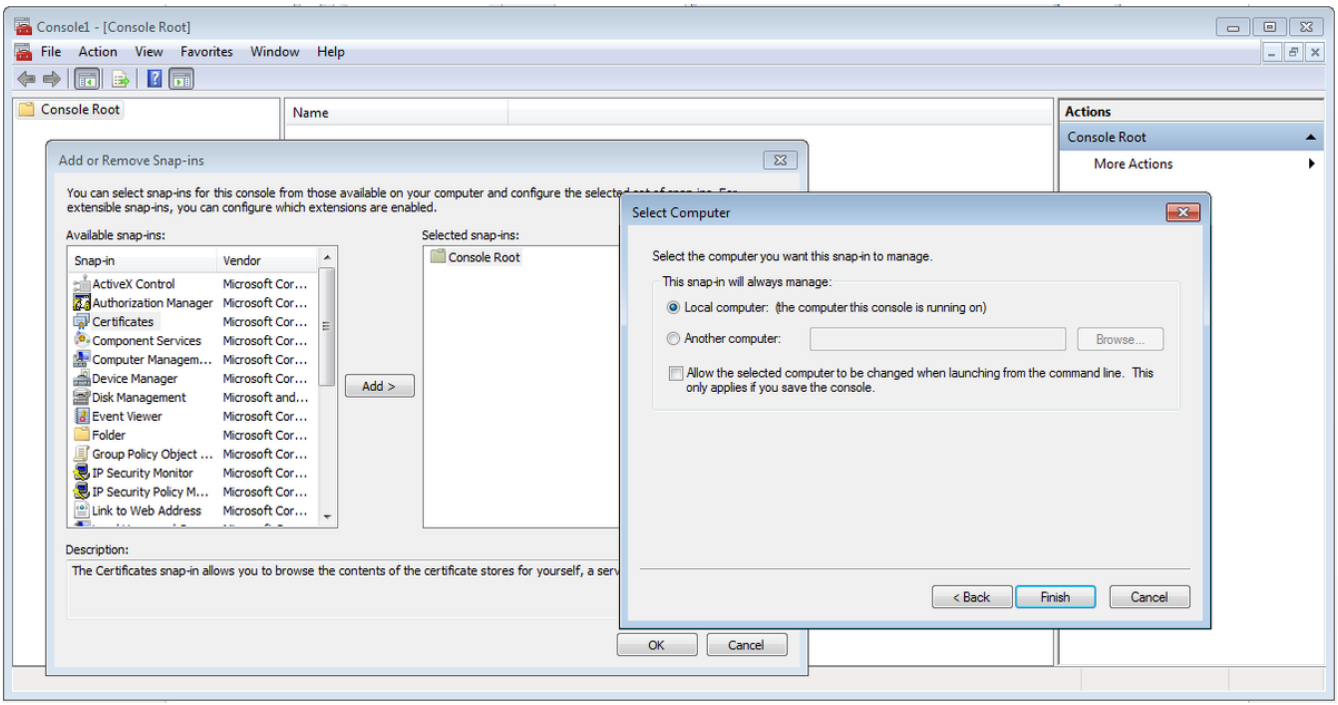
Paso 4. Vaya a **Archivo>Agregar o quitar complemento**.



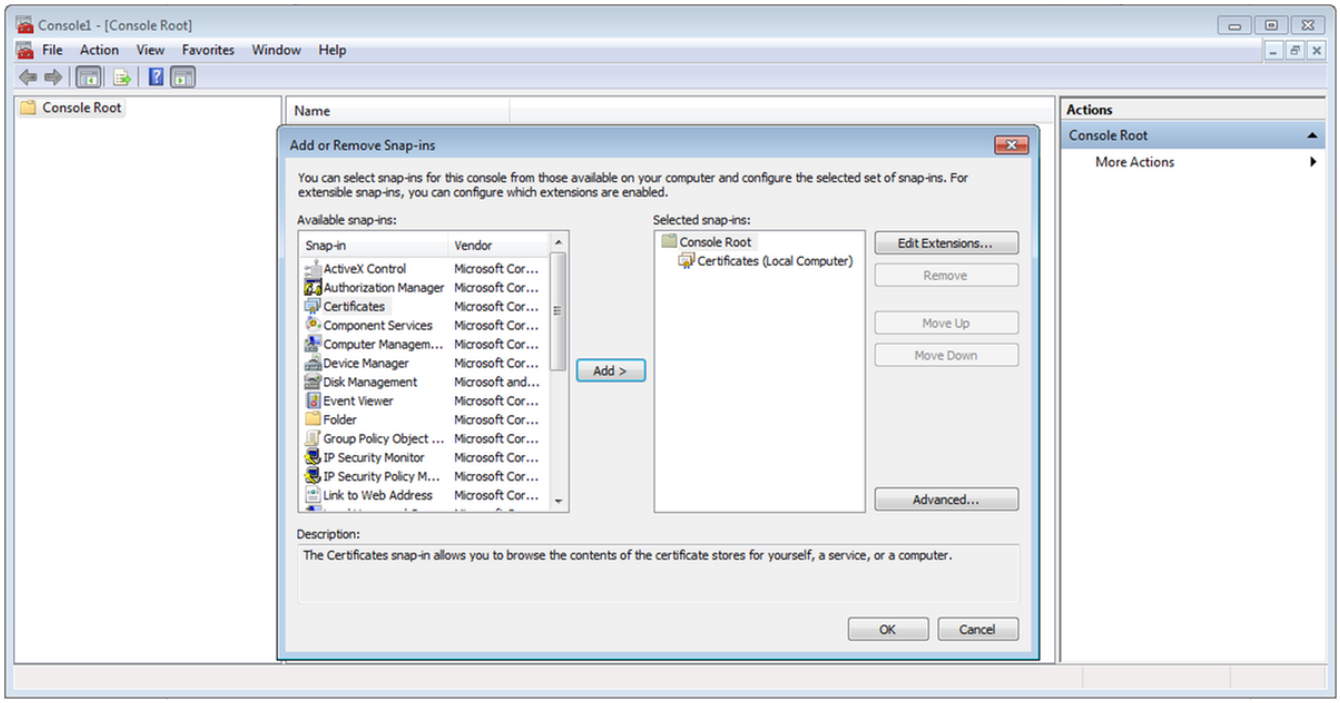
Paso 5. Seleccione **Certificados > Add > Computer Account**.



Paso 6. Seleccione **Siguiente**,

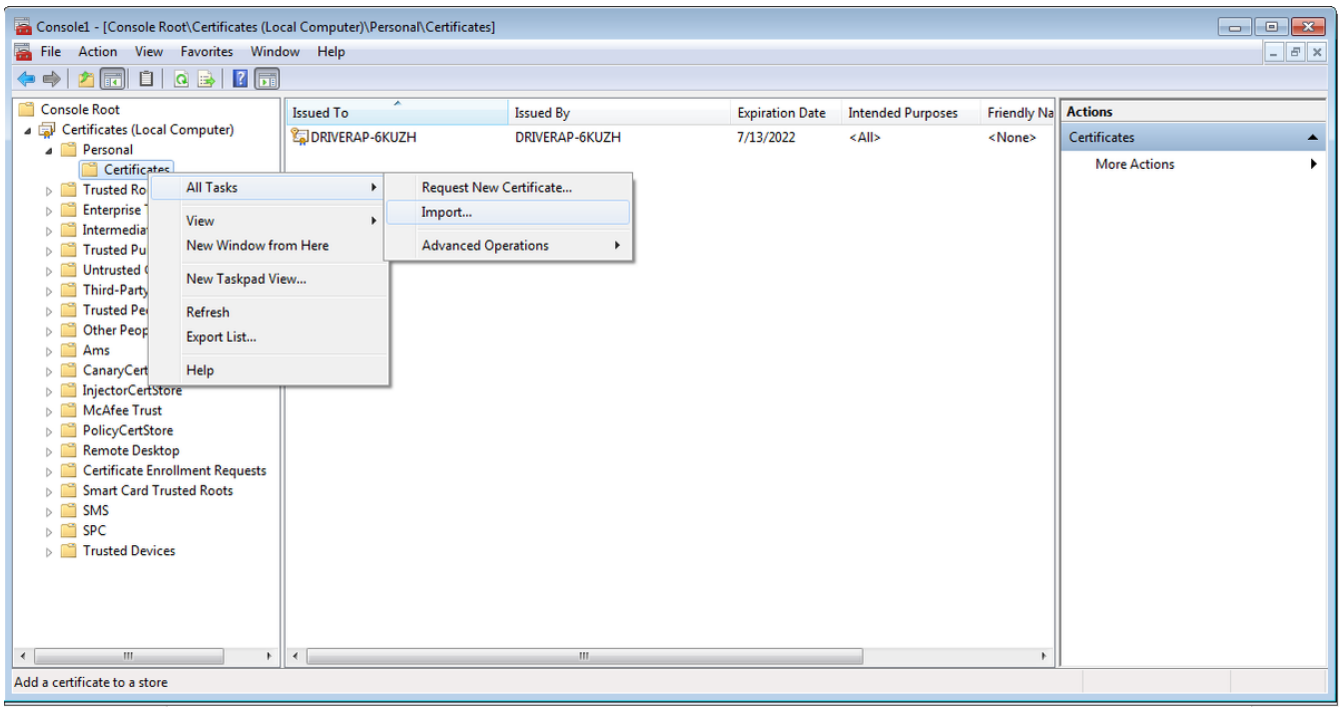


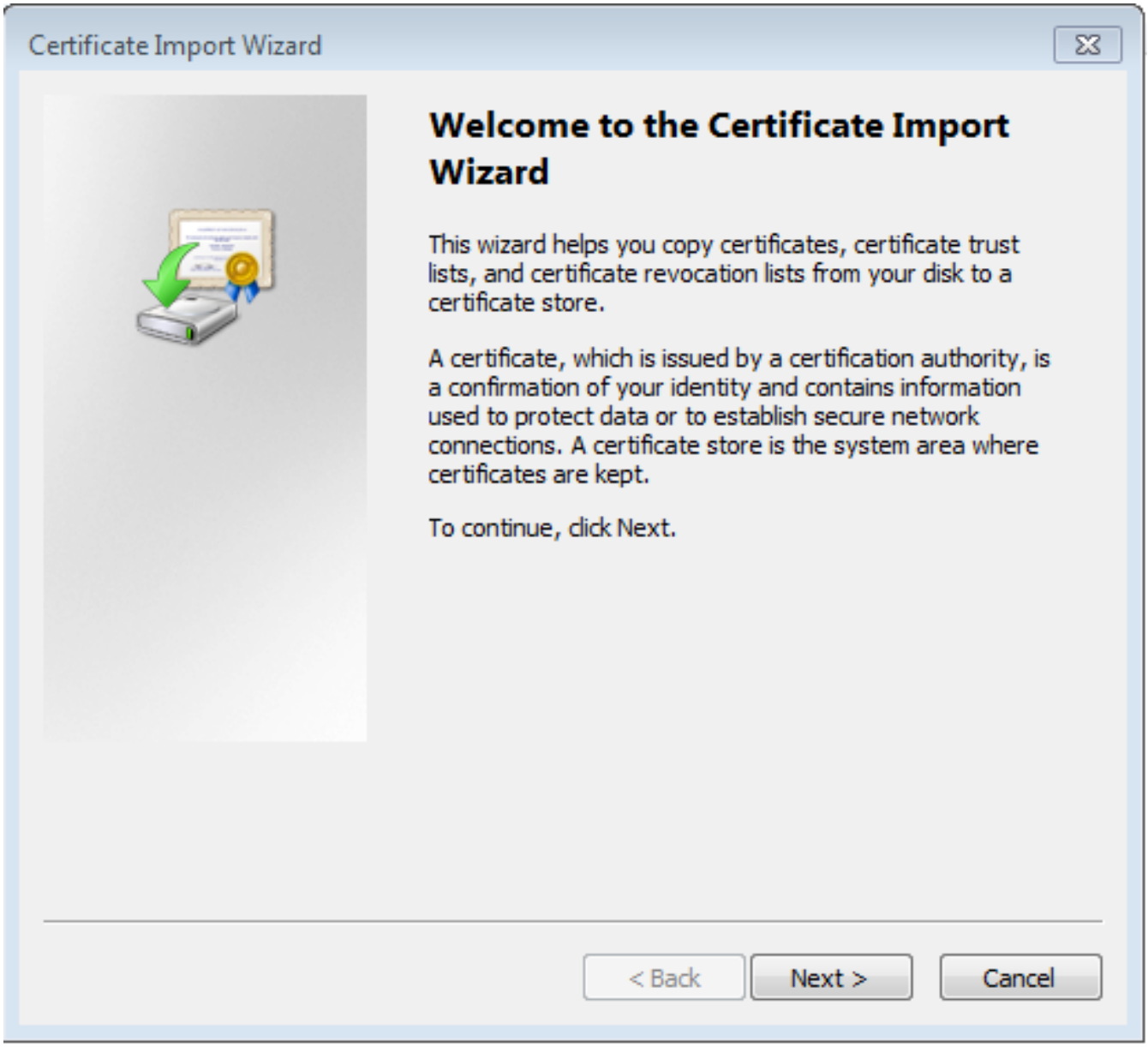
Paso 7. **Terminen**.



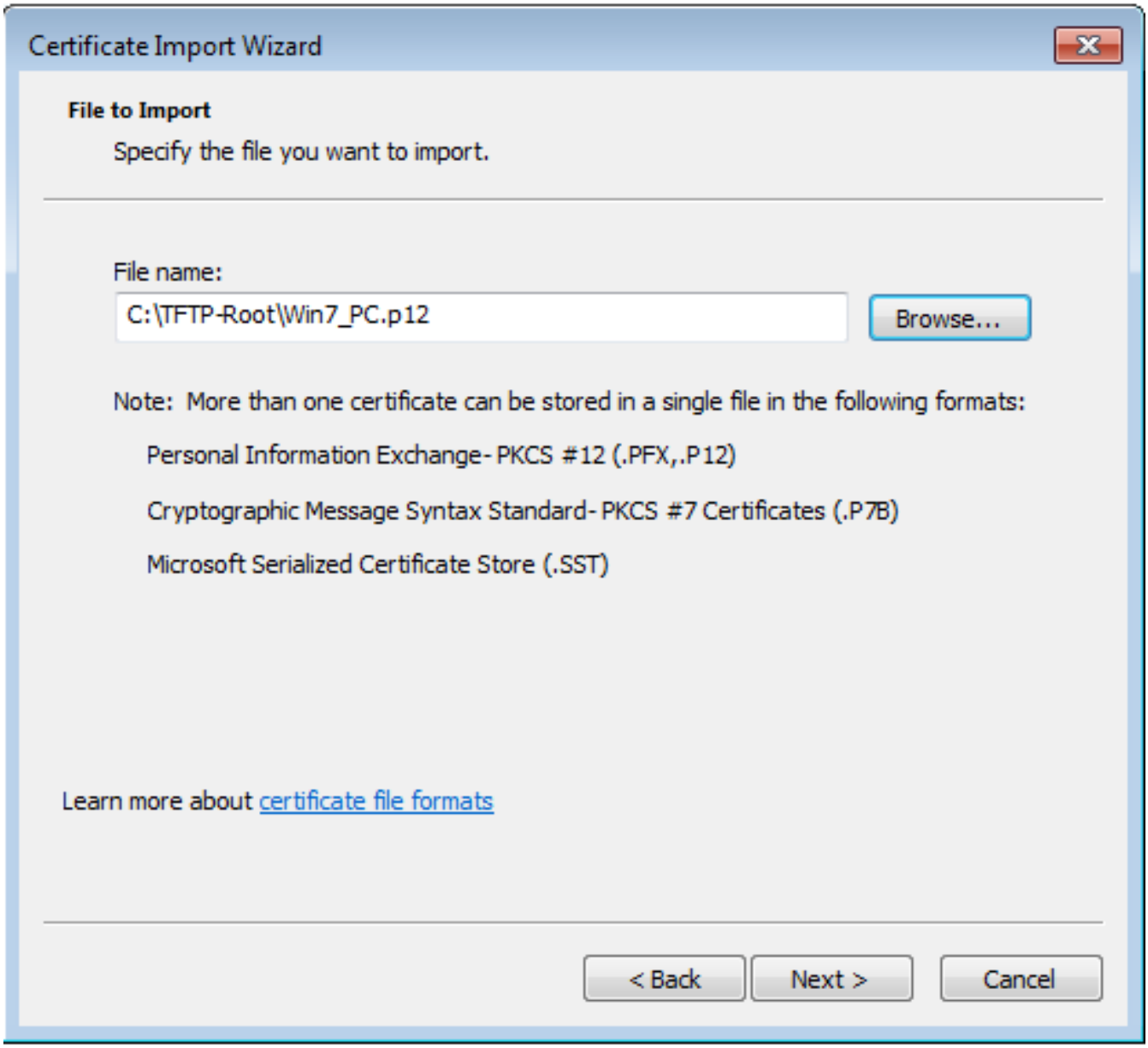
Paso 8. Seleccione **OK**.

Paso 9. Vaya a **Certificados (equipo local)>Personal>Certificados**, haga clic con el botón derecho del ratón en la carpeta y navegue hasta **Todas las tareas>Importar**:

