VPN RA ASA IKEv2 avec clients VPN Windows 7 ou Android et configuration de l'authentification des certificats

Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Aperçu Configurer l'autorité de certification Générer un certificat client Installer le certificat d'identité sur l'ordinateur client Windows 7 Comment installer le certificat d'identité sur votre appareil mobile Android Configurer la tête de réseau ASA pour RA VPN avec IKEv2 Configurer le client intégré de Windows 7 Configurer le client intégré de Windows 7 Configurer le client VPN natif Android Vérification Dépannage

Introduction

Ce document décrit comment configurer Cisco Adaptive Security Appliance (ASA) Version 9.7.1 et ultérieure afin de permettre aux clients VPN natifs de Windows 7 et Android (réseau privé virtuel) d'établir une connexion VPN d'accès distant avec l'utilisation du protocole IKEv2 (Internet Key Exchange Protocol) et des certificats comme méthode d'authentification.

Avec la collaboration de David Rivera et Cesar Lopez Zamarripa, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Autorité de certification (CA)
- Infrastructure à clé publique (PKI)
- VPN RA avec IKEv2 sur ASA
- Client VPN intégré Windows 7
- Client VPN natif Android

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CISCO1921/K9 15.5(3)M4a en tant que serveur CA IOS
- ASA5506X 9.7(1) en tant que tête de réseau VPN
- Windows 7 comme ordinateur client
- Galaxy J5 Android 6.0.1 en tant que client mobile

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Aperçu

Voici les étapes à suivre pour configurer les clients VPN natifs Windows 7 et Android afin de se connecter à une tête de réseau ASA :

Configurer l'autorité de certification

L'autorité de certification permet d'incorporer l'utilisation de clé étendue (EKU) requise dans le certificat. Pour la tête de réseau ASA, l'unité EKU d'authentification du serveur de certificats est requise, tandis que le certificat client nécessite l'unité EKU d'authentification du client.

Plusieurs serveurs CA peuvent être utilisés, notamment :

- Serveur Cisco IOS CA
- Serveur OpenSSL CA
- Serveur Microsoft CA
- 3^{troisième} CA des parties

IOS CA Server est utilisé pour cet exemple de configuration.

Cette section décrit la configuration de base permettant à un CISCO1921/K9 avec la version 15.5(3)M4a de fonctionner en tant que serveur AC.

Étape 1. Assurez-vous que le périphérique et la version prennent en charge la commande 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

Étape 2. Activez le serveur HTTP sur le routeur.

IOS-CA(config)#ip http server Étape 3. Générez une paire de clés 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)

Etape 4. Configurez un point de confiance.

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>

Note: L'adresse IP de la commande d'inscription est l'une des adresses IP configurées par le routeur pour une interface accessible.

Étape 5. Authentifiez le point de confiance (Obtenir le certificat de l'autorité de certification).

```
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.
Etape 6. Inscrivez le point de confiance (Obtenez le certificat d'identité).
IOS-CA(config)#crypto pki enroll <HeadEnd>
8
% 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
```

```
Étape 7. Vérifiez les certificats.
```

