

# Android strongSwan에서 Cisco IOS로의 IKEv2(EAP 및 RSA 인증)

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[인증서 등록](#)

[Cisco IOS 소프트웨어](#)

[Android](#)

[EAP 인증](#)

[EAP 인증을 위한 Cisco IOS 소프트웨어 구성](#)

[EAP 인증을 위한 Android 구성](#)

[EAP 인증 테스트](#)

[RSA 인증](#)

[RSA 인증을 위한 Cisco IOS 소프트웨어 구성](#)

[RSA 인증을 위한 Android 구성](#)

[RSA 인증 테스트](#)

[NAT 뒤의 VPN 게이트웨이 - strongSwan 및 Cisco IOS 소프트웨어 제한 사항  
다음을 확인합니다.](#)

[문제 해결](#)

[strongSwan CA 다중 CERT\\_REQ](#)

[DVTI의 터널 소스](#)

[Cisco IOS 소프트웨어 버그 및 개선 요청](#)

[관련 정보](#)

## 소개

이 문서에서는 IKEv2(Internet Key Exchange Version 2) 프로토콜을 통해 Cisco IOS<sup>®</sup> 소프트웨어 VPN 게이트웨이에 액세스하기 위해 strongSwan의 모바일 버전을 구성하는 방법에 대해 설명합니다.

세 가지 예가 제시됩니다.

- Extensible Authentication Protocol - EAP-MD5(Message Digest 5) 인증을 사용하여 Cisco IOS 소프트웨어 VPN 게이트웨이에 연결하는 strongSwan이 있는 Android 폰
- RSA(Certificate Authentication)를 사용하여 Cisco IOS 소프트웨어 VPN 게이트웨이에 연결하

는 strongSwan이 포함된 Android 폰.

- NAT(Network Address Translation) 뒤에 있는 Cisco IOS 소프트웨어 VPN 게이트웨이에 연결하는 strongSwan이 있는 Android 폰. VPN 게이트웨이 인증서에 2개의 x509 확장 주체 대체 이름이 있어야 합니다.

Cisco IOS 소프트웨어 및 strongSwan 제한 사항도 포함되어 있습니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- OpenSSL 구성에 대한 기본 지식
- Cisco IOS 소프트웨어 CLI(Command Line Interface) 컨피그레이션에 대한 기본 지식
- IKEv2에 대한 기본 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Android 4.0 이상(strongSwan 포함)
- Cisco IOS Software 릴리스 15.3T 이상
- Cisco ISE(Identity Services Engine) 소프트웨어, 버전 1.1.4 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

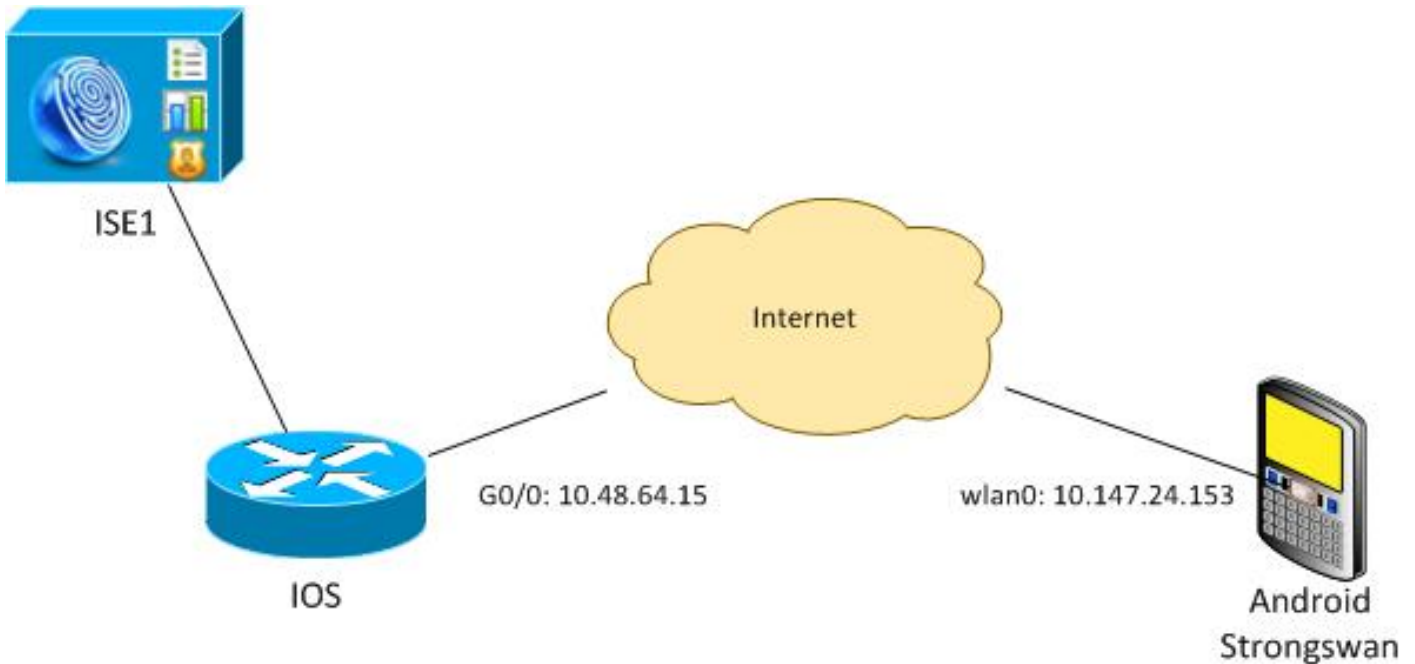
## 구성

### 참고:

Output [Interpreter 도구](#)([등록된](#) 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

**debug** 명령을 사용하기 전에 [디버그 명령에 대한 중요 정보](#)를 참조하십시오.

## 네트워크 다이어그램



Android strongSwan은 내부 네트워크에 안전하게 액세스하기 위해 Cisco IOS 소프트웨어 게이트웨이로 IKEv2 터널을 설정합니다.

