

IKEv2 van Android strongSwan naar Cisco IOS met EAP en RSA-verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[certificaatschrijving](#)

[Cisco IOS-software](#)

[Android](#)

[EAP-verificatie](#)

[Cisco IOS-softwareconfiguratie voor EAP-verificatie](#)

[Android-configuratie voor EAP-verificatie](#)

[EAP-verificatietest](#)

[RSA-verificatie](#)

[Cisco IOS-softwareconfiguratie voor RSA-verificatie](#)

[Android-configuratie voor RSA-verificatie](#)

[RSA-verificatietest](#)

[VPN-gateway achter NAT - strong Swan en Cisco IOS-software-releases](#)

[Verifiëren](#)

[Problemen oplossen](#)

[strongSwan CA meerdere CERT_REQ](#)

[Tunnel bron via DVTI](#)

[Cisco IOS-software-releases en -verbeteringsaanvragen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de mobiele versie van strongSwan kunt configureren om toegang te krijgen tot een Cisco IOS[®] software VPN-gateway via het Internet Key Exchange Protocol, versie 2 (IKEv2).

Er worden drie voorbeelden gegeven:

- Android-telefoon met strongSwan die zich verbindt met de Cisco IOS-software VPN-gateway met Extensible Authentication Protocol - Message Digest 5 (EAP-MD5) verificatie.
- Android-telefoon met strongSwan die zich verbindt met de Cisco IOS software VPN-gateway

met certificatie (RSA).

- Android-telefoon met strongSwan die zich verbindt met de Cisco IOS-software VPN-gateway achter Network Address Translation (NAT). Er is een vereiste om twee x509 extensies te hebben Onderwerp Alternatieve Naam in het VPN poort certificaat.

De beperkingen van Cisco IOS-software en strongSwan zijn ook inbegrepen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de OpenSSL-configuratie
- Basiskennis van de configuratie van Cisco IOS-softwareopdrachtregel-interface (CLI)
- Basiskennis van IKEv2

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Android 4.0 of hoger met strong Swan
- Cisco IOS-software release 15.3T of hoger
- Software voor Cisco Identity Services Engine (ISE), versie 1.1.4 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

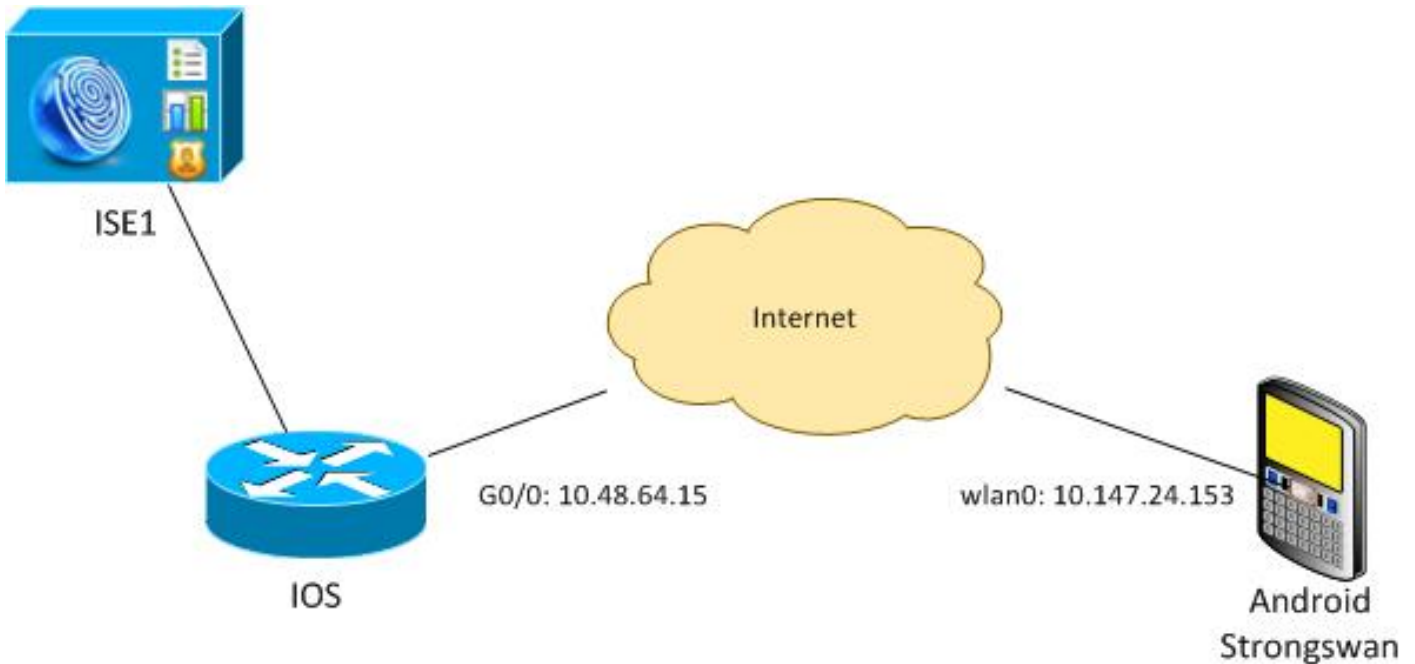
Configureren

Opmerkingen:

De [Output Interpreter Tool \(alleen voor geregistreerde klanten\) ondersteunt bepaalde opdrachten met show](#). Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

Raadpleeg [Important Information on Debug Commands \(Belangrijke informatie over opdrachten met debug\)](#) voordat u **opdrachten met debug opgeeft**.

Netwerkdigram



Android strongSwan stelt een IKEv2-tunnel in met een Cisco IOS-softwaregateway om veilig toegang te krijgen tot interne netwerken.

certificaatschrijving

Certificaten zijn een voorwaarde voor zowel op MAP gebaseerde als op RSA gebaseerde authenticatie.

Bij het MAP-verificatiescenario is alleen op de VPN-gateway een certificaat nodig. De client sluit alleen aan op de Cisco IOS-software wanneer de software een certificaat indient dat is ondertekend door een certificaatinstantie (CA) en op Android is vertrouwd. Een EAP-sessie begint dan voor de client om te authenticeren aan de Cisco IOS-software.