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: A000000
     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: 8600000
     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
```

Étape 8. Exportez le point de confiance HeadEnd vers le terminal au format PKCS12 pour obtenir le certificat d'identité. Le certificat de l'autorité de certification et la clé privée sont ajoutés dans un seul fichier.

<cisco123>

Exported pkcs12 follows:

MIIL3wIBAzCCC5kGCSqGSIb3DQEHAaCCC4oEqquGMIILqjCCC34GCSqGSIb3DQEH BqCCC28wqqtrAqEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz Fa6tZyACAQGAggs4qNTJi7l/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74qYMU5NJwtOVsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+qnNZLWs3eU1n84rryZq5Pjw3MRTu2yXDvr799qvx7NIZH5yUZyV11T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg VbYsR+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFqJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0dilrvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3HlHCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7LOlCeUcVDM8aQfy HJSPk/VmfQ0lXwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/XOkEvp3SqOkLQZiCzZ20iMWUTWX1XfqrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0qzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAilrYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd121HurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD5l+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9qnMqMJmikP2qhqOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/clNsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD416VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGgX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6egZSOSjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHISA92pplS7VFrAWP65wrhs4XOf4YSFlM89Sn4 GD/yEsGVJzwGrxgCNnOZkLIKsFbI0jp2lMps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/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. Étape 9. Créez un point de confiance vide sur l'ASA.

ASA(config)# crypto ca trustpoint <HeadEnd> DRIVERAP(config-ca-trustpoint)# exit Étape 10. Importer le fichier 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 ${\tt BqCCC28wggtrAgEAMIILZAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIocGz}$ Fa6tZyACAQGAggs4qNTJi71/f0IvQr8n1c/SCeaSYRLBvcY9yPgJ2K2/Nmu9+KNB 3dAoYkCrGwDdfpobJE0XqBpIE1uBOtAeF7zdFJt/Pgpie4fcqpCVIbDXG8Ansmhj v0j6W9Z/IJHe7JrENatbi4nhTnCDP79Z65QSkzrb9DenkCGjoQsWP9zLHTiCDNzV ajMlWFuCFb0wSW/6L73BLTjS7rwtE74gYMU5NJwt0VsJM2LdwuQ+iOnpsnp6q9fu niUFEutPe8imOCRApe0tpPqhDp74hKziKT8JEsQ8HMO/lX1y/LIXdLISnz1nkoN3 vxD4AMGRFYACPH8PiGcVSx+vD+wmNaHp1vAOrq4pS7ZQ37ko4mFudnftdOUzaPIz EzTrOwlRE6il/gF8vb14EfeR09vumJBsajF12hrFGugIJTZnElp5go+oHEEAo4Y+ Yhoj/MIOyhZzo3/ujhjKqtsAJXybYF9YqVkTee9u4Xjkcsg5AmbaqeUUfd7Q8CC2 bi39S1maoWbTYiNcHFs/bWKWJsgZwPzfWtmPch/8MNvXn46AJAwIwRQjHruuFE9F bhv7SRhYSRQZPf7j1PTmJuMkKA3AzjdbmmJuLidbX3yKbTt4PxPMusbv+ojc6Nam RCsRf7+gnNZLWs3eU1n84rryZg5Pjw3MRTu2yXDvr799gvx7NIZH5yUZyVl1T70b eC4KbflcmpM6mJ2UVnaoP2N5u892m41BWuk9rt5isl2f/Z/ZuSbkFaxzU0456zSg Vbysr+51XfQEH5xu88E5EUPWZ86YdUS1bD8ky6WOn0M104K6rNDLkgwXcxw3CaZ8 zhao+dE3qoEYWaKPgCQzPqW0BW3y7WSIELug2uSEsXQjIQcF+42CX6RA3yCmy2T8 C+osKlSSao0nzjrlpTWnPiFss9KRFgJDZhV2ItisiALNw9PqruddcmYtw44LXvdc +OfnyRvuLS6LE/AMmGk0GaVetAXPezD+5pVZW13UMT/ZdzUjLiXjV9GzF6V8i8qN Ua0MbDEa8T5Le4dCigaA+t1QxQ0PGb+w0ZAQzWN4gZpSEk3ejRixOt14SU5ivj/O lGXNn8Fvebk42CHohjXG9fq/IfbsVWSkxn2OZ/fhXkZztv4ic1VgprgJURjCtcBw 9Qp/ONda+9aDHiSBrKeHC/urgX6rgWXv9+hpRKIRfj3b8WE+N1sivuQEjlWxbD7h 9fpwxXb+/i7HisjzSkOWUNw4lyulfYSiOv86FPWK0H9Vjbg0G0di1rvGZ8uJHQCC 77RLFXp4jrvCgeo4oWKQbphgPAng7rT794vMwq0rYOb4D3H1HCUvU3JJmScDJQy2 zQxbG2q8Htm44COOuJEUBzx1ImayH2XvDck6VmLTGn8XH5Vq7L0lCeUcVDM8aQfy HJSPk/VmfQ01XwPIaxxYlr+jOpcorFkH+OH04hz07grAsGyLRoFICTEvHAzVnF0X 2A1j/z/BFAPG86ssAtInRZVeYUS72NwPEtpKmlHZnl+2iWno5iwTZgtjv7oREZKE RE6m708RiPSD2RjjamCmmmnH5dK5wxF7YlleK/+ZVrfwLecEPRl+eVw0isM/JN/a WmkZkCcVMx/ec1P8jp8LzCx17HgVNYbg9lsiffD4xo0G/k0QLUlpliAt7LA2BeGs yl55wtYUcOBH0/Es39yWnm2Ea//IK6BLw98PvU90vkXWwiD3ajFmcHmssDeU/tZR 4KKNuNor7Le9ycXZFM9ofKZ6AIJ9A1AYvOyhG088voq8MMGXEe/q+DIjaVE1htYu k0ELmYAD/X0kEvp3Sq0kLQZiCzZ20iMWUTWX1XfgrfLEH0utwHTyr3J2vQk5CD37 ZAfsF6zxEvtU2t41J0e90jWJw9WtWnnS0gzLeXWtW3H0YAIw3QodKNzbaY4eLP4y BEdsLmWbM4eza0m9BoZOmMUSkhvFrEz5Q5X5r9vCuAilrYDqyIjhgdme56tVV0Vg ZauhbNX59PQQzwOdIZJVVL5tgjf0h7XCm90Bsqd12lHurCCmHy7kM5pqf0MMlhH7 oM/DhXdTU+1sEabt/9c2qs1ihJLS1Zaw2q1AaS5h00+xL8Lxwh2/1/R7Q8FferhR QZDpix+CmtakRu7uPOMa0zsyOko3P9mf74AWDrThAwMA6G238TC6XI1vrXhvEX11 BVplQq0Wh/p7ZorSjD51+z7TkXmJNp7iIxAqp0yobC6vOBwQP7/QAs88q9JNSAte ErdCXoizvs8YmZMoEap948oplYFaIP+xCnCr8l3v7znwfZwTMQPoPvqEFqUmWYgt xkJ0qaE645ihTnLgk4eglsBLslwPR1RJU+t6kGGAUmxqhPFxb3/1xNRPVzOGn12w S9yw+XLC6kS4PmKoxkxax4nnCx7s3e7B5e0qmYtgRTJ0GuW7Uf+T3royT0uYm0d+ ik6bmxcn00qdcHtt2HTbI+kYpken3YrF0h9Jnm9ZKT63gQSqQWL800ZVd4dAZceg FciNKs9r26fyy+L3rGCh+U9TLf6mNuWu8RstjjIGPHEPKZ9qnMqMJmikP2qhqOAd XVhs6ashXx33bZ9dIuhRx6uTNMrppsXyg6SxUyeGDYhpxsPt7uRwBswOpi6iDMZn ISSzQjrkxoNwwOfn8705fTCLhHlTZa8HS5HMK3KE7LiZv9pa1z6KTo4z+LCQSLDy FoRJhSaEsCYJsLDS5nYBoR8hE/eMvQDX1f+RZBrJDcftxx7FQ+8RtvHSJRcJK9N/ Ph/pL62NBlSbvCfn1AbisKrbbgCVLOSj/doufPvpMT2UDL0TY8UnQiyWMH1MF3tZ jJy6Si2glLwA9hu/c1NsREbA0gxMTjAREb5BjAUmlc3fuv2DWpwnkwyZNyHdm9B9 TPRoByGPvSZXa8MwY/8DUEwUQEsfDJi5jlAD4I6VFFUB72ZS7wn/mVR02fPkfOMp 3yhnGqX29OaDDiDlKw1Xwj1NybOhpZ6unDo5J3stMxlbv5TYL2Tl6eqZS0SjsLmn cj5zkyUU22/93E5vfKD1CMiXx9/e4j2rRh3QCIXqaCjC9acTJ8a/k9/bp8Nz5Cir pnaCbuQsvna92nxVUqcmLlSbVIvGqlH9qm4DurhcLh59j20tX6K8AMJ90+azaYbX AJV/MCElhJg6wcN8QnCHMhiuK9+zpsUK2FQgfbcgaaNe3xGaXuoOIGQmlbAGtEkp kuauRzQ8/pwszaZuPh/5rE77z8zMut3+0E5CslB9npzNi0b0itaaRl13bBBml1xn r6SBUw7AWapZwRx6pihvptLJaqU1IzaV5SWk0zTABR7BmR84L0+/8v/bedcPSioG ecside21F6CcW05ywABBxDYQXM1P9qkC/2bkPkEJ0jB15P5L1+Yqb8hTlone/InR B8ktEd8+QW8o60h0seONXumTqBfAuNBkprOA3ssXLeEGB0IpeC5oGW+VSziyS9id zYq8WaehpAIf3pqwn8gsi0B/wd57T0KK91+v0Ei4z+yIdu8Kh9GTiqGvgNAeakgr ECDiXoKAwltYAn7cLKNpZaojSs2Jt+60oBA5crT04Mtgpjb9Pd/DLqWQDJTyoRVv cJRb68a0yZvVBU0yoLbox84QKLHISA92pplS7VFrAWP65wrhs4X0f4YSF1M89Sn4 GD/yEsGVJzwGrxqCNnOZkLIKsFbIOjp21Mps5jVKoFfpPJCie3F2FB3ecS+xRpHo 5u2KOTmH0rFQ6Vu+JYCo/qWh0ERtL/8gczP7C9ehiaZfemw2bq9xrUo+6y3H9Q+Z LADwMlAkI+kzbng3R+fj4AYBvf8GTJdpBs8s/t7mZXHiXCtH6qxTMRWJx5Xuxs9F I8Ii8TA9MCEwCQYFKw4DAhoFAAQUj0/On/REYODupznP9SwYnFX92BYEFESx1MSa ho3Cv1cZYM0TzZEzlsKdAqIEAA==

quit

INFO: Import PKCS12 operation completed successfully

Étape 11. Vérifiez les informations de certificat.

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

Générer un certificat client

Étape 1. Générez une paire de clés 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
fit = 2.2 for the seconds

Étape 2. Configurez un point de confiance.

