Cisco IOS إلى Android StrongSwan من IKEv2 مع EAP و RSA ةقداصم

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين إصدار الهاتف المحمول من StrongSwan للوصول إلى بوابة VPN ببرنامج Cisco IOS® من خلال بروتوكول تبادل مفتاح الإنترنت الإصدار 2 (IKEv2).

وهناك ثلاثة أمثلة على ذلك:

- هاتف Android مع StrongWAN الذي يتصل ببوابة VPN ببرنامج Cisco IOS مع بروتوكول المصادقة المتوسع - مصادقة الرسالة (EAP-MD5) Digest 5).
- هاتف Android مع StrongSwan الذي يتصل ببوابة VPN ببرنامج Cisco IOS مع مصادقة الشهادة (RSA).
- هاتف Android مع StrongSwan الذي يتصل ب ال cisco ios برمجية VPN مدخل خلف شبكة عنوان ترجمة

(NAT). هناك متطلب أن يكون لديك ملحقان x509 موضوعان اسم بديل في شهادة عبارة VPN.
كما يتم تضمين برنامج Cisco IOS وقيود StrongSwan.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين OpenSSL
- معرفة أساسية بتكوين واجهة سطر الأوامر (CLI) لبرنامج Cisco IOS Software
- معرفة أساسية ب IKEv2

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Android 4.0 أو إصدار أحدث مع StrongSwan
- برنامج IOS الإصدار 15.3T من Cisco أو إصدار أحدث
- برنامج محرك خدمات الهوية من Cisco، الإصدار 1.1.4 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

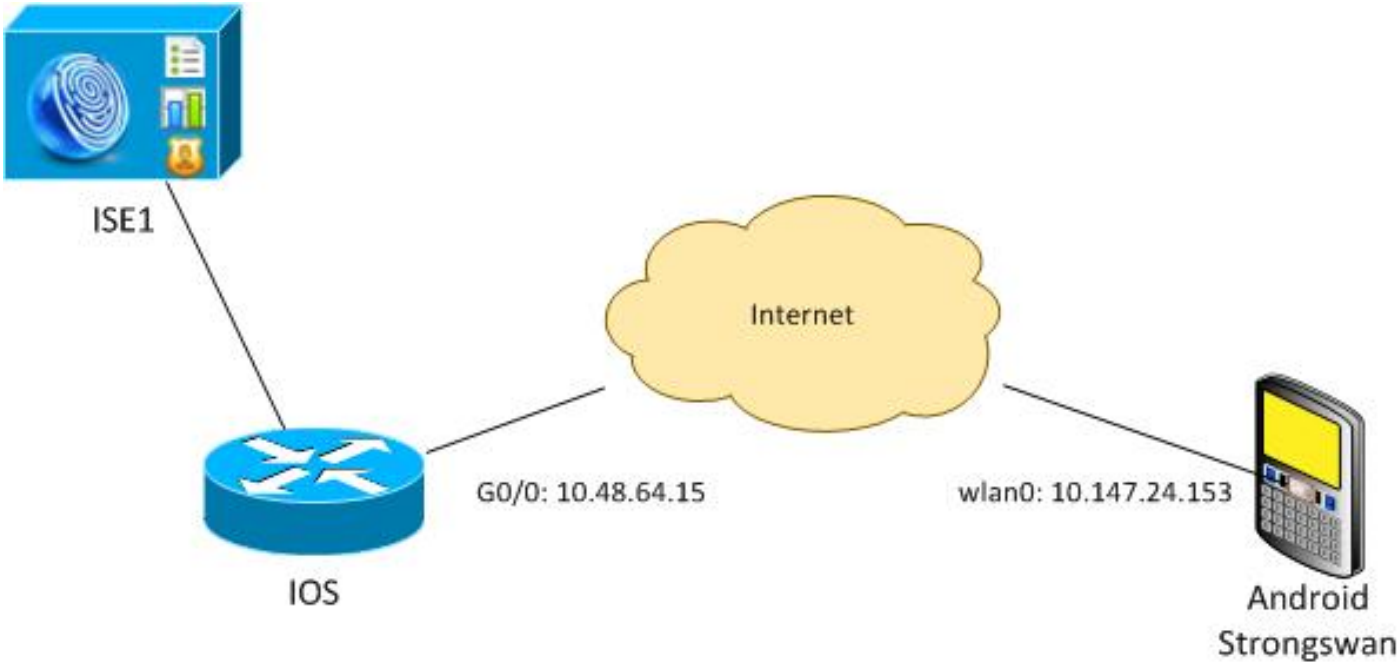
التكوين

ملاحظات:

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

الرسم التخطيطي للشبكة



يقوم Android StrongSwan بإنشاء نفق IKEv2 مع بوابة برنامج Cisco IOS للوصول إلى الشبكات الداخلية بشكل آمن.

تسجيل الشهادة

الشهادات هي شرط أساسي لكل من المصادقة المستندة إلى EAP والمصادقة المستندة إلى RSA.

في سيناريو مصادقة EAP، يلزم وجود شهادة فقط على بوابة الشبكة الخاصة الظاهرية (VPN). يتصل العميل ببرنامج Cisco IOS فقط عندما يقدم البرنامج شهادة موقعة من قبل مرجع مصدق (CA) موثوق به على Android. ثم تبدأ جلسة EAP للعميل للمصادقة على برنامج Cisco IOS software.

بالنسبة للمصادقة المستندة إلى RSA، يجب أن يكون لكلا نقطتي النهاية شهادة صحيحة.

عند إستخدام عنوان IP كمعرف نظير، هناك متطلبات إضافية للشهادة. يتحقق Android StrongSwan من تضمين عنوان IP الخاص ببوابة VPN في الاسم البديل لموضوع الامتداد x509. وإذا لم يكن الأمر كذلك، يقوم نظام التشغيل Android بإسقاط الاتصال، فهذه ممارسة جيدة بالإضافة إلى توصية خاصة ب RFC 6125.

يتم إستخدام OpenSSL كمرجع مصدق لأن برنامج Cisco IOS لديه تحديد: لا يمكنه إنشاء شهادات باستخدام ملحق يتضمن عنوان IP. يتم إنشاء جميع الشهادات بواسطة OpenSSL ويتم إستيرادها إلى Android وبرنامج Cisco IOS.

في برنامج Cisco IOS software، يمكن إستخدام الأمر **subject-name** لإنشاء ملحق يتضمن عنوان IP، ولكن الأمر يعمل فقط مع الشهادات الموقعة ذاتيا. يعد معرف تصحيح الأخطاء من "IOS PKI ،CSCui44783 Cisco يمكن إنشاء CSR مع امتداد subject-alt-name"، طلب تحسين للسماح لبرنامج Cisco IOS بإنشاء الملحق لجميع أنواع عمليات التسجيل.

هذا مثال من الأمر أن يخلق CA:

```
generate key#
openssl genrsa -des3 -out ca.key 2048

generate CSR#
openssl req -new -key ca.key -out ca.csr

remove protection#
```

```
cp ca.key ca.key.org
openssl rsa -in ca.key.org -out ca.key

self sign certificate#
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
extensions v3_req -extfile conf_global.crt-
```

conf_global.crt هو ملف تكوين. يجب تعيين ملحق المرجع المصدق على TRUE:

```
[ req ]
default_bits            = 1024          # Size of keys
default_md              = md5                   # message digest algorithm
string_mask             = nombstr       # permitted characters
string_mask             = pkix  # permitted characters#
distinguished_name      = req_distinguished_name
req_extensions          = v3_req

[ v3_req ]
basicConstraints        = CA:TRUE
subjectKeyIdentifier    = hash
```

الأوامر التي تقوم بإنشاء شهادة متشابهة جدا لبرنامج Cisco IOS و Android. يفترض هذا المثال وجود مرجع مصدق مستخدم لتوقيع الشهادة بالفعل:

```
generate key#
openssl genrsa -des3 -out server.key 2048

generate CSR#
openssl req -new -key server.key -out server.csr

remove protection#
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key

sign the cert and add Alternate Subject Name extension from#
conf_global_cert.crt file with configuration
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
out server.crt -days 365 -extensions v3_req -extfile conf_global_cert.crt-

create pfx file containig CA cert and server cert#
openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
certfile ca.crt-
```

conf_global_cert.crt هو ملف تكوين. يعد ملحق اسم الموضوع البديل إعداد مفتاح. في هذا المثال، يتم تعيين ملحق CA على FALSE:

```
[ req ]
default_bits            = 1024          # Size of keys
default_md              = md5                   # message digest algorithm
string_mask             = nombstr       # permitted characters
string_mask             = pkix  # permitted characters#
distinguished_name      = req_distinguished_name
req_extensions          = v3_req

[ v3_req ]
basicConstraints        = CA:FALSE
subjectKeyIdentifier    = hash
subjectAltName          = @alt_names

[alt_names]
IP.1                    = 10.48.64.15
```

يجب إنشاء شهادة لكل من برنامج Cisco IOS و Android.