Voor op RSA gebaseerde authenticatie moeten beide eindpunten een correct certificaat hebben.

Wanneer een IP-adres wordt gebruikt als een peer-ID, gelden er extra eisen voor het certificaat. Android strongSwan verifieert of het IP-adres van de VPN-gateway is opgenomen in de x509-extensie Onderwerp Alternatieve naam. Zo niet, dan laat Android de verbinding vallen; dit is zowel een goede praktijk als een aanbeveling van RFC 6125.

OpenSSL wordt als CA gebruikt omdat de Cisco IOS-software een beperking heeft: het kan geen certificaten genereren met een uitbreiding die een IP-adres omvat. Alle certificaten worden gegenereerd door OpenSSL en geïmporteerd naar Android en de Cisco IOS-software.

In de Cisco IOS-software kan de opdracht **onderwerpregel-naam** gebruikt worden om een uitbreiding te maken die een IP-adres bevat maar de opdracht werkt alleen met zelfgetekende certificaten. Cisco Bug ID [CSCui4783](#), "IOS ENH PKI-mogelijkheid om CSR te genereren met onderwerpregel-uitbreiding", is een verbeteringsverzoek om de Cisco IOS-software toe te staan om de uitbreiding te genereren voor alle typen inschrijving.

Dit is een voorbeeld van de opdrachten die een CA genereren:

```
#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 is een configuratiebestand. De CA-extensie dient op TRUE te worden ingesteld:

```
[ 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
```

De opdrachten die een certificaat genereren, lijken sterk op die van Cisco IOS-software en Android. In dit voorbeeld wordt ervan uitgegaan dat er reeds een CA is gebruikt om het certificaat te ondertekenen:

```
#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 is een configuratiebestand. De extensie Onderwerp Alternate Name is een belangrijke instelling. In dit voorbeeld, wordt de CA extensie ingesteld op 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
```

Er moet een certificaat worden gegenereerd voor zowel Cisco IOS-software als Android.

Het IP-adres 10.48.64.15 behoort tot de Cisco IOS-softwaregateway. Wanneer u een certificaat voor de Cisco IOS-software genereert, zorg er dan voor dat de onderwerpAltName is ingesteld op 10.48.64.15. Android bevestigt het certificaat dat van Cisco IOS-software is ontvangen en probeert het IP-adres van de patiënt AltName te vinden.

Cisco IOS-software

De Cisco IOS-software moet beschikken over een correct certificaat dat is geïnstalleerd voor zowel op RSA gebaseerde als op MAP gebaseerde verificatie.

Het pfx-bestand (dat een PC12-container is) voor de Cisco IOS-software kan worden geïmporteerd:

```
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.
```

Gebruik de opdracht van de **show crypto pki certificaten** om te verifiëren dat de import is geslaagd:

```
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

Android

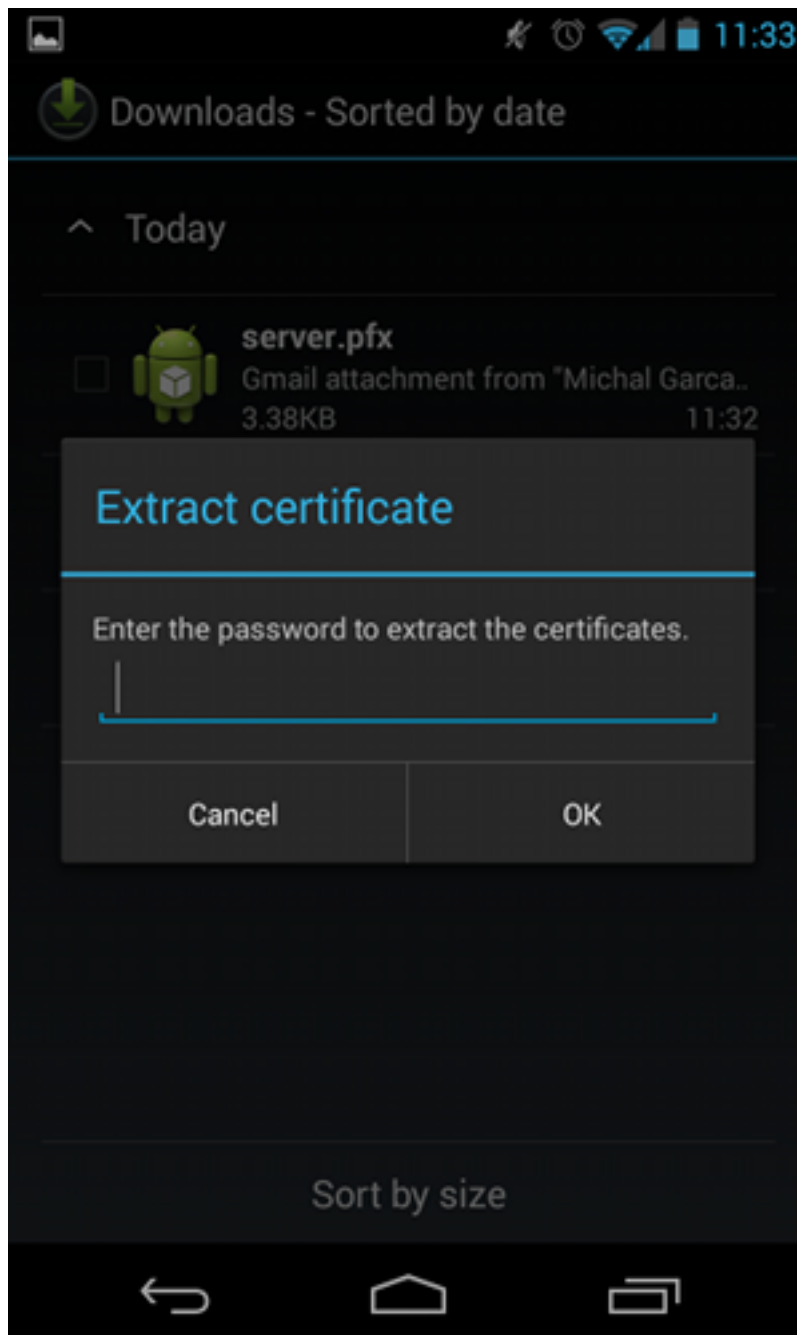
Voor MAP-gebaseerde authenticatie moet Andorra beschikken over het juiste CA-certificaat.