```
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>
```

Etape 3. Authentifiez le point de confiance configuré (Obtenir le certificat de l'autorité de certification).

```
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.
```

Étape 4. Inscrivez le point de confiance authentifié (Obtenir le certificat d'identité).

```
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
Étape 5. Vérifiez les informations des certificats.
```

```
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: A000000
     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
        date: 13:24:35 UTC Jul 12 2020
    end
 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: 8600000
     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
```

Installer le certificat d'identité sur l'ordinateur client Windows 7

Étape 1. Exportez le point de confiance Win7_PC nommé vers un serveur FTP/TFTP (installé sur votre ordinateur Windows 7) au format PKCS12 (.p12) pour obtenir le certificat d'identité, le certificat d'autorité de certification et la clé privée dans un seul fichier.

```
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.
```

Voici l'aspect du fichier exporté sur une machine cliente.

						×
Search Re	sults in TFTP-Root 🕨			✓ ✓ Win7_PC		×
Organize 👻 Save searc	:h				•	0
★ Favorites ★ Favorites ★ Recent Places ★ Decision	Win7_PC C:\TFTP-Root		Type: Personal Information Exch	Date modified: 7/13/2017 9:01 Size: 2.97 KB	AM	
Downloads	Search again in: [] Libraries II Computer	F Custom 💿 Internet	File Contents			
 ☐ Libraries ☐ Documents J Music ☐ Pictures ☐ Videos 						
I單 Computer 을 os (C:)						
🙀 Network						
) 1 item						

Étape 2. Appuyez sur Ctrl + R et tapez mc pour ouvrir Microsoft Management Console (MMC).



Étape 3. Sélectionnez OK.

🚡 Console1 - [Console Root]			
File Action View Favorites Wind	dow Help		_ <i>8</i> ×
Console Root	Name		Actions
		There are no items to show in this view.	Console Root
			More Actions
	11		,

Étape 4. Accédez à Fichier>Ajouter/Supprimer un composant logiciel enfichable.

🚡 Console1 - [Console Root]			X
🔚 File Action View Favorites Wind	dow Help		_ 8 ×
🗢 🔿 🔲 🗟 🚺)	
Console Root	Add or Remove Snap-ins	Actions	
	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	Console Root	^
	Available snan-ins: Selected snan-ins:	More Actions	•
	Snap-in Vendor A Edit Extensions		
	Control Microsoft Cor		
	Certification Manager Microsoft Cor		
	Component Services Microsoft Cor Move Up		
	Move Down		
	Book Management Microsoft and		
	Event Viewer Microsoft Cor		
	Folder Microsoft Cor		
	P Security Monitor Microsoft Cor		
	B IP Security Policy M Microsoft Cor		
	Advalceu		
	Description: The ActiveX Control ency is eaching you to add as MMC ands with a concilibution contribution on ActiveX control		
	The Actives control shapen endoles you to add an electrode with a results view containing an Actives control.		
	OK Cancel		
		JI	
	И		

Étape 5. Sélectionnez Certificats > Ajouter > Compte d'ordinateur.

Console1 - [Console Root]	
	<u> </u>
Console Root Name	Actions
	Console Root
Add or Remove Snap-ins	More Actions
You can select snap-ins for this console from those available on your computer and configure the selected services by you can configure which extensions are enabled. Certificates snap-in Available snap-ins: Selected snap-ins: This snap-in will always manage certificates for: Active X Control Microsoft Cor Console Root My user account Computer Manager Microsoft Cor Add > Selected snap-ins: This snap-in will always manage certificates for: Device Manager Microsoft Cor Add > Computer Microsoft Cor Or power account Disk Management Microsoft Cor Add > Computer account Computer account Disk Management Microsoft Cor Add > Computer account Computer account Disk Management Microsoft Cor Add > Computer account Computer account Disk Management Microsoft Cor Add > Computer account Computer account Disk Management Microsoft Cor Core policy Object Microsoft Cor Computer account Discription: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, < Back	Next > Cancel

Étape 6. Sélectionnez Suivant,

Console Root			Actions	
Add or Remove Snap-ins You can select snap-ins for this console from those available on yo extensible snap-ins, you can configure which extensions are enable Available snap-ins, you can configure which extensions are enable Available snap-ins; Snap-in Vendor ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Component Services Microsoft Cor Device Manager Microsoft Cor Device Manager Microsoft Cor Folder Microsoft Cor IP Security Monitor Microsoft Cor IP Microsoft Cor IP Security Monitor Microsoft Cor IP Security Mo	ur computer and configure the sele ed. Selected snap-ins: Console Root	Cto Interference Provide Prov	Actions Console Root More Actions	

Étape 7. Terminez.

Console1 - [Console Root]		
🚡 File Action View Favorites Win	ndow Help	_ <i>6</i> ×
Console Boot	News	Actions
	Name	Actions
	Add or Remove Snap-ins	Console Root
	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins; you can configure which extensions are enabled. Available snap-ins: Snap-in Vendor ActiveX Control Microsoft Cor Computer Microsoft Cor Computer Managem. Microsoft Cor	More Actions
	Event Viewer Microsoft Cor Folder Microsoft Cor foroup Policy Object Microsoft Cor F Security Policy M Microsoft Cor P Security Policy M Microsoft Cor Link to Web Address Microsoft Cor Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. OK Cance	

Étape 8. Sélectionnez OK.

Étape 9. Accédez à **Certificates (Local Computer)>Personal>Certificates**, cliquez avec le bouton droit sur le dossier et accédez à **All Tasks>Import** :

_										
Console1 - [Console Roo	ot\Certificates (Loo	al Computer)\Pe	ersonal\Certificates]							
🚡 File Action View	Favorites Wind	ow Help								_ 8 ×
🗢 🔿 🖄 📰 📋	o 🔒 🛛 🖬									
🧮 Console Root		Issued To	^	Issued By	Expirati	on Date	Intended Purposes	Friendly Na	Actions	
4 🗐 Certificates (Local C	Computer)	DRIVERAP-6	KUZH	DRIVERAP-6KUZH	7/13/20	22	<all></all>	<none></none>	Certificates	
⊿ Personal									More Actions	•
Trusted Ro	All Tasks	•	Request New	Certificate						
Enterprise	View		Import							
▷ Intermediar▷ Intermediar▷ Intermediar	New Window fro	m Here	Advanced Operations							
 Untrusted (Third-Party 	New Taskpad Vie	ew								
Trusted Per	Refresh									
Other Peop	Export List									
 Ams CanaryCert 	Help									
InjectorCertStore	e		-							
McAfee Trust										
Poincycentstore Remote Desktop	,									
Certificate Enrol	Iment Requests									
D Smart Card Trus	ted Roots									
SPC Trusted Devices										
		4								
Add a certificate to a store		•						•	1	

Certificate Import Wizard



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

	< Back	Next >	Cancel
	- C Duck	- next /	Cancer

Étape 10. Cliquez sur Next (Suivant). Indiquez le chemin d'accès au fichier PKCS12.

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
File name:	
C:\TFTP-Root\Win7_PC.p12 Browse	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange-PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cano	el

Étape 11. Sélectionnez **Suivant** à nouveau et tapez le mot de passe entré dans la commande *crypto pki export <Win7_PC> pkcs12 <tftp://10.152.206.175/ Win7_PC.p12> password <cisco123>*

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
 Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about <u>protecting private keys</u>
< Back Next > Cancel

Étape 12. Sélectionnez Suivant.

Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Place all certificates in the following store Certificate store:	
Personal Browse	
Learn more about <u>certificate stores</u>	
< Back Next > Cance	ł

Étape 13. Sélectionnez Suivant une fois de plus.



Étape 14. Sélectionnez Terminer.

Certificate Import Wizard	
The import was successful.	
ОК	

Étape 15. Sélectionnez **OK**. Vous verrez maintenant les certificats installés (le certificat CA et le certificat d'identité).

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							
🚡 File Action View Favorites Wind	ow Help						_ 8 ×
🗢 🔿 🖄 🗔 📋 🙆 🛃 🗊							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
Certificates (Local Computer)	calo_root	calo_root	7/12/2020	<all></all>	cn=calo_ro	Certificates	^
Certificates	DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	More Actions	•
Trusted Root Certification Author	Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati	cn=Win7_P		
Enterprise Trust							
Intermediate Certification Author							
Trusted Publishers							
Untrusted Certificates Third-Pathy Root Certification Aut							
Trusted People							
Other People							
Ams							
CanaryCertStore							
InjectorCertStore							
McAtee Trust PolicyCertStore							
Remote Desktop							
Certificate Enrollment Requests							
Smart Card Trusted Roots							
SMS							
SPC							
Finisted Devices							
	•	m			۱.		
Personal store contains 3 certificates.							

Étape 16. Faites glisser et déposez le certificat CA à partir de **Certificates (Local Computer)>Personal>Certificates** vers **Certificates (Local Computer)>Trusted Root Certification Authority>Certificates.**

🚰 Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]							
🚡 File Action View Favorites Wind	ow Help						- 8 ×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly ^	Actions	
Certificates (Local Computer) Personal	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati	The USE	Certificates	^
Certificates	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati	DigiCert	More Actions	•
Trusted Root Certification Author	calo_root	calo_root	7/12/2020	<all></all>	cn=calo	and a second	
Certificates	Certum CA	Certum CA	6/11/2027	Server Authenticati	Certum	calo_root	
Enterprise Trust	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati	Certum =	More Actions	•
Intermediate Certification Author	Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>		
Trusted Publishers	Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Untrusted Certificates	Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>		
Third-Party Root Certification Aut	Cisco Root CA M2	Cisco Root CA M2	11/12/2037	<all></all>	<none></none>		
Trusted People	Cisco RXC-R2	Cisco RXC-R2	7/9/2034	<all></all>	<none></none>		
Other People	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Secure Email, Client	VeriSign		
Ams	COMODO RSA Certification Au	COMODO RSA Certification Auth	1/18/2038	Server Authenticati	COMOE		
CanaryCertStore	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microso		
InjectorCertStore	Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serve	Deutsch		
McAfee Trust	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati	DigiCert		
PolicyCertStore	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati	DigiCert		
Remote Desktop	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Server Authenticati	DigiCert		
Certificate Enrollment Requests	🛱 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>		
Smart Card Trusted Roots	DRIVERAP-6KUZH.cisco.com	DRIVERAP-6KUZH.cisco.com	1/12/2021	<all></all>	<none></none>		
▷ SMS	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
SPC	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
Fusted Devices	Entrust Root Certification Auth	Entrust Root Certification Authority	11/27/2026	Server Authenticati	Entrust		
	Entrust Root Certification Auth	Entrust Root Certification Authori	12/7/2030	Server Authenticati	Entrust.		
	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Server Authenticati	Entrust		
< >	Fouries Secure Certificate Auth	Fauifay Secure Certificate Authority	8/22/2018	Service Emsil Serve	GenTrue		
Trusted Root Certification Authorities store co	ntains 60 certificates.						

🚡 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]								
🖀 File Action View Favorites Window Help								
🗢 🤿 🖄 🔂 📋 🙆 🔂 🖬								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions		
Certificates (Local Computer)	2 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	Certificates	^	
Certificates	Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati	cn=Win7_P	More Actions	•	
a 🚞 Trusted Root Certification Author								
Certificates								
Enterprise Trust Intermediate Certification Author								
Trusted Publishers								
Untrusted Certificates								
Third-Party Root Certification Aut								
Trusted People								
Ams								
CanaryCertStore								
InjectorCertStore								
McAfee Trust								
PolicyCertStore								
Certificate Enrollment Requests								
Smart Card Trusted Roots								
SMS								
▷ C								
Trusted Devices								
<	•				۶.			
Personal store contains 2 certificates.								

Comment installer le certificat d'identité sur votre appareil mobile Android

Note: Android prend en charge les fichiers de magasin de clés PKCS#12 avec l'extension .pfx ou .p12.

Note: Android prend uniquement en charge les certificats SSL X.509 encodés en DER.

Étape 1. Après l'exportation du certificat client à partir du serveur AC IOS au format PKCS12 (.p12), envoyez le fichier au périphérique Android par e-mail. Une fois que vous l'avez, effleurez le nom du fichier pour démarrer l'installation automatique. (**Ne pas télécharger le fichier**)

🗆 🖬 🛓			r af 531	6 8 7:24	PM
÷		•		\simeq	÷
-					
					.
					1
					e.
A	ndroid_Smartp	hone.p12	2 ±	≙	
Reply	Re	(ply all		➡ Forward	

Étape 2. Entrez le mot de passe utilisé pour exporter le certificat, dans cet exemple, le mot de passe est **cisco123**.

Extract certificate
Enter the password to extract the certificates.
CANCEL OK

Étape 3. Sélectionnez **OK** et saisissez un **nom de certificat**. Il peut s'agir de n'importe quel mot, dans cet exemple, le nom est **Android ID Cert**.



Étape 4. Sélectionnez **OK** et le message "Android ID Cert installé " s'affiche.

Étape 5. Afin d'installer le certificat d'autorité de certification, extrayez-le du serveur d'autorité de certification IOS au format base64 et enregistrez-le avec l'extension .crt. Envoyez le fichier à votre périphérique android par e-mail. Cette fois, vous devez télécharger le fichier en tapant sur la flèche située en regard du nom du fichier.

⊟ ±		7 🛋 51	6:54	PI
-			\simeq	:
calo_ro	oot.crt	<u>+</u>	۵	
*	~		*	
Deplu	Reply all		Forward	

6:54 PM Tue, July 18	۰ م
🔶 🔍 🔹	⊗ 🛞
Wi-Fi Location Sound	Auto Bluetooth rotate
*	Outdoors
calo_root.crt Download complete.	6:54 PM
NOTIFICATION SETTINGS	CLEAR
-	
and the second second	
_	
calo_root.crt	± ۵
Reply Reply all	# Forward
Emergency calls	only

Étape 6. Accédez à **Paramètres** et **Verrouillage, écran et sécurité.**



Étape 7. Sélectionnez Autres paramètres de sécurité.

⊡ ±	7 🖬 50%	6:57 PM
← Lock s	creen and security	
Notification Show content	ns on lock screen	
Secure loc Set your secure and Lock insta	k settings e lock functions, such as Aut ntly with Power key.	o lock
Security		
Find My Mo Locate and co Samsung acco	obile ntrol your device remotely us unt.	ing your
