ASA IKEv2 RA VPN com clientes VPN Windows 7 ou Android e configuração de autenticação de certificado

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Overview Configurar autoridade de certificado Gerar um certificado de cliente Instalar o certificado de cliente Instalar o certificado de identidade na máquina cliente Windows 7 Como instalar o certificado de identidade no seu dispositivo móvel Android Configurar o headend do ASA para VPN RA com IKEv2 Configurar o cliente incorporado do Windows 7 Configurar o cliente de VPN nativo do Android Verificar Troubleshoot

Introduction

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) versão 9.7.1 e posterior para permitir que os clientes VPN nativos (Virtual Private Network) do Windows 7 e Android estabeleçam uma conexão VPN RA (Remote Access) com o uso do Internet Key Exchange Protocol (IKEv2) e de Certificados como o método de autenticação.

Contribuído por David Rivera e Cesar Lopez Zamarripa, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- autoridade de certificado (CA)
- Public Key Infrastructure (PKI)
- VPN RA com IKEv2 no ASA
- cliente VPN incorporado do Windows 7
- Cliente VPN nativo Android

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- CISCO1921/K9 15.5(3)M4a como servidor de CA do IOS
- ASA5506X 9.7(1) como headend de VPN
- Windows 7 como máquina cliente
- Galaxy J5 Android 6.0.1 como cliente móvel

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Overview

Estas são as etapas para configurar os clientes VPN nativos do Windows 7 e Android para se conectar a um headend do ASA:

Configurar autoridade de certificado

A CA permite incorporar a EKU (Extended Key Usage, uso de chave estendida) necessária no certificado. Para o headend do ASA, o certificado Server Auth EKU é necessário, enquanto o certificado do cliente precisa do Client Auth EKU.

Uma variedade de servidores CA podem ser usados, como:

- servidor Cisco IOS CA
- servidor de CA OpenSSL
- Microsoft CA server
- 3rd ACs de terceiros

O IOS CA Server é usado para este exemplo de configuração.

Esta seção descreve a configuração básica para fazer com que um CISCO1921/K9 com a versão 15.5(3)M4a funcione como um Servidor CA.

Etapa 1. Verifique se o dispositivo e a versão suportam o 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

Etapa 2. Ative o Servidor HTTP no Roteador.

IOS-CA(config)#ip http server
Etapa 3. Gere um par de chaves RSA exportável.

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)

Etapa 4. Configure um ponto de confiança.

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: O endereço IP do comando de inscrição é um dos endereços IP configurados pelo Roteador para uma interface alcançável.

Etapa 5. Autentique o ponto confiável (Obtenha o certificado 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.
Etapa 6. Inscreva o ponto confiável (Obtenha o certificado de identidade).
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
```

```
Passo 7. Verifique os 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: 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
```

Etapa 8. Exporte o ponto confiável HeadEnd para o terminal no formato PKCS12 para obter o certificado de identidade. O certificado CA e a chave privada são adicionados em um único arquivo.

<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.

Etapa 9. Crie um ponto de confiança vazio no ASA.

ASA(config)# crypto ca trustpoint <HeadEnd> DRIVERAP(config-ca-trustpoint)# exit Etapa 10. Importar o arquivo 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 ho3Cv1cZYM0TzZEzlsKdAgIEAA==

quit

INFO: Import PKCS12 operation completed successfully Etapa 11. Verifique as informações do 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

Gerar um certificado de cliente

Etapa 1. Gere um par de chaves RSA exportável.

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

Etapa 2. Configure um ponto de confiança.

```
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>
Etapa 3. Autentique o ponto confiável configurado (Obtenha o certificado 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.

Etapa 4. Inscreva o ponto confiável autenticado (Obter o certificado de identidade).

```
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
Etapa 5. Verifique as informações dos 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: 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
```