Voor op RSA gebaseerde authenticatie moet Andorra zowel het CA-certificaat als zijn eigen

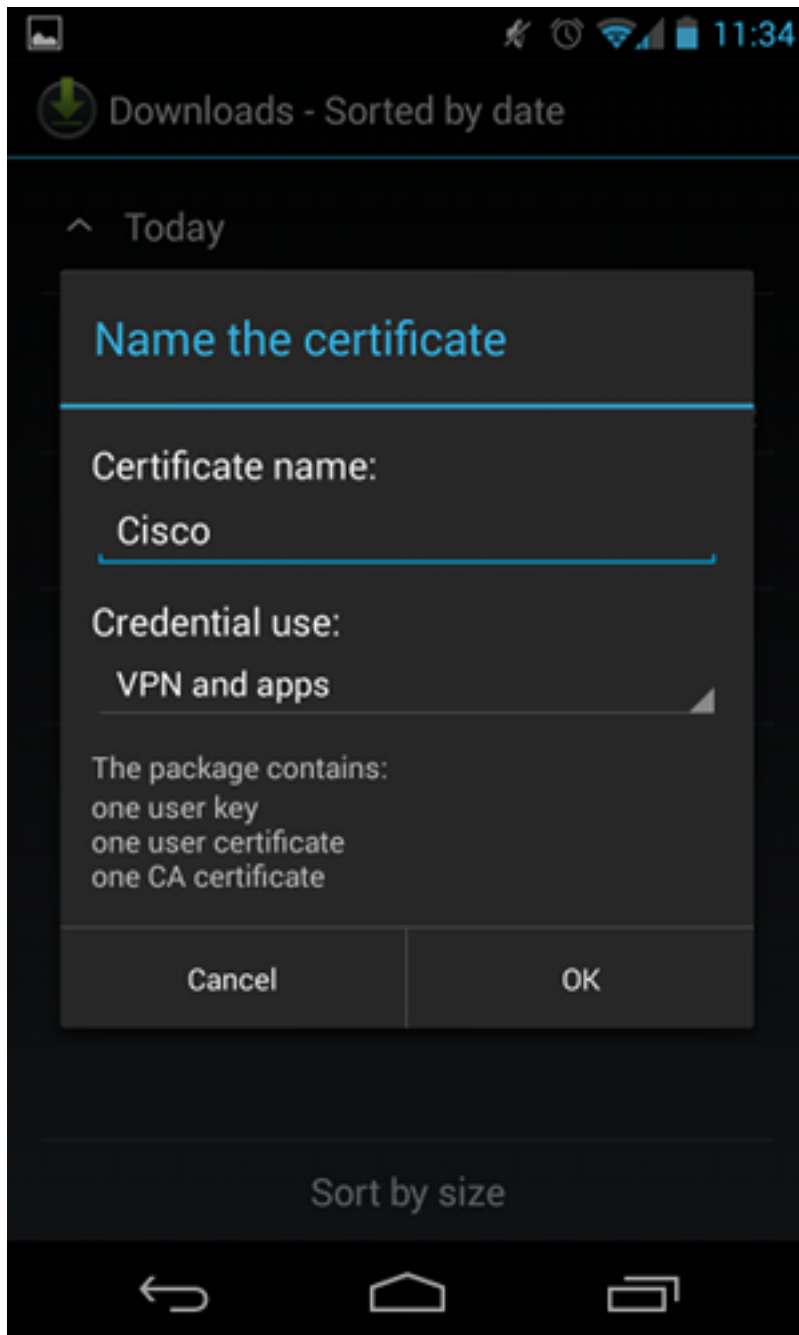
certificaat laten installeren.

In deze procedure wordt beschreven hoe beide certificaten worden geïnstalleerd:

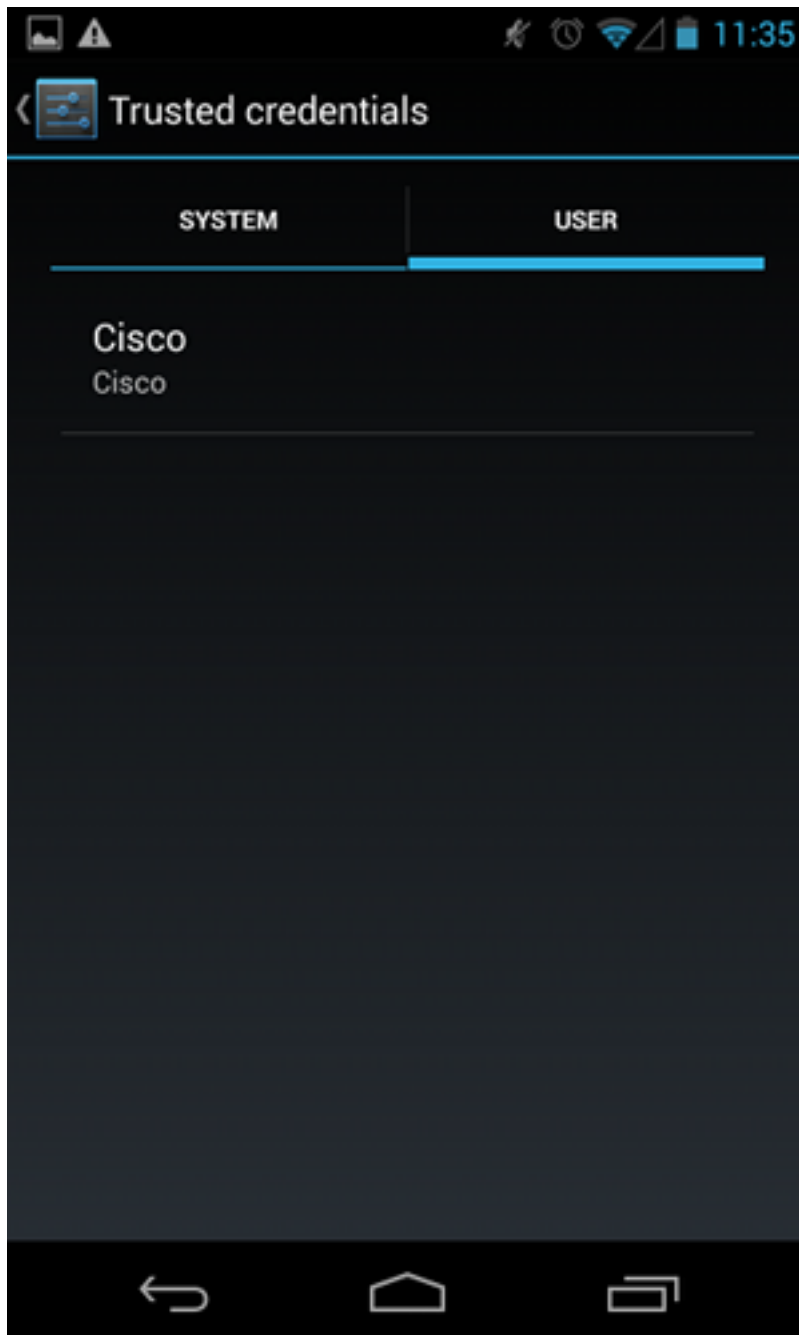
1. Verzend het pfx-bestand per e-mail en open het.
2. Geef het wachtwoord op dat werd gebruikt toen het PDF-bestand gegenereerd werd.