Unknown s Allow installati other than the	ources on of apps from sources Play Store.	
Encrypt der Protect your de	vice evice by encrypting its data.	
Encrypt SD No SD card ins	card	
Other secu Change other s security update	rity settings becurity settings, such as tho es and credential storage.	se for

Étape 8. Accédez à Installer à partir du stockage de périphérique.

A 🖂 🖬 🛓

🕆 📶 54% 🛢 7:29 PM

Other security settings

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

Usage data access

View which applications can access your device's usage history.

Étape 9. Sélectionnez le fichier .crt et appuyez sur Terminé.

Select file	DONE
e calo_root-1.crt	

Étape 10. Entrez un **nom de certificat**. Il peut s'agir de n'importe quel mot, dans cet exemple, le nom est **calo_root-1**.



Étape 10. Sélectionnez **OK** et vous verrez le message " calo_root-1 " installé.

Select file	
C calo_root-1.crt	
calo_root-1 installed.	

Étape 11. Afin de vérifier que le certificat d'identité est installé, accédez à **Paramètres/Verrouiller** l'écran et Sécurité/Autre > Paramètres de sécurité/Certificats d'utilisateur/onglet Système.

A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

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

JII

Lloono data annon



Android_Smartphone.david.com

Étape 12. Pour vérifier que le certificat d'autorité de certification est installé, accédez à Paramètres/Verrouiller l'écran et sécurité/Autres paramètres de sécurité/Afficher les certificats de sécurité/onglet Utilisateur.

A = ± ± = ±

🖀 📶 54% 🖹 7:45 PN

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

JII

Lloono data annon

▲ 🗆 ± ± 🖾 ±	常 ⊿l 54% â 7:45 PM					
 View security certificates 						
SYSTEM	USER					
calo_root						

Configurer la tête de réseau ASA pour RA VPN avec IKEv2

Étape 1. Sur ASDM, accédez à **Configuration>Remote Access VPN > Network (client) Access> Anyconnect Connection Profiles**. Cochez la case **Accès IPSec (IKEv2), Autoriser l'accès** sur l'interface faisant face aux clients VPN (l'option **Activer les services client** n'est pas nécessaire).

Étape 2. Sélectionnez **Device Certificate** et supprimez la coche **Use the same device certificate for SSL and IPSec IKEv2**.

Étape 3. Sélectionnez le certificat de tête de réseau pour la connexion IPSec et sélectionnez Aucun pour la connexion SSL.

Cette option place la crypto ikev2, crypto ipsec, crypto dynamic-map et la configuration crypto map.

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254								
File View Tools Wizards Window Help							Type topic to search Go	ahaha
Home Configuration 🔯 Monitoring 🔚 S	ave 🔇 Refresh 🕻	Back 🔘 Forwar	rd 🦻 Help					CISCO
Remote Access VPN	Configuration >	Remote Access VPM	<pre>1 > Network (Client)</pre>	Access > AnyConnect	Connection Profiles			
2 Introduction			dentities Care An Ca			***	Interface shake The Class Art Connect 1001 C	
Part Retwork (Client) Access	IPsec (IKEv2) tur	nnel as well as SSL tunr	nel with Datagram Tran	sport Layer Security (DTLS) tunneling options.	me initial clent deployment requires end-user admin	is a sive rights. The cisco Anyconnect vervice	ient supports
AnyConnect Customization /Localization	Access Interfaces							
AnyConnect Client Profile	Enable Cisco	AnyConnect VPN Clien	nt access on the interfa	ces selected in the table b	wole			
AnyConnect Client Software Dynamic Access Policies	SSL access must	be enabled if you allow	v AnyConnect client to	be launched from a browse	r (Web Launch) .			
Group Policies		SSL Access		IPsec (IKEv2) Acces	s			
IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles	Interface	Allow Access	Enable DTI S	Allow Access	Enable Client Service	Device Certificate		
- Secure Mobility Solution	outside	Alloin Access	Endole Dites			Port Sattings		
Address Assignment	inside			m		For CSecongs		
Clientless SSL VPN Access								
Host Scan Image	Bypass interf	face access lists for inb	ound VPN sessions					
Secure Desktop Manager	Access lists from	group policy and user	policy always apply to	the traffic.				
Certificate Management Language Localization	Login Page Setting							
Load Balancing	Allow user to	select connection prof	file on the login page.	0				
DHCP Server	Shutdown po	rtal login page.						
Advanced	Connection Profiler							
	Connection prof	ile (tunnel aroun) speci	ifies how user is auther	nticated and other naramet	ers. You can configure th	he manning from certificate to connection profile he		
							<u>-</u>	
	Se Add	dit Delete Find:		Match Case				
	Name	SSL En	abled	IPsec Enabled	Alia	ases Authentication Metho	d Group Policy	
	DefaultRAGroup				V	AAA(LOCAL)	DfltGrpPolicy	
	DefaultWEBVPN	Group			√	AAA(LOCAL)	DfltGrpPolicy	
						Specify Device Certificate		— ×
B Davida Sahan						Device certificate is a digital certificate that ide	ntifies this ASA to the clients.	
Device Setup						Ise the same device certificate for SSI an	d IPsec IKEv2	
Firewall								
Remote Access VPN						Device Certificate for SSL Connection:	ne	•
						Device Certificate for IPsec Connection: Hear	dend:hostname=Connected_2_INET-B, cn=He	sadEnd.da 👻
Site-to-Site VPN	Let group UR	L take precedence if o	roup URL and certificat	e map match different con	nection profiles. Otherwis	54	Manage Certificates	
Device Management						ОК	Cancel Help	
»					Apply			

Voici l'aspect de la configuration sur l'interface de ligne de commande (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

Étape 4. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** pour créer une stratégie de groupe

p			
Carl Add Internal Group Policy			×
Add Internal Group Policy	Name: GP_David Banner: Inherit SCEP forwarding URL: Inherit Address Pools: Inherit IPv6 Address Pools: Inherit More Options Inherit Tunneling Protocols: Filter: Access Hours: Simultaneous Logins: Simultaneous Logins: Restrict access to VLAN: Connection Profile (Tunnel Group) Lock: Maximum Connect Time: Idle Timeout: Security Group Tag (SGT): On smart card removal: Periodic Certificate Authentication Interval	Inherit Clentless SSL VPN Clent IPsec IXEv1 IPsec IXEv2 LZTP/IPsec Vinherit	Select Select
Find:	Next Previous		
		OK Cancel Help	

Sur CLI.

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

Étape 5. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Address Pools** et sélectionnez **Add** pour créer un pool IPv4.

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254				
File View Tools Wizards Window Help			Type topic to search Go	aduate
Home 🍪 Configuration 🔯 Monitoring 🔲 Sa	ave 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help			cisco
Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access	s > Address Assignment > Address Pools		
Introduction I	Configure named IP Address Pools. The IP Address Pools ca dustering. Add v C Edit Delete Pool Name Starting Addr ACPool 192.168.50.1	In be used in either a VPN [Desc(IKEV.1) Connection Profiles, AnyConnect Conne ass Ending Address;Number of Addresses [192.156.50.100	ection Profiles, Group Policies configuration , or in <u>Interfaces</u> configuration Subnet Mask/Prefix Length 255:255:255:0	related to ASA
Gindress SSU VPI Access AdAlocal Users Analocal Users Advanced		Ending IP Address: 192.168.50.100		
Device Setup Device Setup Setup				
Device Management		Apply Reset		

ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0

Étape 6. Accédez à Configuration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles et sélectionnez Add pour créer un nouveau groupe de tunnels.