Instalar o certificado de identidade na máquina cliente Windows 7

Etapa 1. Exporte o ponto confiável Win7_PC nomeado para um servidor FTP/TFTP (instalado na sua máquina Windows 7) no formato PKCS12 (.p12) para obter o certificado de identidade, o certificado CA e a chave privada em um único arquivo.

```
<ciscol23>
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.

Éassim que o arquivo exportado fica em uma máquina cliente.



Etapa 2. Pressione Ctrl + R e digite mmc para abrir o Microsoft Management Console (MMC).

📨 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse

Etapa 3. Selecione OK.

The console - [Console Root]			
🔚 File Action View Favorites Wind	low Help		_ 8 ×
🗢 🔿 🖬 😖 🛛 🖬			
Console Root	Name		Actions
		There are no items to show in this view.	Console Root
			More Actions

Etapa 4. Navegue até Arquivo > Adicionar/remover snap-in.

Console1 - [Console Root]		
File Action View Favorites Wind	ow Help	_ & ×
📫 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 snap-ins: Selected snap-ins:	More Actions
	Snap-in Vendor Console Root Edit Extensions	
	ActiveX Control Microsoft Cor	
	Certificates Microsoft Cor =	
	Component Services Microsoft Cor	
	Computer Managem Microsoft Cor Device Managem Microsoft Cor Move Down	
	Bisk Management Microsoft and	
	Event Viewer Microsoft Cor	
	Group Policy Object Microsoft Cor	
	B IP Security Monitor Microsoft Cor	
	B IP Security Policy M Microsoft Cor	
	Advalced	
	Description:	
	The ActiveX Control shap-in enables you to add an MMC hode with a results view containing an ActiveX control.	
	OK Cancel	
J		

Etapa 5. Selecione Certificados > Adicionar > Conta do Computador.

Console1 - [Console Root]		
File Action View Favorites Window Help		_ <u>-</u> <u>-</u> ×
Console Root Name		Actions
		Console Root 🔺
Add or Remove Snap-ins	23	More Actions
You can select snap-ins for this console from those available on your computer and configure the selected se extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Selected snap-ins:	Certificates snap-in	
Snap-in Vendor Console Root	This snap-in will always manage certificates for:	
ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Component Services Microsoft Cor Computer Manager Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Folder Microsoft Cor Group Policy Object Microsoft Cor Group Policy Object Microsoft Cor Description: Description:	My user account Service account Computer account	
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service,	< Back OK Cancel	Next > Cancel
]	J

Etapa 6. Selecione Avançar,

Console1 - [Console Root]		
Console1 - [Console Root] File Action View Favorites Window Help Console Root Add or Remove Snap-ins You can select snap-ins for this console from those available on your computer and configure the select extensible snap-ins; you can configure which extensions are enabled. Available snap-ins: Snap-in Vendor Add or Component Services Microsoft Cor Device Managem Microsoft Cor Folder Microsoft Cor Microsoft Cor Korsoft Cor	Select Computer Select the computer you want this snap-in to manage. This snap-in will always manage:	Actions Console Root More Actions
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a serv	Cancel	sh Cancel

Passo 7. Termine.

Console1 - [Console Root]						
File Action View Favorites Win	dow Help					_ = = ×
	10				1	
Console Root	Name				Actions	
	Add or Remove Snap-ins			—	Console Root	•
	You can select snap-ins for th extensible snap-ins, you can Available snap-ins: Snap-in ActiveX Control ActiveX Control ActiveX Control ActiveX Control Certificates Component Services Computer Manager Device Manager	is console from those available configure which extensions are Vendor Microsoft Cor Microsoft Cor	e on your computer and configure the selected seabled. Selected snap-ins: Console Root Certificates (Local Computer) of the certificate stores for yourself, a service	Edit Extensions Remove Move Up Move Down	More Actions	•
				OK Cancel		
	ų,					

Etapa 8. Selecione OK.

Etapa 9. Vá para Certificados (Computador Local)>Pessoal>Certificados, clique com o botão direito do mouse na pasta e navegue para Todas as Tarefas>Importar:

Console1 - [Console Root\Certificates (Loo	Jel - [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)	DRIVERAP-6	KUZH	DRIVERAP-6KUZH		7/13/2022	<all></all>	<none></none>	Certificates	
Personal								More Actions	•
Certificates	•	Request New	Certificate						
Enterprise		Import							
Intermedia	•								
Trusted Pu New Window fro	om Here	Advanced Op	erations •						
Ontrusted New Taskpad Vie	ew								
Trusted Per Refresh									
Other Peop Export List									
Ams									
CanaryCert Help									
McAfee Trust									
PolicyCertStore									
Remote Desktop									
Certificate Enrollment Requests									
SMS									
▶ 📫 SPC									
Trusted Devices									
< III +	•								
Add a certificate to a store								,	