3. Geef de naam op voor het geïmporteerde certificaat.



4. Navigeer naar **Instellingen > Beveiliging > Vertrouwde Credentials** om de installatie van het certificaat te controleren. Het nieuwe certificaat moet in de gebruikerswinkel worden weergegeven:



Op dit moment worden zowel een gebruikerscertificaat als een CA-certificaat geïnstalleerd. Het pfx-bestand is een pc12-container met zowel het gebruikerscertificaat als het CA-certificaat.

Android heeft precieze eisen wanneer certificaten worden ingevoerd. Bijvoorbeeld, voor een CA certificaat om succesvol te worden ingevoerd vereist Android dat de x509v3 extensie Basic Constraint CA op TRUE wordt ingesteld. Dus wanneer u een CA genereert of uw eigen CA gebruikt, is het belangrijk om te verifiëren dat deze de juiste extensie heeft:

```
pluton custom_ca # openssl x509 -in ca.crt -text
Certificate:
  Data:
    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>

EAP-verificatie

Cisco IOS-softwareconfiguratie voor EAP-verificatie

IKEv2 maakt het gebruik van een EAP-protocolstack mogelijk om gebruikersverificatie uit te voeren. De VPN-poort geeft het certificaat weer. Zodra de cliënt dat certificaat vertrouwt, reageert de cliënt op de MAP-aanvraag-identiteit vanaf de poort. De Cisco IOS-software gebruikt die identiteit en stuurt een bericht van Radius-aanvraag naar de verificatie, autorisatie en accounting (AAA) server en een EAP-MD5 sessie wordt ingesteld tussen de aanvrager (Android) en de authenticatieserver (Access Control Server [ACS] of ISE).

Na succesvolle MAP-MD5-verificatie, zoals aangegeven door een bericht Radius-Accept, gebruikt de Cisco IOS-software de configuratie-modus om het IP-adres naar de client te drukken en door te gaan met onderhandeling over verkeersselectie.

Merk op dat Android IKEID=cisco (zoals ingesteld) heeft verstuurd. Deze IKEID is ontvangen op de Cisco IOS-software die overeenkomt met 'ikev2-profiel PROF'.

```
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

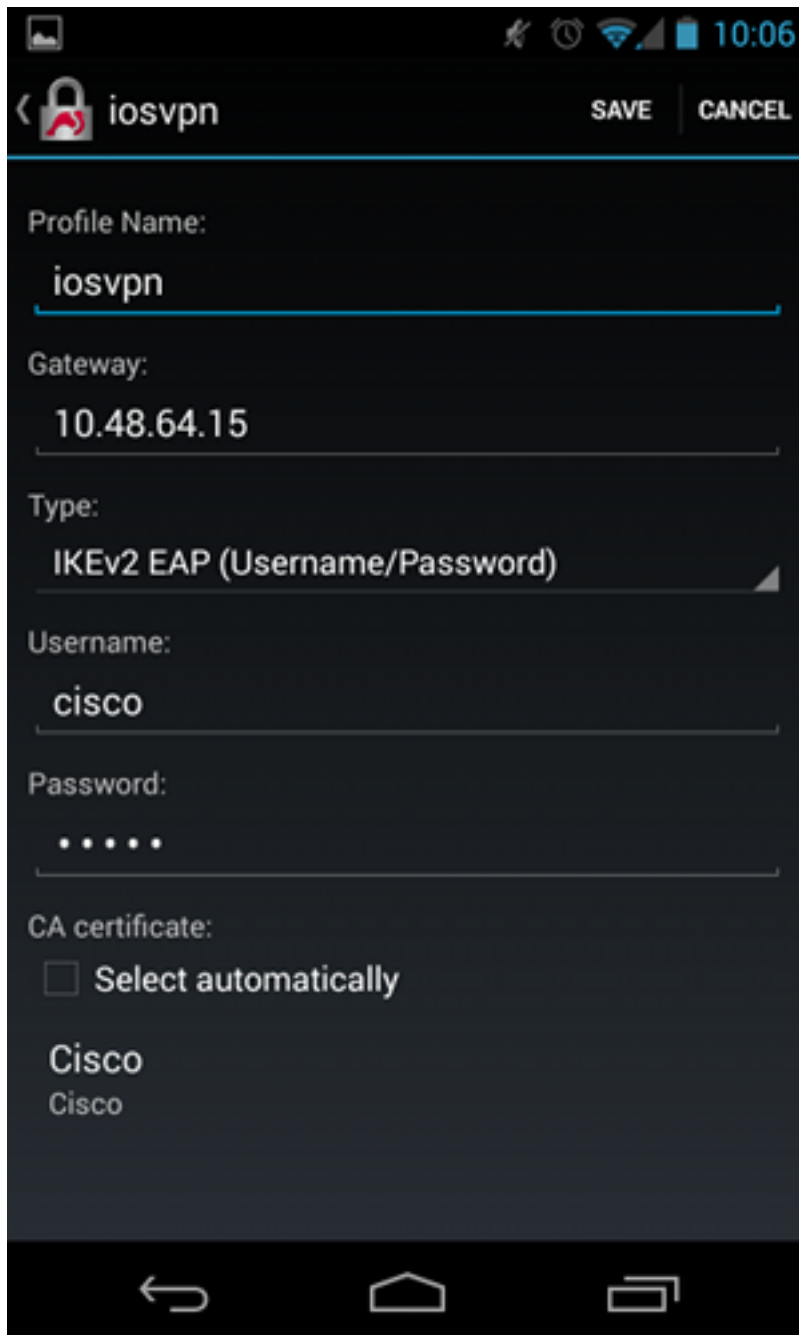
ip local pool POOL 192.168.0.1 192.168.0.10