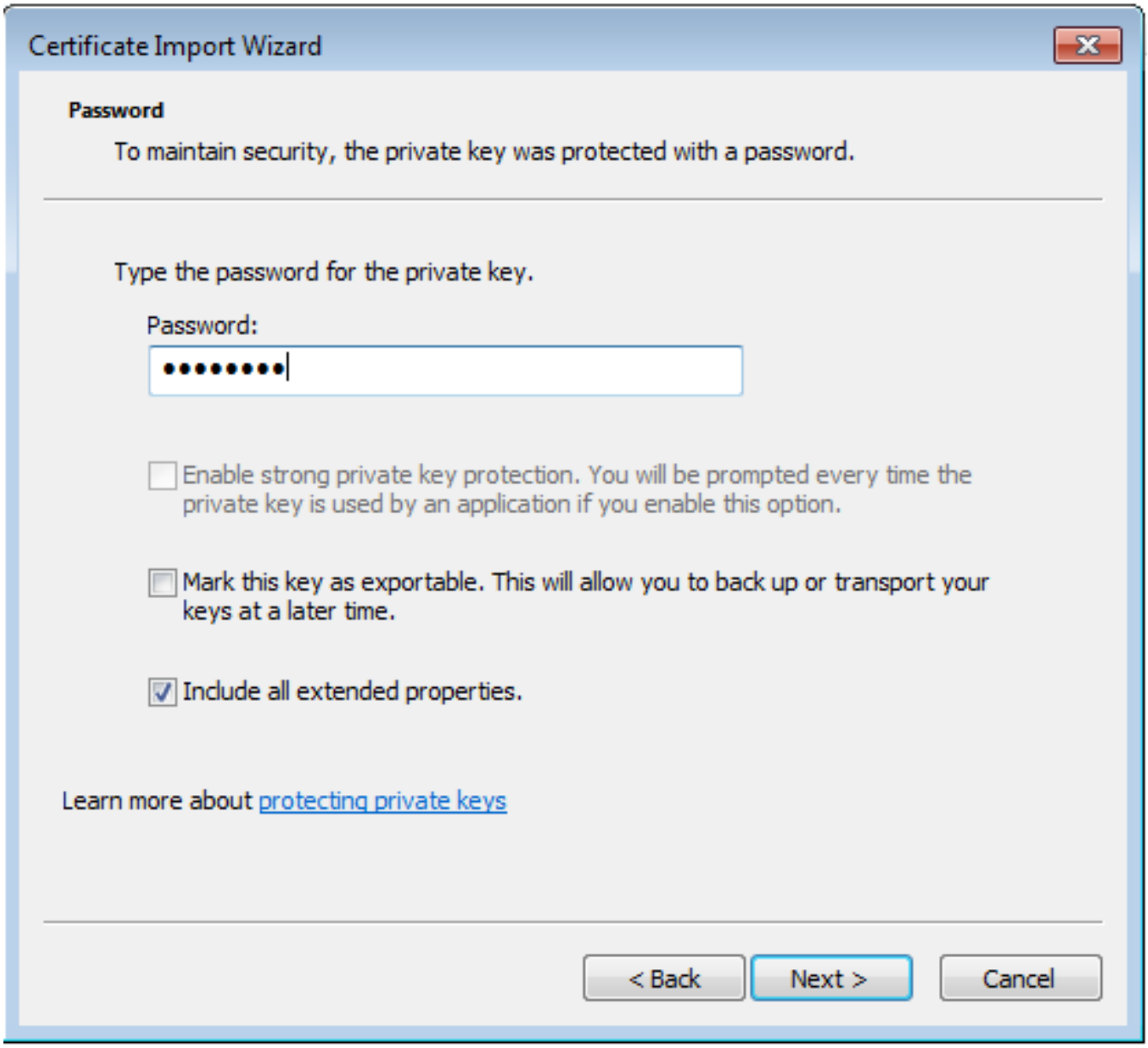




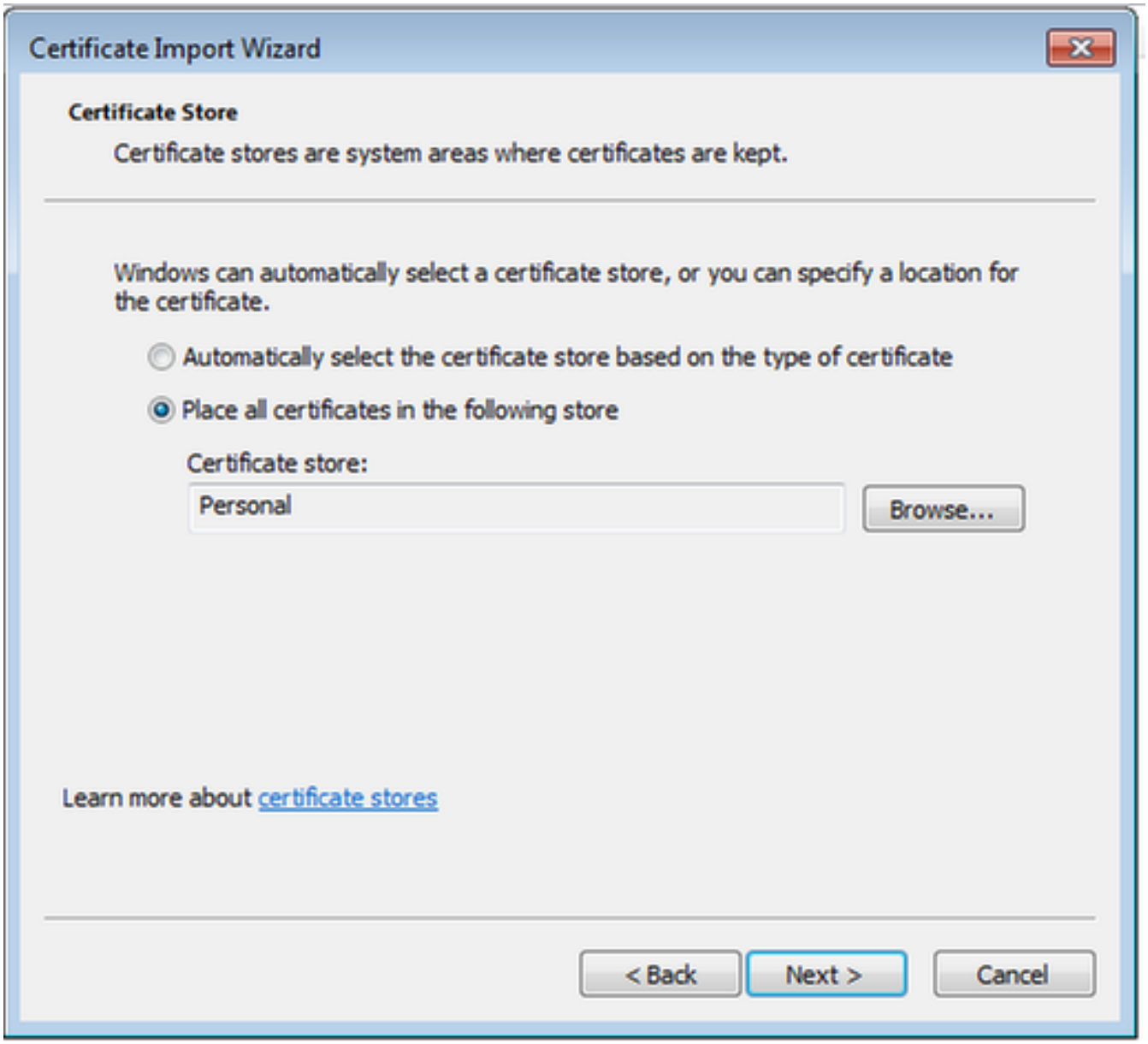
Paso 10. Haga clic en Next (Siguiente). Indique la ruta de acceso donde se almacena el archivo PKCS12.



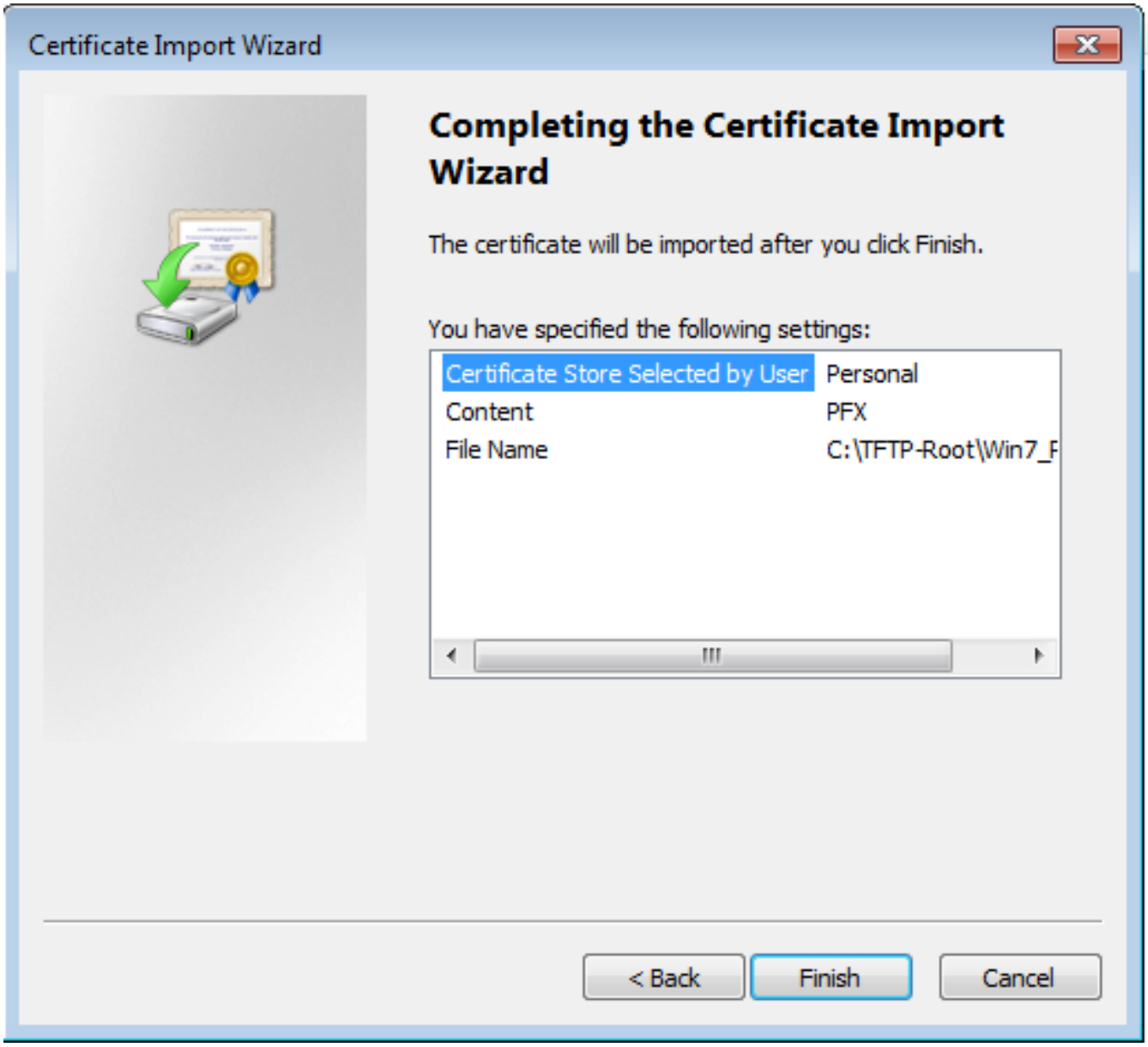
Paso 11. Seleccione **Next** nuevamente y escriba la contraseña ingresada en el comando *crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>*



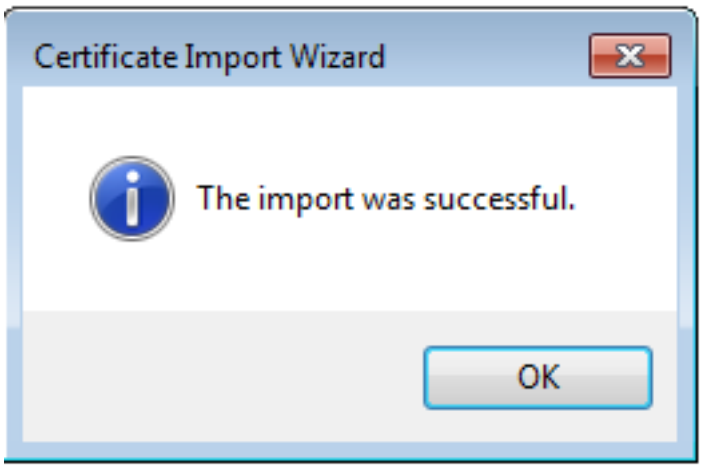
Paso 12. Seleccione **Next**.



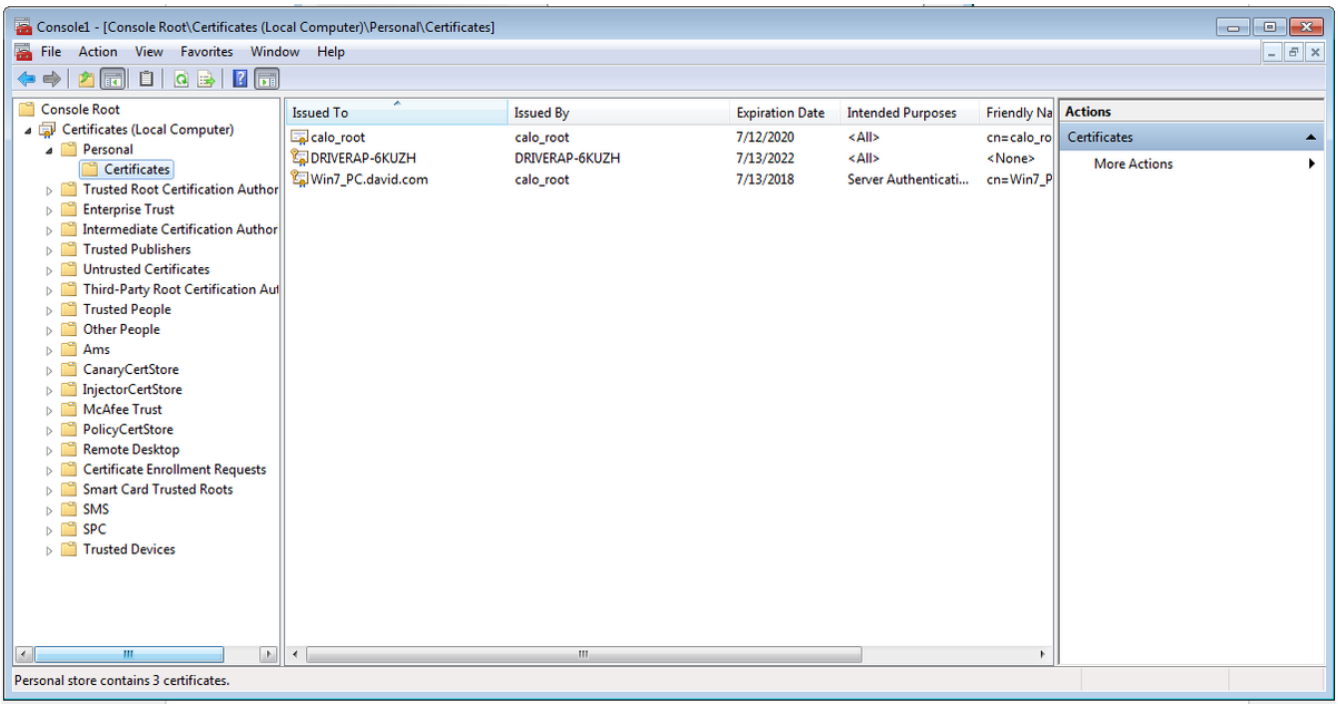
Paso 13. Seleccione **Siguiente** una vez más.



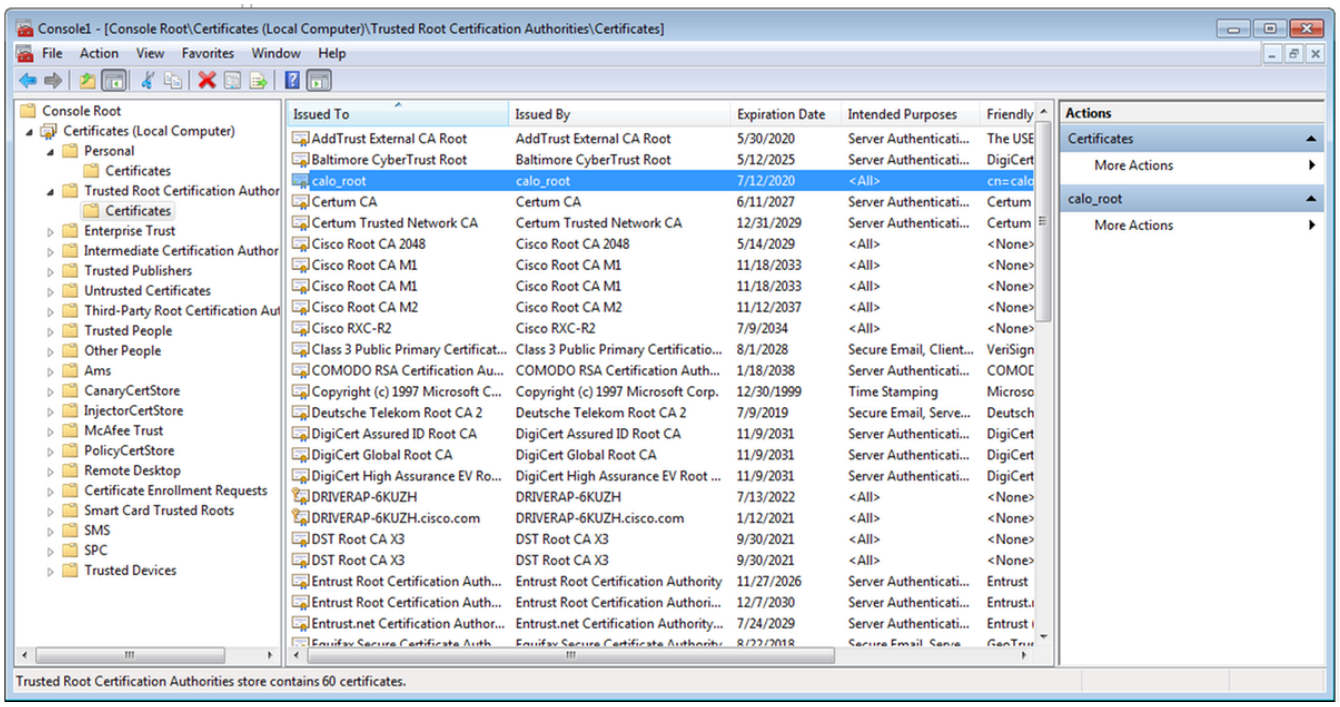
Paso 14. Seleccione **Finalizar**.

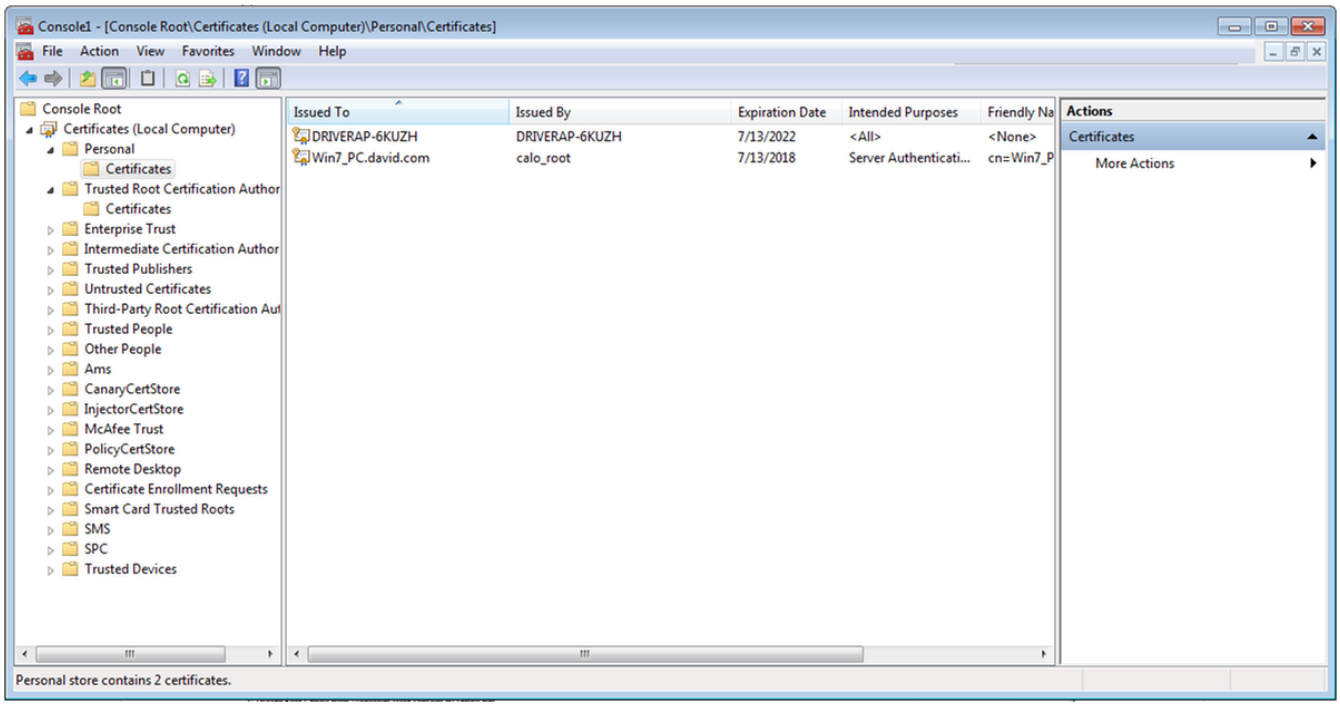


Paso 15. Seleccione **OK**. Ahora verá los certificados instalados (tanto el certificado de CA como el certificado de identidad).