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

Etapa 10. Clique em Next. Indique o caminho onde o arquivo PKCS12 está armazenado.

Certificate Import Wizard	×	
File to Import		
Specify the file you want to import.		
Eile name:		
C:\TETP-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 > Can	cel	

Etapa 11. Selecione **Next** novamente e digite a senha inserida no comando *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

Etapa 12. Selecione Avançar.

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 > Cancel	

Etapa 13. Selecione Avançar mais uma vez.



Etapa 14. Selecione Concluir.

Certificate Import Wizard
The import was successful.
ОК

Etapa 15. Selecione **OK**. Agora você verá os certificados instalados (o certificado CA e o certificado de identidade).

Image: Index Action View Favorites Window Help	🚡 Console1 - [Console Root\Certificates (Lo	cal Computer)\Personal\Certificates]						- • •
Image: Stand Decision Root Issued To Issued By Expiration Date Intended Purposes Friendly Na Image: Conscience (Local Computer) Image: Conscience Root Calo_root 7/12/2020 <all> Cnecked.org Certificates Image: Conscience Root Root Root Root Root Root Root Roo</all>	🚡 File Action View Favorites Wind	low Help						_ 8 ×
Image: marked marked marked marked purposes Finendly Nations Image: marked marked purpose purpose Finendly Nations </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
Image: Certificates (local Computer) Image: Certificates Image: Certificates <t< td=""><td>Console Root</td><td>Issued To</td><td>Issued By</td><td>Expiration Date</td><td>Intended Purposes</td><td>Friendly Na</td><td>Actions</td><td></td></t<>	Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na	Actions	
↓ Personal Certificates More Actions ↓ Trusted Root Certification Author Calo_root 7/13/2018 Server Authenticat cn=Win7_P ↓ Trusted People Calo_root 7/13/2018 Server Authenticat cn=Win7_P ↓ Trusted People CanaryCertification Author Nore Actions Nore Actions ↓ Trusted People CanaryCertificates Nore Actions ↓ CanaryCertificates Nore Actions ↓ PolicyCertificate Nore Actions ↓ PolicyCertificate Enrollment Requests Server Authenticat Calo_root ↓ PolicyCertificate Enrollment Requests Server Authenticat Nore Actions	 Certificates (Local Computer) 	🔄 calo_root	calo_root	7/12/2020	<all></all>	cn=calo_ro	Certificates	
Win7_PC.david.com Calo_root 7/13/2018 Server Authenticati cn=Win7_P Win7_PC.david.com Calo_root Y Win7_PC.david.com Calo_root Y Vertile Publishers Vertile Publishers<	A Personal	🛱 DRIVERAP-6KUZH	DRIVERAP-6KUZH	7/13/2022	<all></all>	<none></none>	More Actions	•
Intermediate Certification Author Intermediate Certification Author Intrade Publishers Untrusted Certificates Third-Party Root Certification Aut Intrusted People Ams InjectorCertStore InjectorCertStore Remote Desktop Staff Staff Staff Staff Staff Staff	Trusted Root Certification Author	Win7_PC.david.com	calo_root	7/13/2018	Server Authenticati	cn=Win7_P		
Intermediate Certification Author Trusted Publishers Trusted Poplificates Trusted People Ams CanayCentStore Ams PolicyCentStore PolicyCentStore PolicyCentStore Smart Card Trusted Roots Smart Card Trusted Roots Soft Same Soft Same Trusted Devices It is the state of the stat	Enterprise Trust							
Image: Second Secon	Intermediate Certification Author							
> Untrusted Certification Aut > Third-Party Root Certification Aut > Other People > Other People > CanaryCertStore > InjectorCertStore > PolicyCertStore > PolicyCertStore > PolicyCertStore > Smart Card Trusted Roots > SMS > SPC > Trusted Devices	Trusted Publishers							
Indr-Party Not Certification Adi Other People Other People Ams CanaryCertStore DiptectorCertStore McAfee Trust PolicyCertStore Certificate Enrollment Requests Smart Card Trusted Roots SMS SPC Trusted Devices	Untrusted Certificates							
Conter People CanaryCertStore CanaryCertStore McAfee Trust McAfee Trust McAfee Trust Some Desktop Smart Card Trusted Requests SMS SSMS SPC Trusted Devices	Trusted People							
Ams CanaryCertStore InjectorCertStore PolicyCertStore PolicyCertStore Remote Desktop Smart Card Trusted Requests SMS SPC SPC Trusted Devices	Other People							
▷ CanaryCertStore ▷ InjectorCertStore ▷ McAfee Trust ▷ PolicyCertStore ▷ Remote Desktop ▷ Certificate Enrollment Requests ▷ Smart Card Trusted Roots ▷ SPC ▷ Trusted Devices	⊳ 🛗 Ams							
Image: Solution of the second seco	CanaryCertStore							
McAte Trust PolicyCertStore Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots SMS SPC Trusted Devices	InjectorCertStore							
> > </td <td>McAfee Trust</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	McAfee Trust							
> ☐ Certificate Enrollment Requests > ☐ Smart Card Trusted Roots > ☐ SMS > ☐ SPC > ☐ Trusted Devices	Bemote Deskton							
Image: Smart Card Trusted Roots	Certificate Enrollment Requests							
▷ SMS ▷ SPC ▷ Trusted Devices	Smart Card Trusted Roots							
SPC ⇒ Trusted Devices ✓ M M	SMS							