radius-server host 10.48.66.185 key cisco
```

Android-configuratie voor EAP-verificatie

Android strongSwan moet zijn geconfigureerd voor EAP:

1. Automatische selectie van certificaten uitschakelen; anders worden er 100 of meer CERT_REQs verzonden in de derde verpakking.
2. Kies een specifiek certificaat (CA) dat in de vorige stap is geïmporteerd; de gebruikersnaam en het wachtwoord moeten dezelfde zijn als op de AAA-server.



EAP-verificatietest

In de Cisco IOS-software zijn dit de belangrijkste onderdelen voor MAP-verificatie. De meeste output is weggelaten voor duidelijkheid:

```
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_REC'D_VERIFY_IPSEC_POLICY

%LINEPROTO-5-UPDOWN: Line protocol on **Interface Virtual-Access1, changed state to up**

De Android-logboeken schrijven voor:

```
00[DMN] Starting IKE charon daemon (strongSwan 5.1.0dr2,  
Linux 3.4.0-perf-gf43c3d9, armv7l)  
00[KNL] kernel-netlink plugin might require CAP_NET_ADMIN capability  
00[LIB] loaded plugins: androidbridge charon android-log openssl fips-prf  
random nonce pubkey pkcs1 pkcs8 pem xcbc hmac socket-default kernel-netlink  
00[LIB] unable to load 9 plugin features (9 due to unmet dependencies)  
00[JOB] spawning 16 worker threads  
13[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]  
(648 bytes)  
11[NET] received packet: from 10.48.64.15[500] to 10.147.24.153[45581]  
(497 bytes)  
11[ENC] parsed IKE_SA_INIT response 0 [ SA KE No V V N(NATD_S_IP) N(NATD_D_IP)  
CERTREQ N(HTTPS_CERT_LOOKUP) ]  
11[ENC] received unknown vendor ID:  
43:49:53:43:4f:2d:44:45:4c:45:54:45:2d:52:45:41:53:4f:4e  
11[ENC] received unknown vendor ID:  
46:4c:45:58:56:50:4e:2d:53:55:50:50:4f:52:54:45:44  
11[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,  
OU=Cisco TAC, CN=Cisco"  
11[IKE] establishing CHILD_SA android  
11[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ  
CP(ADDR ADDR6 DNS DNS6) N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP)  
11[NET] sending packet: from 10.147.24.153[35564] to 10.48.64.15[4500]  
(508 bytes)  
10[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]  
(1292 bytes)  
10[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,  
OU=TAC, CN=IOS"  
10[CFG] using certificate "C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC,  
CN=IOS"  
10[CFG] using trusted ca certificate "C=PL, ST=Malopolskie, L=Krakow, O=Cisco,  
OU=Cisco TAC, CN=Cisco"  
10[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]  
(76 bytes)
```

```

09[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(76 bytes)
09[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]
(76 bytes)
08[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(92 bytes)
08[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]
(92 bytes)
07[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(76 bytes)
07[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]
(92 bytes)
06[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(236 bytes)
06[ENC] parsed IKE_AUTH response 5 [ AUTH CP(ADDR) SA TSi TSr N(SET_WINSIZE)
N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG) ]
06[IKE] authentication of '10.48.64.15' with EAP successful
06[IKE] IKE_SA android[1] established between
10.147.24.153[cisco]...10.48.64.15[10.48.64.15]
06[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
TS 192.168.0.1/32 === 0.0.0.0/0
06[DMN] setting up TUN device for CHILD_SA android{1}
06[DMN] successfully created TUN device