## 인증서 등록

인증서는 EAP 기반 인증과 RSA 기반 인증을 모두 위한 필수 조건입니다.

EAP 인증 시나리오에서는 VPN 게이트웨이에서만 인증서가 필요합니다. Android에서 신뢰할 수 있는 CA(Certificate Authority)가 서명한 인증서를 소프트웨어에서 제공하는 경우에만 클라이언트가 Cisco IOS 소프트웨어에 연결됩니다. 그런 다음 클라이언트가 Cisco IOS 소프트웨어를 인증하기 위해 EAP 세션이 시작됩니다.

RSA 기반 인증의 경우 두 엔드포인트 모두 올바른 인증서가 있어야 합니다.

IP 주소가 피어 ID로 사용되는 경우 인증서에 대한 추가 요구 사항이 있습니다. Android strongSwan은 VPN 게이트웨이의 IP 주소가 x509 확장 주체 대체 이름에 포함되어 있는지 확인합니다. 그렇지 않으면 Android가 연결을 삭제합니다. 이는 RFC 6125의 권장 사항뿐 아니라 유용한 방법입니다.

OpenSSL은 Cisco IOS 소프트웨어에 다음과 같은 제한이 있기 때문에 CA로 사용됩니다. IP 주소가 포함된 확장명을 가진 인증서를 생성할 수 없습니다. 모든 인증서는 OpenSSL에 의해 생성되며 Android 및 Cisco IOS 소프트웨어로 가져옵니다.

Cisco IOS 소프트웨어에서 **subject-alt-name** 명령을 사용하여 IP 주소를 포함하는 확장을 생성할 수 있지만 이 명령은 자체 서명 인증서에서만 작동합니다. Cisco Bug ID [CSCui44783](#), "IOS ENH PKI capability to generate CSR with subject-alt-name extension"은 Cisco IOS 소프트웨어가 모든 유형의 등록에 대한 확장을 생성할 수 있도록 하는 개선 요청입니다.

다음은 CA를 생성하는 명령의 예입니다.

```
#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
-extentions v3_req -extfile conf_global.crt

```

**conf\_global.crt**는 구성 파일입니다.CA 확장은 TRUE로 설정해야 합니다.

```

[ 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

```

인증서를 생성하는 명령은 Cisco IOS 소프트웨어 및 Android와 매우 유사합니다.이 예에서는 인증서 서명에 사용된 CA가 이미 있다고 가정합니다.

```

#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**는 구성 파일입니다.대체 주체 이름 확장자는 키 설정입니다.이 예에서는 CA 확장이 FALSE로 설정됩니다.

```

[ 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
```

Cisco IOS 소프트웨어와 Android 모두에 대해 인증서를 생성해야 합니다.

IP 주소 10.48.64.15은 Cisco IOS 소프트웨어 게이트웨이에 속합니다. Cisco IOS 소프트웨어에 대한 인증서를 생성할 때 subjectAltName이 10.48.64.15으로 설정되어 있는지 확인합니다. Android는 Cisco IOS 소프트웨어에서 받은 인증서를 확인하고 subjectAltName에서 해당 IP 주소를 찾으려고 시도합니다.

## Cisco IOS 소프트웨어

Cisco IOS 소프트웨어는 RSA 기반 인증과 EAP 기반 인증을 위해 올바른 인증서를 설치해야 합니다.

Cisco IOS 소프트웨어의 pfx 파일(pkcs12 컨테이너)을 가져올 수 있습니다.

```
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.
```

가져오기가 성공했는지 확인하려면 show crypto pki certificates verbose 명령을 사용합니다.