ينتمي عنوان IP 10.48.64.15 إلى بوابة برنامج Cisco IOS. عند إنشاء شهادة لبرنامج Cisco IOS، تأكد من تعيين subjectAltName على 10.48.64.15. يتحقق Android من الشهادة التي تم تلقيها من برنامج Cisco IOS ويحاول العثور على عنوان IP الخاص به في subjectAltName.

برنامج Cisco من IOS

يحتاج برنامج Cisco IOS إلى تثبيت شهادة صحيحة لكل من المصادقة المستندة إلى RSA والمصادقة المستندة إلى EAP.

يمكن إستيراد ملف PFX (والذي هو حاوية PKCS12) لبرنامج Cisco IOS:

```
BSAN-2900-1(config)# crypto pki import TP pkcs12
http://10.10.10.1/server.pfx password 123456
...Importing pkcs12 %
?[Source filename [server.pfx
.CRYPTO_PKI: Imported PKCS12 file successfully
```

أستخدم الأمر **show crypto pki certificates verbose** للتحقق من نجاح الاستيراد:

```
BSAN-2900-1# show crypto pki certificates verbose
                                        Certificate
                                  Status: Available
                                  Version: 3
Certificate Serial Number (hex): 00A003C5DCDEFA146C
                Certificate Usage: General Purpose
                                      :Issuer
                                    cn=Cisco
                                 ou=Cisco TAC
                                    o=Cisco
                                   l=Krakow
                                st=Malopolskie
                                      c=PL
                                  :Subject
                                Name: IOS
                        IP Address: 10.48.64.15
                                  cn=IOS
                                  ou=TAC
                                 o=Cisco
                                l=Krakow
                               st=Malopolska
                                  c=PL
                                :Validity Date
                    start date: 18:04:09 UTC Aug 1 2013
                    end   date: 18:04:09 UTC Aug 1 2014
                                :Subject Key Info
                    Public Key Algorithm: rsaEncryption
                            (RSA Public Key: (2048 bit
            Signature Algorithm: SHA1 with RSA Encryption
        Fingerprint MD5: 2C45BF10 0BACB98D 444F5804 1DC27ECF
    Fingerprint SHA1: 26B66A66 DF5E7D6F 498DD653 A2C164D7 4C7A7F8F
                                :X509v3 extensions
X509v3 Subject Key ID: AD598A9B 8AB6893B AB3CB8B9 28B2039C 78441E72
                                :X509v3 Basic Constraints
                                    CA: FALSE
                          :X509v3 Subject Alternative Name
```

```
10.48.64.15
Authority Info Access:
Associated Trustpoints: TP
Storage: nvram:Cisco#146C.cer
Key Label: TP
Key storage device: private config

CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 00DC8EAD98723DF56A
Certificate Usage: General Purpose
Issuer:
  cn=Cisco
  ou=Cisco TAC
  o=Cisco
  l=Krakow
  st=Malopolskie
  c=PL
Subject:
  cn=Cisco
  ou=Cisco TAC
  o=Cisco
  l=Krakow
  st=Malopolskie
  c=PL
Validity Date:
  start date: 16:39:55 UTC Jul 23 2013
  end   date: 16:39:55 UTC Jul 23 2014
Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 0A2432DC 33F0DC46 AAB23E26 ED474B7E
Fingerprint SHA1: A50E3892 ED5C4542 FA7FF584 DE07B6E0 654A62D0
X509v3 extensions:
  X509v3 Subject Key ID: 786F263C 0F5A1963 D6AD18F8 86DCE7C9 0185911E
  X509v3 Basic Constraints:
    CA: TRUE
  Authority Info Access:
Associated Trustpoints: TP
Storage: nvram:Cisco#F56ACA.cer

BSAN-2900-1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.64.15     YES NVRAM  up                    up
```

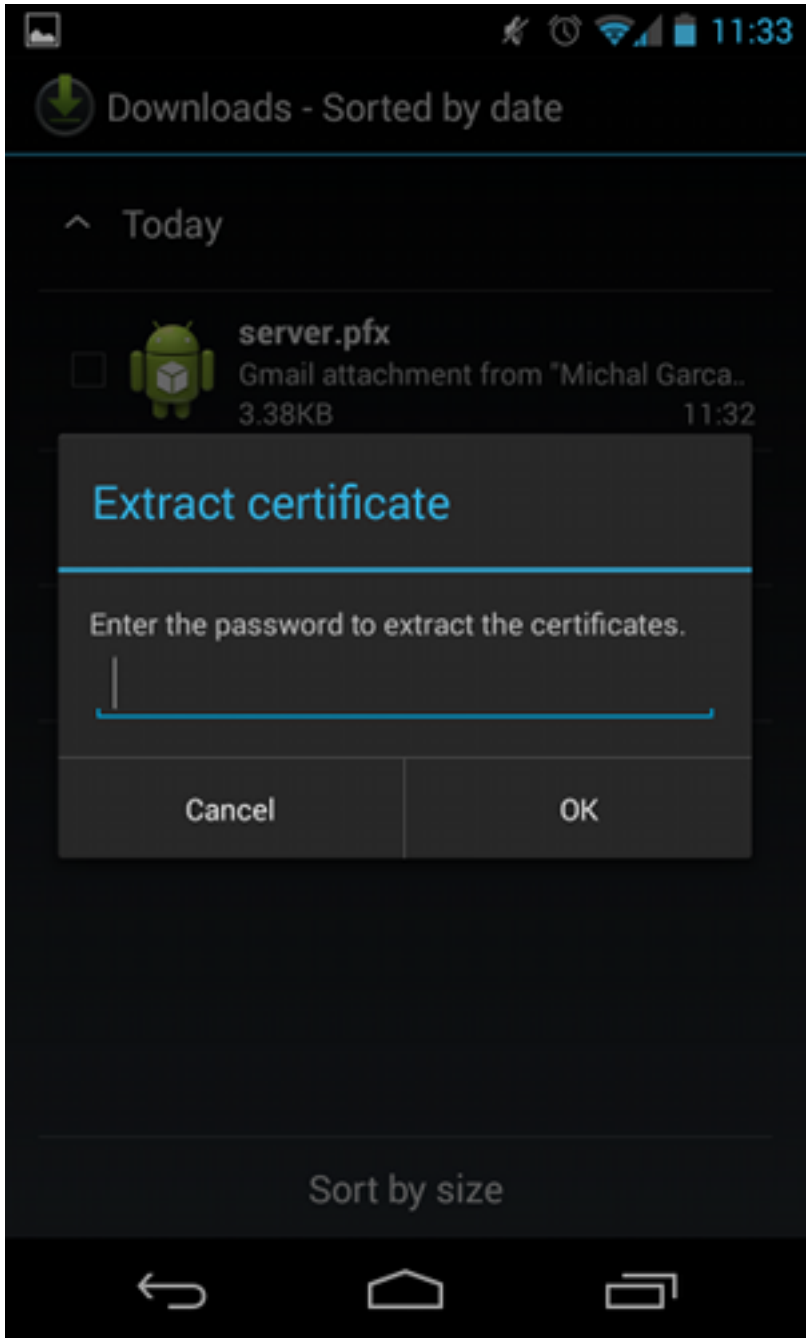
أندرويد

بالنسبة للمصادقة المستندة إلى EAP، يجب تثبيت شهادة CA الصحيحة على وجه التحديد.

