Android strongSwan から Cisco IOS への IKEv2 での EAP 認証および RSA 認証

内容

概要

このドキュメントでは、Internet Key Exchange Version 2（IKEv2）プロトコルで Cisco IOS® ソフトウェア VPN ゲートウェイにアクセスするために strongSwan モバイル バージョンを設定する方法について説明します。

次の 3 つの例を示します。

- Extensible Authentication Protocol - Message Digest 5（EAP-MD5）認証で Cisco IOS ソフトウェア VPN ゲートウェイに接続する strongSwan 対応の Android フォン。
- 証明書認証(RSA)を使用してCisco IOSソフトウェアVPNゲートウェイに接続する

strongSwanを搭載したAndroidフォン。
- ネットワーク アドレス変換（NAT）で Cisco IOS ソフトウェア VPN ゲートウェイに接続する strongSwan 対応の Android フォン。 VPN ゲートウェイ証明書には 2 種類の x509 拡張の Subject Alternative Name が必要です。

Cisco IOS ソフトウェアおよび strongSwan の制限も含まれます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- OpenSSL 設定に関する基礎知識
- Cisco IOS ソフトウェア コマンドライン インターフェイス（CLI）に関する基礎知識
- IKEv2 に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

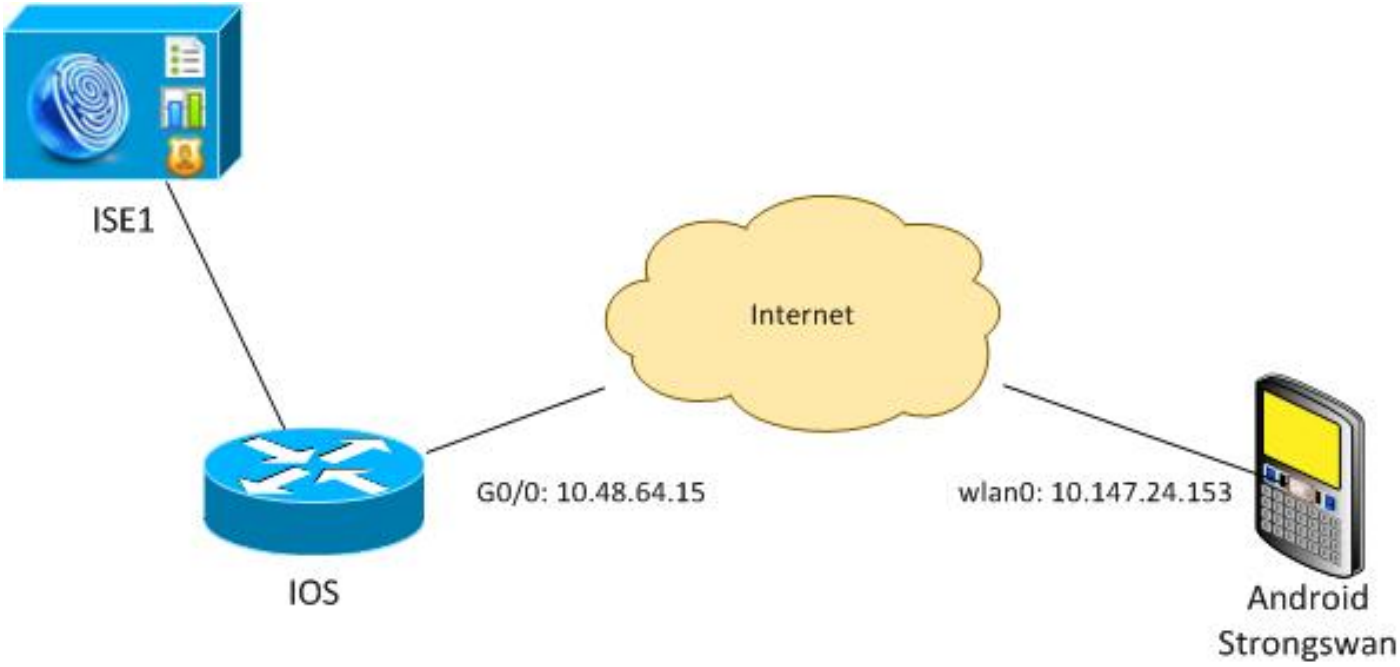
- strongSwan 対応の Android 4.0 以降
- Cisco IOS ソフトウェア リリース 15.3T 以降
- Cisco Identity Services Engine（ISE）ソフトウェア、バージョン 1.1.4 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