```

Dit voorbeeld toont hoe u de status op de Cisco IOS-software kunt controleren:

```
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	fvr/ivrf	Status
1	10.48.64.15/4500	10.147.24.153/60511	none/none	READY

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

Deze cijfers laten zien hoe de status op Android kan worden geverifieerd:

 Saving screenshot...



ADD VPN PROFILE



Status: **Connected**

Profile: iosvpn

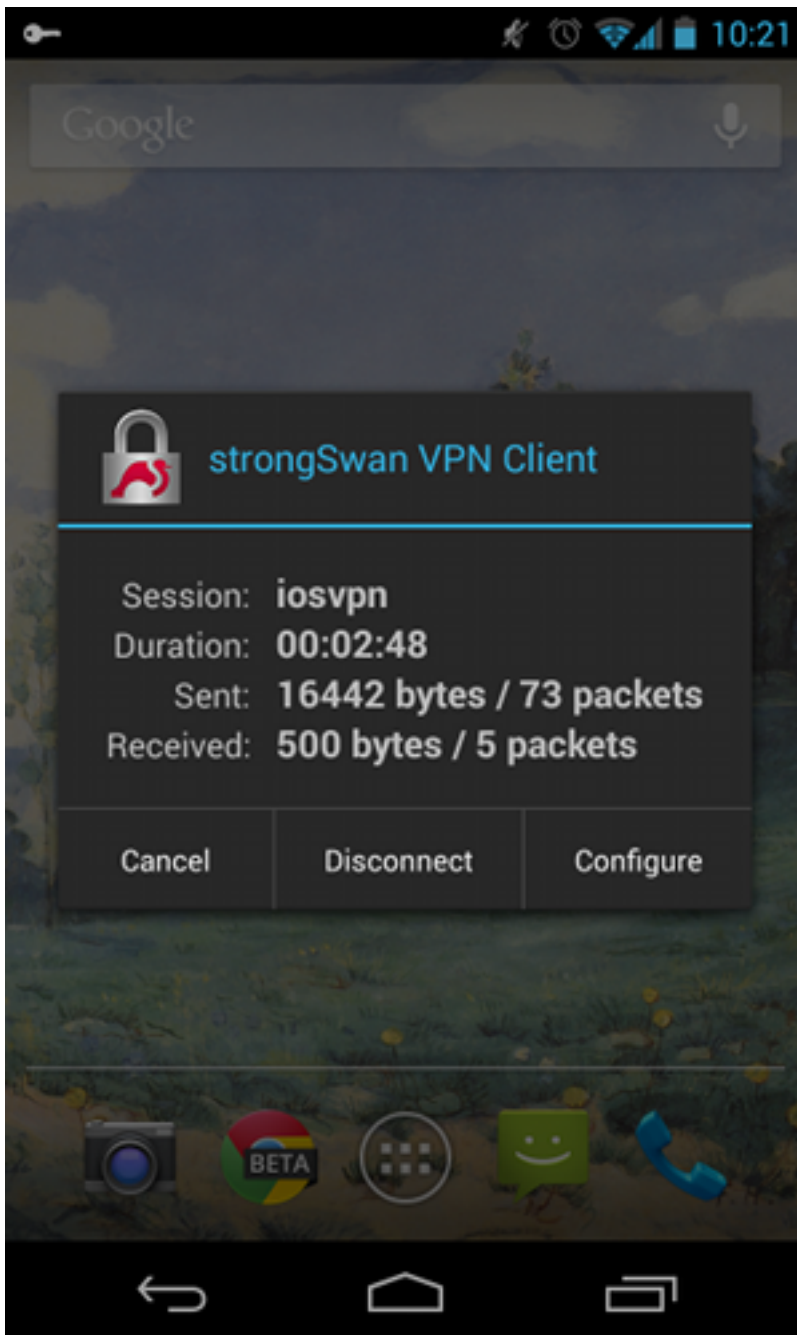
Disconnect

iosvpn

Gateway: 10.48.64.15

Username: cisco





RSA-verificatie

Cisco IOS-softwareconfiguratie voor RSA-verificatie

In Rivest-Shamir-Adleman (RSA)-verificatie, stuurt Android het certificaat om te authenticeren aan de Cisco IOS-software. Dat is de reden dat de certificaatkaart die dat verkeer aan een specifiek IKEv2-profiel bindt nodig is. EE-verificatie door gebruiker is niet vereist.

Dit is een voorbeeld van hoe RSA authenticatie voor een afstandspeer wordt ingesteld:

```
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
```

Android-configuratie voor RSA-verificatie

Gebruikersreferenties zijn vervangen door het gebruikerscertificaat:



RSA-verificatietest

In de Cisco IOS-software zijn dit de belangrijkste onderdelen voor RSA-verificatie. De meeste output is weggelaten voor duidelijkheid:

```
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_REC'D_VERIFY_IPSEC_POLICY
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state
to up
```

De Android-logboeken schrijven voor:

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

05[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]
(648 bytes)
10[NET] received packet: from 10.48.64.15[500] to 10.147.24.153[34697]
(497 bytes)
10[ENC] parsed IKE_SA_INIT response 0 [ SA KE No V V N(NATD_S_IP) N(NATD_D_IP)
CERTREQ N(HTTP_CERT_LOOK) ]
10[ENC] received unknown vendor ID:
43:49:53:43:4f:2d:44:45:4c:45:54:45:2d:52:45:41:53:4f:4e
10[ENC] received unknown vendor ID:
46:4c:45:58:56:50:4e:2d:53:55:50:50:4f:52:54:45:44
10[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,
OU=Cisco TAC, CN=Cisco"
10[IKE] authentication of 'C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC,
CN=android' (myself) with RSA signature successful
10[IKE] sending end entity cert "C=PL, ST=Malopolska, L=Krakow, O=Cisco,
OU=TAC, CN=android"
10[IKE] establishing CHILD_SA android
```

```

10[ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ
AUTH CP(ADDR ADDR6 DNS DNS6) N(ESP_TFC_PAD_N) SA
10[NET] sending packet: from 10.147.24.153[44527] to 10.48.64.15[4500]
(1788 bytes)
12[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[44527]
(1420 bytes)
12[ENC] parsed IKE_AUTH response 1 [ V IDr CERT AUTH CP(ADDR) SA TSi TSr
N(SET_WINSIZE) N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG)
12[IKE] received end entity cert "C=PL, ST=Malopolska, L=Krakow, O=Cisco,
OU=TAC, CN=IOS"
12[CFG] using certificate "C=PL, ST=Malopolska, L=Krakow, O=Cisco, OU=TAC,
CN=IOS"
12[CFG] using trusted ca certificate "C=PL, ST=Malopolskie, L=Krakow, O=Cisco,
OU=Cisco TAC, CN=Cisco"
12[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,
ST=Malopolska, L=Krakow, O=Cisco, OU=TAC,
CN=android]...10.48.64.15[10.48.64.15]
12[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
TS 192.168.0.3/32 === 0.0.0.0/0
12[DMN] setting up TUN device for CHILD_SA android{4}
12[DMN] successfully created TUN device