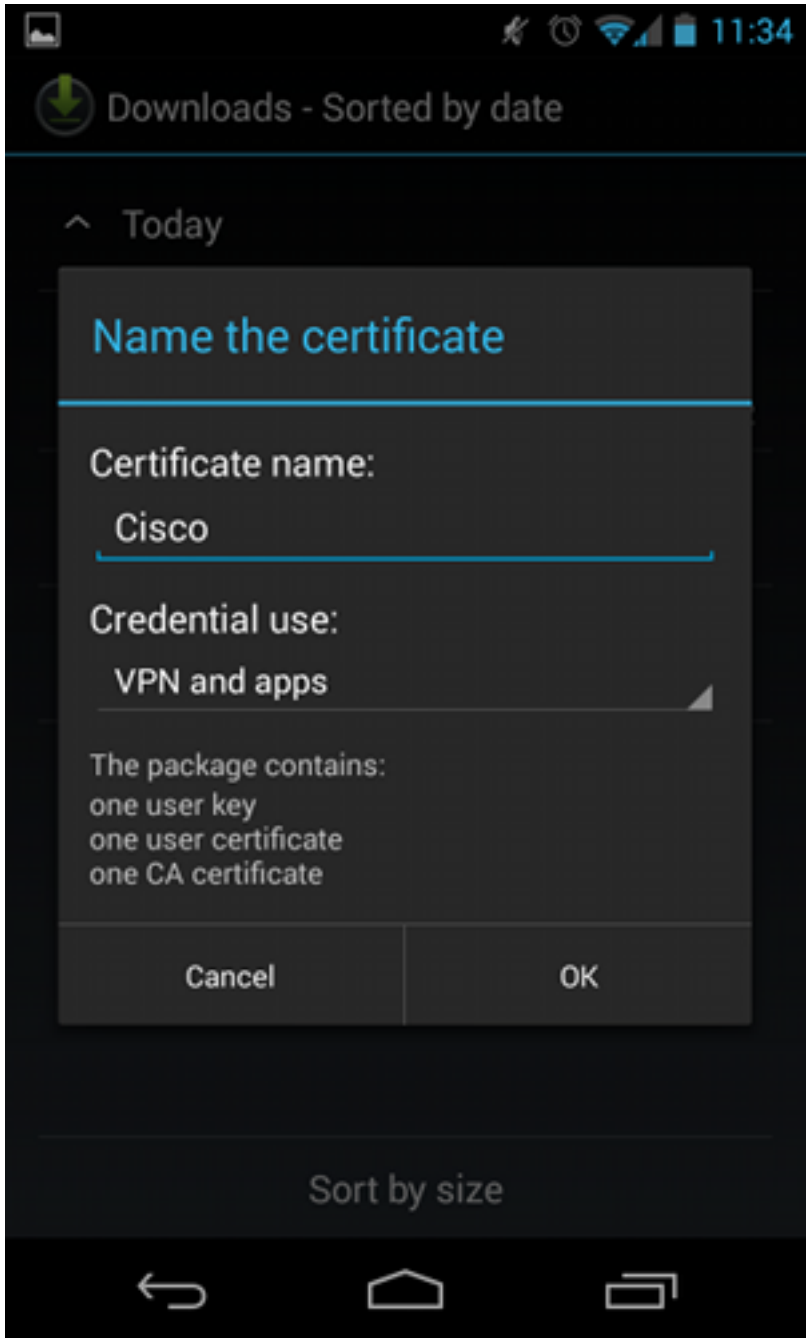
بالنسبة للمصادقة المستندة إلى RSA، يلزم أن تكون شهادة CA وشهادتها مثبتة على حد سواء.

يوضح هذا الإجراء كيفية تثبيت كلا الشهادتين:

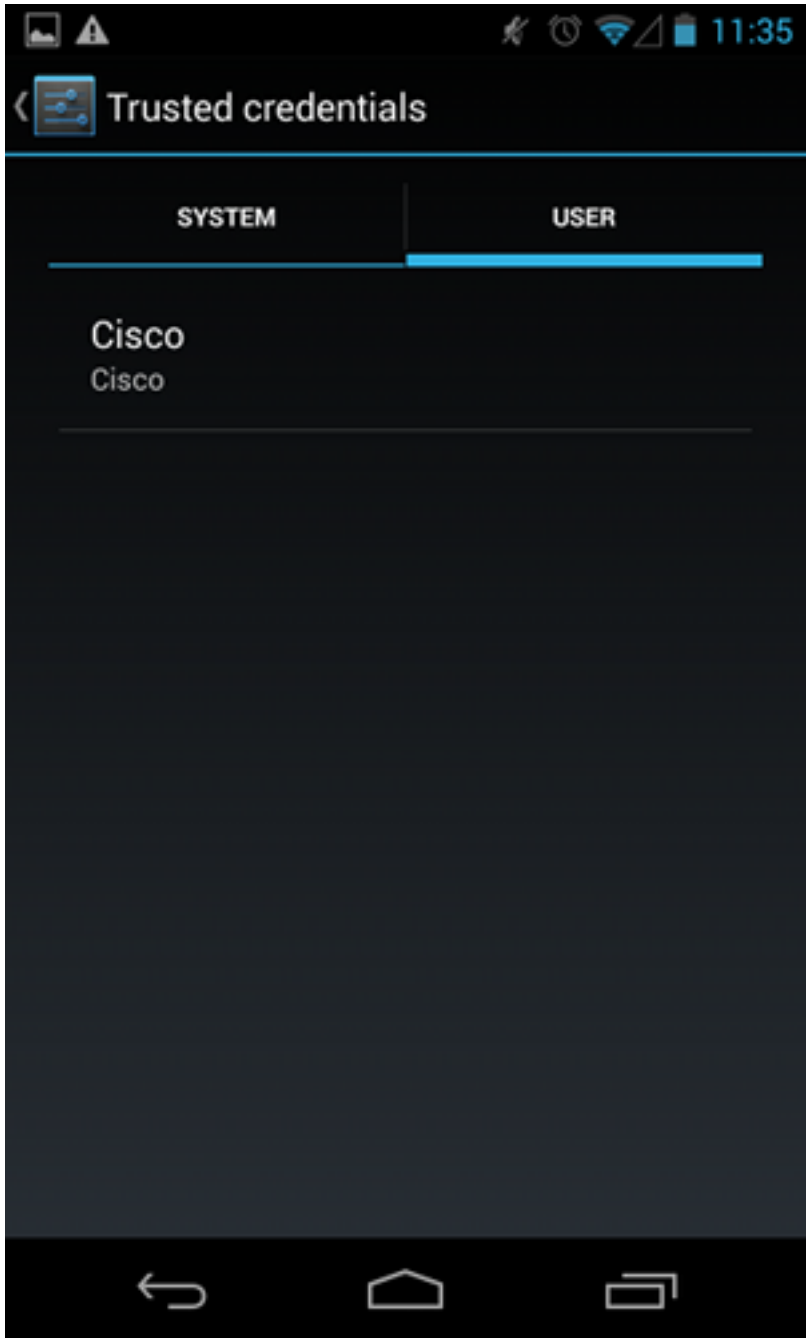
1. أرسل ملف PFX بالبريد الإلكتروني، وافتحه.
2. قم بتوفير كلمة المرور التي تم إستخدامها عند إنشاء ملف pfx.



3. قم بتوفير اسم الشهادة المستوردة.



انتقل إلى **الإعدادات** > **التأمين** > **بيانات الاعتماد الموثوق بها** للتحقق من تثبيت الشهادة. يجب أن تظهر الشهادة4.
الجديدة في مخزن المستخدم:



عند هذه النقطة، يتم تثبيت شهادة مستخدم بالإضافة إلى شهادة مرجع مصدق. ملف PFX هو حاوية PKCS12 مع كل من شهادة المستخدم وشهادة CA.

تشتمل Android على متطلبات دقيقة عند إستيراد الشهادات. على سبيل المثال، من أجل إستيراد شهادة CA بنجاح، يتطلب Android تعيين CA الخاص بقيد أساسي لامتداد x509v3 إلى TRUE. لذلك عندما تقوم بإنشاء مرجع مصدق أو باستخدام المرجع المصدق الخاص بك، فمن المهم التحقق من أن له الملحق الصحيح:

```
pluton custom_ca # openssl x509 -in ca.crt -text
                                        :Certificate
                                      ;Data&colon
                                (Version: 3 (0x2
                                  :Serial Number
                             dc:8e:ad:98:72:3d:f5:6a
                    Signature Algorithm: sha1WithRSAEncryption
Issuer: C=PL, ST=Malopolskie, L=Krakow, O=Cisco, OU=Cisco TAC, CN=Cisco
                                    <output omitted.....>

                                :X509v3 Basic Constraints
                                  CA:TRUE
```

```
<output omitted.....>
```

مصادقة EAP

تكوين برنامج Cisco IOS لمصادقة EAP

يسمح IKEv2 باستخدام مكدس بروتوكول EAP لإجراء مصادقة المستخدم. تقدم بوابة الشبكة الخاصة الظاهرية (VPN) نفسها مع الشهادة. وبمجرد أن يثق العميل في تلك الشهادة، يستجيب العميل لهوية طلب EAP من البوابة. يستخدم برنامج Cisco IOS software تلك الهوية ويرسل رسالة طلب RADIUS إلى خادم المصادقة والتفويض والمحاسبة (AAA)، ويتم إنشاء جلسة عمل EAP-MD5 بين الطالب (Android) وخادم المصادقة (خادم التحكم في الوصول [ACS] أو ISE).