> **注：**
>
> アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。
>
> **debug コマンドを使用する前に、「**デバッグ コマンドの重要な情報」を参照してください。

ネットワーク図



Android の strongSwan は、内部ネットワークに安全にアクセスするために Cisco IOS ソフトウェア ゲートウェイを使用して IKEv2 トンネルを確立します。

証明書登録

証明書は、EAP ベースおよび RSA ベースの認証の前提条件です。

EAP 認証のシナリオでは、証明書が必要なのは VPN ゲートウェイだけです。クライアントは、ソフトウェアが Android で信頼されている認証局（CA）によって署名された証明書を提示した場合にのみ、Cisco IOS ソフトウェアに接続します。その後、EAP セッションが開始され、クライアントが Cisco IOS ソフトウェアへの認証を行います。

RSA ベースの認証には、両方のエンドポイントで正しい証明書が必要です。

IP アドレスを peer-ID として使用している場合、証明書に追加の要件があります。Android の strongSwan は、VPN ゲートウェイの IP アドレスが x509 拡張の Subject Alternative Name に含まれているかどうかを確認します。含まれていない場合、Android は接続切断します。RFC 6125 の勧告に加え、この方法を推奨します。

Cisco IOS ソフトウェアに IP アドレスを含む拡張付きの証明書を生成できないという制限があるため、OpenSSL を CA として使用します。すべての証明書は OpenSSL によって生成され、Android および Cisco IOS ソフトウェアにインポートされます。

Cisco IOS ソフトウェアでは、**subject-alt-name コマンドを使用して、IP アドレスを含む拡張を作成できます。ただし、このコマンドは自己署名証明書でのみ動作します。**Cisco Bug ID CSCui44783、「subject-alt-name 拡張で CSR を生成できる IOS ENH PKI 機能（IOS ENH PKI ability to generate CSR with subject-alt-name extension）」は、Cisco IOS ソフトウェアですべてのタイプの登録に拡張を生成できる拡張要求です。

CA を生成するコマンドの例を次に示します。

```
#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 はコンフィギュレーション ファイルです。CA 拡張を TRUE に設定する必要があります。

```
[ 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
```

証明書を生成するコマンドは、Cisco IOS ソフトウェアと Android でよく似ています。この例は、証明書の署名に使用する CA があることを前提としています。

```
#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 はコンフィギュレーション ファイルです。Alternate Subject Name 拡張はキー設定です。この例では、CA 拡張は FALSE に設定します。

```
[ 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
```

証明書は、Cisco IOS ソフトウェアと Android の両方に生成する必要があります。

IP アドレス 10.48.64.15 は、Cisco IOS ソフトウェア ゲートウェイに属しています。Cisco IOSソフトウェアの証明書を生成する場合は、subjectAltNameが10.48.64.15に設定されていることを確認します。AndroidはCisco IOSソフトウェアから受信した証明書を検証し、subjectAltNameでそのIPアドレスを検索します。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェアには、RSA ベースおよび EAP ベースの認証に正しい証明書がインストールされている必要があります。

Cisco IOS ソフトウェアの pfx ファイル（pkcs12 コンテナである）をインポートすることができます。

```
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.
```