```
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
```

Etape 7. Naviguez jusqu'à Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy et cochez la case Used the configure rules to math a certificate to a Connection Profile.

tunnel-group-map enable rules

Étape 8. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules et créez une nouvelle carte de certificat. Sélectionnez Ajouter et associez-le au groupe de tunnels. Dans cet exemple, le groupe de tunnels est nommé David.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254					
File View Tools Wizards Window Help				Type topic to search Go	ababa
Home 🗞 Configuration 🔯 Monitoring 🔲 Sav	ve 💽 Refresh 🚺 Back 🔘 Forward 🢡 H	telp			CISCO
Remote Access VPN	Configuration > Remote Access VPN > Netwo	ork (Client) Access > Advanced > IPsec > Certifi	icate to Connection Profile Maps > Rules		
Introduction Introduction AnyConnect Connection Profiles AnyConnect Clent Profile AnyConnect Clent Profile AnyConnect Clent Software Oroup Policies Prose(UKEv) Connection Profiles Dese(UKEv) Connection Profiles Desecure Mobility Solution	Define rules to map certificates to desired AnyCon Certificate to Connection Profile Maps	nect or clentiess SSL connection profiles (tunnel groups	I). Use the bottom table to configure certificate fiel Mapped to Connection Profile	ds together with their matching criteria for the selecte	d rule.
- Op Address Assignment	Mapping Criteria				
Assignment Policy Assignment Policy Assignment Policy Assignment Policy Address Pools AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attribute AnyConnect AnyConnec	Add Add Add Add Add Add Add Configure a certificate Matching rule mapped will be ignored. Map: Priority: Mapped to Connection Pl	ing Rule atching rule and associate. It with a connection profile. T and assigns a priority to the rule with lower values havi Personal Centry and Centry and Centry and Centry New CERT_MAP Topile: Device Centry and Centry and Centry Centry Centry and Centry	the rule priority uniquely identifies the rg greater priority. Rules that are not	Value	
Site-to-Site VPN Device Management		A	pply Reset		

Sur CLI.

tunnel-group-map CERT_MAP 10 David

Étape 9. Sélectionnez Ajouter dans la section Critères de mappage et entrez ces valeurs.

Champ: Émetteur

Opérateur : Contient

Valeur: racine_calo

The Ver Took Variants Window Help Provide Contracted Variants	Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254		- - X
Image: Configuration	File View Tools Wizards Window Help	Type topic to search Go	alada
Confunctions > Advanced > Iface > Advanced > Iface > Continue to Connection Profile Hay > Balca The profile Hay Control Control Advanced > Marcone d and the Control advanced > Iface > Control advanced Profile Hay > Balca The profile Hay Control Control Advanced > Marcone d and the State Advanced > Iface > Control and the	Home 🍪 Configuration 🔯 Monitoring 🔚 Sar	we 🚯 Refresh 🔕 Back 💿 Forward 🦻 Help	CISCO
Introduction And Contraction Profiles Deve Understand Profiles And Contraction Profiles Deve Understand Profil	Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules	
generative with Device Management Anniv Reset	Remote Access VPH Remote Access	Configuration Remote Access VMI > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules Define rules to map certificates to desired Any:Connect or dendess SSL connection profiles (turnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected or Certificate to Connection Profile Haps • Add C Edit Cole Prod: Mapping Criteria Rule Priority Nadd Certificate Matching Rule Criterion Rule Priority Mapping Criteria Component Pied Component Operator Vible Pied + - Contains abo_groot	
Appy Acade	Device Management	Apply Reset	

Sur CLI.

crypto ca certificate map CERT_MAP 10 issuer-name co calo_root

Étape 10. Créez un objet avec le réseau du pool d'adresses IP à utiliser afin d'ajouter une règle d'exemption NAT (Traduction d'adresses réseau) à **Configuration > Firewall > Objects > Network Objects/Groups> Add**.

File Yes Tools Wandow Help Yes	Cisco A M 7.8(1)150 for ASA - 192.168.0.254							
Hore Configuration is here for the formation > Encode is included in the last is t	File View Tools Wizards Window Help						Type topic to search Go	dia dia
Increal O Conformation > Hereal > Objects > Herbark Objects > Herbark Objects > Herbark Objects > Herbark Objects Image: Second Sec	Home 🗞 Configuration 🔯 Monitoring 🔲 Sar	re 🔇 Refresh 🔇 Back 🔘 Forward	1 🦓 Нер					cisco
Acces Rules Service Poky Rules A Aules Filter Rules Service Poky Rules A Aules Filter Rules Control Consons Martine Detection Martine Det	Firewall 🗗 🖗	Configuration > Firewall > Objects >	Network Objects/Grou	IDS				
Image: None Address We mask Description Object NAT Address Image: Rules Image: Rules </td <td>Access Rules</td> <td>♣ Add -</td> <td>ere Used 🔍 Not Used</td> <td></td> <td></td> <td></td> <td></td> <td>Filter Clear</td>	Access Rules	♣ Add -	ere Used 🔍 Not Used					Filter Clear
Image: Addie Servers Threat Detection Image: Releng Servers Threat Detection Image: Releng Servers Image: Releng Servers	Filter Rules	Name	IP Address		Netmask	Description	Object NAT Address	
Benvice Setup OK Cancel Help Image: Set of the S	The Proof Pro	Network Objects ● any4 ● any4 ● any6 ■ aniside network ■ aniside network	10.88.243.0 192.158.50.0 192.158.0.0 224.0.0.251 224.0.0.252 Edit Netwo Name: Type: IP Version: IP Address: Netmask: Description: NAT	rk Object NETWORK_OI Network 9 IP2-158-50-0 255-255-255	255.255.255.128 255.255.255.0 255.255.255.0 255.255.255.0 8)_192.168.50.0_24 10 0 X Cancel Help			
Apply Reset	Device Management				Apply	eset		

Sur CLI.

object network NETWORK_OBJ_192.168.50.0_24 subnet 192.168.50.0 255.255.255.0

Étape 11. Accédez à **Configuration > Firewall > NAT Rules** et sélectionnez **Add** pour créer la règle d'exemption NAT pour le trafic VPN RA.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254								- # X
File View Tools Wizards Window Help							Type topic to search Go	de de
Home 🗞 Configuration 🔯 Monitoring 🔚 Save (🔇 Refresh	ack 😱 Forward 🦻 Help						cisco
Firewall 🗇 🖗 🖸	onfiguration > Firev	vall > NAT Rules					Addresses Services	
Access Rules	💠 Add 🗸 🗹 Edit 👔	G Edit NAT Rule					Addresses	a t ×
E NAT Rules	Match Criteri						💠 Add 👻 🎬 Edit 🏢 Delete 🔍 Where U	Ised 🔍 Not Used
AAA Rules 4	=	Match Criteria: Original Packet —				Options	Filter:	Filter Clear
Filter Rules	Source Intr	Source Interface:	inside 👻	Destination Interface:	outside 👻	No Provid	Name	
URL Filtering Servers	"Network Object" N	Source Address:	any	Destination Address:	<_OBJ_192.168.50.0_24 -	INOPTOXY	-Network Objects	
Threat Detection				Service:	any –		🎱 any	
- 2 Identity Options		Actions Translated Darket					- 🌍 any4	
E Dijects		Source NAT Tures	Challe					
Network Objects/Groups Service Objects/Groups		Source tott Type:					NETWORK_OBJ_192.168.50.0_24	
- 🙀 Local Users		Source Address:	Original	Destination Address:	Original		outside-network/24	
- Security Groups		Use one-to-one address transla	ation					
Class Maps		PAT Pool Translated Address:		Service:	Original			
Regular Expressions		Round Robin						
TCP Maps		Extend PAT uniqueness to pe	er destination instead of per in	terface				
Time Ranges		Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-102	3			
B- 🔁 Advanced		Fall through to interface PAT						
		Use IPv6 for source interface P	PAT	Use IPv6 for desti	nation interface PAT			
		Options						
		Chable rule						
		Translate DNS replies that mate	ch this rule					
		V Disable Proxy ARP on egress in	terface					
		V Lookup route table to locate eg	gress interface					
Sevice Setup		Direction: Both -						
S. Fraval		Description:						
Kemote Access VPIV			Cancel	nep				
Site-to-Site VPN								
Device Management			m			+		
»,			Apply	set				

Sur 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 II s'agit de la configuration ASA complète utilisée pour cet exemple.