```

In de Cisco IOS-software wordt RSA gebruikt voor zowel het tekenen als de verificatie; In het vorige scenario werd EAP gebruikt ter verificatie:

```

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

```

```

Tunnel-id Local Remote fvr/ivrf Status
1 10.48.64.15/4500 10.147.24.153/44527 none/none READY
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

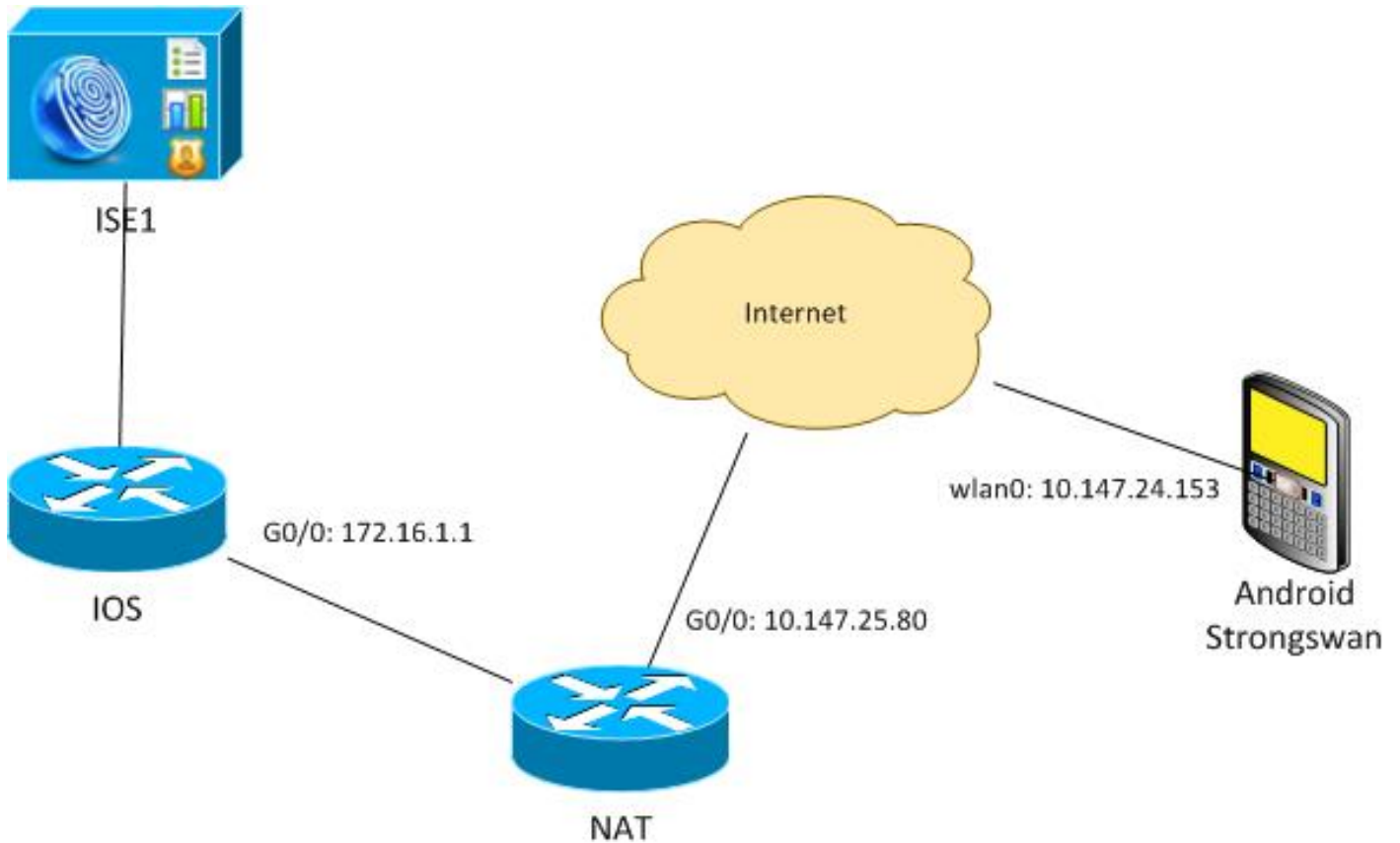
```

De statusverificatie bij Android is vergelijkbaar met die bij het vorige scenario.

VPN-gateway achter NAT - strong Swan en Cisco IOS-software releases

Dit voorbeeld verklaart een beperking van sterkeSwan certificatie verificaties.

Stel dat het Cisco IOS VPN-gateway-adres van de software statistisch wordt vertaald van 172.16.1.1 naar 10.147.25.80. EAP-verificatie wordt gebruikt.



Ga er ook van uit dat het Cisco IOS-software release een Onderwerp Alternatief Naam heeft voor zowel 172.16.1.1 als 10.147.25.80.

Na succesvolle MAP-verificatie voert Android verificatie uit en probeert het IP-adres van de peer te vinden die in Android-configuratie (10.147.25.80) werd gebruikt in de Onderwerp Alternative Name-extensie. De verificatie mislukt:

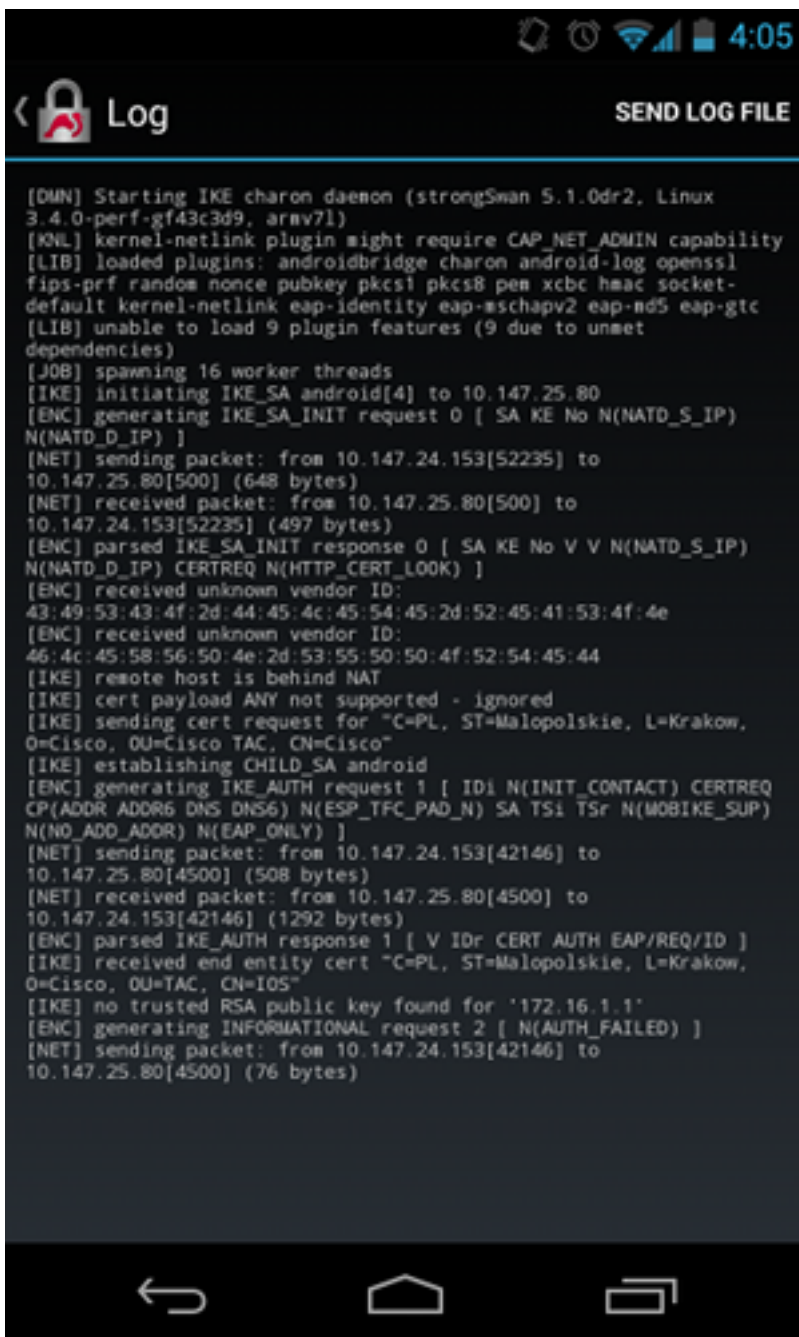


De logboeken duiden op:

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

De fout is opgetreden omdat Android alleen de eerste Onderwerp Alternatieve Naam extensie (172.16.1.1) kan lezen.

Ga er nu van uit dat het Cisco IOS-softwarecertificaat beide adressen in Onderwerp Alternatieve Naam maar in de omgekeerde volgorde heeft: 10.147.25.80 en 172.16.1.1. Android voert validatie uit wanneer het IKEID, het IP-adres van VPN-gateway (172.16.1.1), in het derde pakket ontvangt:



Het logbestand toont nu:

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

Wanneer Android de IKEID ontvangt, moet zij de IKEID in de alternatieve naam van het onderwerp vinden en alleen het eerste IP-adres gebruiken.

Opmerking: Bij MAP-verificatie is het IKEID dat door de Cisco IOS-software wordt verzonden het IP-adres standaard. Bij RSA-verificatie is IKEID standaard het certificaat DN. Gebruik de opdracht **identiteit** onder het ikev2-profiel om deze waarden handmatig te wijzigen.

Verifiëren

In de voorbeelden van de configuratie zijn verificaties en testprocedures beschikbaar.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

strongSwan CA meerdere CERT_REQ

Wanneer de certificaatinstelling op strongswan Automatisch selecteren is (de standaardinstelling), stuurt Android CERT_REQ voor alle vertrouwde certificaten in de lokale winkel in het derde pakket. De Cisco IOS-software kan het verzoek laten vallen omdat het een groot aantal certificaatverzoeken herkent als een aanval van de Staat van de Dienst:

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

Tunnel bron via DVTI

Hoewel het vrij gebruikelijk is om de tunnelbron op een virtuele tunnelinterface (VTI) in te stellen, is dit hier niet nodig. Stel dat de opdracht **tunnelbron** onder een dynamische VTI (DVTI) valt:

```
interface Virtual-Templat1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROF
```

Als de Cisco IOS-software na verificatie probeert een virtuele toegangsinterface te maken die van een virtuele sjabloon is gekloond, wordt er een fout hersteld:

```
*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
```

Twee seconden na de mislukking ontvangt de Cisco IOS software een opnieuw uitgezonden IKE_AUTH van Android. Dat pakje is gevallen.

Cisco IOS-software releases en -verbeteringsaanvragen

- Cisco Bug ID [CSCui46418](#), "IOS Ikev2 ip-adres verzonden als identiteit voor RSA-verificatie." Dit insect is geen probleem, zolang strongSwan een correcte alternatieve naam voor het onderwerp (het IP-adres) kan zien wanneer het naar de IKEID in het certificaat op zoek is om de verificatie uit te voeren.
- Cisco Bug ID [CSCui4976](#), "IOS PKI onjuist weergegeven X509v3 extensie Onderwerp Alternatieve naam." Dit bug treedt alleen op als er meerdere IP-adressen in de naam Onderwerp Alternatief zijn. Alleen het laatste IP-adres wordt weergegeven, maar dit heeft geen invloed op het gebruik

van certificaten. Het hele certificaat wordt correct verzonden en verwerkt.

- Cisco plug-in [CSCui4783](#), "IOS ENH PKI-mogelijkheid om CSR te genereren met onderwerpregel-naam-extensie."
- Cisco Bug ID [CSCui4335](#), "ASA ENH certificaatverlenger x509 weergegeven".

Gerelateerde informatie

- [Cisco IOS 15.3 VPN-configuratiegids](#)
- [Cisco IOS 15.3 opdrachtreferentie](#)
- [Cisco IOS Flex VPN-configuratiegids](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)