	▷ SPC							
	Irusted Devices							
		•	III			+		
Personal store contains 3 certificates.	Personal store contains 3 certificates.							

Etapa 16. Arraste e solte o Certificado CA de **Certificados (Computador** Local)>Pessoal>Certificados para Certificados (Computador Local)>Autoridade de Certificação de Raiz Confiável>Certificados.

Console1 - [Console Root\Certificates (Lo	cal Computer)\Trusted Root Certificatio	on Authorities\Certificates]					
Tile Action View Favorites Wind	ow Help						- 8 ×
🗢 🔿 🙍 🔂 🐇 🛸 🗶 🗈 😖	? 🗊						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly ^	Actions	
Certificates (Local Computer)	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati	The USE	Certificates	
Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati	DigiCert	More Actions	•
Certificates	🙀 calo_root	calo_root	7/12/2020	<all></all>	cn=calo	moreriettons	
Insted Root Certification Author Certificator	Certum CA	Certum CA	6/11/2027	Server Authenticati	Certum	calo_root	
Enterprice Trust	Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati	Certum E	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	2 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>		
D SPC	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>		
p inusted 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		
۰	Equifav Secure Certificate Auth	Equifax Secure Certificate Authority III	8/22/2018	Servire Emsil Serve	GenTrue *		
Trusted Root Certification Authorities store co	ntains 60 certificates.						

🚡 Console1 - [Console Root\Certificates (Lo	cal Computer)\Personal\Certificates]						- • •
Tile Action View Favorites Wind	low 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.							

Como instalar o certificado de identidade no seu dispositivo móvel Android

Note: O Android suporta arquivos de armazenamento de chaves PKCS#12 com extensão .pfx ou .p12.

Note: O Android suporta apenas certificados SSL X.509 codificados por DER.

Etapa 1. Após a exportação do certificado do cliente do IOS CA Server no formato PKCS12 (.p12), envie o arquivo para o dispositivo Android por e-mail. Quando estiver lá, toque no nome do arquivo para iniciar a instalação automática. (**Não baixar o arquivo**)

🗆 🖬 ±		7	al 53%	8 7:24	PM
÷			ī	\simeq	÷
-					
					.
Andr	roid_Smartpho	ne.p12	<u>+</u>		
					_
Reply	Reply	all		+ Forward	

Etapa 2. Digite a senha usada para exportar o certificado, neste exemplo, a senha é cisco123.

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

Etapa 3. Selecione **OK** e insira um **nome de certificado**. Pode ser qualquer palavra, neste exemplo o nome é **Android ID Cert**.



Etapa 4. Selecione **OK** e a mensagem "Android ID Cert installed" (Certificado de ID do Android instalado) será exibida.

Etapa 5. Para instalar o certificado CA, extraia-o do IOS CA Server no formato base64 e salve-o com a extensão .crt. Envie o arquivo para seu dispositivo android por e-mail. Desta vez, você precisa fazer o download do arquivo ao tocar na seta ao lado do nome do arquivo.

🛛 ±		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
second second s	
the second se	
Calo_root.crt	± 🛆
Reply Reply all	IIII Forward

Etapa 6. Navegue até Configurações e Bloquear tela e segurança.



Passo 7. Selecione Outras configurações de segurança.

ω±	7∎ 50% ≣ 6:57	PM
← (Lock screen and security	
Noti Show	fications on lock screen	
Set yo and L	ure lock settings our secure lock functions, such as Auto lock ock instantly with Power key.	
Secu	rity	
Find Locat Sams	My Mobile e and control your device remotely using you ung account.	ur
Unk Allow other	nown sources installation of apps from sources than the Play Store.	
Encr	rypt device ct your device by encrypting its data.	
Encr No SE	card inserted	
Othe Chang secur	er security settings ge other security settings, such as those for ity updates and credential storage.	

Etapa 8. Navegue até Instalar a partir do armazenamento do dispositivo.

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.

Etapa 9. Selecione o arquivo .crt e toque em Concluído.

Select file	DONE
calo_root-1.crt	

Etapa 10. Introduza um **nome de certificado**. Pode ser qualquer palavra, neste exemplo, o nome é **calo_root-1**.



Etapa 10. Selecione OK e você verá a mensagem "calo_root-1 installed".

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

Etapa 11. Para verificar se o certificado de identidade está instalado, navegue até a guia Configurações/Tela de bloqueio e Segurança/Outros > Configurações de segurança/Certificados de usuário/Sistema.

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

Etapa 12. Para verificar se o certificado CA está instalado, navegue até a **tela Configurações/Bloqueio e segurança/Outras configurações de segurança/Exibir certificados de segurança/guia Usuário.**

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

▲ 🗆 ± ± 🛤 ±	≆ ⊿l 54% 🖹 7:45 PM
← View security of	certificates