```
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

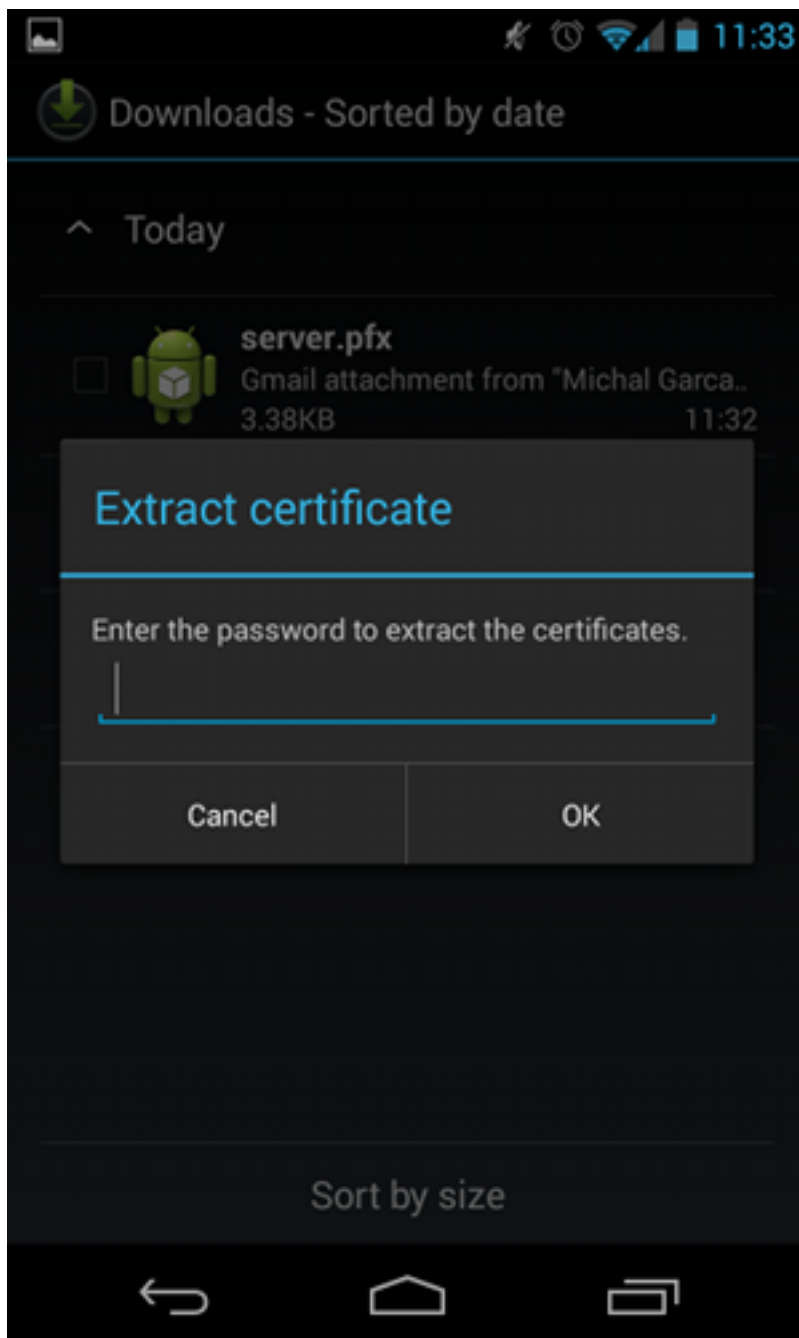
## Android

EAP 기반 인증의 경우 Android는 올바른 CA 인증서만 설치해야 합니다.

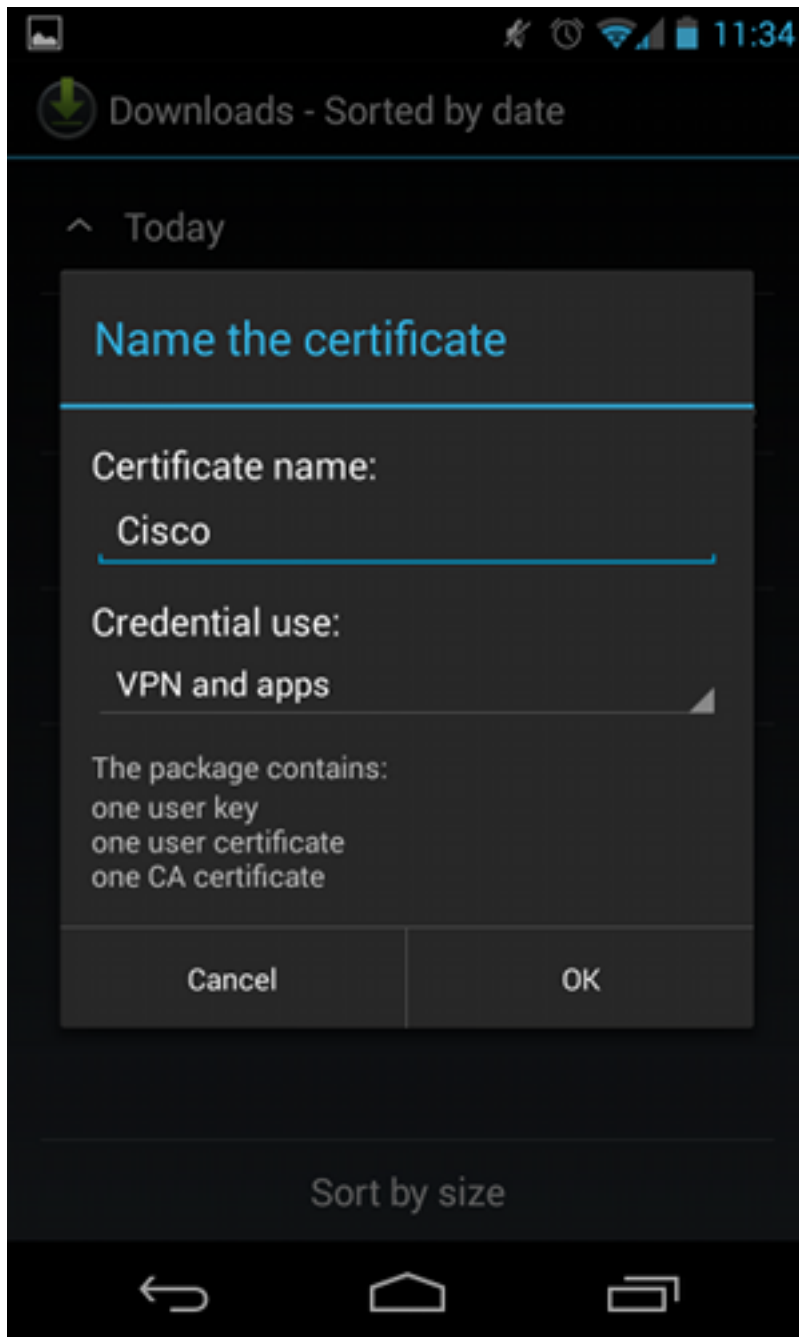
RSA 기반 인증의 경우 Android는 CA 인증서와 자체 인증서를 모두 설치해야 합니다.

다음 절차에서는 두 인증서를 모두 설치하는 방법에 대해 설명합니다.

1. 전자 메일로 pfx 파일을 보내고 엽니다.
2. pfx 파일을 생성할 때 사용한 암호를 제공합니다.