بعد مصادقة EAP-MD5 الناجحة، كما هو موضح بواسطة رسالة قبول RADIUS، يستخدم برنامج Cisco IOS software وضع التكوين لدفع عنوان IP إلى العميل ومتابعة تفاوض محدد حركة مرور البيانات.

لاحظ أن Android قد أرسل IKEID=cisco (كما تم تكوينه). يتطابق هذا IKEID الذي تم تلقيه على برنامج Cisco IOS مع 'PROF' لملف تعريف IKEv2'.

```
                                                aaa new-model
                                aaa authentication login eap-list-radius group radius
                                    aaa authorization network IKE2_AUTHOR_LOCAL local

                                                crypto pki trustpoint TP
                                                  revocation-check none

                                crypto ikev2 authorization policy IKE2_AUTHOR_POLICY
                                                        pool POOL
                                                                !
                                        crypto ikev2 proposal ikev2-proposal
                                                     encryption aes-cbc-128
                                                             integrity sha1
                                                                   group 14
                                                                !
                                            crypto ikev2 policy ikev2-policy
                                                    proposal ikev2-proposal
                                                                !
                                                                !
                                                        crypto ikev2 profile PROF
                                                  match identity remote key-id cisco
                                               authentication remote eap query-identity
                                                        authentication local rsa-sig
                                                             pki trustpoint TP
                                                  aaa authentication eap eap-list-radius
                        aaa authorization group eap list IKE2_AUTHOR_LOCAL IKE2_AUTHOR_POLICY
                                                    aaa authorization user eap cached
                                                         virtual-template 1

                                    crypto ipsec transform-set 3DES-MD5 esp-aes esp-sha-hmac
                                                                mode tunnel
                                                                !
                                                    crypto ipsec profile PROF
                                                set transform-set 3DES-MD5
                                                    set ikev2-profile PROF
```

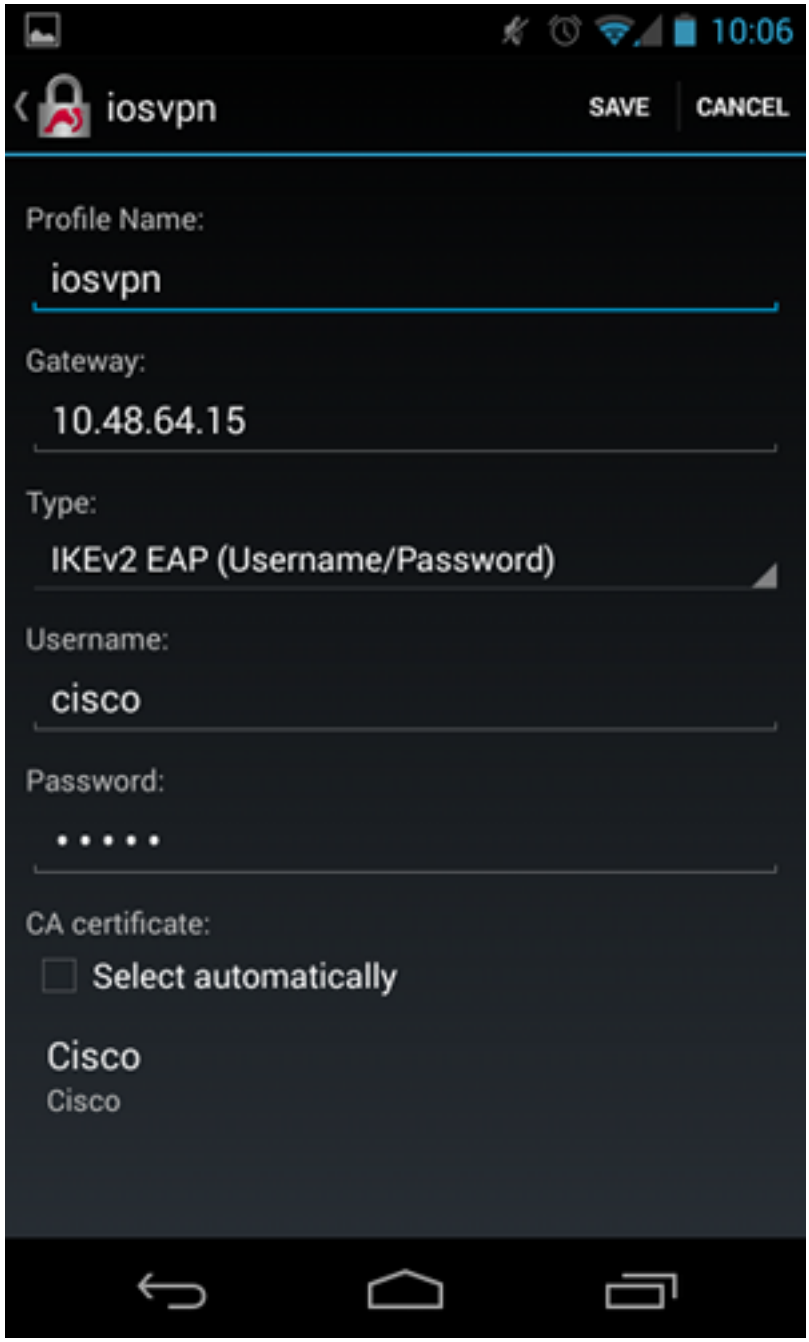
```
interface GigabitEthernet0/0
 ip address 10.48.64.15 255.255.255.128

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROF

ip local pool POOL 192.168.0.1 192.168.0.10

radius-server host 10.48.66.185 key cisco
```

تكوين Android لمصادقة EAP

يجب أن يحتوي Android StrongSwan على EAP مكون:

1. قم بتعطيل تحديد الشهادة التلقائي، وإلا يتم إرسال 100 أو أكثر من CERT_REQs في الحزمة الثالثة.

2. أختر شهادة معينة (CA) تم إستيرادها في الخطوة السابقة، ويجب أن يكون اسم المستخدم وكلمة المرور نفس الشيء كما هو الحال على خادم AAA.



إختبار مصادقة EAP

في برنامج Cisco IOS software، تكون هذه هي أهم تصحيح الأخطاء لمصادقة EAP. تم حذف معظم المخرجات للوضوح:

```
debug crypto ikev2 error
debug crypto ikev2 internal
debug radius authentication
debug radius verbose

IKEv2:New ikev2 sa request admitted
IKEv2:(SA ID = 1):Searching policy based on peer's identity 'cisco' of type
'FQDN'
IKEv2:(1): Choosing IKE profile PROF
IKEv2:Sending certificates as X509 certificates

RADIUS(00000025): Send Access-Request to 10.48.66.185:1645 id 1645/4,len 110
RADIUS: Received from id 1645/4 10.48.66.185:1645, Access-Challenge, len 79
```

```
RADIUS(00000025): Send Access-Request to 10.48.66.185:1645 id 1645/5,len 141
RADIUS: Received from id 1645/5 10.48.66.185:1645, Access-Challenge, len 100
RADIUS(00000025): Send Access-Request to 10.48.66.185:1645 id 1645/6,len 155
    RADIUS: Received from id 1645/6 10.48.66.185:1645, Access-Accept, len 76

IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=AABAB198FACAAEDE R_SPI=D61F37C4DC875001
     R) MsgID = 00000004 CurState: R_PROC_EAP_RESP Event: EV_RECV_EAP_SUCCESS)

                'IKEv2:IKEv2 local AAA author request for 'IKE2_AUTHOR_POLICY
IKEv2:Received group author attributes: ipv4-pool: POOL, route-accept any tag:1
                                                                distance:1
                          IKEv2:Allocated addr 192.168.0.2 from local pool POOL
IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=AABAB198FACAAEDE R_SPI=D61F37C4DC875001
                            :R) MsgID = 00000005 CurState: R_VERIFY_AUTH Event)
                                                EV_OK_RECD_VERIFY_IPSEC_POLICY
LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state%
                                                                to up
```