SYSTEM	USER
calo_root	

Configurar o headend do ASA para VPN RA com IKEv2

Etapa 1. No ASDM, navegue para Configuration>Remote Access VPN > Network (client) Access> Anyconnect Profiles. Marque a caixa Acesso IPSec (IKEv2), Permitir Acesso na interface voltada para os clientes VPN (a opção Habilitar Serviços de Cliente não é necessária).

Etapa 2. Selecione **Device Certificate** e remova a marca de seleção de **Use the same device certificate for SSL and IPSec IKEv2**.

Etapa 3. Selecione o certificado Headend para a conexão IPSec e selecione — None — para a conexão SSL.

Essa opção coloca em prática a configuração crypto ikev2, crypto ipsec, crypto dynamic-map e crypto map.

								- 🗗 🔀
File View Tools Wizards Window Help							Type topic to search Go	alate
Home Configuration 🔯 Monitoring 🔲 Se	ave 💽 Refresh 🕻	Back O Forward	e de la composición de la composicinde la composición de la composición de la composición de la compos					cisco
Remote Access VPN	Configuration >	Remote Access VPN	> Network (Client)	Access > AnyConnect	Connection Profiles			
Throduction Throducti	The security app IPsec (IKEv2) tur Access Interfaces Enable Cisco SSL access must	iance automatically dep inel as well as SSL tunn AnyConnect VPN Client be enabled if you allow	loys the Cisco AnyCom el with Datagram Trans access on the interfac AnyConnect client to b	nect VPN Client to remote port Layer Security (DTLS es selected in the table b e launched from a brows	users upon connection. Th) tunneling options. dow r (Web Launch) .	e initial client deployment requires end-user admin	istrative rights. The Cisco AnyConnect VPN Clie	nt supports
Group Policies	SSL Access IPsec /		IPsec (IKEv2) Acces	IPsec (IKEv2) Access				
IPsec(IKEv2) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate		
George Mobility Solution Address Assignment	outside					Port Settings		
Advanced	inside							
Cerfictaria Cardination Cardinati	Login Page Setting Allow user to Shutdown po Connection Profiles Connection profi	select connection profi rtal login page. le (tunnel group) specif dt m Delete	le on the login page. (ies how user is authent	icated and other parame	ers. You can configure the	mapping from certificate to connection profile (<u>her</u>	6	
	Name	SSL Ena	bled	IPsec Enabled	Alias	es Authentication Method	Group Policy	
	DefaultRAGroup	Group			V 7	AAA(LOCAL)	DittGroPolicy	
					¥	AAA(LOCAL)	DfltGrpPolicy	

Esta é a aparência da configuração na CLI (Command Line Interface, interface de linha de comando).

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

Etapa 4. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Group Policies para criar uma política de grupo

p			
Add Internal Group Policy			×
Add Internal Group Policy	Name: GP_David Banner: Inherit SCEP forwarding URL: Inherit Address Pools: Inherit IPv6 Address Pools: Inherit IPv6 Address Pools: Inherit IPv6 Address Pools: Inherit More Options Inherit Tunneling Protocols: Filter: Access Hours: 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 SSL VPN Clent IPsec IKEv1 V Inherit	Select Select Manage Manage
Find:	Next Previous		
		OK Cancel Help	

Na CLI.

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

Etapa 5. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Address Pools e selecione Add para criar um pool IPv4.

Tisco ASDM 7.8(1)150 for ASA - 192.168.0.254				X
File View Tools Wizards Window Help			Type topic to search Go	alate
Home 🖧 Configuration 🔯 Monitoring 🔲 Sav	ive 💽 Refresh 🔇 Back 🔘 Forward 🤶 Help			cisco
Remote Access VPN 🗗 🖗	Configuration > Remote Access VPN > Network (Client) Acce	ss > Address Assignment > Address Pools		
Introduction Introduction Aryconnect Connection Profiles AnyConnect Connection Profiles AnyConnect Clent Profile AnyConnect Clent Software AnyConnect Clent Software Aryconnect Clent Software Propraitic Access Profiles Pr	Configure named IP Address Pools. The IP Address Pools of dustering.	can be used in either a VPN [Psec[IKEv1] Connection Profiles, AnsConnect Connect ress Ending Address/Number of Addresses 1 192:165.50,100	on Profiles, Group Policies configuration , or in <u>Interfaces</u> configuration Subnet Mask/Prefix Length 255:255:255:0	related to ASA
Boscie Scholl Advanced Advisor Addigment Linguage Localization PLOP Server DVS Advanced		Edit IPv4 Pool Name: ACPool Starting IP Address: 192.168.50.10 Ending IP Address: 192.168.50.100 Subnet Mask: 255.255.0 OK Cancel		
Fryewall Got Remote Access VPN Got Stet-to-Stete VPN				
Device Management		Apply Reset		

ip local pool ACPool 192.168.50.1-192.168.50.100 mask 255.255.255.0

Etapa 6. Navegue até Configuration > Remote Access VPN > Network (Client) Access > IPSec(IKEv2) Connection Profiles (Configuração > VPN de acesso remoto > Acesso de rede (cliente) > IPSec(IKEv2) Connection Profiles e selecione Add para criar um novo grupo de túneis.



Na 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
```