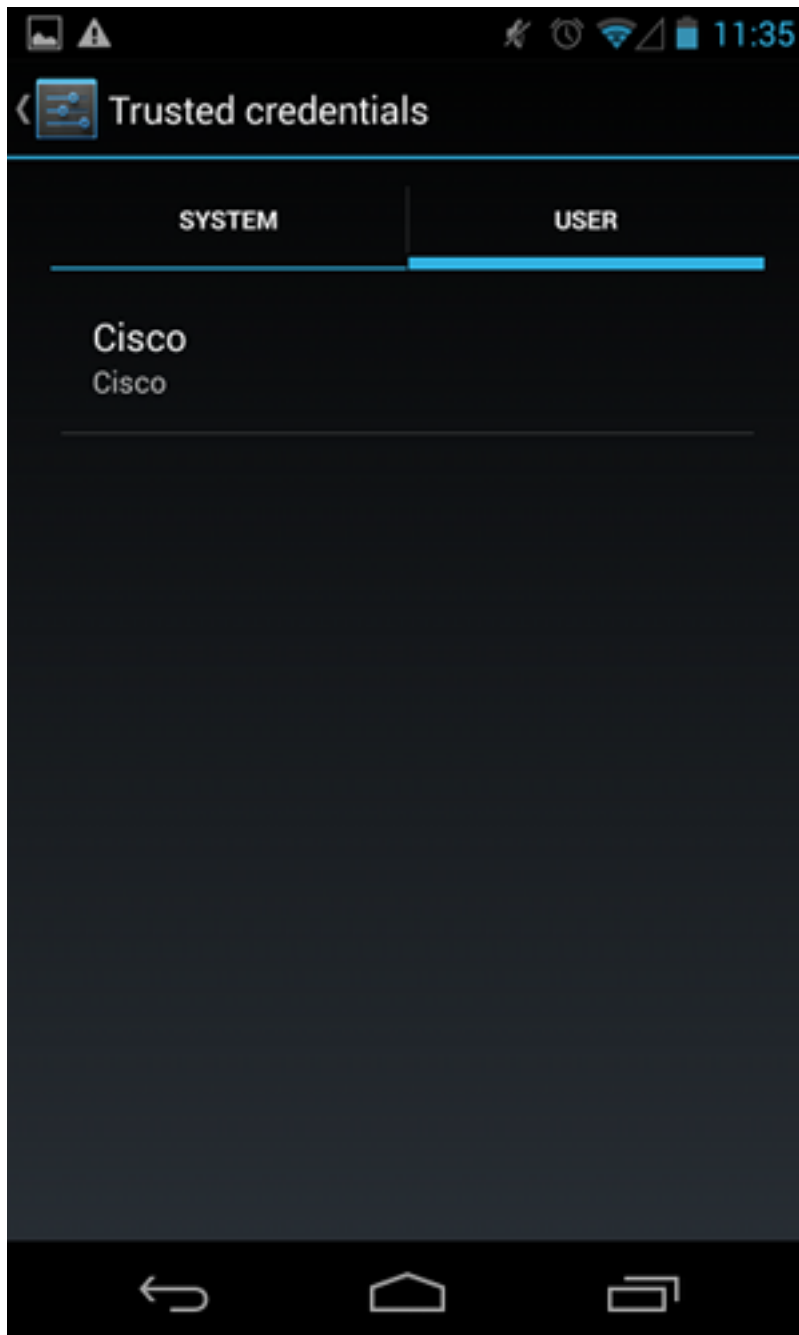


3. 가져온 인증서의 이름을 제공합니다.



4. 인증서 설치를 확인하려면 **Settings > Security > Trusted Credentials**로 이동합니다. 새 인증서가 사용자 저장소에 나타나야 합니다.





이때 사용자 인증서와 CA 인증서가 설치됩니다.pfx 파일은 사용자 인증서 및 CA 인증서를 모두 포함하는 pkcs12 컨테이너입니다.

Android에는 인증서를 가져올 때 정확한 요구 사항이 있습니다.예를 들어, CA 인증서를 성공적으로 가져오려면 Android에서 x509v3 확장 Basic Constraint CA를 TRUE로 설정해야 합니다.따라서 CA를 생성하거나 자체 CA를 사용할 때는 CA가 올바른 확장명을 가지고 있는지 확인해야 합니다.

```
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 인증

### EAP 인증을 위한 Cisco IOS 소프트웨어 구성

IKEv2에서는 사용자 인증을 수행하기 위해 EAP 프로토콜 스택을 사용할 수 있습니다. VPN 게이트웨이는 인증서와 함께 표시됩니다. 클라이언트가 해당 인증서를 신뢰하면 클라이언트는 게이트웨이의 EAP 요청 ID에 응답합니다. Cisco IOS 소프트웨어는 해당 ID를 사용하고 AAA(Authentication, Authorization, and Accounting) 서버로 RADIUS 요청 메시지를 전송하며, 서플리컨트(Android)와 인증 서버(ACS[Access Control Server] 또는 ISE) 간에 EAP-MD5 세션이 설정됩니다.

EAP-MD5 인증 성공 후 Radius-Accept 메시지에 표시된 대로 Cisco IOS 소프트웨어는 구성 모드를 사용하여 IP 주소를 클라이언트에 푸시하고 트래픽 선택기 협상을 계속합니다.

Android에서 IKEID=cisco(구성된 대로)를 전송했습니다. Cisco IOS 소프트웨어에서 받은 이 IKEID는 'ikev2 프로파일 PROF'와 일치합니다.