تشير سجلات Android إلى:

```
                                ,DMN] Starting IKE charon daemon (strongSwan 5.1.0dr2]00
                                                    (Linux 3.4.0-perf-gf43c3d9, armv7l
                      KNL] kernel-netlink plugin might require CAP_NET_ADMIN capability]00
                  LIB] loaded plugins: androidbridge charon android-log openssl fips-prf]00
                random nonce pubkey pkcs1 pkcs8 pem xcbc hmac socket-default kernel-netlink
                    (LIB] unable to load 9 plugin features (9 due to unmet dependencies]00
                                                    JOB] spawning 16 worker threads]00
                                    IKE] initiating IKE_SA android[1] to 10.48.64.15]13
[ (ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP]13
                      [NET] sending packet: from 10.147.24.153[45581] to 10.48.64.15[500]13
                                                                    (bytes 648)
                    [NET] received packet: from 10.48.64.15[500] to 10.147.24.153[45581]11
                                                                    (bytes 497)
 (ENC] parsed IKE_SA_INIT response 0 [ SA KE No V V N(NATD_S_IP) N(NATD_D_IP]11
                                                    [ (CERTREQ N(HTTP_CERT_LOOK
                                                :ENC] received unknown vendor ID]11
                                43:49:53:43:4f:2d:44:45:4c:45:54:45:2d:52:45:41:53:4f:4e
                                                :ENC] received unknown vendor ID]11
                                      46:4c:45:58:56:50:4e:2d:53:55:50:50:4f:52:54:45:44
                                IKE] faking NAT situation to enforce UDP encapsulation]11
                                        IKE] cert payload ANY not supported - ignored]11
    ,IKE] sending cert request for "C=PL, ST=Malopolskie, L=Krakow, O=Cisco]11
                                                        "OU=Cisco TAC, CN=Cisco
                                                IKE] establishing CHILD_SA android]11
                          ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ]11
                            (CP(ADDR ADDR6 DNS DNS6) N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP
                      [NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]11
                                                                    (bytes 508)
                       [NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]10
                                                                    (bytes 1292)
                             [ ENC] parsed IKE_AUTH response 1 [ V IDr CERT AUTH EAP/REQ/ID]10
     ,IKE] received end entity cert "C=PL, ST=Malopolska, L=Krakow, O=Cisco]10
                                                        "OU=TAC, CN=IOS
    ,CFG] using certificate "C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC]10
                                                                    "CN=IOS
,CFG] using trusted ca certificate "C=PL, ST=Malopolskie, L=Krakow, O=Cisco]10
                                                        "OU=Cisco TAC, CN=Cisco
                                CFG] reached self-signed root ca with a path length of 0]10
                          IKE] authentication of '10.48.64.15' with RSA signature successful]10
                               'IKE] server requested EAP_IDENTITY (id 0x3B), sending 'cisco]10
                                            [ ENC] generating IKE_AUTH request 2 [ EAP/RES/ID]10
                      [NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]10
                                                                    (bytes 76)
```

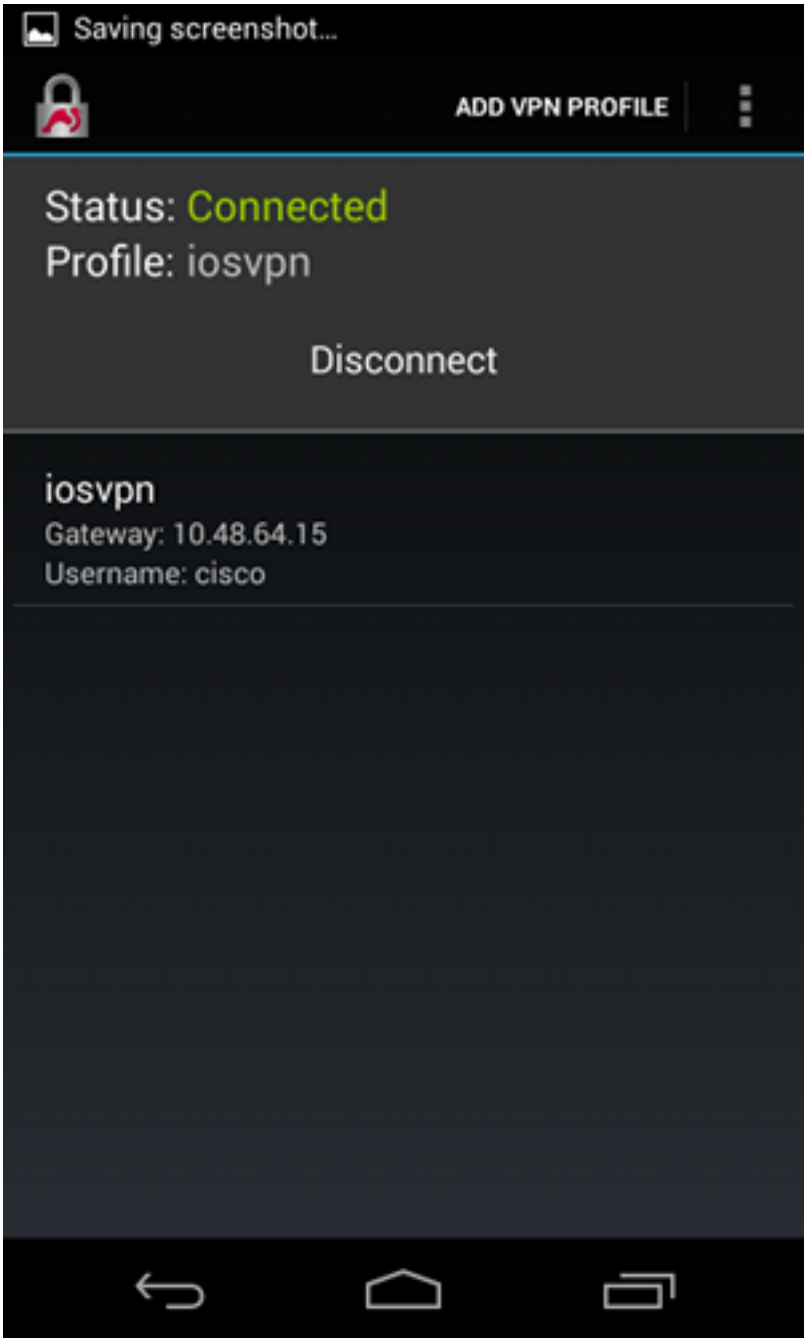
```
[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]09
                                                                (bytes 76)
                        [ ENC] parsed IKE_AUTH response 2 [ EAP/REQ/TLS]09
                (IKE) server requested EAP_TLS authentication (id 0x59]09
                        IKE] EAP method not supported, sending EAP_NAK]09
                   [ ENC] generating IKE_AUTH request 3 [ EAP/RES/NAK]09
 [NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]09
                                                                (bytes 76)
[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]08
                                                                (bytes 92)
                        [ ENC] parsed IKE_AUTH response 3 [ EAP/REQ/MD5]08
                (IKE) server requested EAP_MD5 authentication (id 0x5A]08
                   [ ENC] generating IKE_AUTH request 4 [ EAP/RES/MD5]08
 [NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]08
                                                                (bytes 92)
[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]07
                                                                (bytes 76)
                           [ ENC] parsed IKE_AUTH response 4 [ EAP/SUCC]07
                 IKE] EAP method EAP_MD5 succeeded, no MSK established]07
                      IKE] authentication of 'cisco' (myself) with EAP]07
                           [ ENC] generating IKE_AUTH request 5 [ AUTH]07
 [NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]07
                                                                (bytes 92)
[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]06
                                                               (bytes 236)
(ENC] parsed IKE_AUTH response 5 [ AUTH CP(ADDR) SA TSi TSr N(SET_WINSIZE]06
                                      [ (N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG
               IKE] authentication of '10.48.64.15' with EAP successful]06
                                   IKE] IKE_SA android[1] established between]06
                                  [cisco]...10.48.64.15[10.48.64.15]10.147.24.153
                                            IKE] scheduling rekeying in 35421s]06
                                          IKE] maximum IKE_SA lifetime 36021s]06
                                   IKE] installing new virtual IP 192.168.0.1]06
 IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding]06
 IKE] CHILD_SA android{1} established with SPIs c776cb4f_i ea27f072_o and]06
                                               TS 192.168.0.1/32 === 0.0.0.0/0
                        {DMN] setting up TUN device for CHILD_SA android{1]06
                                      DMN] successfully created TUN device]06
```