Passo 7. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Policy e marque a caixa Used the configured rules to matth a certificate to a Connection Profile.





tunnel-group-map enable rules

Etapa 8. Navegue até **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile maps > Rules** e crie um novo Certificate Map. Selecione **Adicionar** e associe-o ao grupo de túneis. Neste exemplo, o grupo do túnel é chamado **David**.

Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254					- a X
File View Tools Wizards Window Help				Type topic to search Go	dia di
Home 🗞 Configuration 😥 Monitoring 🔲 Save 🌘	🔁 Refresh 🔇 Back 🔘 Forward 🢡 Help				cisco
Remote Access VPN	onfiguration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to	Connection Profile Maps > Rules		
Prectice Police P	Define rules to map certificates to desired AnyConnect ertificate to Connection Profile Maps Add I Edit Delete Find: Map Name	or clentless SSL connection profiles (tunnel groups). Use th	e bottom table to configure certificate fields toge Mapped to Connection Profile	ther with their matching criteria for the selected r	ule.
Address Assignment Mag	apping Criteria				
Address Pools Advanced Advanced AnyConnect Custom Attributes BaryConnect Custom Attribute Nam	Add I Edit Add Certificate Matching R Field Configure a certificate matching rule and a mapped will be ignored.	ule ng rule and associate it with a connection profile. The rule p usigns a priority to the rule with lower values having greate	riority uniquely identifies the r priority. Rules that are not Value		
Police Police Pre Polices Pre Portagenetation Polices Prese Prefagmentation Polices Certificate to Connection Profile Policy Policy Police Police Police	Map: Priority: Mapped to Connection Profile:				
Conc Lass Integrity Server System Options System Options Act, Manager Add, Manager Macess More Add, Accel Users Mathematical Users Mathematical Users					
Bevice Setup Freval Genete Access VPN Genete Access VPN Genete Access VPN Device Management					
»		Apply	Reset		

Na CLI.

tunnel-group-map CERT_MAP 10 David

Etapa 9. Selecione Adicionar na seção Critérios de Mapeamento e insira esses valores.

Campo: Emissor

Operador: Contém

Valor: calo_root

Circo ACDM 7 9/11/150 for ACA 102 169 0 254			
Cisco Asom 7.5(1)150 for ASA - 192108.0.2.54		Type topic to search	
Home Configuration A Monitoring Sa	re 🕞 Refresh 🚫 Back 💭 Forward 🦻 Help	Type ope of Jon and Go	cisco
Remote Access VPN	Configuration > Remote Access VPII > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules		
Commercial and provided market of the second m	Configuration > Remote Access VPII > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Haps > Rules Define rules to map certificates to desired AnyConnect or clientess SSL connection profiles (turnel groups). Use the bottom table to configure certificate fields together v Certificate to Connection Profile Maps	ith their matching criteria for the selected	rule.
Bre Policies Bre Policies Bre Policies Bre Portagenetation Policies Brescherfagmentation Policies Bolory Bolory Bolory Sone Labs Integrity Server System Cotions System Cotions System Cotions Bolory System Cotions System Cotions System Cotions	Field Component Operator Value Issuer Issuer <		
AAA,Local Users			
Firewall			
Site-to-Site VPN			
Device Management	Apply Reset		

Na CLI.

crypto ca certificate map CERT_MAP 10 issuer-name co calo_root

Etapa 10. Crie um objeto com a rede do pool de IP a ser usado para adicionar uma regra de isenção de NAT (Network Address Translation) em **Configuration > Firewall > Objects > Network Objects/Groups> Add**.

Cisco A M 7.8(1)150 for ASA - 192.168.0.254							
File View Tools Wizards Window Help Type topic to search Go							dia dia
🚳 Home 🗞 Configuration 🔯 Monitoring 🔚 Save 🗞 Refresh 🔇 Back 💭 Forward 🦻 Help							cisco
Firewall 🗗 🖓	configuration > Firewall > Objects > Network Objects/Groups						
Access Rules	♣ Add ▼ 2 Edit 1 Delete Q, V Filter:	Where Used 🔍 Not Used					Filter Clear
Filter Rules	Name	IP Address		Netmask	Description	Object NAT Address	
The Rules The Rules	Partie Network Objects → any → an	10.88.243.0 10.88.243.0 192.158.50.0 192.168.0.0 224.0.0.251 224.0.0.252 Edit Netwon Name: Type: IP Version: IP Address: Description: NAT	rk Object NETWORK_OB Network © IP4 0 1 192.158.50.0 255.255.255.0	Implement 255.255.255.128 255.255.255.0 255.255.255.0 255.255.255.0 31_192.168.50.0_24 IPv6 0			
Site-to-Site VPN							
Device Management				Apply	teset		

Na CLI.

object network NETWORK_OBJ_192.168.50.0_24 subnet 192.168.50.0 255.255.255.0

Etapa 11. Navegue até **Configuration > Firewall > NAT Rules** e selecione **Add** para criar a regra de isenção de NAT para o tráfego de VPN RA.