```
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

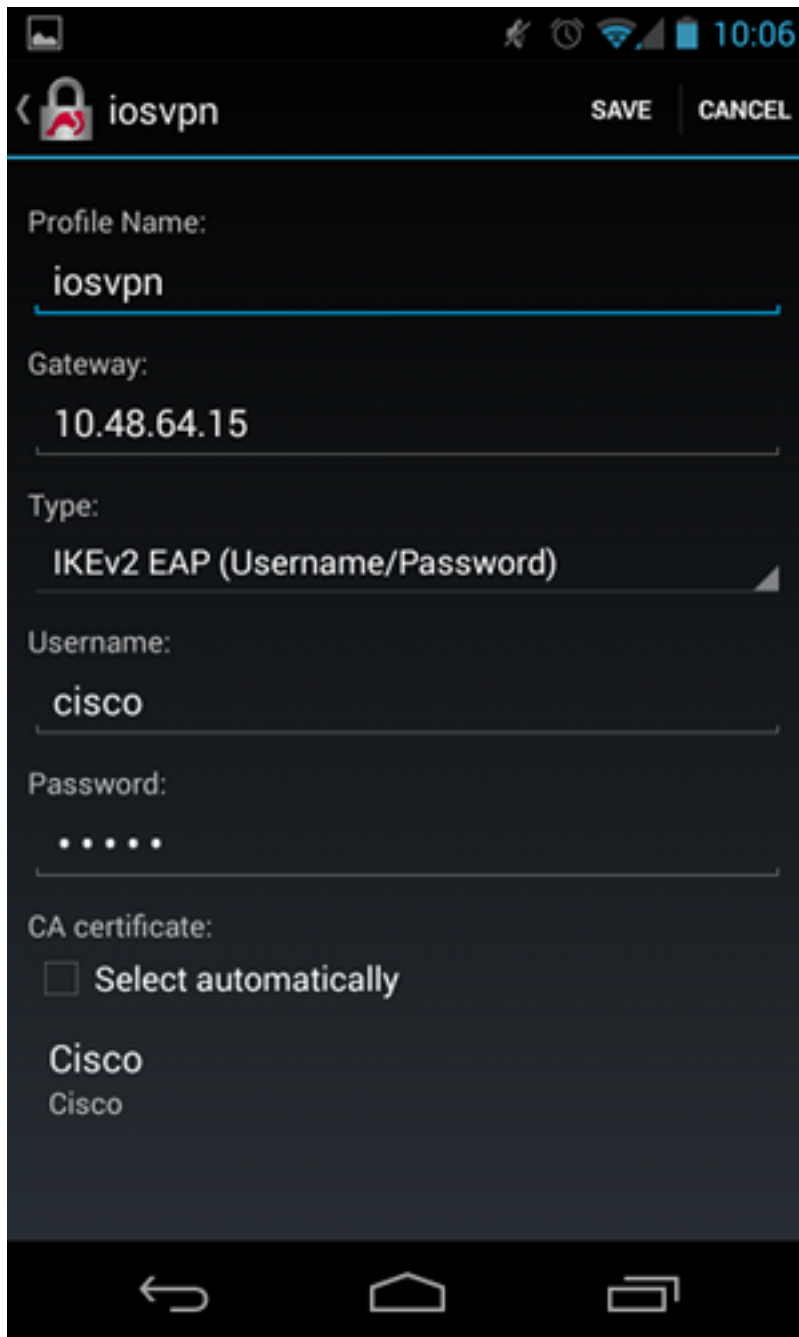
ip local pool POOL 192.168.0.1 192.168.0.10

radius-server host 10.48.66.185 key cisco
```

## EAP 인증을 위한 Android 구성

Android strongSwan은 EAP를 구성해야 합니다.

1. 자동 인증서 선택을 비활성화합니다. 그렇지 않으면 세 번째 패킷에서 100개 이상의 CERT\_REQ가 전송됩니다.
2. 이전 단계에서 가져온 특정 인증서(CA)를 선택합니다. 사용자 이름과 비밀번호는 AAA 서버의 사용자 이름과 같아야 합니다.



## EAP 인증 테스트

Cisco IOS 소프트웨어에서는 EAP 인증을 위한 가장 중요한 디버그입니다. 대부분의 출력은 명확성을 위해 생략되었습니다.

```
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**

Android 로그에는 다음이 표시됩니다.

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(HTTP\_CERT\_LOOK) ]  
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

```

다음 예에서는 Cisco IOS 소프트웨어에서 상태를 확인하는 방법을 보여줍니다.

```

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)

```

```

  Phasel_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

다음 그림은 Android에서 상태를 확인하는 방법을 보여줍니다.

 Saving screenshot...