Paso 16. Arrastre y suelte el certificado CA desde **Certificados (equipo local)>Personal>Certificados** a **Certificados (equipo local)>Autoridad de certificación raíz de confianza>Certificados.**



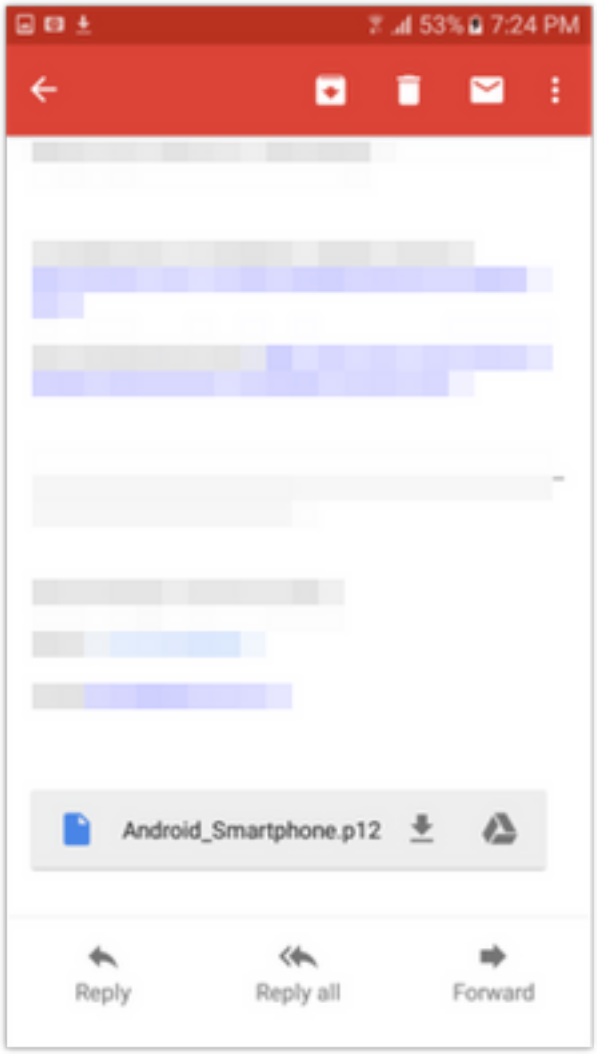


Cómo instalar el certificado de identidad en el dispositivo móvil Android

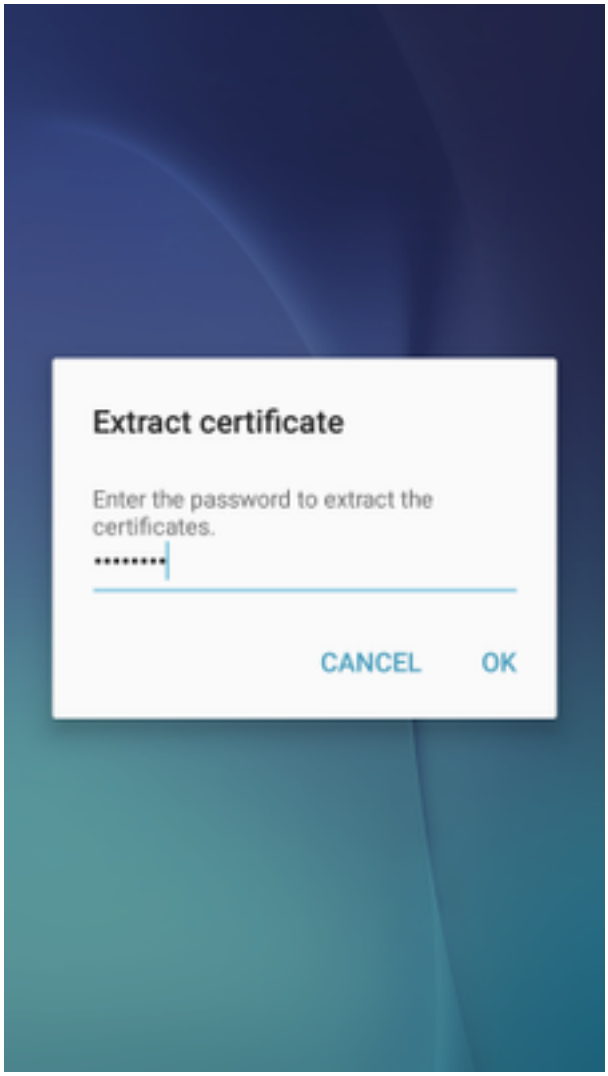
Nota: Android admite archivos de almacenamiento de claves PKCS#12 con extensión .pfx o .p12.

Nota: Android sólo admite certificados SSL X.509 codificados por DER.

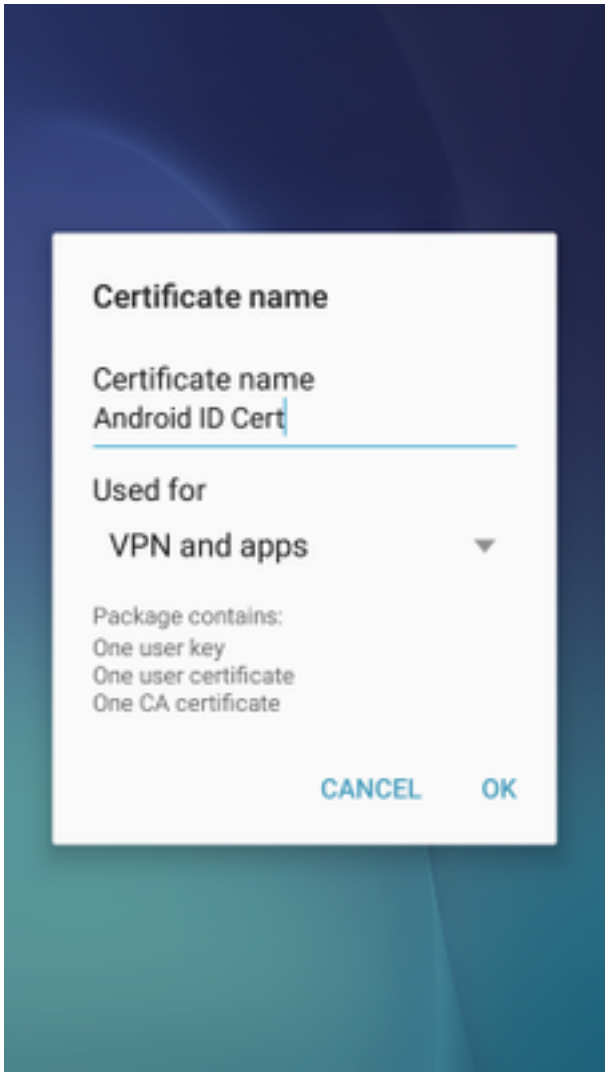
Paso 1. Después de la exportación del certificado de cliente del servidor de CA del IOS en formato PKCS12 (.p12), envíe el archivo al dispositivo Android por correo electrónico. Una vez que lo tenga, toque el nombre del archivo para iniciar la instalación automática. (**No descargar el archivo**)



Paso 2. Ingrese la contraseña utilizada para exportar el certificado, en este ejemplo, la contraseña es **cisco123**.

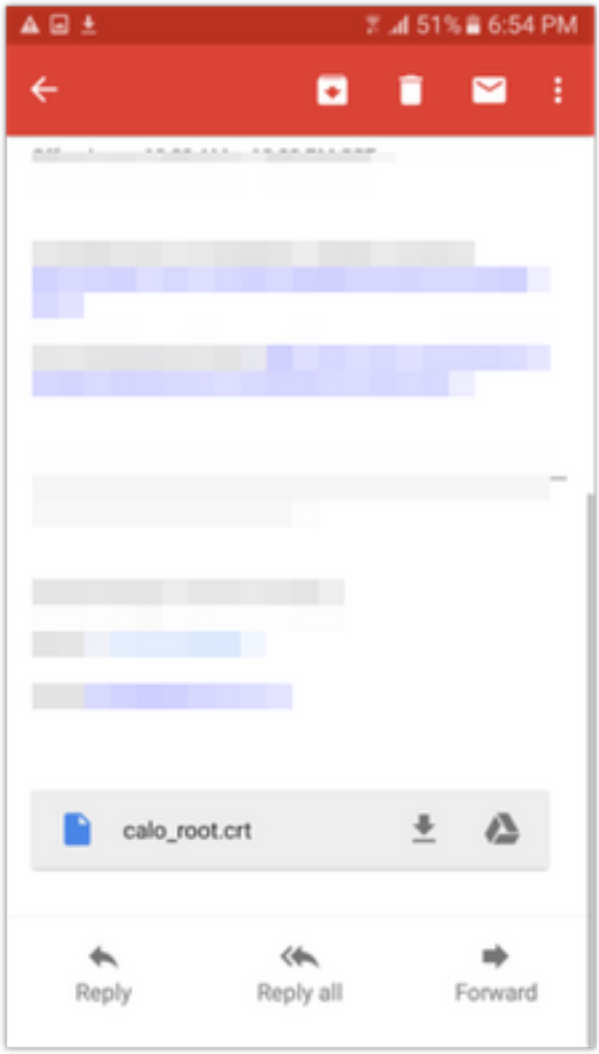


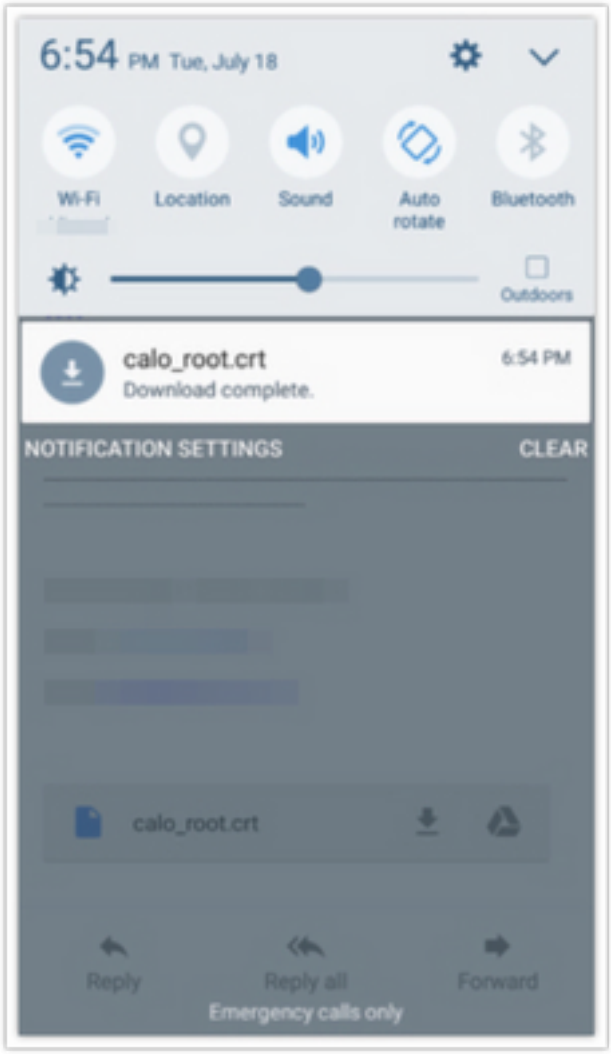
Paso 3. Seleccione **Aceptar** e introduzca un **nombre de certificado**. Puede ser cualquier palabra, en este ejemplo el nombre es **Certificado de ID de Android** .



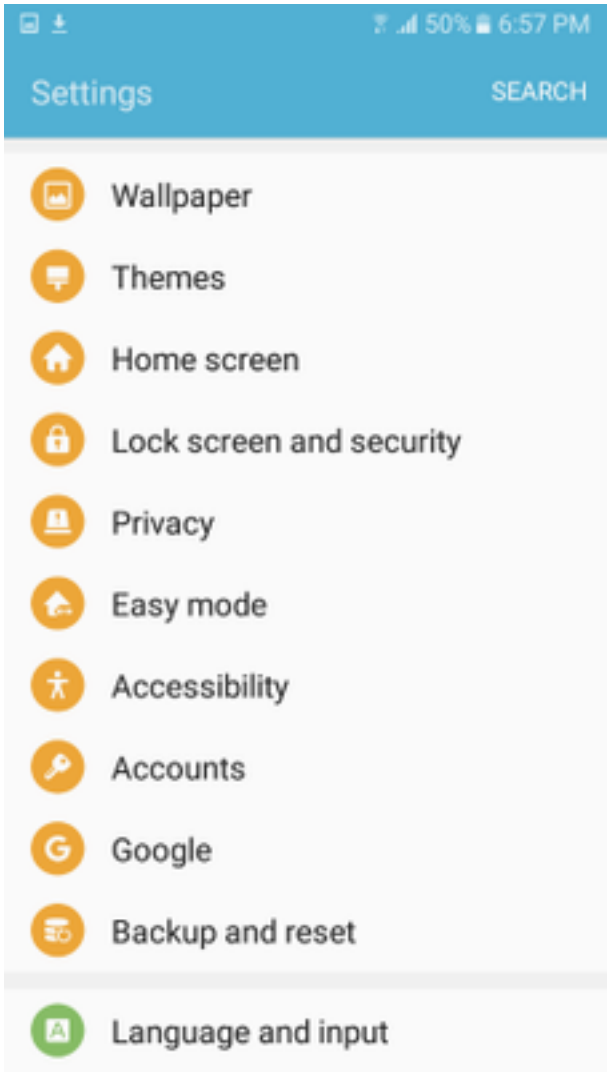
Paso 4. Seleccione **OK** y aparecerá el mensaje "Android ID Cert installed" (Certificado de ID de Android instalado).

Paso 5. Para instalar el certificado de CA, extráigalo del servidor de CA del IOS en el formato base64 y guárdelo con la extensión .crt. Envíe el archivo al dispositivo android por correo electrónico. Esta vez, debe descargar el archivo pulsando en la flecha situada junto al nombre del archivo.


51% 6:54 PM
calo_root.crt
Reply
Reply all
Forward

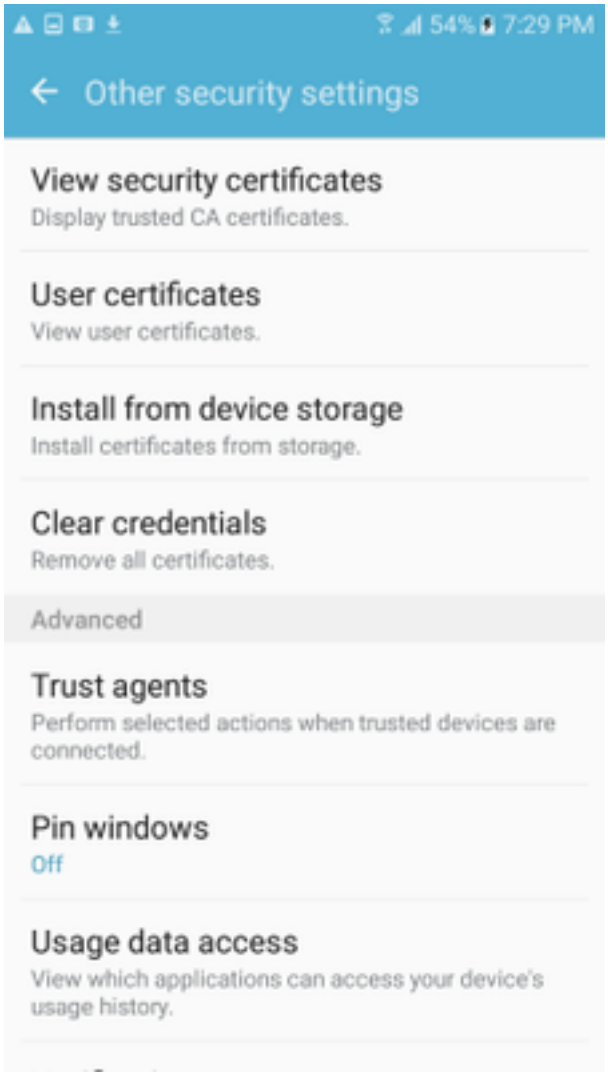


Paso 6. Navegue hasta **Configuración** y **Bloquear pantalla y seguridad.**

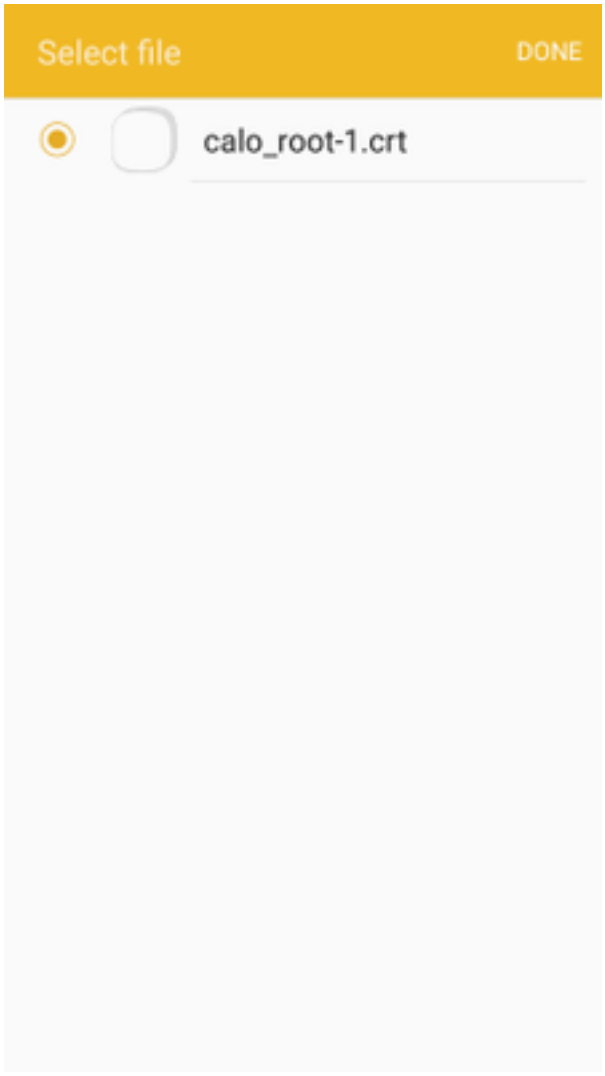


Paso 7. Seleccione **Otros parámetros de seguridad.**

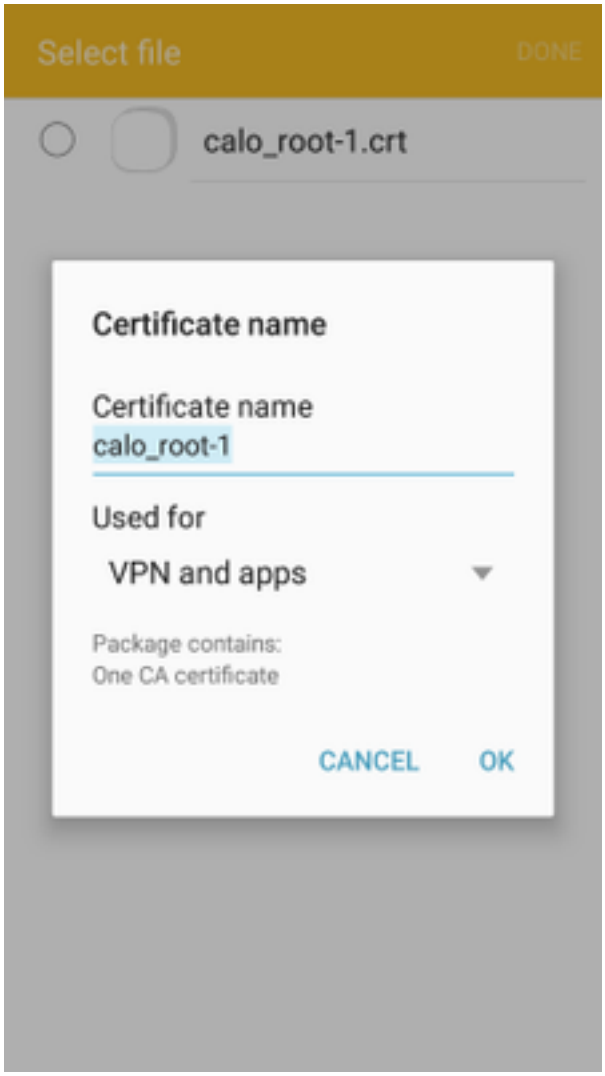
Paso 8. Vaya a **Instalación desde el almacenamiento de dispositivos.**



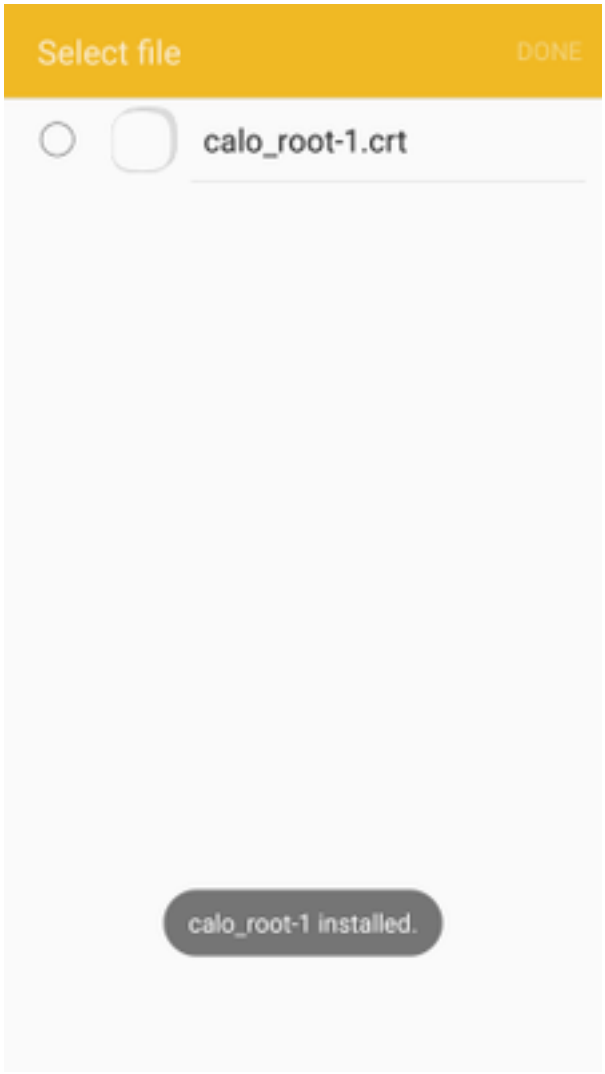
Paso 9. Seleccione el archivo .crt y toque **Finalizado.**