```
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
```

Configurer le client intégré de Windows 7

Étape 1. Accédez à Panneau de configuration > Réseau et Internet > Centre Réseau et partage.

Control Panel 🕨	Network and Internet Network and Sharing Center 	← 🍫 Search Control Panel	م
Control Panel Home	View your basic network information and s	set up connections	^ (§)
Manage wireless networks	i i i i i i i i i i i i i i i i i i i	See full map	
Change adapter settings	DRIVERAP-6KUZH cisco.com	Internet	
Change advanced sharing settings	(This computer) View your active networks	Connect or disconnect	t
	cisco.com Domain network	Access type: Internet Connections: M Wireless Network Connection (blizzard)	E
	Change your networking settings Set up a new connection or network Set up a wireless, broadband, dial-up, ad hoc,	or VPN connection; or set up a router or access point.	
See also HomeGroup	Connect to a network Connect or reconnect to a wireless, wired, dia	I-up, or VPN network connection.	
Internet Options Windows Firewall	Choose homegroup and sharing options Access files and printers located on other net	work computers, or change sharing settings.	-

Étape 2. Sélectionnez Configurer une nouvelle connexion ou un nouveau réseau.

🕎 Set Up a Connection or Network	
Choose a connection option	
Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.	
Set up a new network Configure a new router or access point.	r
Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.	
Connect to a workplace Set up a dial-up or VPN connection to your workplace.	-
Set up a dial-up connection Connect to the Internet using a dial-up connection.	
Ne	ext Car

Étape 3. Sélectionnez Se connecter à un lieu de travail et Suivant.

Étape 4. Sélectionnez Non, créez une nouvelle connexion et Suivant.

Étape 5. Sélectionnez Utiliser ma connexion Internet (VPN) et ajoutez la chaîne Nom commun (CN) du certificat HeadEnd dans le champ Adresse Internet. Dans le champ Nom de la destination, saisissez le nom de la connexion. Il peut s'agir de n'importe quelle chaîne. Assurezvous de vérifier le bouton Ne pas vous connecter maintenant ; il suffit de le configurer pour que je puisse me connecter plus tard box.

		- • •
📀 🗽 Connect to a Workplace		
Type the Internet addr	ess to connect to	
Your network administrator of	an give you this address.	
Internet address:	HeadEnd.david.com	
Destination name:	RA VPN to ASA with IKEv2	
Use a smart card Control Use a smart card Use a smart card Control Use a smart card Control	o use this connection yone with access to this computer to use this connection. ust set it up so I can connect later	
	Ne	t Cancel

Étape 6. Sélectionnez Suivant.

📀 🗽 Connect to a Workpla	ice	
Type your user nam	ne and password	
User name:	1]
Password:]
	Show characters Remember this password	
Domain (optional):]
		Create Cancel

Étape 7. Sélectionnez Créer.

Étape 8. Sélectionnez **Fermer** et accédez à **Panneau de configuration > Réseau et Internet > Connexions réseau**. Sélectionnez la connexion réseau créée et cliquez dessus avec le bouton droit de la souris. Sélectionnez **Properties**.

RA Dis	VPN to ASA with I	KEv2			VirtualBox Host
W/	AN Miniport (IKEv2		Connect		
VM	Aware Network Ad		Status		
Dis VN	sabled ⁄Iware Virtual Ether		Set as Def	ault Conn	ection
			Create Co	ру	
			Create Sh	ortcut	
		۲	Delete		
		۲	Rename		
		0	Properties	5	

Étape 9. Dans l'onglet **Général**, vous pouvez vérifier que le nom d'hôte approprié pour la tête de réseau est correct. Votre ordinateur va convertir ce nom en adresse IP ASA utilisée pour connecter les utilisateurs VPN d'accès distant.

RA VPN to ASA with IKEv2 Properties
General Options Security Networking Sharing
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):
HeadEnd.david.com
First connect
Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.
Dial another connection first:
See our online privacy statement for data collection and use information.
OK Cancel

Étape 10. Accédez à l'onglet **Sécurité** et sélectionnez **IKEv2** comme **type de VPN**. Dans la section **Authentification**, sélectionnez **Utiliser les certificats de machine**.

RA VPN to ASA w	ith IKEv2 Pr	operties		— ×
General Options	Security Ne	tworking	Sharing	1
Type of VPN:				
IKEv2				•
Data encryption:			Adv	vanced settings
Require encryption	(disconnect	if server d	eclines)	•
Authentication				
O Use Extensible	Authenticati	on Protoco	ol (EAP)	
				-
			(Properties
Ose machine o	ertificates			
			ОК	Cancel

Étape 11. Sélectionnez **OK** et accédez à **C:\Windows\System32\drivers\etc**. Ouvrez le fichier **hosts** à l'aide d'un éditeur de texte. Configurez une entrée pour résoudre le nom de domaine complet (FQDN) configuré dans la connexion réseau à l'adresse IP de votre tête de réseau ASA (dans cet exemple, l'interface externe).