🖞 Cisco ASDM 7.8(1)150 for ASA - 192.168.0.254 💿 🐼 🐼								
File View Tools Wizards Window Help	Type topic to search Go						de de	
Home 🗞 Configuration 🔯 Monitoring 🗐 Sa	h Home 🖓 Configuration 📴 Monitoring 🎧 Save 🚱 Refresh 🕥 Back 😱 Forward 🤶 Help CLSCO							
Firewall 🗗 🖓	Configuration > Fire	anfiguration > Firewall > NAT Rules Addresses Services						
2 Access Rules	💠 Add 👻 🗹 Edit 👔	Edit NAT Rule			—		Addresses	ə و ×
Q Service Policy Rules	Match Criteri	Match Criteria: Original Packet					P Add - P Edit Delete Where U	Jsed Q Not Used
AAA Rules	# Source Intf	Source Interface:	inside 👻	Destination Interface:	outside 🗸	Options	Filter:	Filter Clear
Public Servers	1 inside	Source Address:	any	Destination Address:	COBJ 192.168.50.0 24	No Proxy	Name	
Threat Detection	"Network Object" N			Service				
Jentity Options				Service.	ony E		🌍 any4	
- 22 Identity by Trustsec		Action: Translated Packet	r					
Network Objects/Groups		Source NAT Type:	Static +					
- Service Objects/Groups		Source Address:	Original	Destination Address:	Original		outside-network/24	
- Sourity Groups		Use one-to-one address transl	ation					
Gass Maps		PAT Pool Translated Address:	-	Service:	Original		224.0.0.252	
R Regular Expressions		Round Robin						
TCP Maps		Extend PAT uniqueness to p	er destination instead of per ir	iterface				
Ime Ranges Ime Ranges Ime Ranges Ime Ranges		Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-102	3			
B-B Advanced		Fall through to interface PAT						
		Use IPv6 for source interface F	PAT	Use IPv6 for desti	nation interface PAT			
		Options						
		📝 Enable rule						
		Translate DNS replies that mat	ch this rule					
		Disable Proxy ARP on egress in	terface					
		V Lookup route table to locate egress interface						
Device Setup		Direction: Both +						
Firewall		Description:						
Remote Access VPN			OK Cancel	Help				
Site-to-Site VPN								
Device Management	•		m			Þ		
*			Apply	eset				

Na 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 é a configuração completa do ASA usada para este exemplo.

```
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 o cliente incorporado do Windows 7

Etapa 1. Navegue até **Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento**.

~~~~			
Control Panel	Network and Internet  Network and Sharing Center	✓ Search Control Panel	Q
Control Panel Home	View your basic network information and s	et up connections	• 9
Manage wireless networks	in in iteration in	See full map	
Change adapter settings	DRIVERAP-6KUZH cisco.com	Internet	
settings	(This computer) View your active networks	Connect or disconnect	
	cisco.com Domain network	Access type: Internet Connections: attll 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, dial	-up, or VPN network connection.	
Internet Options Windows Firewall	Choose homegroup and sharing options Access files and printers located on other netw	vork computers, or change sharing settings.	Ŧ

Etapa 2. Selecione Configurar uma nova conexão ou rede.

🔵 💇 Set	Up a Connection or Network	
Choo	se a connection option	
	<ul> <li>Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.</li> <li>Set up a new network Configure a new router or access point.</li> <li>Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.</li> <li>Connect to a workplace Set up a dial-up or VPN connection to your workplace.</li> <li>Set up a dial-up connection Connect to the Internet using a dial-up connection.</li> </ul>	E
		Next Cancel

Etapa 3. Selecione Conectar-se a um local de trabalho e Avançar.



Etapa 4. Selecione Não, crie uma nova conexão e Avançar.

🚱 🗽 Connect to a Workplace	
How do you want to connect?	
Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.	
ing	
Dial directly Connect directly to a phone number without going through the Internet.	
What is a VPN connection?	
	Cancel

Etapa 5. Selecione **Usar minha conexão com a Internet (VPN)** e adicione a string do Nome Comum do Certificado HeadEnd (CN) no campo **endereço da Internet**. No campo **Nome do destino**, digite o nome da conexão. Pode ser qualquer cadeia. Certifique-se de verificar a opção **Não ligar agora; basta configurá-lo para que eu possa conectar mais tarde**.

		- • •			
🚱 🌆 Connect to a Workplace					
Type the Internet address to connect to					
Your network administrator of	can give you this address.				
Internet address:	HeadEnd.david.com				
Destination name:	RA VPN to ASA with IKEv2				
<ul> <li>Use a smart card</li> <li>Image: Image and the second s</li></ul>	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			

Etapa 6. Selecione Avançar.

🚱 🗽 Connect to a Workpla	ce	
Type your user nam	e and password	
User name:		
Password:		
	Show characters Remember this password	
Domain (optional):		]
		Create Cancel

Passo 7. Selecione Criar.



Etapa 8. Selecione **Fechar** e navegue até **Painel de controle > Rede e Internet > Conexões de rede**. Selecione a conexão de rede criada e clique com o botão direito do mouse nela. Selecione Properties.