インポートが成功したことを確認するには、**show crypto pki certificates verbose コマンドを使用します。**

```
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

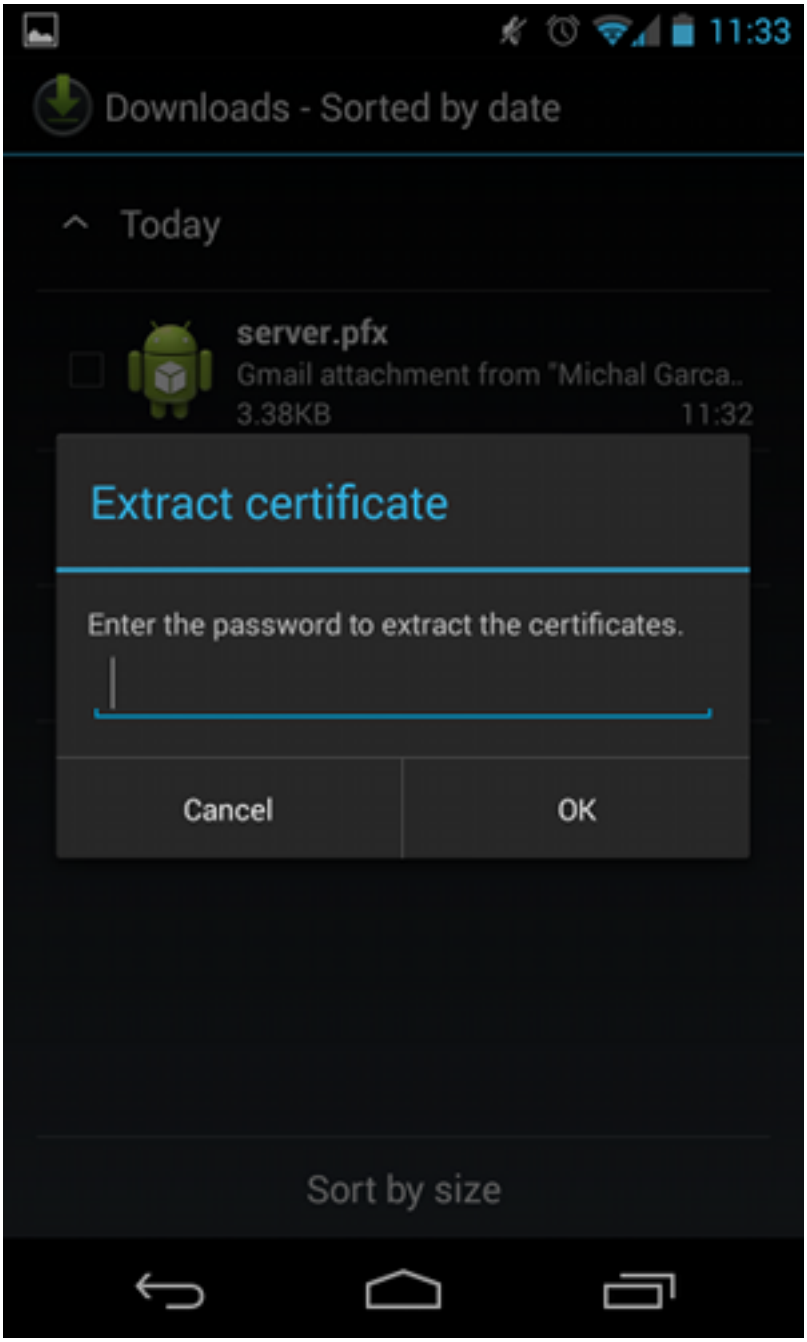
EAP ベースの認証では、Andorid に正しい CA 証明書がインストールされている必要があります。

RSA ベースの認証では、Andorid に CA 証明書とそれ自身の証明書の両方がインストールされている必要があります。

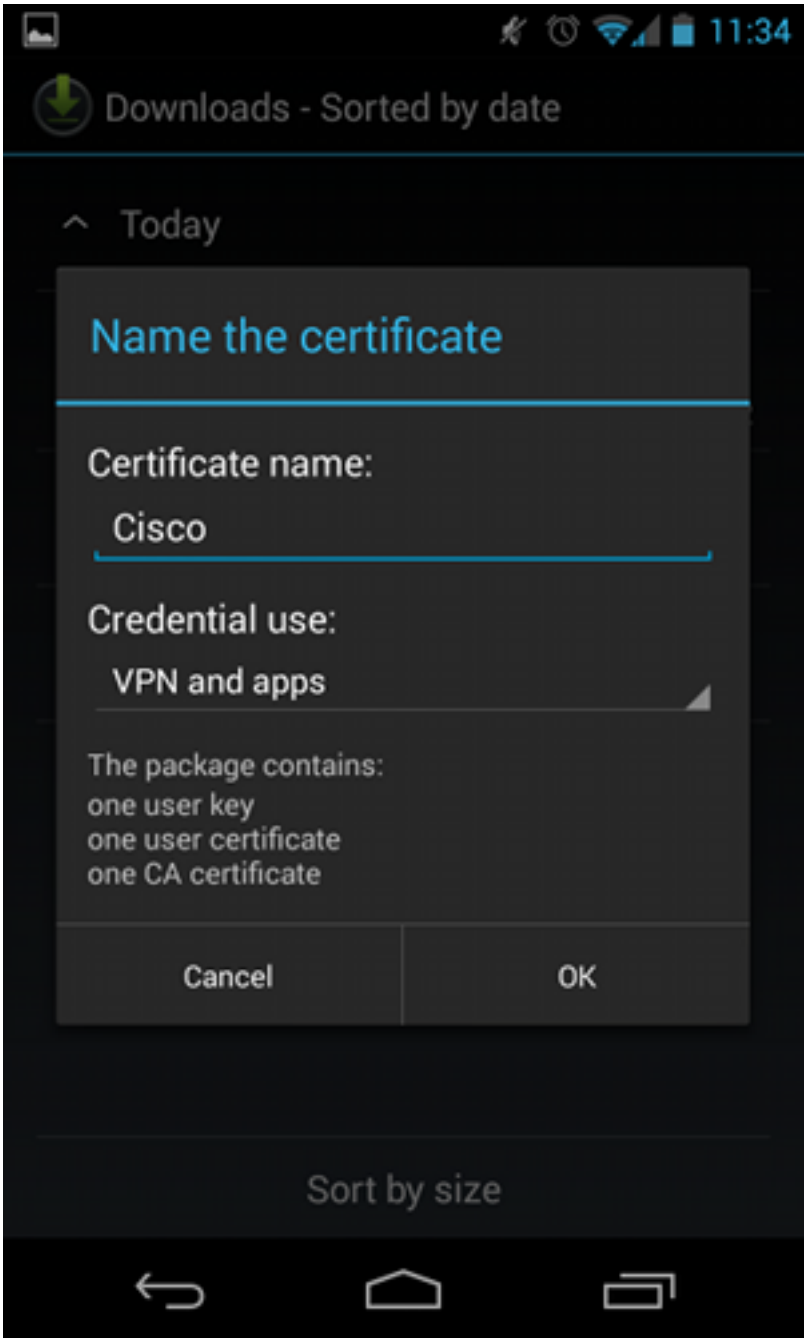
この手順では、両方の証明書をインストールする方法について説明します。

1. pfx ファイルを電子メールで送信して開きます。

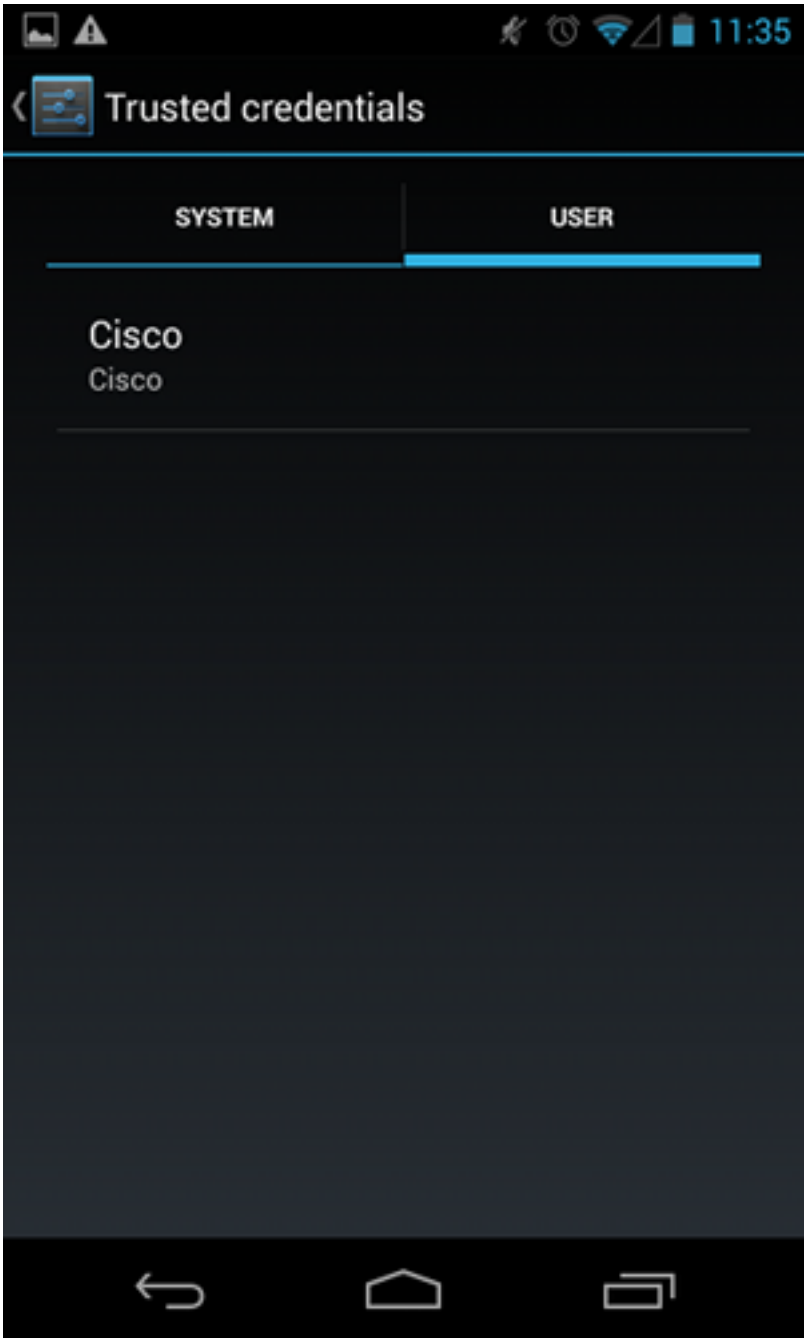
2. pfx ファイルの生成時に使用したパスワードを入力します。



3. インポートした証明書の名前を入力します。