يوضح هذا المثال كيفية التحقق من الحالة على برنامج Cisco IOS software:

```
                                                BSAN-2900-1#show crypto session detail
                                                        Crypto session current status

                                    Code: C - IKE Configuration mode, D - Dead Peer Detection
                                    K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
                                       X - IKE Extended Authentication, F - IKE Fragmentation

                                                          Interface: Virtual-Access1
                                                                   Uptime: 00:02:12
                                                    Session status: UP-ACTIVE
                                     (Peer: 10.147.24.153 port 60511 fvrf: (none) ivrf: (none
                                                        Phase1_id: cisco
                                                            (Desc: (none
                IKEv2 SA: local 10.48.64.15/4500 remote 10.147.24.153/60511 Active
                                        Capabilities:NX connid:1 lifetime:23:57:48
                                  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.0.2
                                                Active SAs: 2, origin: crypto map
                                 Inbound:  #pkts dec'ed 40 drop 0 life (KB/Sec) 4351537/3468
                                 Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) 4351542/3468

                                                BSAN-2900-1#show crypto ikev2 sa detailed
                                                          IPv4 Crypto IKEv2  SA
```

```
Tunnel-id Local                  Remote                fvrf/ivrf         Status
 none/none          READY   10.147.24.153/60511      10.48.64.15/4500         1
     ,Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA
                                                                Auth verify: EAP
                                          Life/Active Time: 86400/137 sec
                                               CE id: 1002, Session-id: 2
                                     Status Description: Negotiation done
          Local spi: D61F37C4DC875001       Remote spi: AABAB198FACAAEDE
                                                 Local id: 10.48.64.15
                                                      Remote id: cisco
                                                  Remote EAP id: cisco
                 Local req msg id:  0              Remote req msg id:  6
                 Local next msg id: 0              Remote next msg id: 6
                 Local req queued:  0              Remote req queued:  6
                 Local window:      5              Remote window:      1
                                    DPD configured for 0 seconds, retry 0
                                            .Fragmentation not configured
                                          .Extended Authentication configured
                                                   NAT-T is detected  outside
                                     Cisco Trust Security SGT is disabled
                                          Assigned host addr: 192.168.0.2
                                                 Initiator of SA : No
```

توضح هذه الأرقام كيفية التحقق من الحالة على Android:


Saving screenshot...
ADD VPN PROFILE
Status: Connected
Profile: iosvpn
Disconnect
iosvpn
Gateway: 10.48.64.15
Username: cisco

مصادقة RSA

تكوين برنامج Cisco IOS لمصادقة RSA

في مصادقة RSA (Rivest-Shamir-Adleman)، يرسل Android الشهادة للمصادقة على برنامج Cisco IOS software. ولهذا السبب تكون خريطة الشهادة التي تربط حركة المرور بملف تعريف IKEv2 معين مطلوبة. مصادقة EAP للمستخدم غير مطلوبة.

هذا مثال على كيفية تعيين مصادقة RSA للنظير البعيد:

```
crypto pki certificate map CERT_MAP 10
 subject-name co android

crypto ikev2 profile PROF
match certificate CERT_MAP
```

```
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
aaa authorization group cert list IKE2_AUTHOR_LOCAL IKE2_AUTHOR_POLICY
 virtual-template 1
```

تكوين Android لمصادقة RSA

تم إستبدال بيانات اعتماد المستخدم بشهادة المستخدم:

إختبار مصادقة RSA

في برنامج Cisco IOS software، تعد هذه أهم تصحيح الأخطاء لمصادقة RSA. تم حذف معظم المخرجات للوضوح:

```
debug crypto ikev2 error
```

```
debug crypto ikev2 internal
debug crypto pki transactions
debug crypto pki validation
debug crypto pki messages

IKEv2:New ikev2 sa request admitted
,IKEv2:(SA ID = 1):Searching policy based on peer's identity 'cn=android,ou=TAC
'o=Cisco,l=Krakow,st=Malopolska,c=PL' of type 'DER ASN1 DN
IKEv2:(1): Choosing IKE profile PROF
IKEv2:Sending certificates as X509 certificates
'IKEv2:(SA ID = 1):Peer's authentication method is 'RSA
IKEv2:Peer has sent X509 certificates
CRYPTO_PKI: Found a issuer match
CRYPTO_PKI: (9000B) Certificate is verified
CRYPTO_PKI: (9000B) Certificate validation succeeded
IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] Verification of signed
authentication data PASSED

'IKEv2:IKEv2 local AAA author request for 'IKE2_AUTHOR_POLICY
IKEv2:Received group author attributes: ipv4-pool: POOL, route-accept any tag:1
distance:1
IKEv2:Allocated addr 192.168.0.3 from local pool POOL
IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=E53A57E359A8437C R_SPI=A03D273FC75EEBD9
:R) MsgID = 00000001 CurState: R_VERIFY_AUTH Event)
EV_OK_RECD_VERIFY_IPSEC_POLICY
LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state%
to up
```

تشير سجلات Android إلى:

```
,DMN] Starting IKE charon daemon (strongSwan 5.1.0dr2]00
(Linux 3.4.0-perf-gf43c3d9, armv7l
KNL] kernel-netlink plugin might require CAP_NET_ADMIN capability]00
LIB] loaded plugins: androidbridge charon android-log openssl fips-prf]00
random nonce pubkey pkcs1 pkcs8 pem xcbc hmac socket-default
(LIB] unable to load 9 plugin features (9 due to unmet dependencies]00
JOB] spawning 16 worker threads]00
,CFG] loaded user certificate 'C=PL, ST=Malopolska, L=Krakow, O=Cisco]05
OU=TAC, CN=android' and private key
,CFG] loaded CA certificate 'C=PL, ST=Malopolskie, L=Krakow, O=Cisco]05
'OU=Cisco TAC, CN=Cisco

IKE] initiating IKE_SA android[4] to 10.48.64.15]05
[ (ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP]05
[NET] sending packet: from 10.147.24.153[34697] to 10.48.64.15[500]05
(bytes 648)
[NET] received packet: from 10.48.64.15[500] to 10.147.24.153[34697]10
(bytes 497)
(ENC] parsed IKE_SA_INIT response 0 [ SA KE No V V N(NATD_S_IP) N(NATD_D_IP]10
[ (CERTREQ N(HTTP_CERT_LOOK
:ENC] received unknown vendor ID]10
43:49:53:43:4f:2d:44:45:4c:45:54:45:2d:52:45:41:53:4f:4e
:ENC] received unknown vendor ID]10
46:4c:45:58:56:50:4e:2d:53:55:50:50:4f:52:54:45:44
IKE] faking NAT situation to enforce UDP encapsulation]10
IKE] cert payload ANY not supported - ignored]10
,IKE] sending cert request for "C=PL, ST=Malopolskie, L=Krakow, O=Cisco]10
"OU=Cisco TAC, CN=Cisco
,IKE] authentication of 'C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC]10
CN=android' (myself) with RSA signature successful
,IKE] sending end entity cert "C=PL, ST=Malopolska, L=Krakow, O=Cisco]10
"OU=TAC, CN=android
IKE] establishing CHILD_SA android]10
```

```
ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ]10
                        AUTH CP(ADDR ADDR6 DNS DNS6) N(ESP_TFC_PAD_N) SA
  [NET] sending packet: from 10.147.24.153[44527] to 10.48.64.15[4500]10
                                                              (bytes 1788)
  [NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[44527]12
                                                              (bytes 1420)
 ENC] parsed IKE_AUTH response 1 [ V IDr CERT AUTH CP(ADDR) SA TSi TSr]12
                        (N(SET_WINSIZE) N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG
,IKE] received end entity cert "C=PL, ST=Malopolska, L=Krakow, O=Cisco]12
                                                          "OU=TAC, CN=IOS
,CFG] using certificate "C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC]12
                                                                  "CN=IOS
,CFG] using trusted ca certificate "C=PL, ST=Malopolskie, L=Krakow, O=Cisco]12
                                                  "OU=Cisco TAC, CN=Cisco
            CFG] reached self-signed root ca with a path length of 0]12
     IKE] authentication of '10.48.64.15' with RSA signature successful]12
        ,IKE] IKE_SA android[4] established between 10.147.24.153[C=PL]12
                                    ,ST=Malopolska, L=Krakow, O=Cisco, OU=TAC
                                       [CN=android]...10.48.64.15[10.48.64.15
                                        IKE] scheduling rekeying in 35413s]12
                                       IKE] maximum IKE_SA lifetime 36013s]12
                                IKE] installing new virtual IP 192.168.0.3]12
IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding]12
IKE] CHILD_SA android{4} established with SPIs ecb3af87_i b2279175_o and]12
                                                  TS 192.168.0.3/32 === 0.0.0.0/0
                                {DMN] setting up TUN device for CHILD_SA android{4]12
                                DMN] successfully created TUN device]12
```

في برنامج Cisco IOS software، يتم إستخدام RSA لكل من التوقيع والتحقق؛ في السيناريو السابق، تم إستخدام EAP للتحقق:

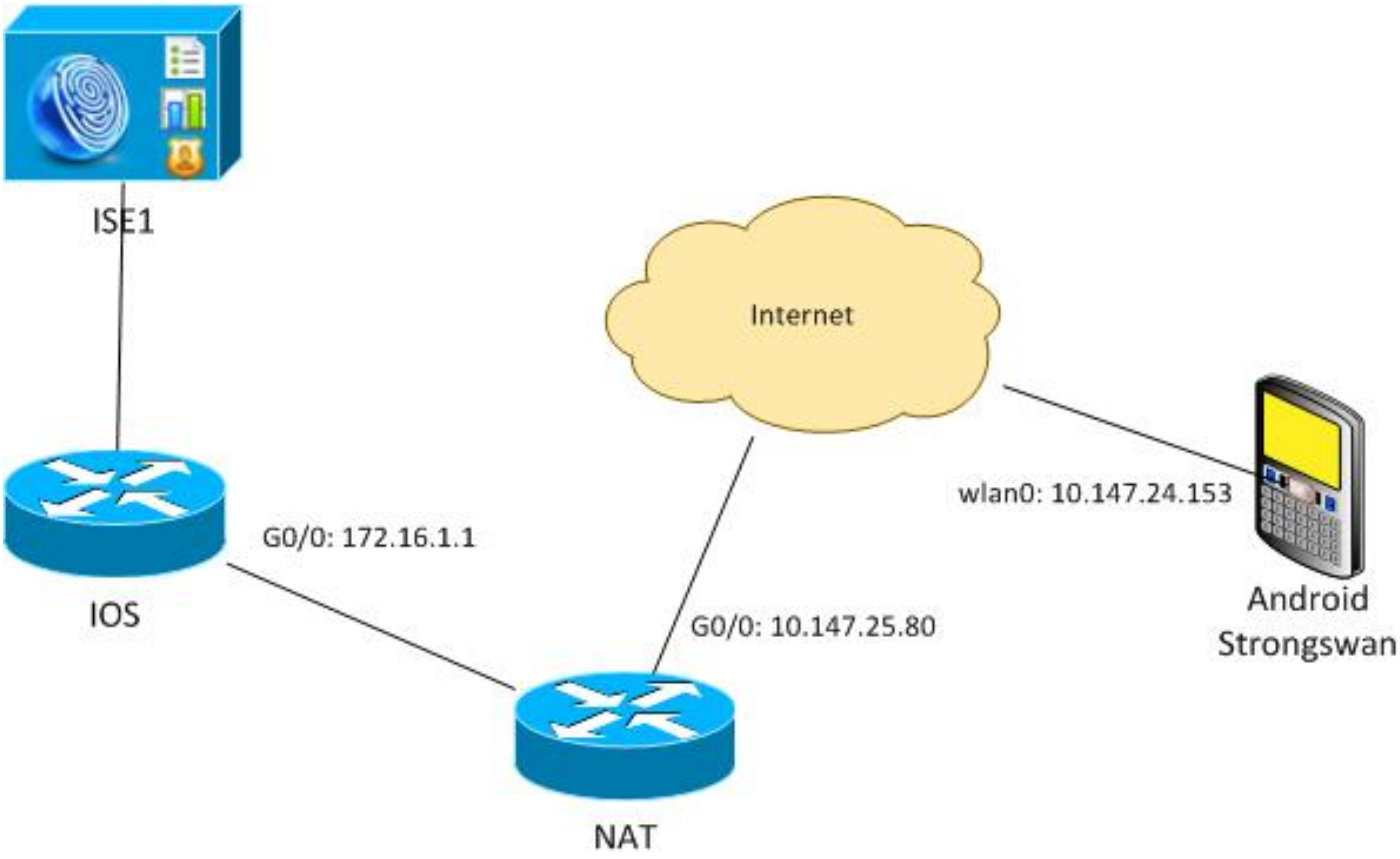
```
                                BSAN-2900-1#show crypto ikev2 sa detailed
                                  IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf          Status
 none/none          READY   10.147.24.153/44527      10.48.64.15/4500         1
      ,Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA
                                                          Auth verify: RSA
                                       Life/Active Time: 86400/16 sec
                                           CE id: 1010, Session-id: 3
                                    Status Description: Negotiation done
          Local spi: A03D273FC75EEBD9       Remote spi: E53A57E359A8437C
                                                 Local id: 10.48.64.15
    Remote id: cn=android,ou=TAC,o=Cisco,l=Krakow,st=Malopolska,c=PL
            Local req msg id:  0              Remote req msg id:  2
            Local next msg id: 0              Remote next msg id: 2
            Local req queued:  0              Remote req queued:  2
            Local window:      5              Remote window:      1
                                 DPD configured for 0 seconds, retry 0
                                         .Fragmentation not configured
                                .Extended Authentication not configured
                                           NAT-T is detected  outside
                                  Cisco Trust Security SGT is disabled
                                       Assigned host addr: 192.168.0.3
                                           Initiator of SA : No
```

يعد التحقق من الحالة على Android مماثلا لذلك الموجود في السيناريو السابق.

عبارة VPN خلف NAT - شبكة StrongWAN وتحديد برنامج Cisco IOS

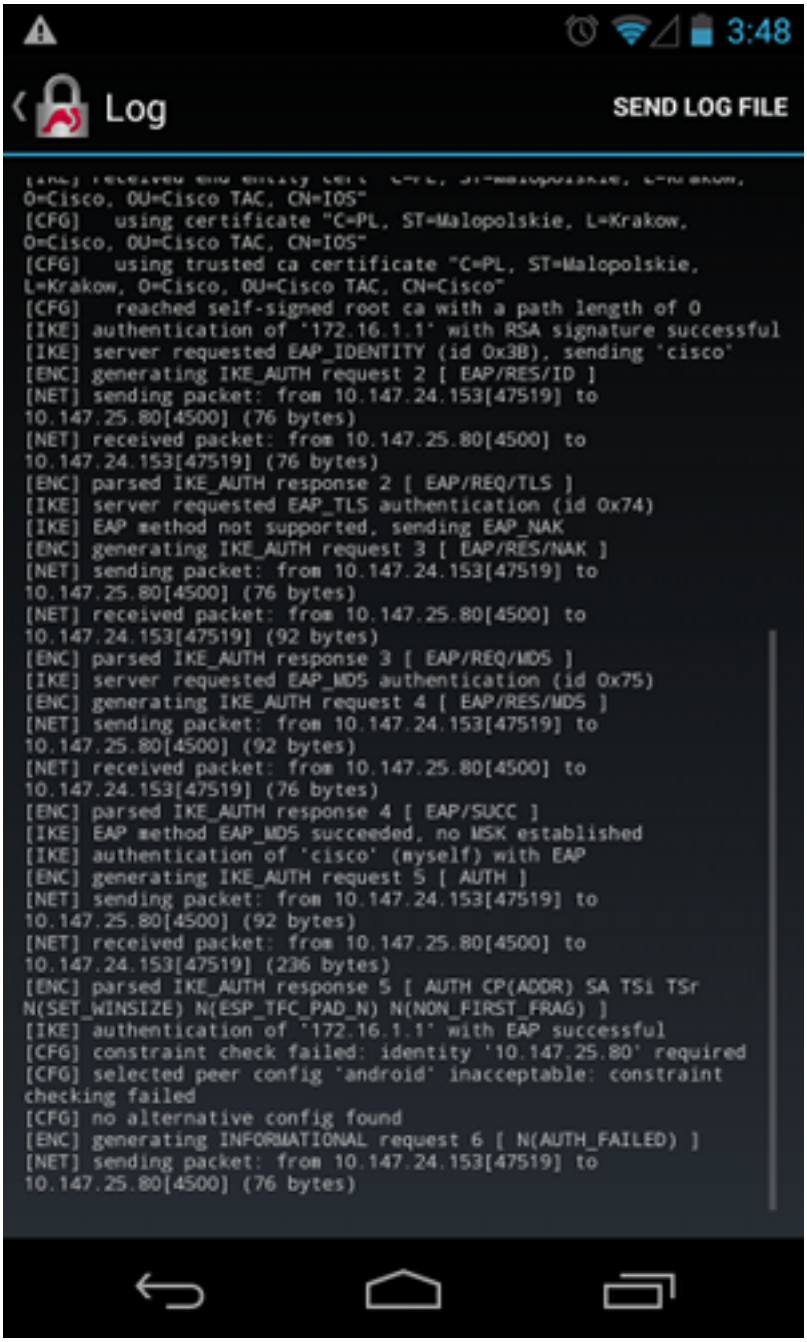
يشرح هذا المثال تحديد عمليات التحقق من شهادة StrongSwan.

بافتراض أن عنوان IP لبوابة VPN ببرنامج Cisco IOS software مترجم بشكل ثابت من 172.16.1.1 إلى 10.147.25.80. يتم إستخدام مصادقة EAP.