RA VE Disco WAN	PN to ASA with IKEv nnected Miniport (IKEv2	2 VirtualBox Host
VMware Network Ad Disabled VMware Virtual Ether	are Network Ad	Status
	are Virtual Ether	Set as Default Connection
		Create Copy
		Create Shortcut
	1	Delete
	۲	Rename
	۲	Properties

Etapa 9. Na guia **Geral**, você pode verificar se o nome de host apropriado para o headend está correto. Seu computador resolverá esse nome para o endereço IP do ASA usado para conectar usuários de RA VPN.

📱 RA VPN	to ASA with	IKEv2 Prop	perties			×		
General (	Options Sec	urity Netw	vorking	Sharing				
Host nam 157.54.0.	e or IP addres 1 or 3ffe:1234	ss of destina 4::1111):	ation (suc	ch as micros	soft.com o	r		
HeadEnd	d.david.com							
- First cor	nnect					_		
Windo	ows can first c et, before tryin	onnect to a g to establis	public n sh this vi	etwork, suc tual conne	h as the ction.			
Dial another connection first:								
See our o informatio	online <u>privacy</u> n.	<u>statement</u> fo	or data c	ollection an	d use			
				ОК	Cano	el		

Etapa 10. Navegue até a guia **Segurança** e selecione **IKEv2** como o **Tipo de VPN**. Na seção **Autenticação,** selecione **Usar certificados da máquina**.

RA VPN to ASA with IKEv2 Properties	<b>X</b>
General Options Security Networking	Sharing
Type of VPN:	
IKEv2	•
Data encryption:	Advanced settings
Require encryption (disconnect if server	declines) 🔹
Authentication	
O Use Extensible Authentication Protoc	col (EAP)
	*
	Properties
I les machine certificates	
Se machine centineates	
	OK Cancel

Etapa 11. Selecione **OK** e navegue até **C:\Windows\System32\drivers\etc**. Abra o arquivo **hosts** usando um editor de texto. Configure uma entrada para resolver o FQDN (Nome de domínio totalmente qualificado) configurado na Conexão de rede para o endereço IP do headend do ASA (neste exemplo, a interface externa).

```
# 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
```

Etapa 12. Volte para **Painel de Controle > Rede e Internet > Conexões de Rede**. Selecione a conexão de rede criada. Clique com o botão direito do mouse nele e selecione **Conectar**.

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	
	۲	Properties	

Etapa 13. O status da conexão de rede passa de Desconectado para Conectado e, em seguida, para Conectado. Finalmente, o nome que você especificou para a conexão de rede é mostrado.



O computador está conectado ao headend da VPN neste ponto.

### Configurar o cliente de VPN nativo do Android

Etapa 1. Navegue até Configurações>Mais configurações de conexão



Etapa 2. Selecionar VPN

#### A 🖬 🗄 🗄 🖬 🛓

🕆 🛣 54% 🖹 7:45 PN

More connection settings

### Nearby device scanning

On

Printing

Download booster

#### VPN

Set up and manage Virtual Private Networks (VPNs).

Etapa 3. Selecione Adicionar VPN. Se a conexão já estiver criada como neste exemplo, toque no ícone do mecanismo para editá-la. Especifique IPSec IKEv2 RSA no campo Tipo. O endereço do servidor é o endereço IP da interface ASA habilitada para IKEv2. Para o certificado de usuário IPSec e o certificado de CA IPSec, selecione os certificados instalados tocando nos menus suspensos. Deixe o certificado do servidor IPSec com a opção padrão, Received from server (Recebido do servidor).



± ± 🛛 ±	7 🚽 52% 🖹 7:52 PM
Edit VPN netwo	RE ork
Name RA VPN to ASA	Headend with IK
Туре	
IPSec IKEv2 RSA	•
Server address 10.88.243.108	
IPSec user certifi	cate
Android ID Cert	
IPSec CA certific	ate
calo_root-1 💌	
IPSec server cert	ificate
Received from se	erver 🔻
DELETE	CANCEL SAVE

Etapa 4. Selecione **Save** (Salvar) e toque no nome da nova conexão VPN.



Etapa 5. Selecione Conectar.





Etapa 6. Digite a conexão VPN mais uma vez para verificar o status. Agora, ele é exibido como **Connected (Conectado)**.



### Verificar

Comandos de verificação no Headend do 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
           : 0
Bytes Tx
                                   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, l	KEV2,	}			
slot: U, conn_1d: 983U4, crypto-map: Anyconnect							
TV size: 16 by	tes	TILCUL		CC)• 20	5707		
replay detecti	on support						
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		: DISAB	LED				
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	:	<b>2</b> 5	:	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 seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

**Note**: Consulte <u>Informações Importantes sobre</u> Comandos <u>de Depuração</u> antes de usar comandos debug.

**Cuidado**: no ASA, você pode definir vários níveis de depuração; por padrão, o nível 1 é usado. Se você alterar o nível de depuração, a verbosidade das depurações aumentará. Faça isso com cuidado, especialmente em ambientes de produção.

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