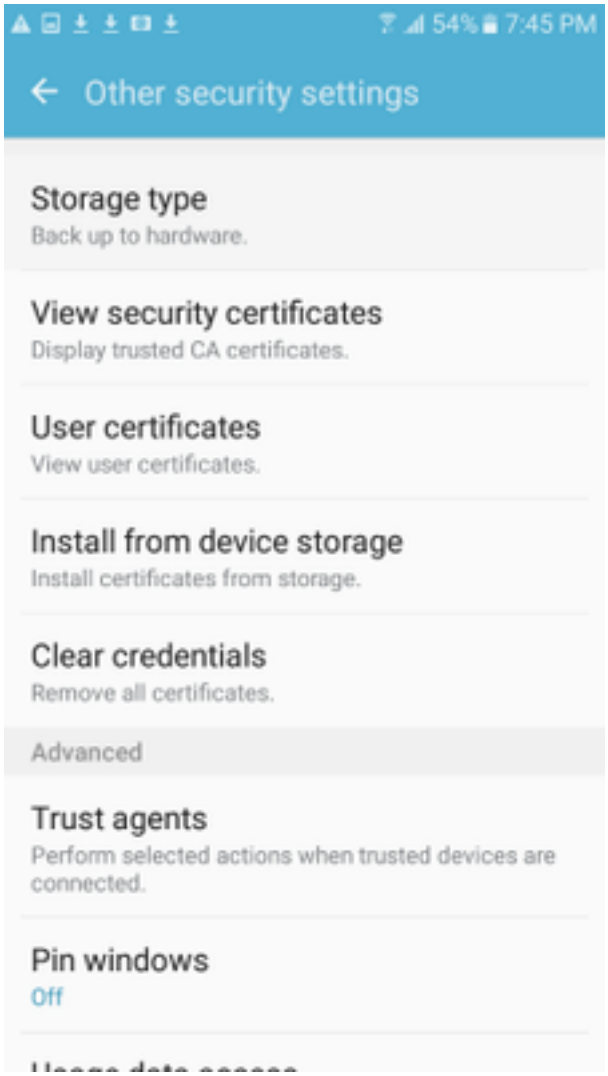
Paso 10. Introduzca un **nombre de certificado**. Puede ser cualquier palabra, en este ejemplo, el nombre es **calo_root-1**.



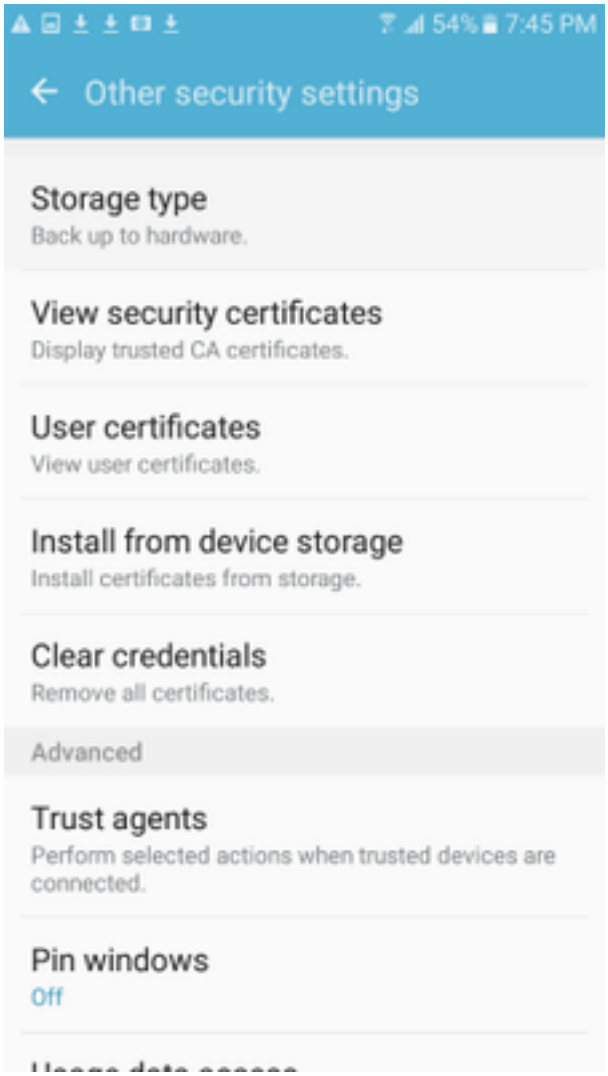
Paso 10. Seleccione **OK** y verá el mensaje "calo_root-1 instalado".



Paso 11. Para verificar que el certificado de identidad está instalado, navegue a **Settings/Lock Screen y Security/Other > Security Settings/User Certificates/System tab.**


54% 7:45 PM
Other security settings
Storage type
Back up to hardware.
View security certificates
Display trusted CA certificates.
User certificates
View user certificates.
Install from device storage
Install certificates from storage.
Clear credentials
Remove all certificates.
Advanced
Trust agents
Perform selected actions when trusted devices are connected.
Pin windows
Off

Paso 12. Para comprobar que el certificado de CA está instalado, vaya a **Configuración/Bloquear pantalla y seguridad/Otros parámetros de seguridad/Ver certificados de seguridad/ficha Usuario.**


54% 7:45 PM
Other security settings
Storage type
Back up to hardware.
View security certificates
Display trusted CA certificates.
User certificates
View user certificates.
Install from device storage
Install certificates from storage.
Clear credentials
Remove all certificates.
Advanced
Trust agents
Perform selected actions when trusted devices are connected.
Pin windows
Off

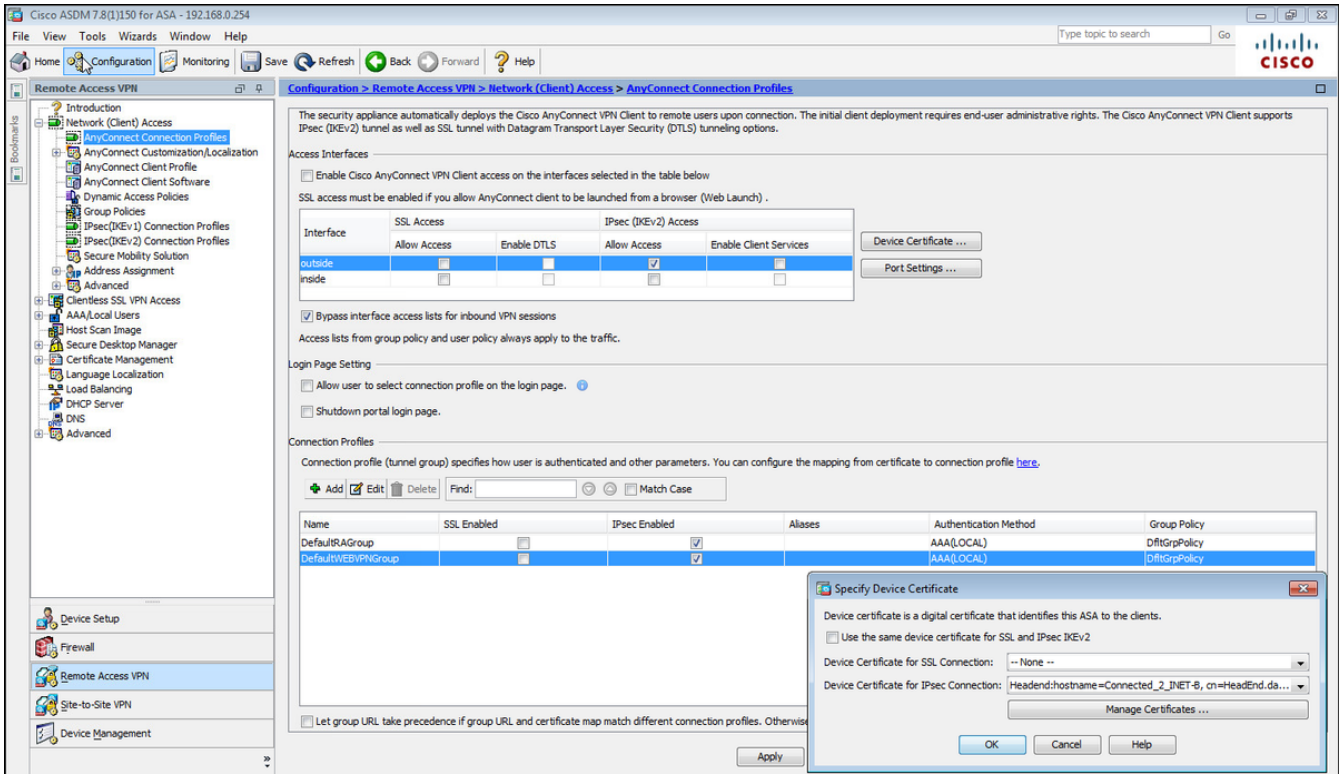
Configuración de la cabecera ASA para RA VPN con IKEv2

Paso 1. En ASDM, navegue hasta **Configuration>Remote Access VPN > Network (client) Access> Anyconnect Connection Profiles**. Marque la casilla **IPSec (IKEv2), Permitir acceso** en la interfaz que se encuentra frente a los clientes VPN (la opción **Habilitar servicios de cliente** no es necesaria).

Paso 2. Seleccione **Device Certificate** y quite la marca de verificación de **Use el mismo certificado de dispositivo para SSL e IPSec IKEv2**.

Paso 3. Seleccione el certificado de cabecera para la conexión IPSec y seleccione — Ninguno — para la conexión SSL.

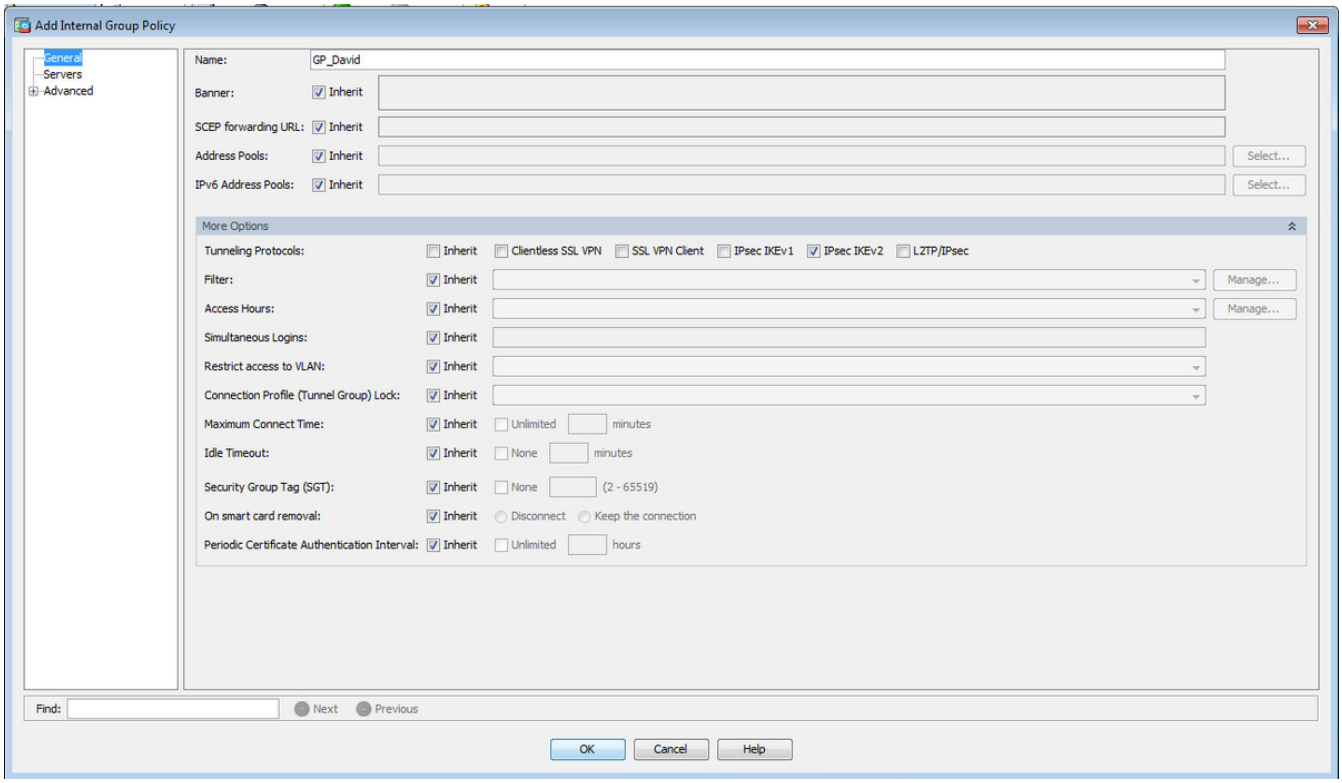
Esta opción coloca el crypto ikev2, crypto ipsec, crypto dynamic-map y la configuración de crypto map.



Así es como se ve la configuración en la interfaz de línea de comandos (CLI).

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

crypto ikev2 remote-access trustpoint HeadEnd
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5

crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256
crypto map outside_map 65535 ipsec-isakmp dynamic Anyconnect
crypto map outside_map interface outside
```

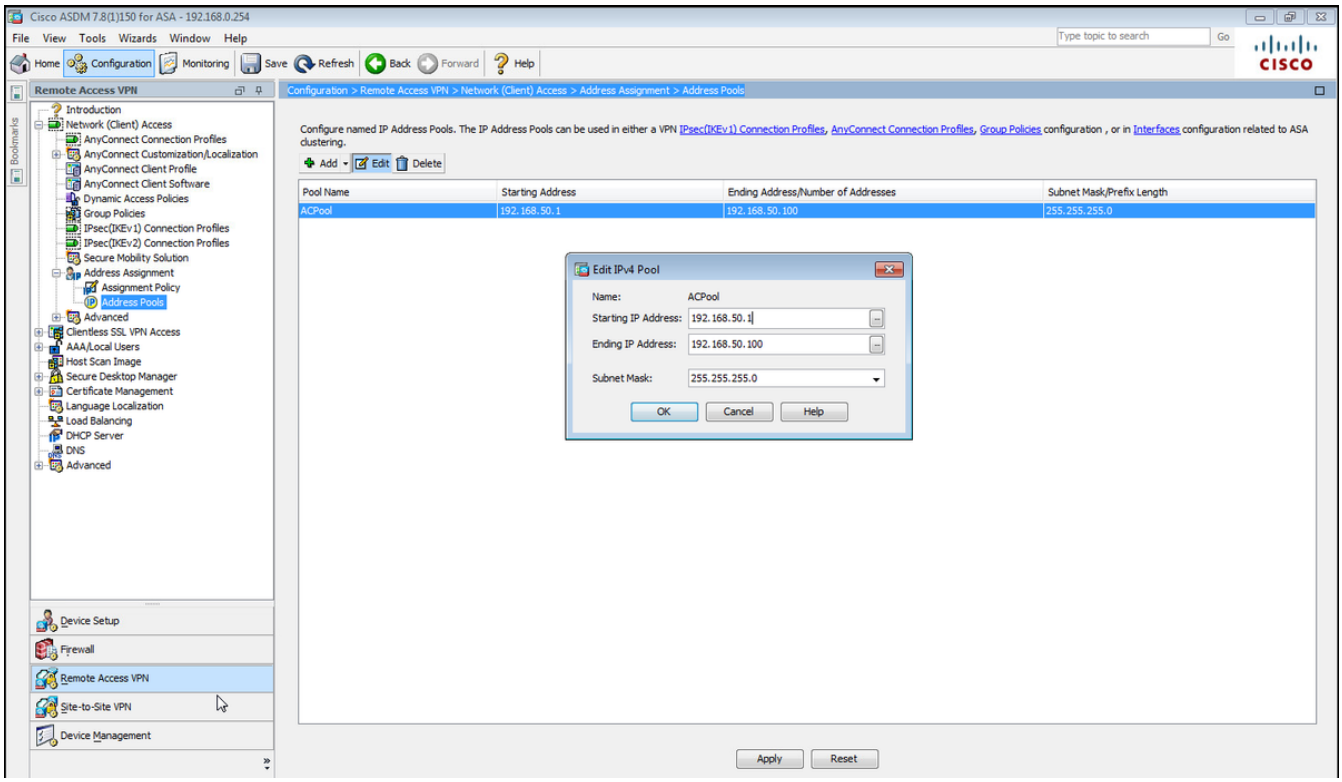
Paso 4. Vaya a **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** para crear una política de grupo



En CLI.

```
group-policy GP_David internal
group-policy GP_David attributes
 vpn-tunnel-protocol ikev2
```

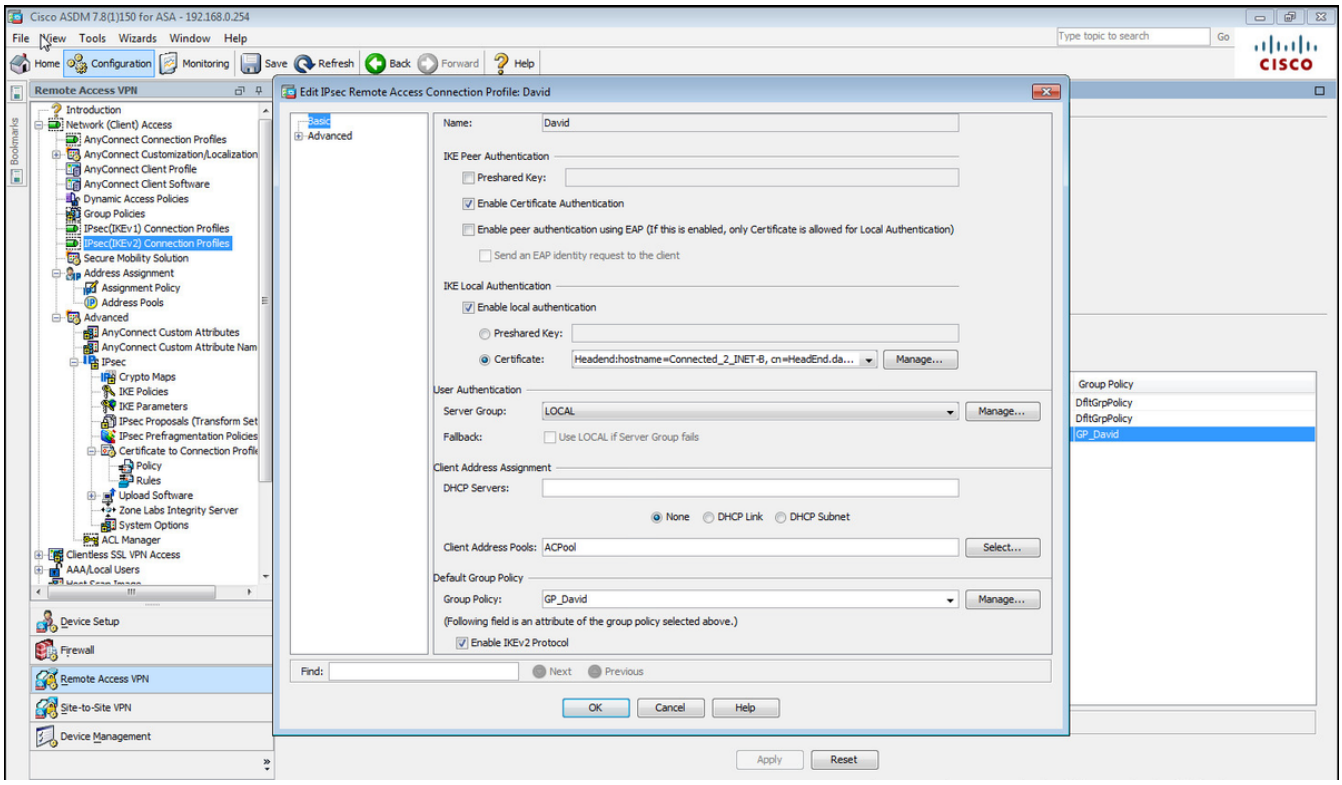
Paso 5. Navegue hasta **Configuration > Remote Access VPN > Network (Client) Access > Address Pools** y seleccione **Add** para crear un Pool IPv4.



En CLI.