افترض أيضا أن شهادة برنامج Cisco IOS تحتوي على اسم بديل للموضوع لكل من 172.16.1.1 و 10.147.25.80.

بعد مصادقة EAP الناجحة، يقوم Android بإجراء التحقق ويحاول العثور على عنوان IP الخاص بالنظير الذي تم إستخدامه في تكوين 10.147.25.80) Android) في ملحق "الاسم البديل للموضوع". فشل التحقق:

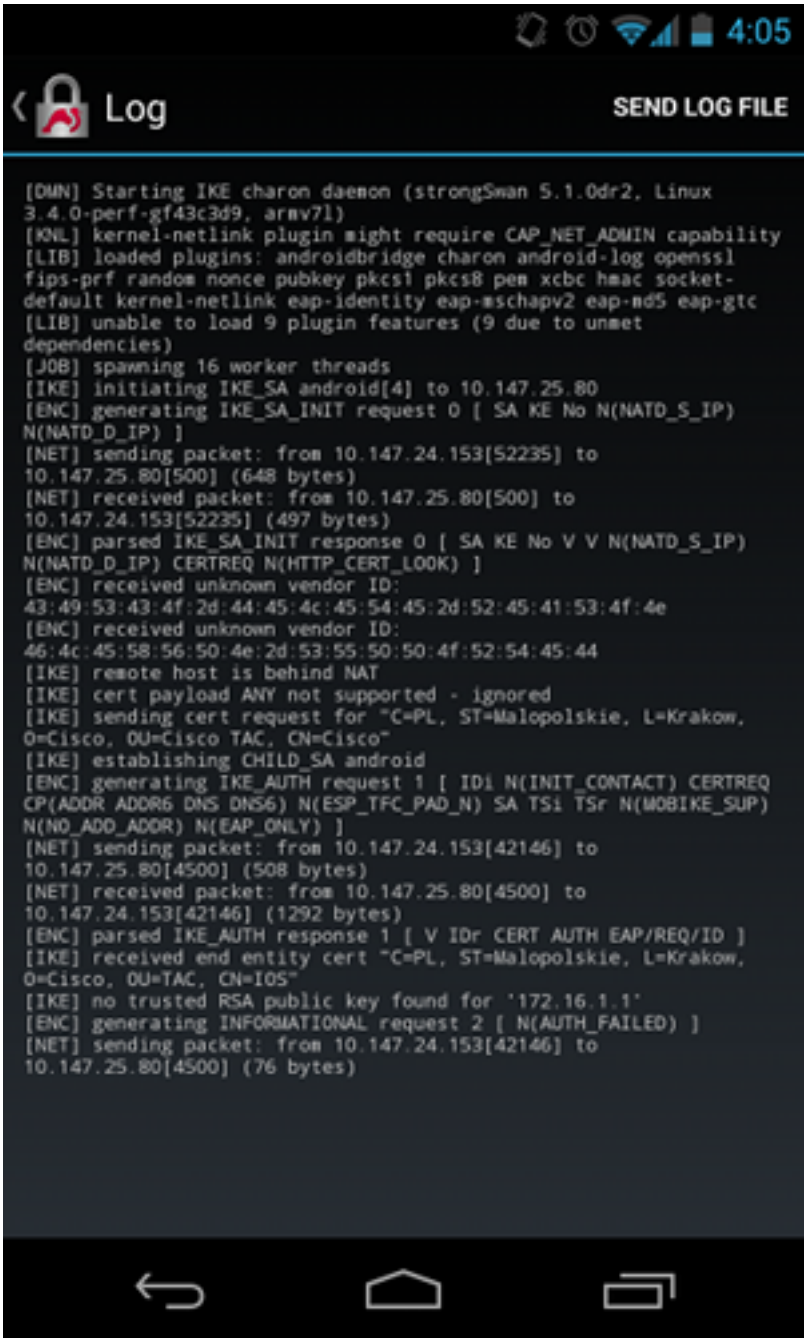


تشير السجلات إلى:

```
constraint check failed: identity '10.147.25.80' required
```

حدث الفشل لأن Android يمكنه قراءة ملحق الاسم البديل للموضوع الأول فقط (172.16.1.1).

الآن، افترض أن شهادة برنامج Cisco IOS تحتوي على كلا العناوين في اسم الموضوع البديل ولكن بالترتيب العكسي: 10.147.25.80 و 172.16.1.1. يقوم Android بإجراء التحقق عندما يستلم IKEID، وهو عنوان IP لبوابة VPN (172.16.1.1)، في الحزمة الثالثة:



والآن يظهر السجل:

```
'no trusted RSA public key found for '172.16.1.1
```

وبالتالي، عندما يستلم Android IKEID، يحتاج إلى العثور على IKEID في اسم الموضوع البديل ويستطيع إستخدام عنوان IP الأول فقط.

ملاحظة: في مصادقة EAP، يكون IKEID الذي يرسل بواسطة برنامج Cisco IOS هو عنوان IP بشكل افتراضي. في مصادقة RSA، يكون iKEID هو DN الشهادة بشكل افتراضي. أستخدم الأمر **identity** ضمن ملف تعريف ikeV2 لتغيير هذه القيم يدويا.

التحقق من الصحة

تتوفر إجراءات التحقق والاختبار ضمن أمثلة التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

CERT_REQ المتعدد ل StrongSwan CA

عندما يكون إعداد الشهادة في StrongSwan هو تحديد تلقائي (الافتراضي)، يرسل Android CERT_REQ لجميع الشهادات الموثوق بها في المخزن المحلي في الحزمة الثالثة . قد يقوم برنامج Cisco IOS software بإسقاط الطلب لأنه يقوم بالتعرف على عدد كبير من طلبات الشهادات على أنها هجوم لمنع الخدمة:

```
*(Jul 15 07:54:13: IKEv2:number of cert req exceeds the reasonable limit (100
```

مصدر النفق على DVTI

على الرغم من أنه من الشائع إلى حد ما تعيين مصدر النفق على واجهة النفق الظاهرية (VTI)، إلا أنه ليس ضروريا هنا. افترض أن أمر **مصدر النفق** تحت VTI ديناميكي (DVTI):

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROF
```

بعد المصادقة، إذا حاول برنامج Cisco IOS software إنشاء واجهة وصول افتراضية يتم نسخها من قالب ظاهري، فإنه يرجع خطأ:

```
*Aug  1 13:34:22 IKEv2:Allocated addr 192.168.0.9 from local pool POOL
*Aug  1 13:34:22 IKEv2:(SA ID = 1):Set received config mode data
*Aug  1 13:34:22 IKEv2:% DVTI create request sent for profile PROF with PSH
                                                                    index 1
*Aug  1 13:34:22 IKEv2:Failed to process KMI delete SA message with error 4
*Aug  1 13:34:24 IKEv2:Got a packet from dispatcher
*Aug  1 13:34:24 IKEv2:Processing an item off the pak queue
*Aug  1 13:34:24 IKEv2:Negotiation context locked currently in use
```

بعد ثانيتين من الفشل، يستقبل برنامج Cisco IOS software إعادة إرسال IKE_AUTH من Android. يتم إسقاط الحزمة.

أخطاء برنامج Cisco IOS وطلبات التحسين

- معرف تصحيح الأخطاء من Cisco CSCui46418، "عنوان IP IOS Ikev2 المرسل كهوية لمصادقة RSA." هذا الخطأ ليس مشكلة، طالما أن StrongSwan يستطيع رأيت عنوان بديل صحيح للموضوع (العنوان) عندما يبحث عن IKEID في الشهادة in order to أنجزت تدقيق.
- معرف تصحيح الأخطاء من "IOS PKI ،CSCui44976 Cisco المعروض بشكل غير صحيح X509v3 Extension Subject Alternative Name."
يحدث هذا الخطأ فقط عندما يكون هناك عناوين IP متعددة في اسم الموضوع البديل. يتم عرض عنوان IP الأخير فقط، ولكن لا يؤثر ذلك على إستخدام الشهادة. يتم إرسال الشهادة بالكامل ومعالجتها بشكل صحيح.
- معرف تصحيح الأخطاء من "IOS PKI ،CSCui44783 Cisco إمكانية إنشاء CSR مع امتداد subject-alt-name."

- معرف تصحيح الأخطاء من CSCui44335 Cisco، "يتم عرض شهادات ASA ENH ل x509 امتدادات."

معلومات ذات صلة

- دليل تكوين Cisco IOS 15.3 VPN
- مرجع أوامر Cisco IOS 15.3
- دليل تكوين Cisco IOS Flex VPN
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).