```
# For example:
#
# 102.54.94.97 rhino.acme.com
# 38.25.63.10 x.acme.com
10.88.243.108 HeadEnd.david.com
```

source server
x client host

Étape 12. Revenez au **Panneau de configuration > Réseau et Internet > Connexions réseau**. Sélectionnez la connexion réseau que vous avez créée. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Connect**.

RA VPN to ASA with IKEv2			VirtualBox Host-Only		
Disconnected WAN Miniport (IKEv2)		Connect			
VMware Network Adapter Disabled VMware Virtual Ethernet A		Status			
		Set as Default Connection			
		Create Copy			
		Create Shortcu	ıt		
	۲	Delete			
	۲	Rename			
	0	Properties			

Étape 13. L'état de la connexion réseau passe de Disconnected à Connecting, puis à Connected. Enfin, le nom que vous avez spécifié pour la connexion réseau s'affiche.

L'ordinateur est connecté à la tête de réseau VPN à ce stade.

Configurer le client VPN natif Android

Étape 1. Accédez à Paramètres >Autres paramètres de connexion

Étape 2. Sélectionner VPN

A 🖬 🗄 🖆 🖬 🛓

🕆 🖬 54% 🛢 7:45 PM

More connection settings

Nearby device scanning

On

Printing

Download booster

VPN

Set up and manage Virtual Private Networks (VPNs).

Étape 3. Sélectionnez Add VPN. Si la connexion est déjà créée comme dans cet exemple, effleurez l'icône du moteur pour la modifier. Spécifiez IPSec IKEv2 RSA dans le champ Type. L'adresse du serveur est l'adresse IP de l'interface ASA IKEv2 activée. Pour le certificat d'utilisateur IPSec et le certificat d'autorité de certification IPSec, sélectionnez les certificats installés en cliquant sur dans les menus déroulants. Laissez le certificat du serveur IPSec avec l'option par défaut, Received from server.

± ± 🛛 ±	¥ "al 52% ≜ 7:52 PM
Edit VPN netwo	rk RE
Name RA VPN to ASA H	leadend with IK
Туре	
IPSec IKEv2 RSA	-
Server address 10.88.243.108	
IPSec user certific	ate
Android ID Cert 🔻	
IPSec CA certifica	te
calo_root-1 💌	
IPSec server certif	ficate
Received from ser	ver 🔻
DELETE	CANCEL SAVE

Étape 4. Sélectionnez Enregistrer puis effleurez le nom de la nouvelle connexion VPN.

Étape 5. Sélectionnez Connect.

Étape 6. Tapez une nouvelle fois la connexion VPN pour vérifier l'état. Il s'affiche maintenant sous la forme **Connected**.

Vérification

Commandes de vérification sur la tête de réseau 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 : TPsec: : 24.2 Tunnel ID Local Addr : 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 Left(T): 28778 Seconds Rekey Int (T): 28800 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 Remote Status Tunnel-id Local Role READY RESPONDER 2119549341 10.88.243.108/4500 10.152.206.175/4500 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) 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: Oxffffffff Oxfffffff

outbound esp sas:									
spi: 0x76131476 (1980961910)	-						
transform: esp	-aes-256 e	sp-sha-	hmac :	no comp	pression	n			
in use setting	s ={RA, Tu	nnel, 1	KEV2,	}					
slot: U, conn_1d: 983U4, crypto-map: Anyconnect									
TV size: 16 by	tes	IIICUI		CC)• 20	5707				
replay detecti	on support	: Y							
Anti replay bi	tmap:	_							
0x000000000	00000001								
ASA#show vpn-sessiondb	license-su	mmary							
VPN Licenses and Config	Jured Limit	s Summa							
							· · · · · · · · · · · · · · · · · · ·		
AnyConnect Premium		: ENAB	LED :		50 :	50	: NONE		
AnyConnect Essentials		: DISAB	LED :		50 :	0	: NONE		
Other VPN (Available by	r Default)	: ENAB	LED :		10 :	10	: NONE		
Shared License Server		: DISABLED							
Shared License Particip	pant	: DISAB	LED						
AnyConnect for Mobile		: ENAB	LED (R	equires	s Premi	um or Esse	entials)		
Advanced Endpoint Asses	sment	: ENAB	LED(R	equires	s Premi	um)			
AnyConnect for Cisco VE	N Phone	: ENAB	LED						
VPN-3DES-AES		: ENAB	LED						
VPN-DES		: ENAB	LED						
VPN Licenses Usage Summ	arv								
	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 won-sessiond	·								
	, 								
VPN Session Summary									
	Ac	tive :	Cumul	ative	Peak	Concur : :	Inactive		
American cit cit									
Anyconnect Client	•	0:		11	•	1.	U		
SSL/TLS/DTLS	:	0 :		1.0		1 :	0		
IKEV2 IPsec	:	0 :		10		1 :	0		
Generic IKEv2 Remote Ac	cess :	1:		14 :	:	1			
Total Active and Inacti	ve :	1		 To	otal Cu	mulative	: 25		
Device Total VPN Capaci	ty :	50							
Device Load	:	2%							
Tunnels Summarv									
		·							
	Ac	tive :	Cumul	ative	Peak (Concurrent	t		

IKEv2	:	1	;	: 25	5	:	1
IPsec	:	1	:	: 14	4	:	1
IPsecOverNatT	:	0	:	: 11	1	:	1
AnyConnect-Parent	:	0	:	: 11	1	:	1
SSL-Tunnel	:	0	:	: 1	1	:	1
DTLS-Tunnel	:	0	:	: 1	1	:	1
Totals	:	2	:	: 63	3		

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Note: Référez-vous <u>à Informations importantes sur les</u> commandes <u>de débogage</u> avant d'utiliser les commandes debugcommand.

Attention : Sur ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, la verbosité des débogages augmente. Faites ceci avec prudence, en particulier dans les environnements de production.

- Debug crypto ikev2 protocol 15
- Debug crypto ikev2 platform 15
- Debug crypto ca 255