```
ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0
```

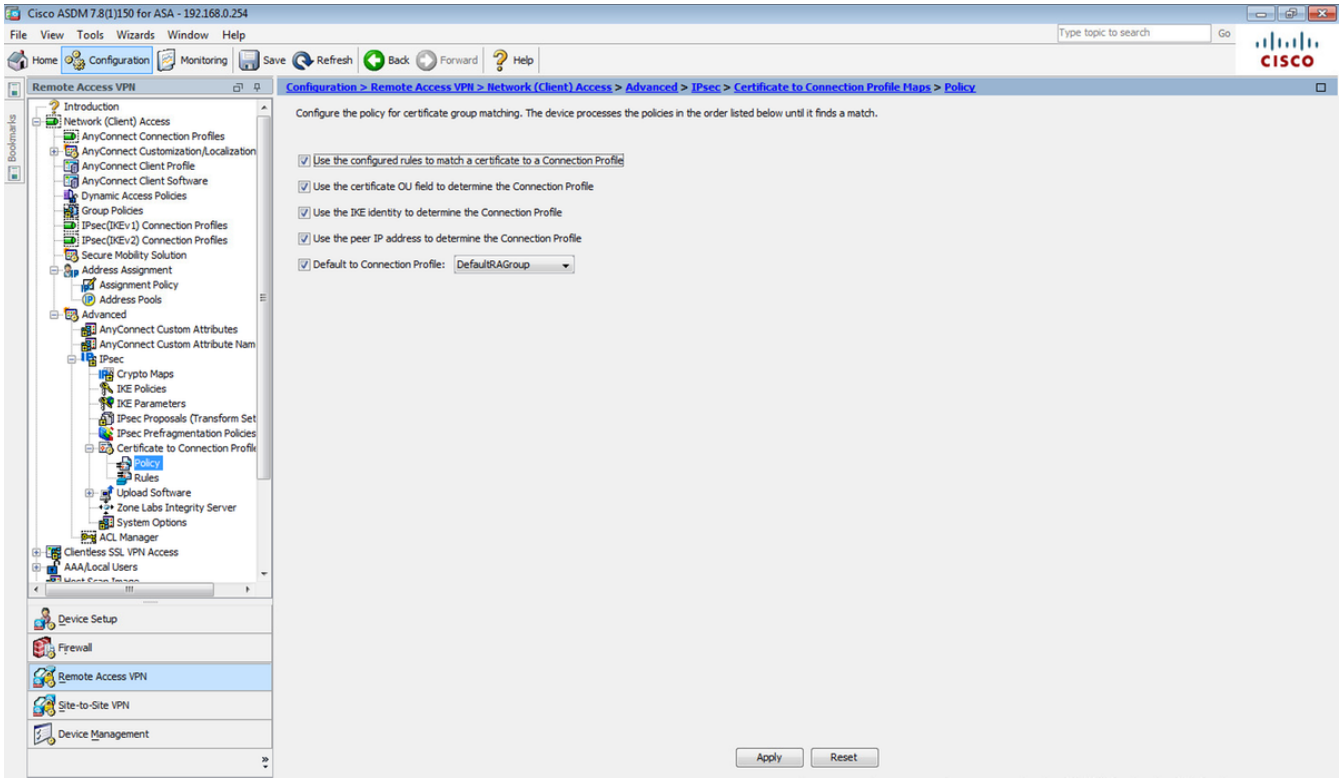
Paso 6. Navegue hasta **Configuration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles** y seleccione **Add** para crear un nuevo grupo de túnel.



En CLI.

```
tunnel-group David type remote-access
tunnel-group David general-attributes
 address-pool ACPool
 default-group-policy GP_David
 authentication-server-group LOCAL
tunnel-group David webvpn-attributes
 authentication certificate
tunnel-group David ipsec-attributes
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate HeadEnd
```

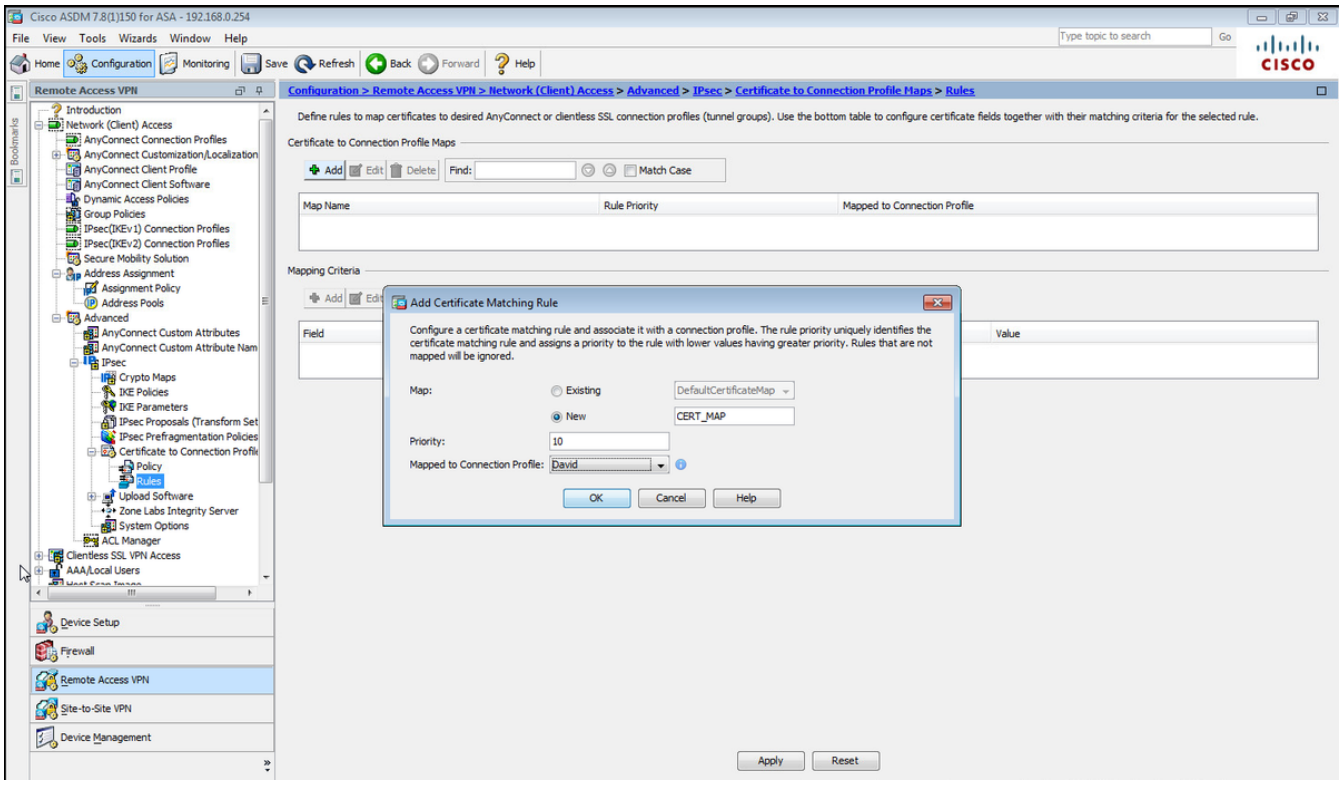
Paso 7. Navegue hasta **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy** y marque la **casilla Utilizando las reglas configuradas para matematizar un certificado en un Connection Profile**.



En CLI.

```
tunnel-group-map enable rules
```

Paso 8. Vaya a **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules** y cree un nuevo Certificate Map. Seleccione **Add** y asócielo al grupo de túnel. En este ejemplo, el grupo de túnel se llama **David**.



En CLI.

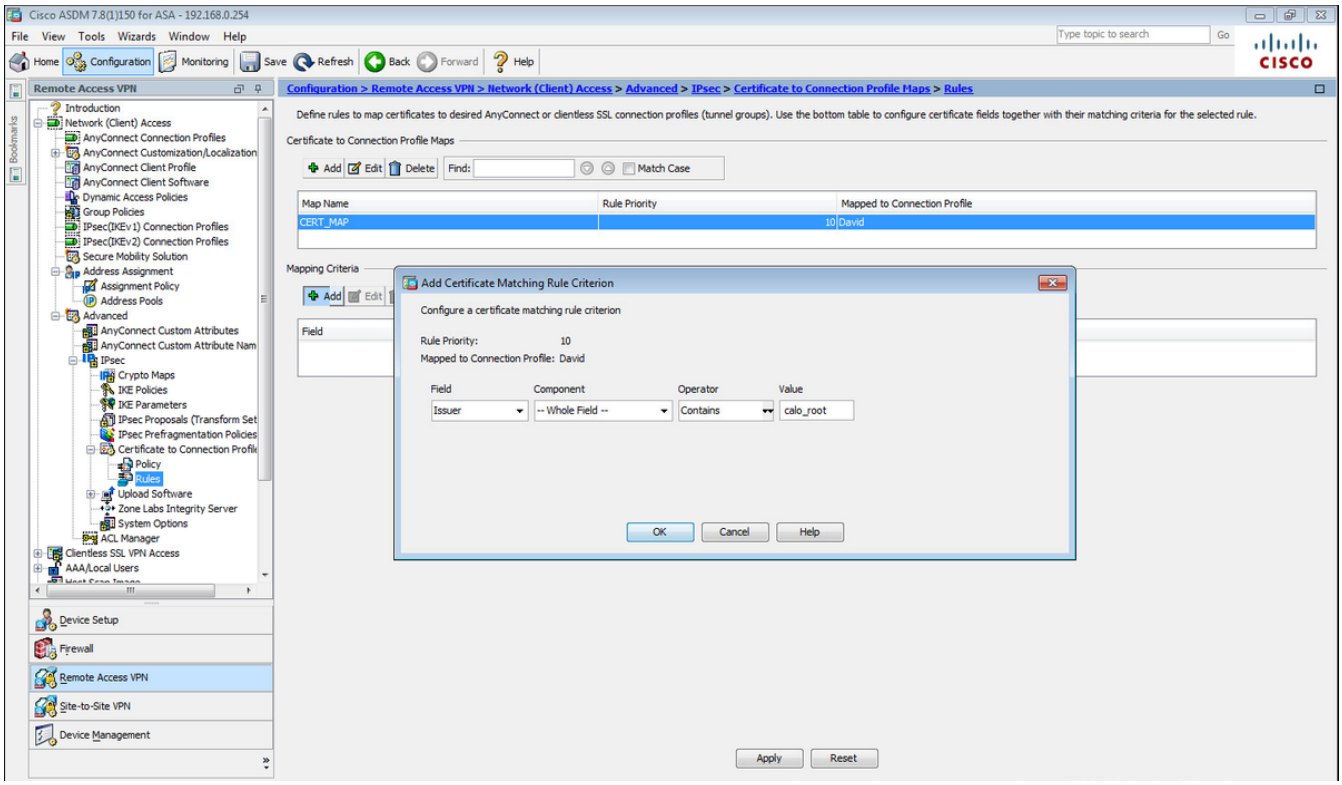
```
tunnel-group-map CERT_MAP 10 David
```

Paso 9. Seleccione **Agregar** en la sección **Criterios de asignación** e introduzca estos valores.

Campo: Emisor

Operador: Contiene

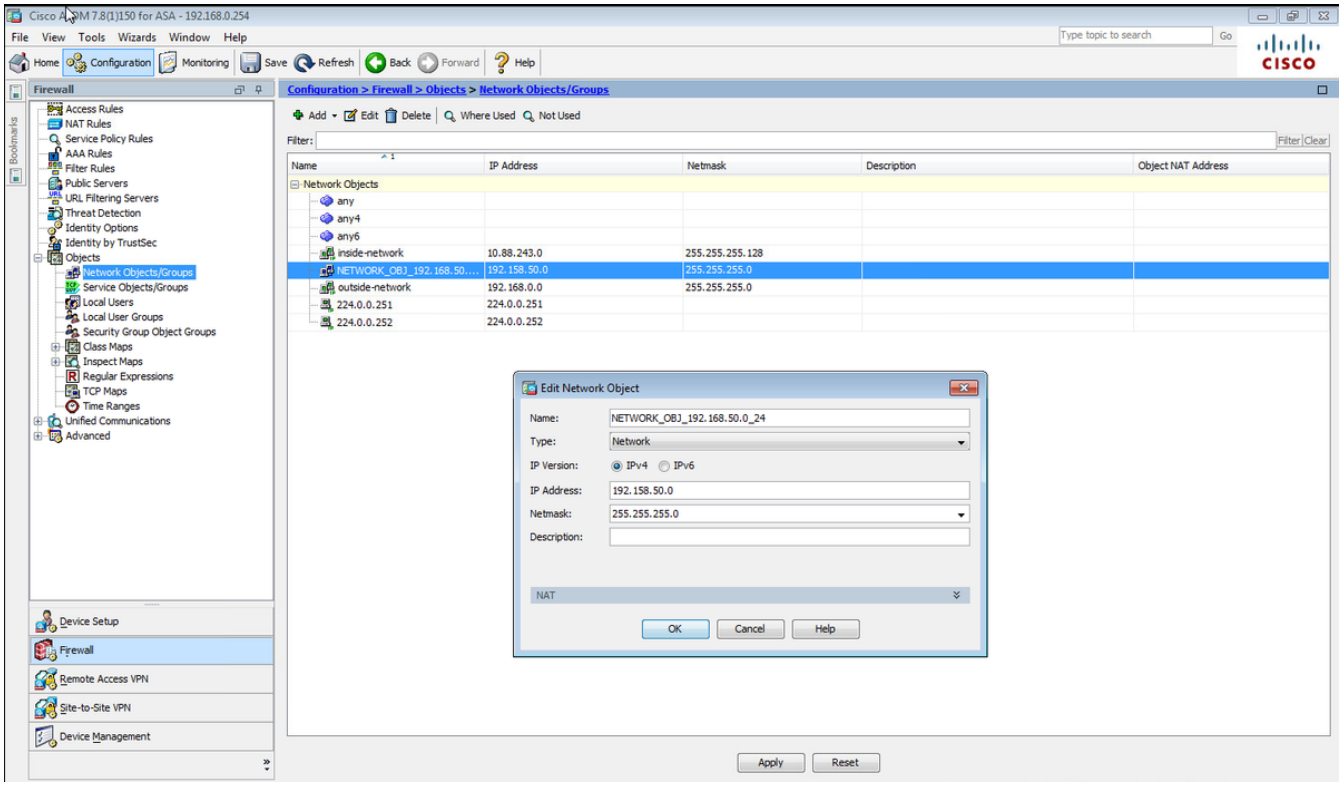
Valor: calo_root



En CLI.

```
crypto ca certificate map CERT_MAP 10
 issuer-name co calo_root
```

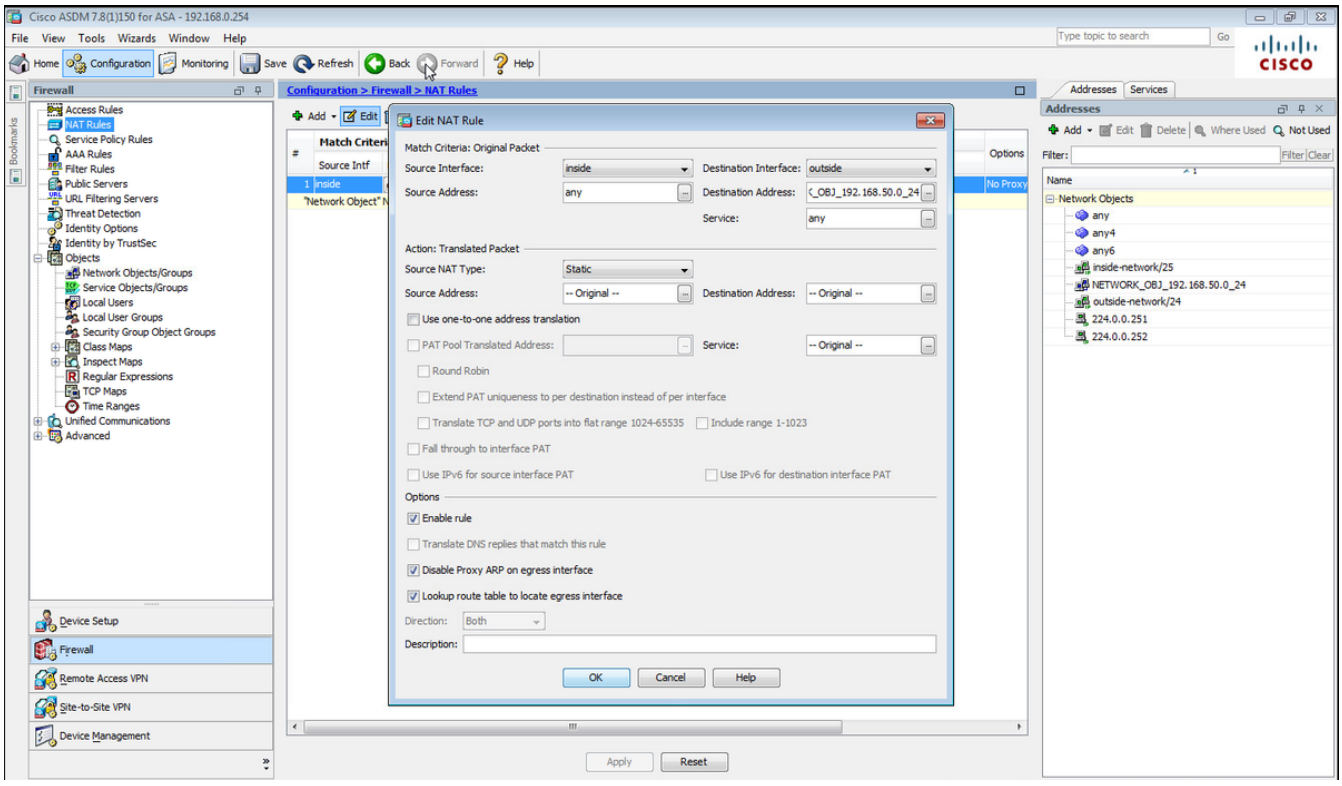
Paso 10. Cree un objeto con la red del conjunto IP que se utilizará para agregar una regla de exención de NAT (traducción de direcciones de red) en **Configuración > Firewall > Objetos > Objetos/Grupos de Red> Agregar**.



En CLI.