ADD VPN PROFILE



Status: **Connected**

Profile: iosvpn

Disconnect

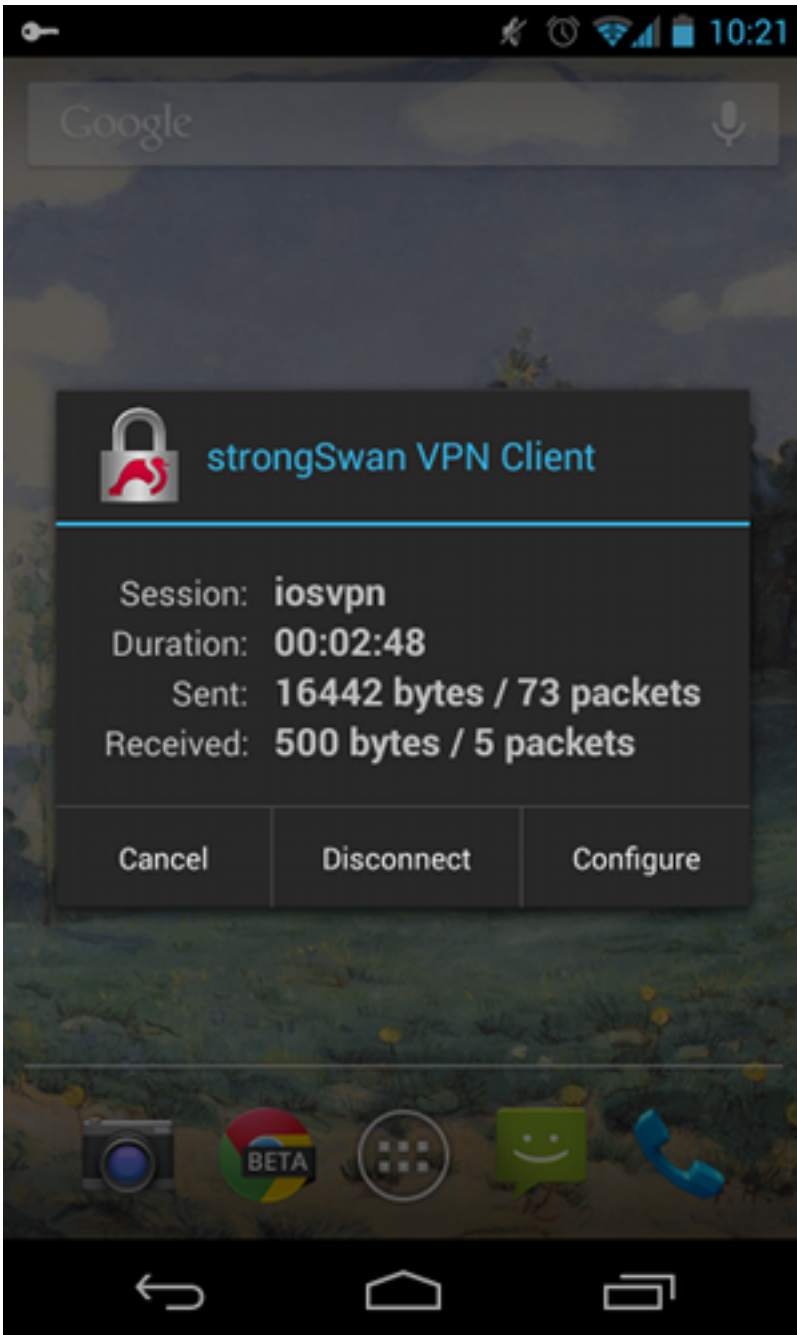
iosvpn

Gateway: 10.48.64.15

Username: cisco







## RSA 인증

### RSA 인증을 위한 Cisco IOS 소프트웨어 구성

Rivest-Shamir-Adleman(RSA) 인증에서 Android는 Cisco IOS 소프트웨어를 인증하기 위해 인증서를 전송합니다. 따라서 특정 IKEv2 프로필에 트래픽을 바인딩하는 인증서 맵이 필요합니다. 사용자 EAP 인증이 필요하지 않습니다.

다음은 원격 피어에 대한 RSA 인증이 설정된 방법의 예입니다.

```
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
```

## RSA 인증을 위한 Android 구성

사용자 인증서가 사용자 인증서로 대체되었습니다.



## RSA 인증 테스트

Cisco IOS 소프트웨어에서는 RSA 인증을 위한 가장 중요한 디버그입니다. 대부분의 출력은 명확성을 위해 생략되었습니다.

```
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
```

Android 로그에는 다음이 표시됩니다.

```
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

```

Cisco IOS 소프트웨어에서 RSA는 서명 및 확인 모두에 사용됩니다. 이전 시나리오에서 EAP는 확인에 사용되었습니다.

```

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

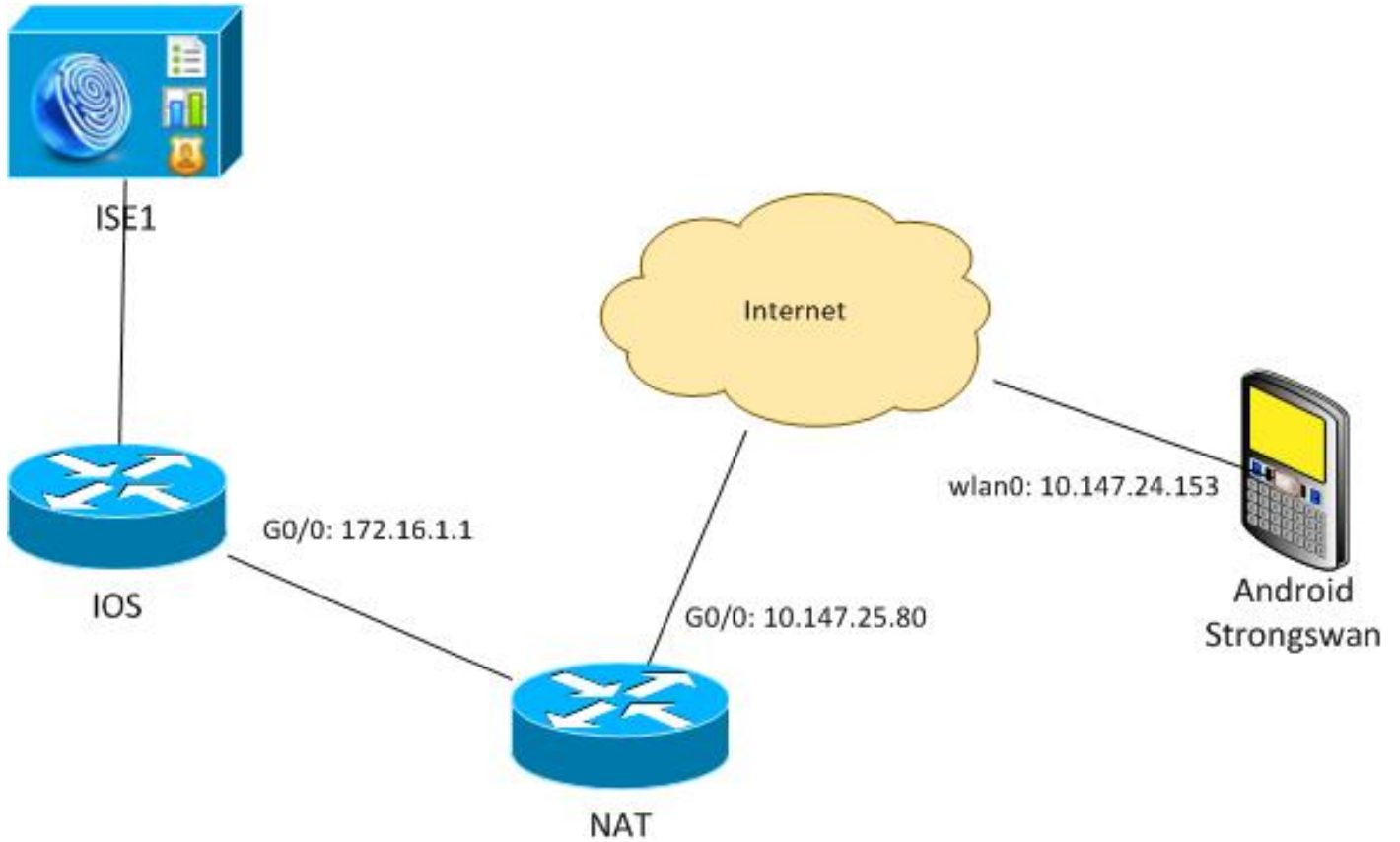
```

Android의 상태 확인은 이전 시나리오와 유사합니다.