```
object network NETWORK_OBJ_192.168.50.0_24
 subnet 192.168.50.0 255.255.255.0
```

Paso 11. Navegue hasta **Configuration > Firewall > NAT Rules** y seleccione **Add** para crear la regla de exención de NAT para el tráfico VPN RA.



En CLI.

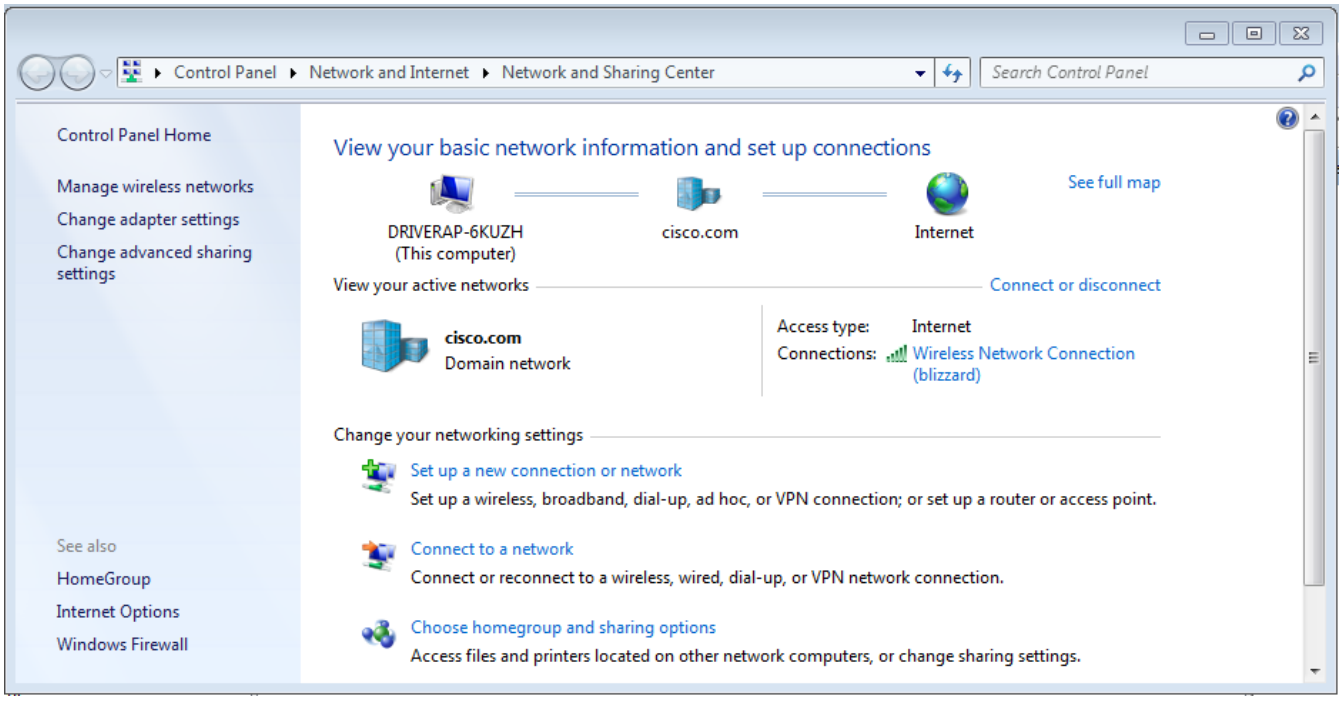
```
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24 no-proxy-arp route-lookup
```

Esta es la configuración ASA completa utilizada para este ejemplo.

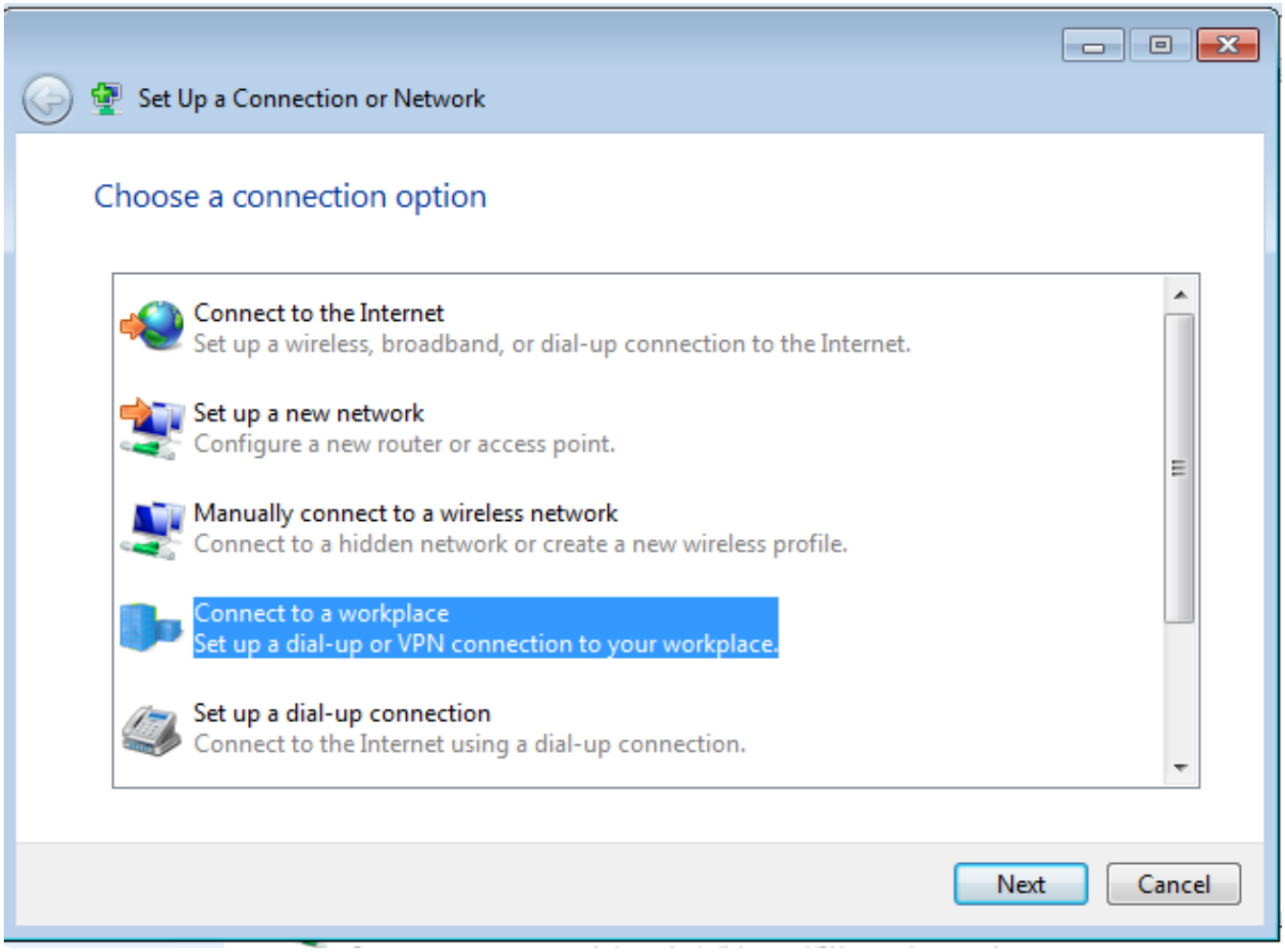
```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.88.243.108 255.255.255.128

object network NETWORK_OBJ_192.168.50.0_24
 subnet 192.168.50.0 255.255.255.0
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.50.0_24
NETWORK_OBJ_192.168.50.0_24
ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

crypto ikev2 remote-access trustpoint HeadEnd

group-policy GP_David internal
group-policy GP_David attributes
 vpn-tunnel-protocol ikev2

tunnel-group David type remote-access
tunnel-group David general-attributes
 address-pool ACPool
 default-group-policy GP_David
 authentication-server-group LOCAL
tunnel-group David webvpn-attributes
 authentication certificate
tunnel-group David ipsec-attributes
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate HeadEnd

tunnel-group-map enable rules
crypto ca certificate map CERT_MAP 10
 issuer-name co calo_root
tunnel-group-map CERT_MAP 10 David

crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5

crypto dynamic-map Anyconnect 65535 set ikev2 ipsec-proposal AES256
crypto map outside_map 65535 ipsec-isakmp dynamic Anyconnect
crypto map outside_map interface outside
```

Configurar cliente integrado de Windows 7

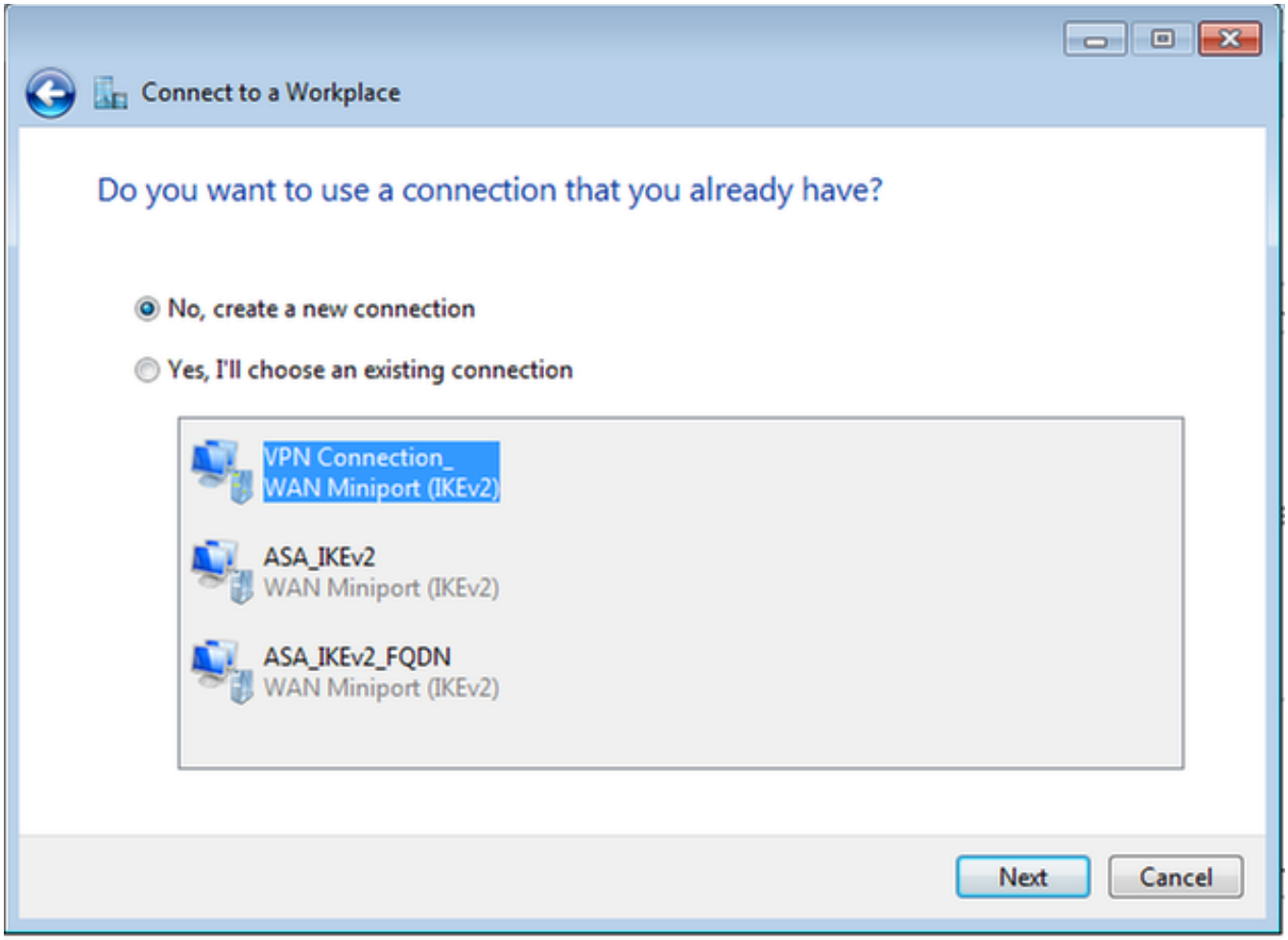
Paso 1. Vaya a **Panel de control > Red e Internet > Centro de redes y recursos compartidos**.



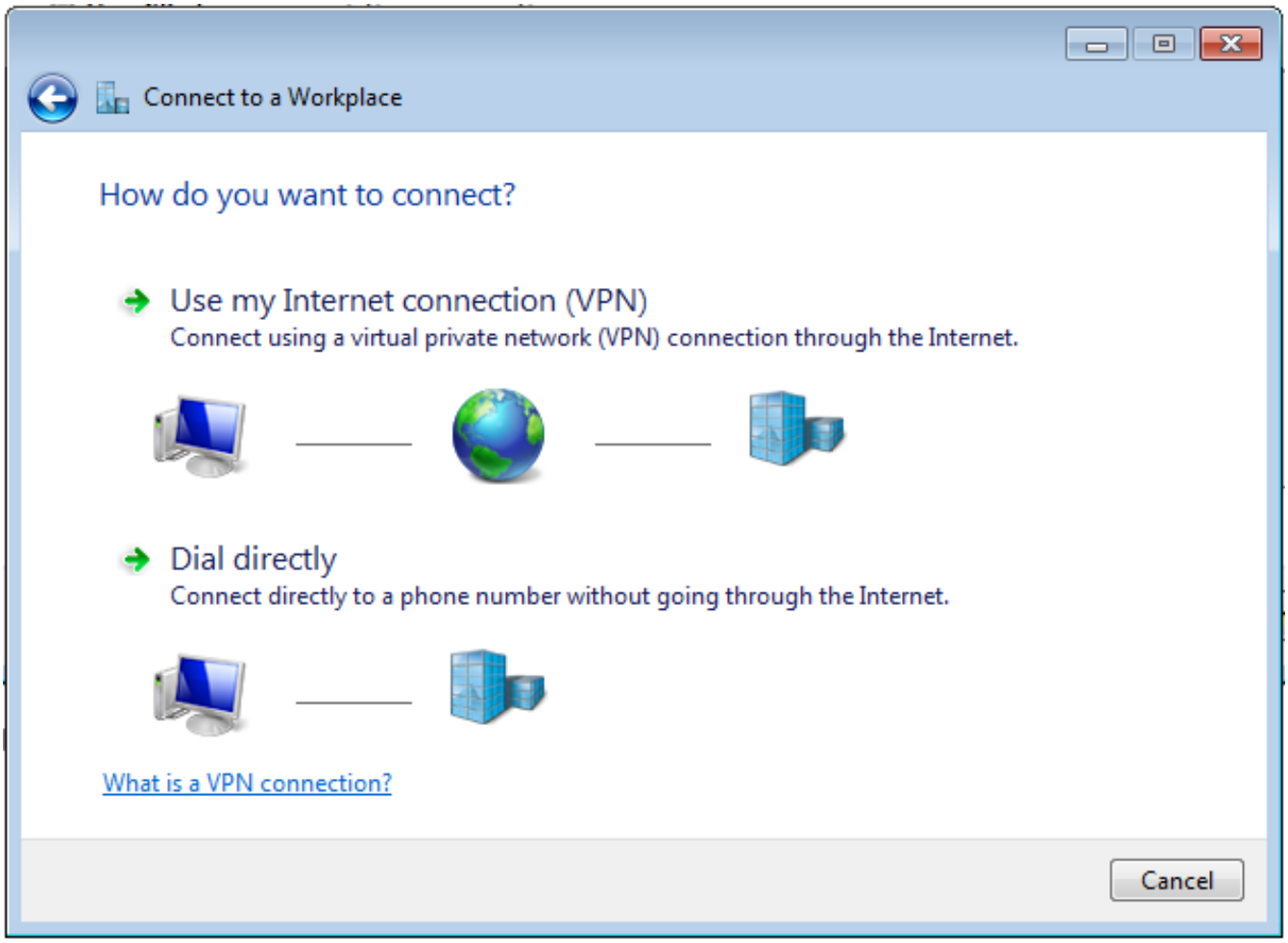
Paso 2. Seleccione **Configurar una nueva conexión o red**.



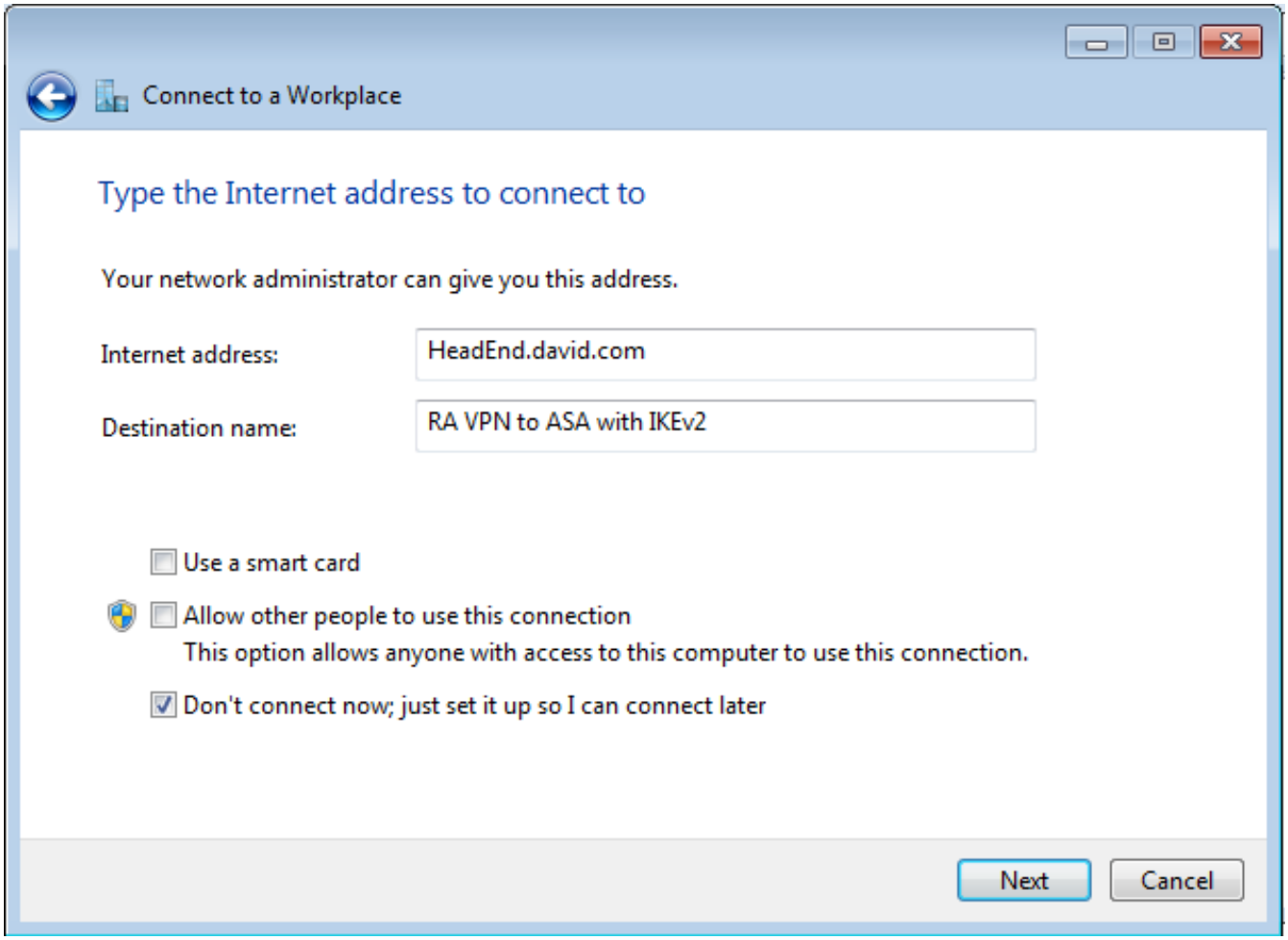
Paso 3. Seleccione **Conectar a un lugar de trabajo** y **Siguiente**.



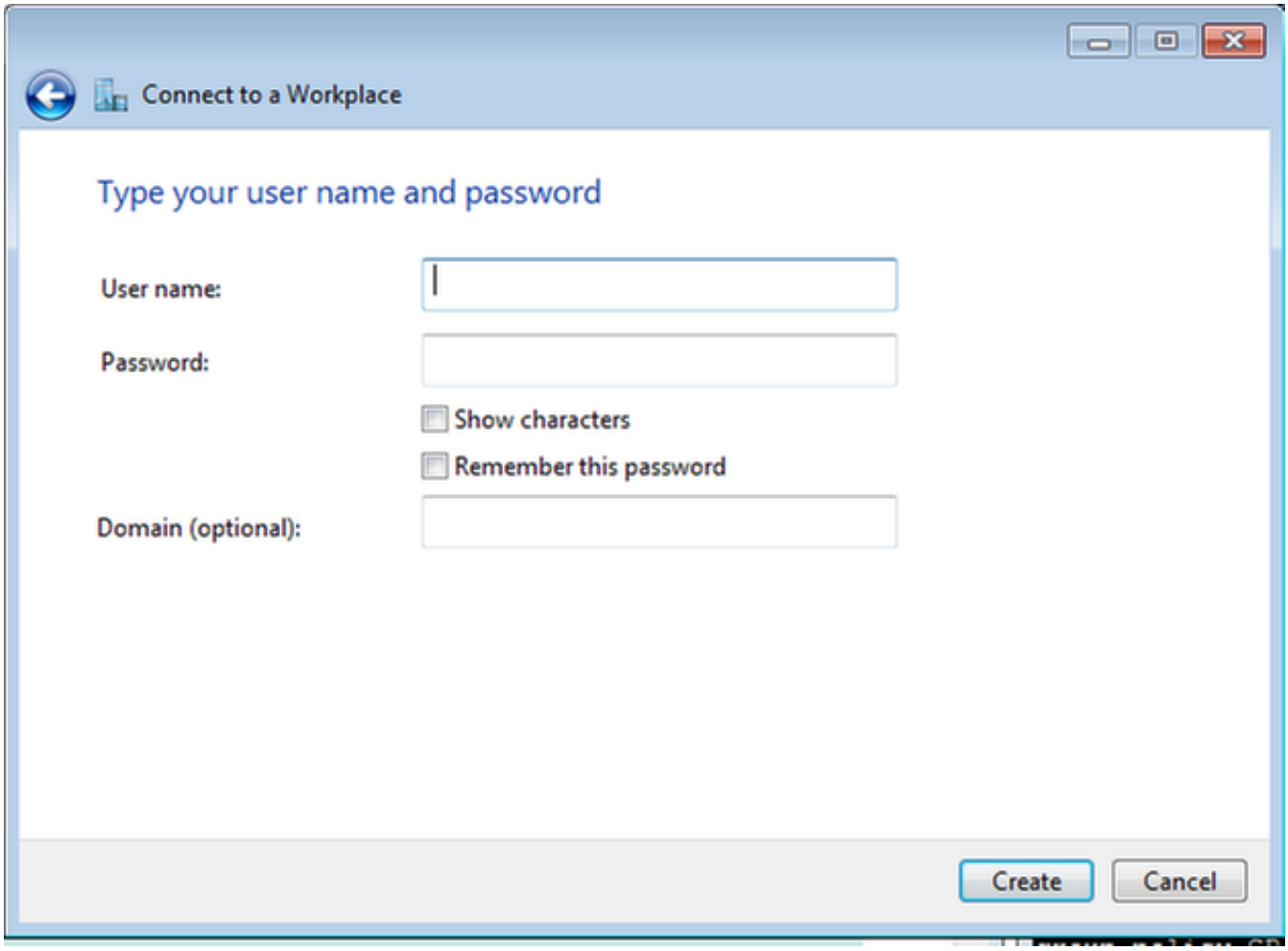
Paso 4. Seleccione **No, cree una nueva conexión** y **Siguiente**.



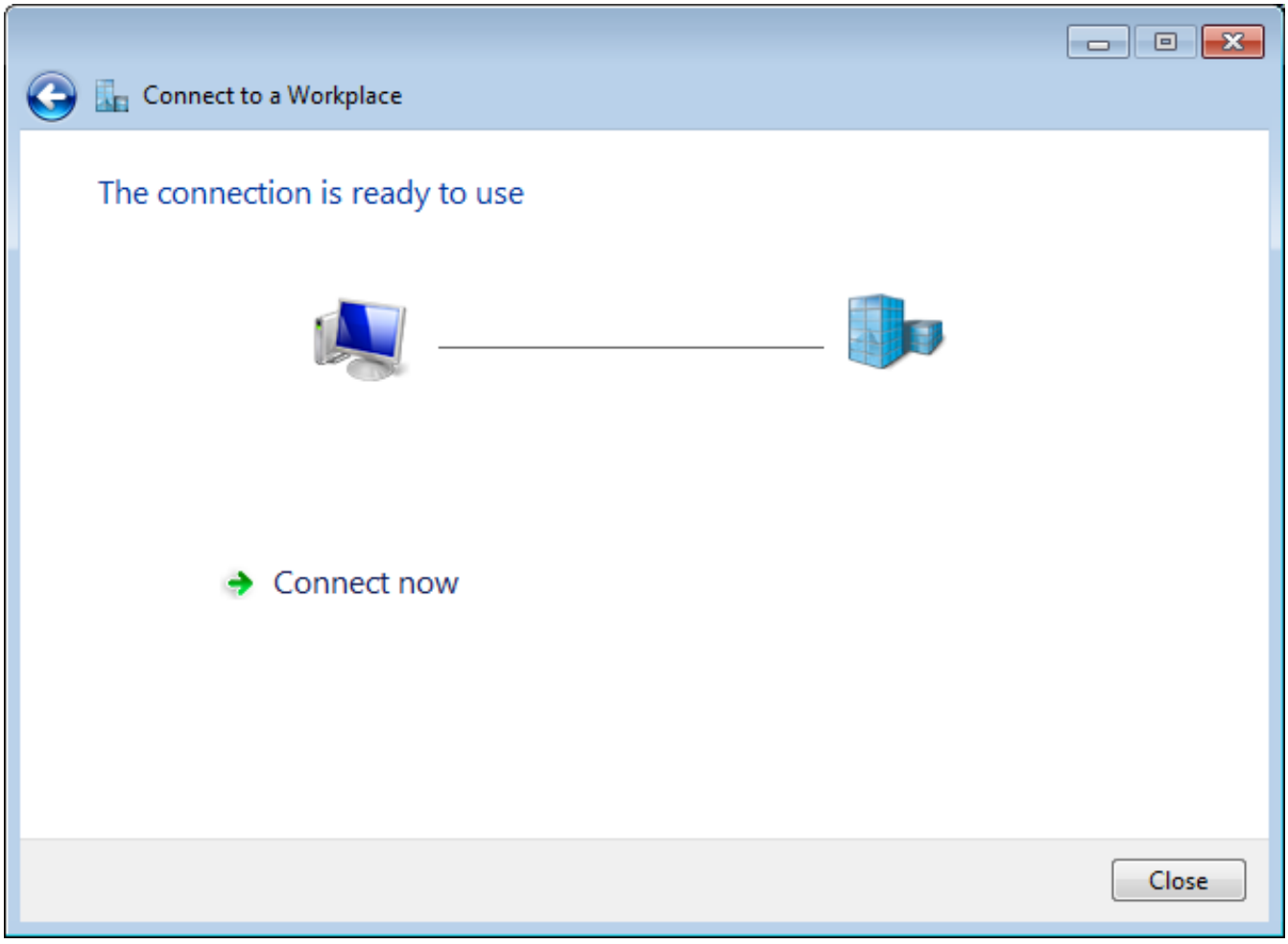
Paso 5. Seleccione **Use my Internet connection (VPN)** y agregue la cadena HeadEnd certificate Common Name (CN) en el campo **Internet address**. En el campo **Nombre de destino**, escriba el nombre de la conexión. Puede ser cualquier cadena. Asegúrese de comprobar el mensaje **No conectar ahora; sólo debe configurarlo para poder conectarlo más adelante**.



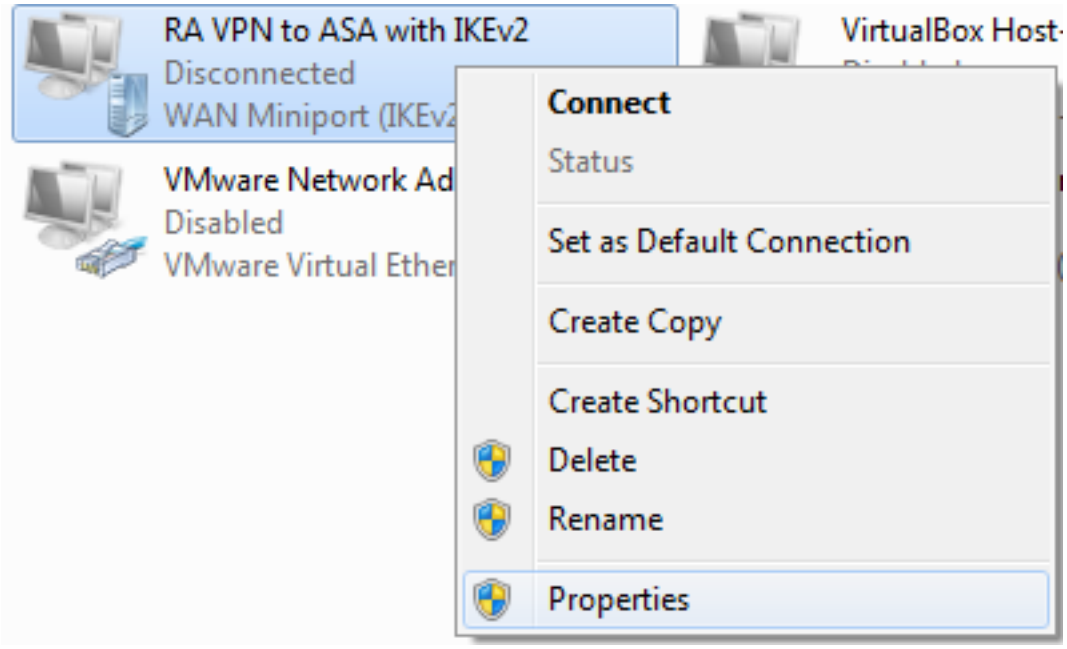
Paso 6. Seleccione **Next**.



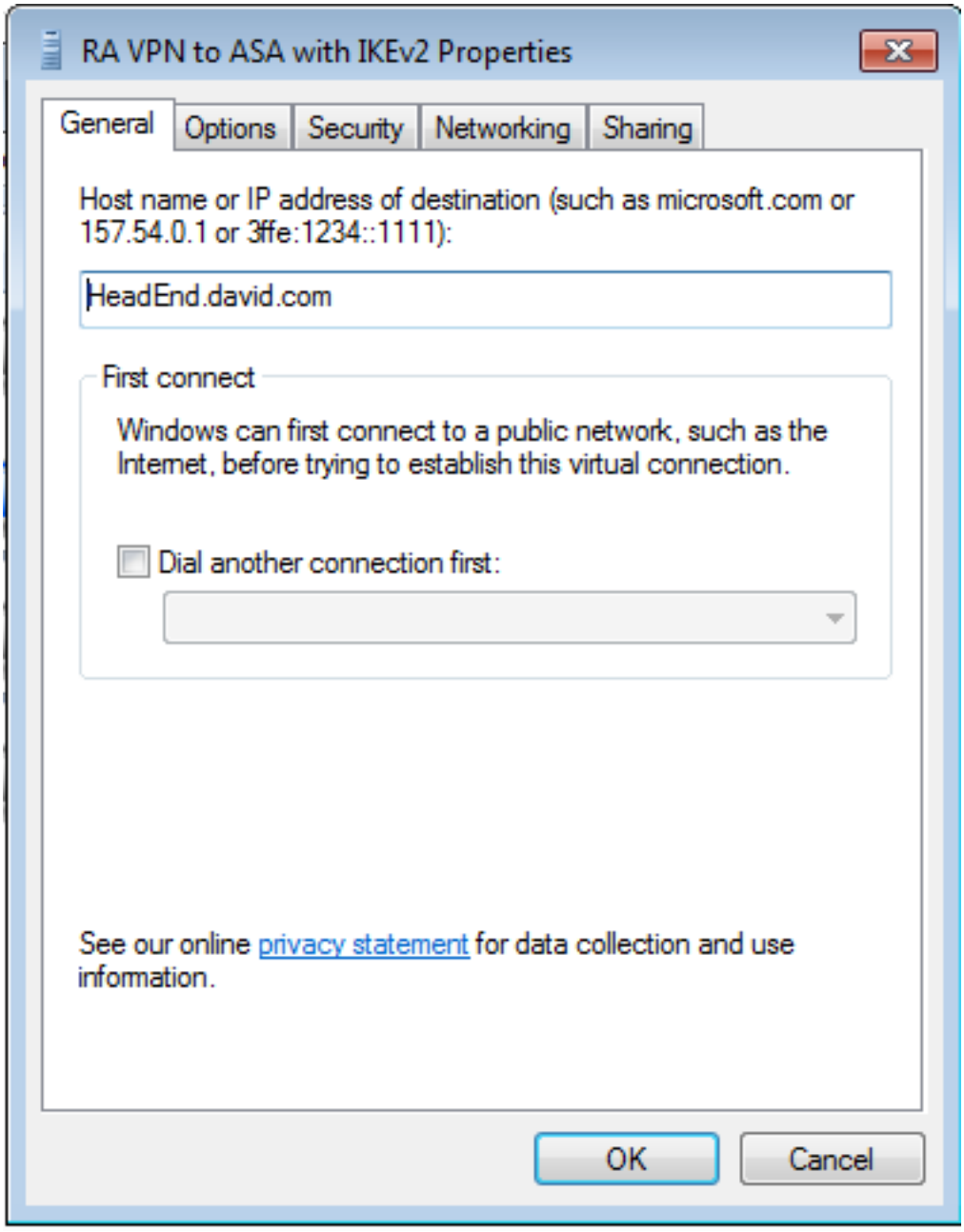
Paso 7. Seleccione **Crear**.



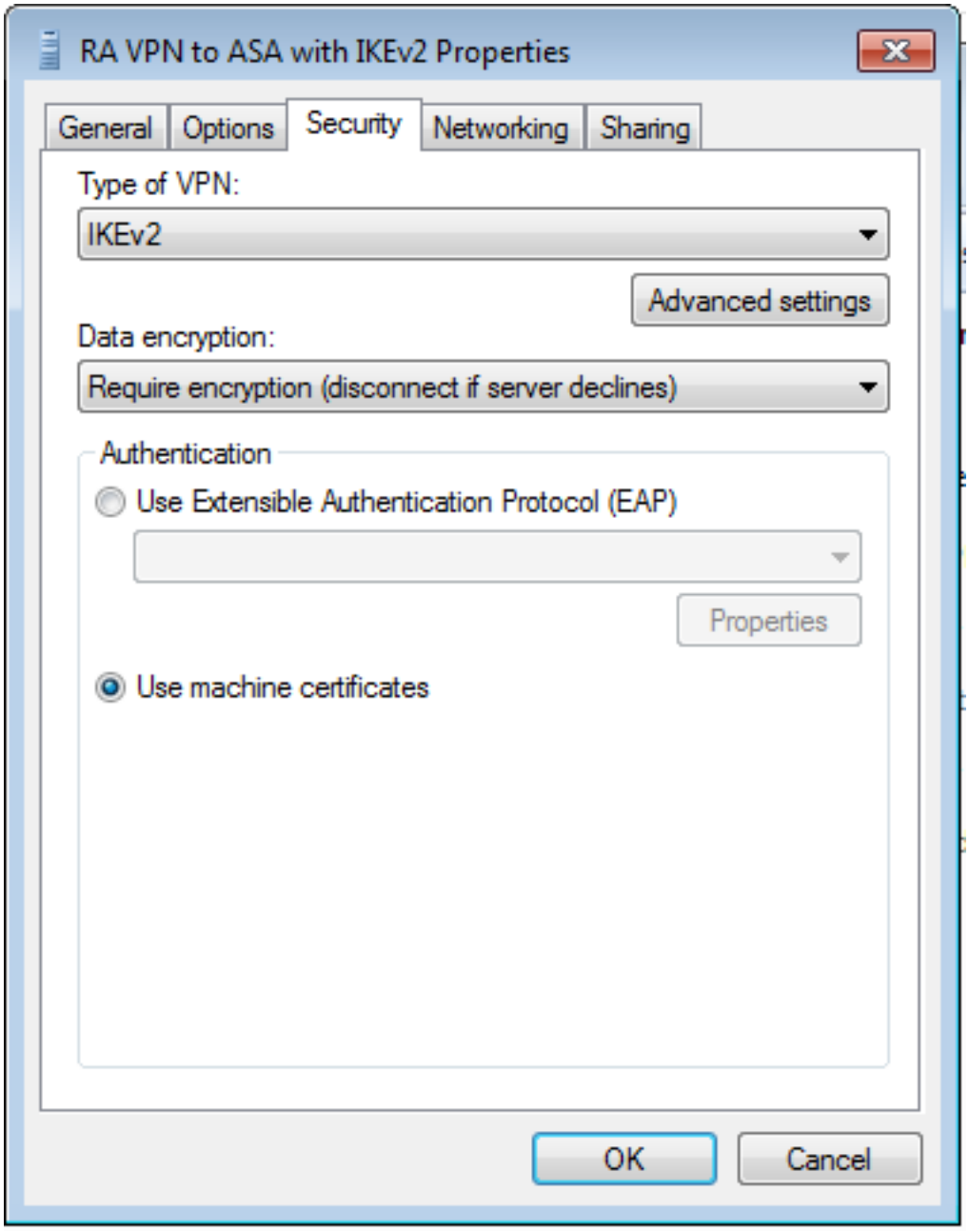
Paso 8. Seleccione **Cerrar** y navegue hasta **Panel de control > Red e Internet > Conexiones de red**. Seleccione la conexión de red creada y haga clic con el botón derecho en ella. Seleccione Properties (Propiedades).



Paso 9. En la pestaña **General** puede verificar que el nombre de host adecuado para la cabecera sea correcto. El ordenador resolverá este nombre a la dirección IP de ASA utilizada para conectar usuarios de VPN de RA.



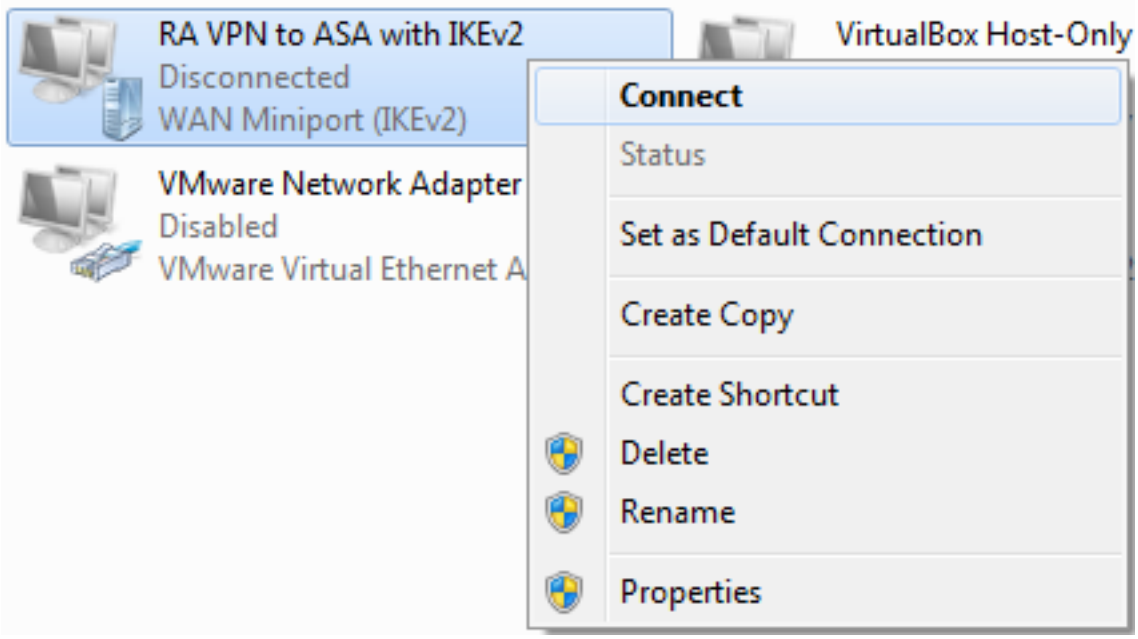
Paso 10. Navegue hasta la pestaña **Seguridad** y seleccione **IKEv2** como el **Tipo de VPN**. En la sección **Autenticación** seleccione **Usar certificados de máquina**.



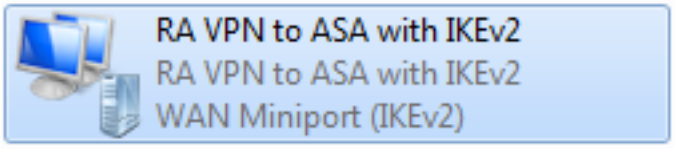
Paso 11. Seleccione **OK** y navegue a **C:\Windows\System32\drivers\etc**. Abra el archivo **host** con un editor de texto. Configure una entrada para resolver el FQDN (Nombre de dominio completo) configurado en la conexión de red a la dirección IP de su cabecera ASA (en este ejemplo, la interfaz externa).