## NAT 뒤의 VPN 게이트웨이 - strongSwan 및 Cisco IOS 소프트웨어 제한 사항

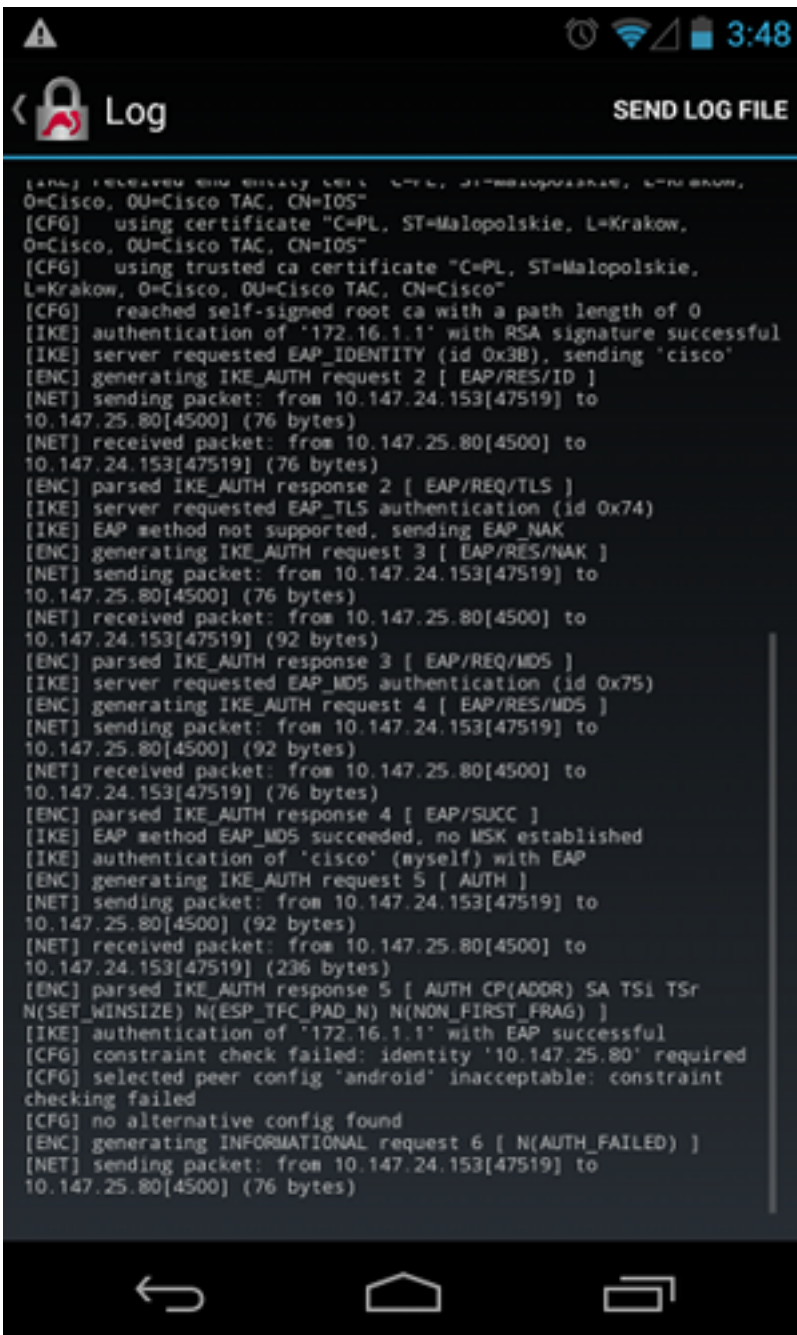
이 예에서는 strongSwan 인증서 확인의 제한에 대해 설명합니다.

Cisco IOS 소프트웨어 VPN 게이트웨이 IP 주소가 172.16.1.1에서 10.147.25.80으로 정적으로 변환된다고 가정합니다. EAP 인증이 사용됩니다.



또한 Cisco IOS 소프트웨어 인증서에 172.16.1.1 및 10.147.25.80 모두에 대한 Subject Alternative Name이 있다고 가정합니다.

EAP 인증에 성공하면 Android는 확인을 수행하고 Subject Alternative Name(주체 대체 이름) 확장에서 Android 구성(10.147.25.80)에 사용된 피어의 IP 주소를 찾으려고 시도합니다. 확인 실패:

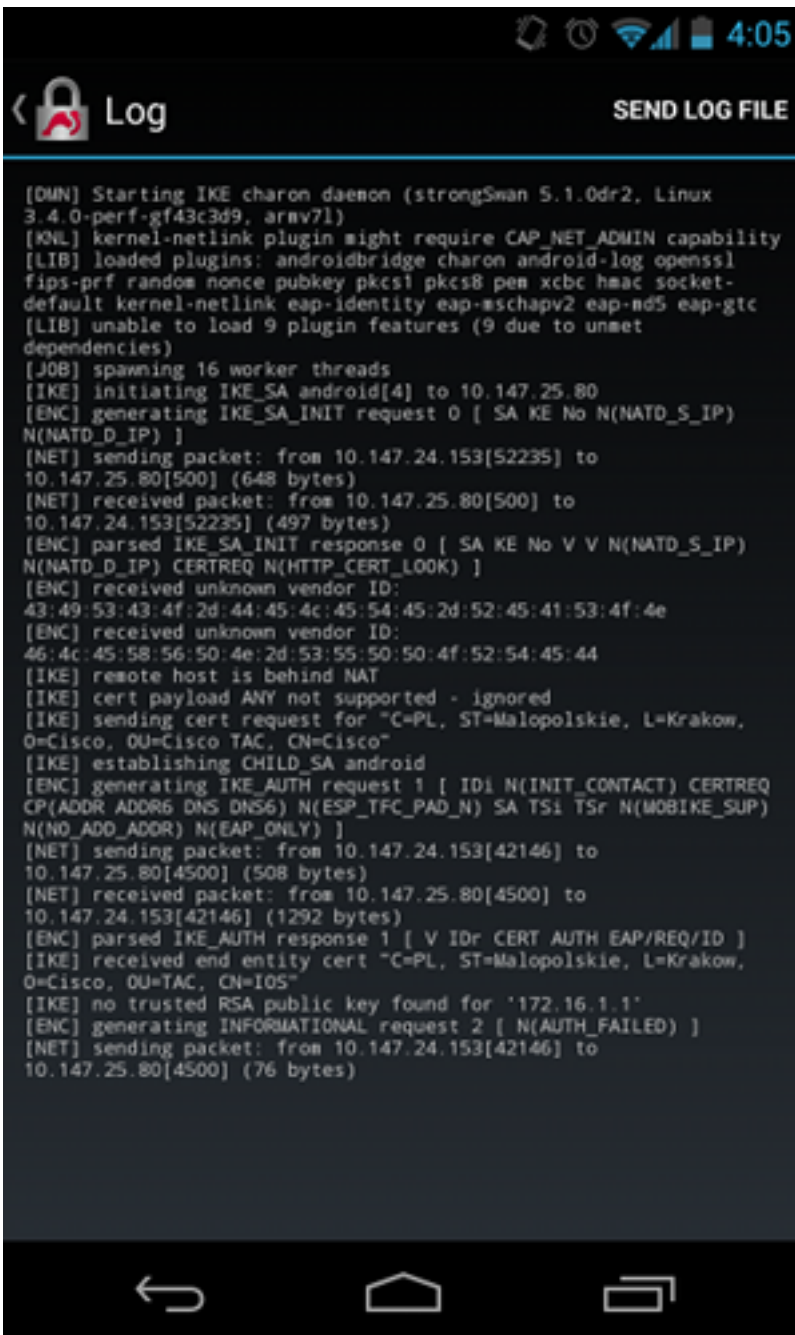


로그는 다음과 같습니다.

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

Android에서 첫 번째 주체 대체 이름 확장자(172.16.1.1)만 읽을 수 있으므로 오류가 발생했습니다.

이제 Cisco IOS 소프트웨어 인증서에 Subject Alternative Name(주체 대체 이름)의 주소가 둘 다 있지만 역순으로 있다고 가정합니다. 10.147.25.80 및 172.16.1.1. Android는 세 번째 패킷에서 VPN 게이트웨이(172.16.1.1)의 IP 주소인 IKEID를 수신하면 검증을 수행합니다.



이제 로그에 다음이 표시됩니다.

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

따라서 Android가 IKEID를 받으면 Subject Alternative Name(주체 대체 이름)에서 IKEID를 찾아야 하며 첫 번째 IP 주소만 사용할 수 있습니다.

**참고:**EAP 인증에서 Cisco IOS 소프트웨어가 전송한 IKEID는 기본적으로 IP 주소입니다.RSA 인증에서 IKEID는 기본적으로 인증서 DN입니다.ikev2 프로파일 아래의 **identity** 명령을 사용하여 이러한 값을 수동으로 변경합니다.

## 다음을 확인합니다.

확인 및 테스트 절차는 컨피그레이션 예에서 확인할 수 있습니다.

# 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

## strongSwan CA 다중 CERT\_REQ

strongSwan의 인증서 설정이 Automatic Selection(기본값)인 경우, Android는 세 번째 패킷의 로컬 저장소에 있는 모든 신뢰할 수 있는 인증서에 대해 CERT\_REQ를 전송합니다. Cisco IOS 소프트웨어는 많은 수의 인증서 요청을 서비스 거부 공격으로 인식하므로 요청을 삭제할 수 있습니다.

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

## DVTI의 터널 소스

VTI(Virtual Tunnel Interface)에서 터널 소스를 설정하는 것이 일반적이지만 여기서는 필요하지 않습니다. tunnel source 명령이 동적 VTI(DVTI) 아래에 있다고 가정합니다.

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

인증 후 Cisco IOS 소프트웨어가 가상 템플릿에서 복제된 가상 액세스 인터페이스를 생성하려고 하면 다음 오류가 반환됩니다.

```
*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
```

장애 발생 2초 후 Cisco IOS 소프트웨어는 Android에서 재전송된 IKE\_AUTH를 수신합니다. 해당 패킷이 삭제됩니다.

## Cisco IOS 소프트웨어 버그 및 개선 요청

- Cisco Bug ID [CSCui46418](#), "RSA 인증을 위한 ID로 IOS Ikev2 ip 주소를 보냈습니다." 이 버그는 확인을 수행하기 위해 인증서에서 IKEID를 찾을 때 strongSwan이 올바른 주체 대체 이름(IP 주소)을 볼 수 있는 한 문제가 아닙니다.
- Cisco Bug ID [CSCui44976](#), "IOS PKI가 X509v3 확장 주체 대체 이름"으로 잘못 표시되었습니다. 이 버그는 Subject Alternative Name(주체 대체 이름)에 여러 IP 주소가 있는 경우에만 발생합니다. 마지막 IP 주소만 표시되지만 인증서 사용에는 영향을 주지 않습니다. 전체 인증서가 올바르게 전송 및 처리됩니다.
- Cisco Bug ID [CSCui44783](#), "IOS ENH PKI 기능은 subject-alt-name 확장명으로 CSR을 생성합



니다."

- Cisco Bug ID [CSCui44335](#), "ASA ENH Certificate x509 extensions displayed."

## 관련 정보

- [Cisco IOS 15.3 VPN 컨피그레이션 가이드](#)
- [Cisco IOS 15.3 명령 참조](#)
- [Cisco IOS Flex VPN 컨피그레이션 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)