```
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
10.88.243.108 HeadEnd.david.com
```

Paso 12. Vuelva al **Panel de control > Red e Internet > Conexiones de red**. Seleccione la conexión de red que ha creado. Haga clic con el botón derecho y seleccione **Connect (Conectar).**



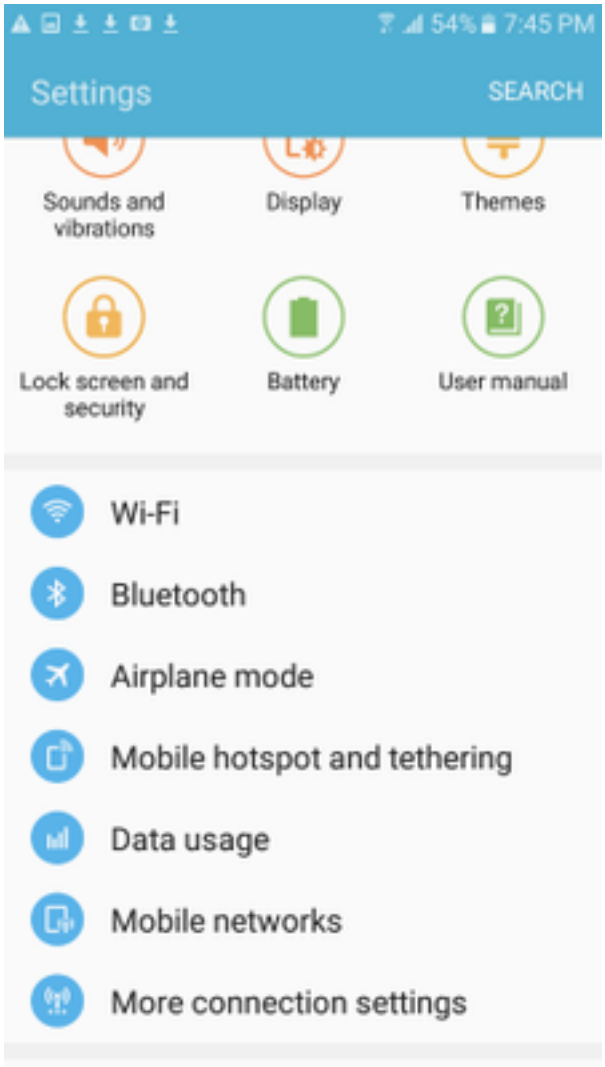
Paso 13. El estado de la conexión de red pasa de Desconectado a Conectando y luego a Conectado. Por último, se muestra el nombre especificado para la conexión de red.



El ordenador está conectado a la cabecera VPN en este momento.

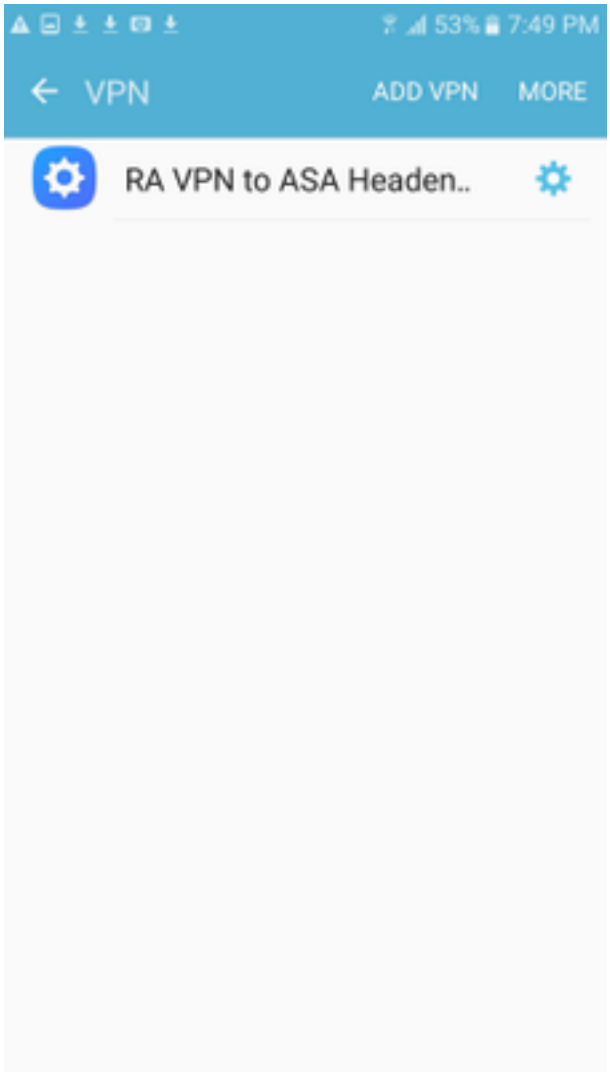
Configuración del cliente VPN nativo de Android

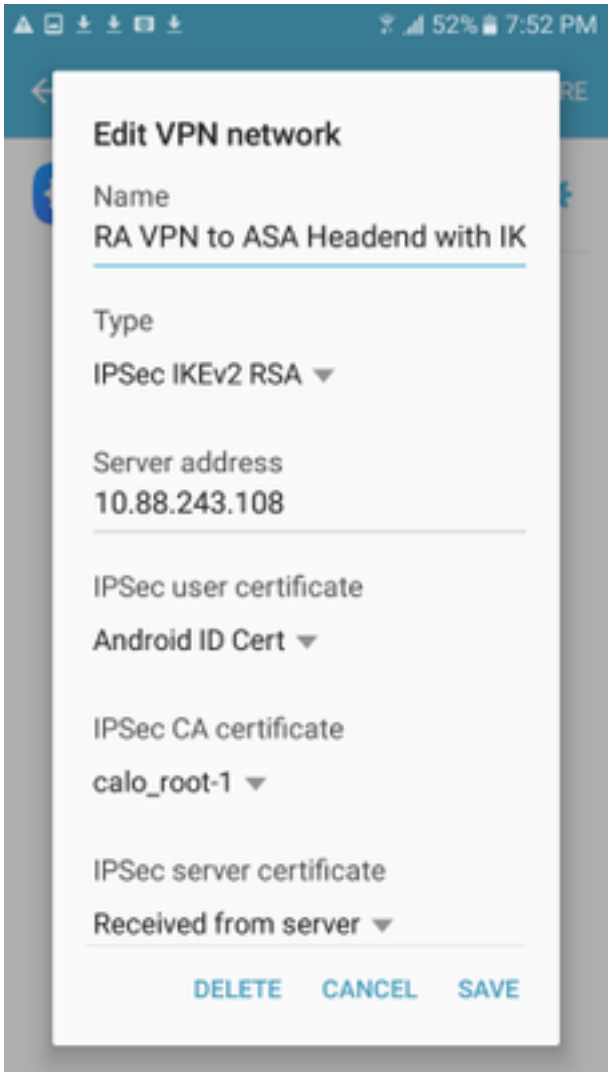
Paso 1. Vaya a **Settings>More connection Settings**



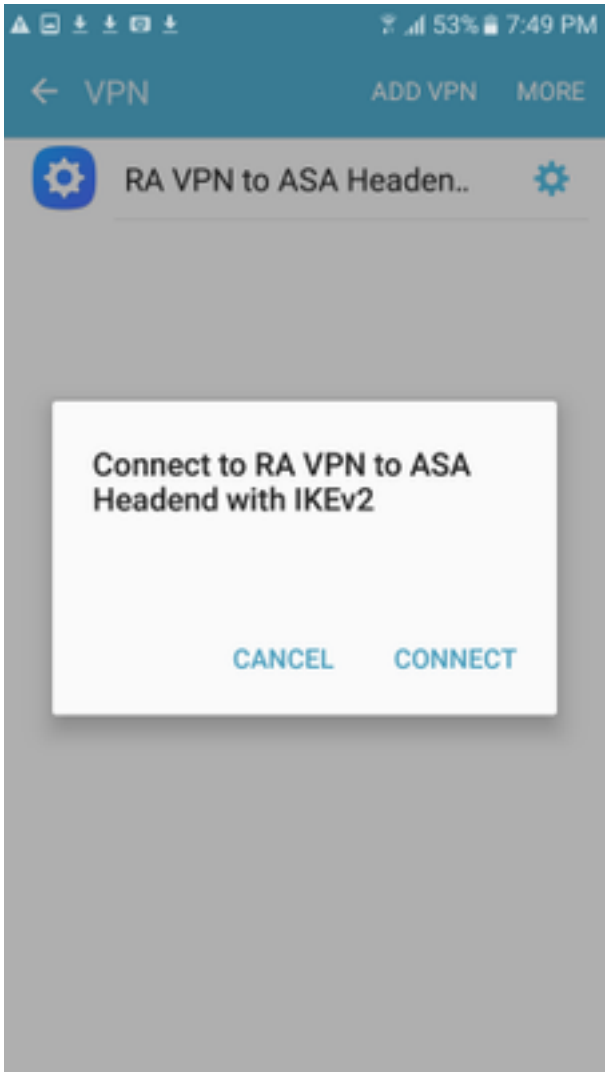
Paso 2. Seleccione **VPN**

Paso 3. Seleccione **Add VPN**. Si la conexión ya se ha creado como en este ejemplo, pulse el icono del motor para editarla. Especifique IPSec IKEv2 RSA en el campo **Type**. La **dirección del servidor** es la dirección IP de la interfaz ASA habilitada para IKEv2. Para el **certificado de usuario IPSec** y el **certificado de CA IPSec**, seleccione los certificados instalados pulsando en los menús desplegables. Deje el **certificado de servidor IPSec** con la opción predeterminada, Recibido del servidor.

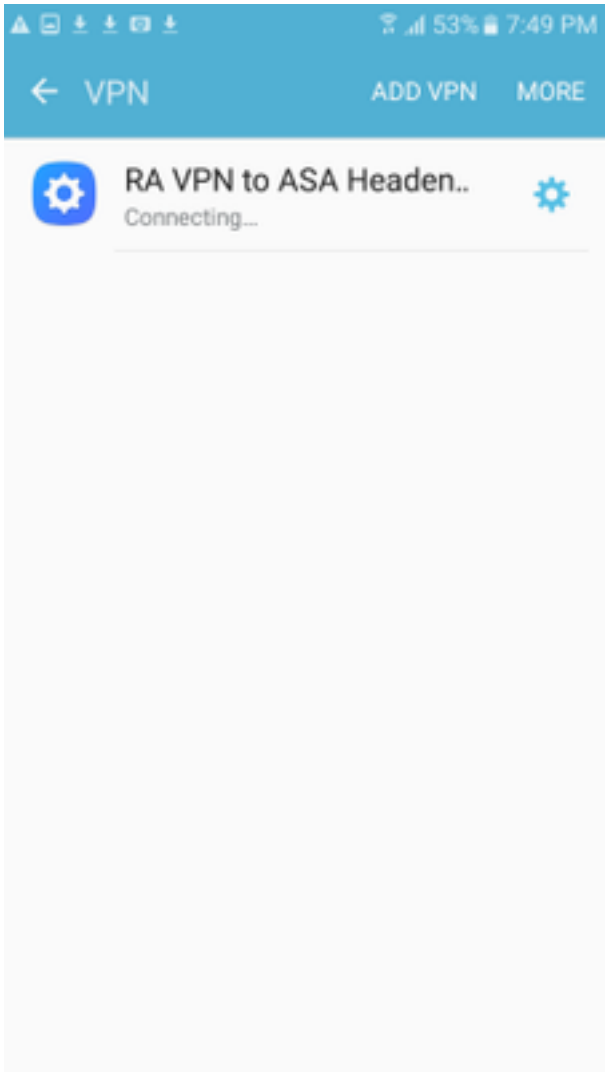

53% 7:49 PM
VPN
ADD VPN
MORE
RA VPN to ASA Headen..

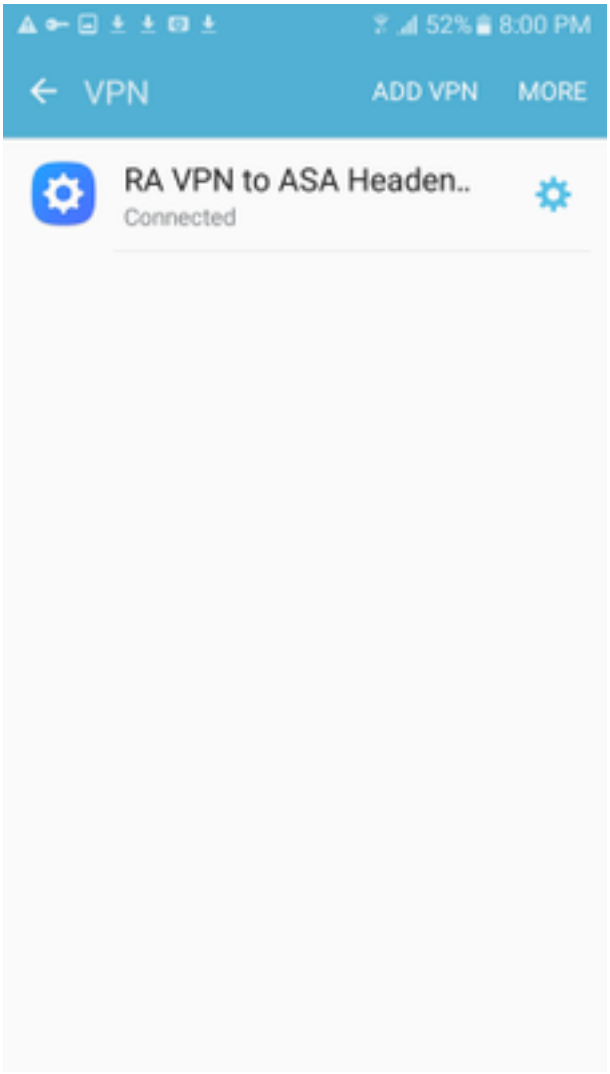


Paso 4. Seleccione **Save** y luego toque el nombre de la nueva conexión VPN.

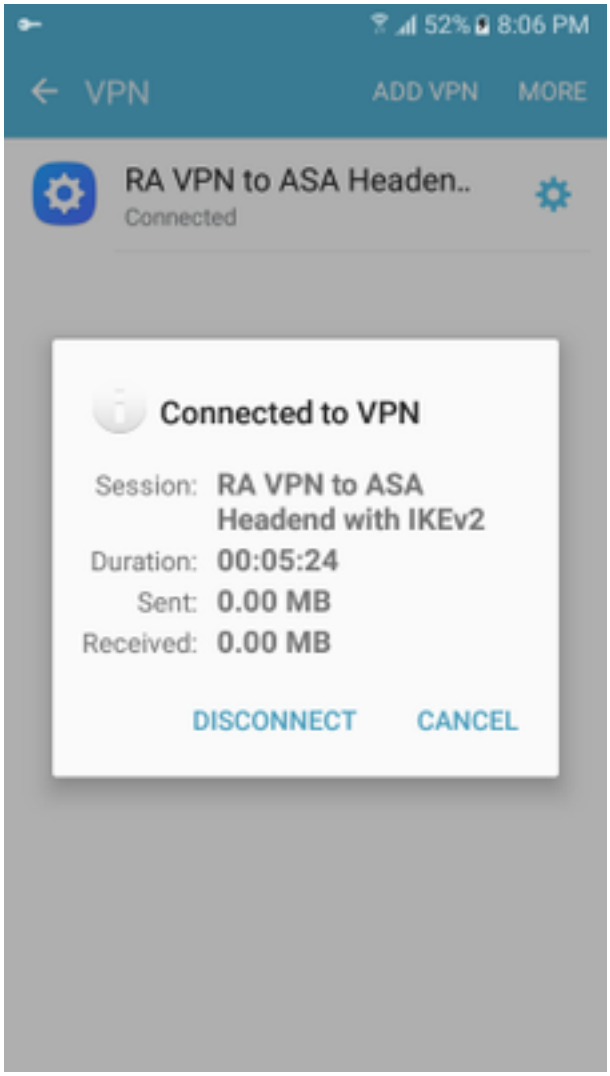


Paso 5. Seleccione **Connect (Conectar).**


53% 7:49 PM
VPN
ADD VPN
MORE
RA VPN to ASA Headen..
Connecting...



Paso 6. Escriba la conexión VPN una vez más para verificar el estado. Ahora se muestra como **Conectado**.



Verificación

Comandos de verificación en la cabecera ASA:

```
ASA#show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username     : Win7_PC.david.com      Index        : 24
Assigned IP  : 192.168.50.1           Public IP    : 10.152.206.175
Protocol     : IKEv2 IPsec
License      : AnyConnect Premium
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 16770
Pkts Tx      : 0                      Pkts Rx      : 241
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GP_David               Tunnel Group : David
Login Time   : 08:00:01 UTC Tue Jul 18 2017
Duration     : 0h:00m:21s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a0a0a0100018000596dc001
Security Grp : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1
IKEv2:
  Tunnel ID    : 24.1
```

```
  UDP Src Port : 4500                   UDP Dst Port : 4500
  Rem Auth Mode: rsaCertificate
  Loc Auth Mode: rsaCertificate
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86379 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  :
IPsec:
  Tunnel ID    : 24.2
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 192.168.50.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28778 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Conn Time Out: 518729 Minutes         Conn TO Left : 518728 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 16947
  Pkts Tx      : 0                      Pkts Rx      : 244

ASA# show crypto ikev2 sa
IKEv2 SAs:
Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id                Local                Remote     Status         Role
2119549341    10.88.243.108/4500   10.152.206.175/4500      READY    RESPONDER      Encr: AES-
CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: RSA
      Life/Active Time: 86400/28 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.50.1/0 - 192.168.50.1/65535
          ESP spi in/out: 0xbfff64d7/0x76131476
ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: Anyconnect, seq num: 65535, local addr: 10.88.243.108
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.50.1/255.255.255.255/0/0)
      current_peer: 10.152.206.175, username: Win7_PC.david.com
      dynamic allocated peer ip: 192.168.50.1
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 339, #pkts decrypt: 339, #pkts verify: 339
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.88.243.108/4500, remote crypto endpt.: 10.152.206.175/4500
      path mtu 1496, ipsec overhead 58(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 76131476
      current inbound spi : BFFF64D7
    inbound esp sas:
      spi: 0xBFFF64D7 (3221185751)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={RA, Tunnel, IKEv2, }
         slot: 0, conn_id: 98304, crypto-map: Anyconnect
         sa timing: remaining key lifetime (sec): 28767
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
```

```
    outbound esp sas:
      spi: 0x76131476 (1980961910)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={RA, Tunnel, IKEv2, }
         slot: 0, conn_id: 98304, crypto-map: Anyconnect
         sa timing: remaining key lifetime (sec): 28767
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
ASA#show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                   Status : Capacity : Installed :  Limit
                                  ----------------------------------------
AnyConnect Premium               :  ENABLED :       50 :        50 :   NONE
AnyConnect Essentials            : DISABLED :       50 :         0 :   NONE
Other VPN (Available by Default) :  ENABLED :       10 :        10 :   NONE
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     :  ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   :  ENABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                         Local : Shared :   All  :   Peak :  Eff.  :
                         In Use : In Use : In Use : In Use :  Limit : Usage
                        ---------------------------------------------------
AnyConnect Premium     :      1 :      0 :      1 :      1 :     50 :    2%
  AnyConnect Client    :                :      0 :      1          :    0%
    AnyConnect Mobile  :                :      0 :      0          :    0%
  Clientless VPN       :                :      0 :      0          :    0%
  Generic IKEv2 Client :                :      1 :      1          :    2%
Other VPN              :                :      0 :      0 :     10 :    0%
  Cisco VPN Client     :                :      0 :      0          :    0%
  L2TP Clients
  Site-to-Site VPN     :                :      0 :      0          :    0%
----------------------------------------------------------------------------
ASA# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client            :      0 :         11 :           1 :        0
  SSL/TLS/DTLS               :      0 :          1 :           1 :        0
  IKEv2 IPsec                :      0 :         10 :           1 :        0
Generic IKEv2 Remote Access  :      1 :         14 :           1
----------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :     25
Device Total VPN Capacity    :     50
Device Load                  :     2%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
```

```
                                  ---------------------------------------------
IKEv2                             :      1 :          25 :                1
IPsec                             :      1 :          14 :                1
IPsecOverNatT                     :      0 :          11 :                1
AnyConnect-Parent                 :      0 :          11 :                1
SSL-Tunnel                        :      0 :           1 :                1
DTLS-Tunnel                       :      0 :           1 :                1
-------------------------------------------------------------------------------
Totals                            :      2 :          63
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

> **Nota:** Consulte Información Importante sobre los Comandos Debug antes de utilizar los comandos debug.

> **Precaución**: En ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, la verbosidad de las depuraciones aumenta. Haga esto con precaución, especialmente en entornos de producción.

- **Debug crypto ikev2 protocol 15**
- **Depurar la plataforma crypto ikev2 15**
- **Debug crypto ca 255**