4. 証明書のインストールを確認するには、[Settings] **> [Security]** > [Trusted Credentials] **に移動します。**新しい証明書がユーザ ストアに表示されます。



この時点で、ユーザ証明書および CA 証明書がインストールされます。pfx ファイルは、ユーザ証明書と CA 証明書の両方を含む pkcs12 コンテナです。

Android には、証明書のインポート時に正確な要件があります。たとえば、CA 証明書を正常にインポートするには、Android で x509v3 拡張の基本制約 CA が TRUE に設定されている必要があります。したがって、CA を生成するか、独自の CA を使用する場合、正しい拡張があることを確認することが重要です。

```
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>
```

EAP Authentication

EAP 認証用の Cisco IOS ソフトウェア設定

IKEv2 により、ユーザ認証の実行に EAP プロトコル スタックを使用することができます。VPN ゲートウェイは証明書で自身を提示します。クライアントは、その証明書を信頼すると、そのゲートウェイからの EAP 要求 ID に応答します。Cisco IOS ソフトウェアでは、その ID を使用して Radius-Request メッセージを認証、許可、アカウンティング（AAA）に送信し、EAP-MD5 セッションがサプリカント（Android）と認証サーバ（Access Control Server（ACS）または ISE）の間に確立されます。

Radius-Accept メッセージに示されているように、EAP-MD5 認証が成功した後、Cisco IOS ソフトウェアでは、コンフィギュレーション モードを使用して IP アドレスをクライアントにプッシュし、トラフィック セレクタ ネゴシエーションを続行します。

Android が IKEID=cisco を送信している（設定どおりに）ことに留意してください。 Cisco IOS ソフトウェアで受信したこの IKEID は、「ikev2 profile PROF」と一致します。

```
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
!
```

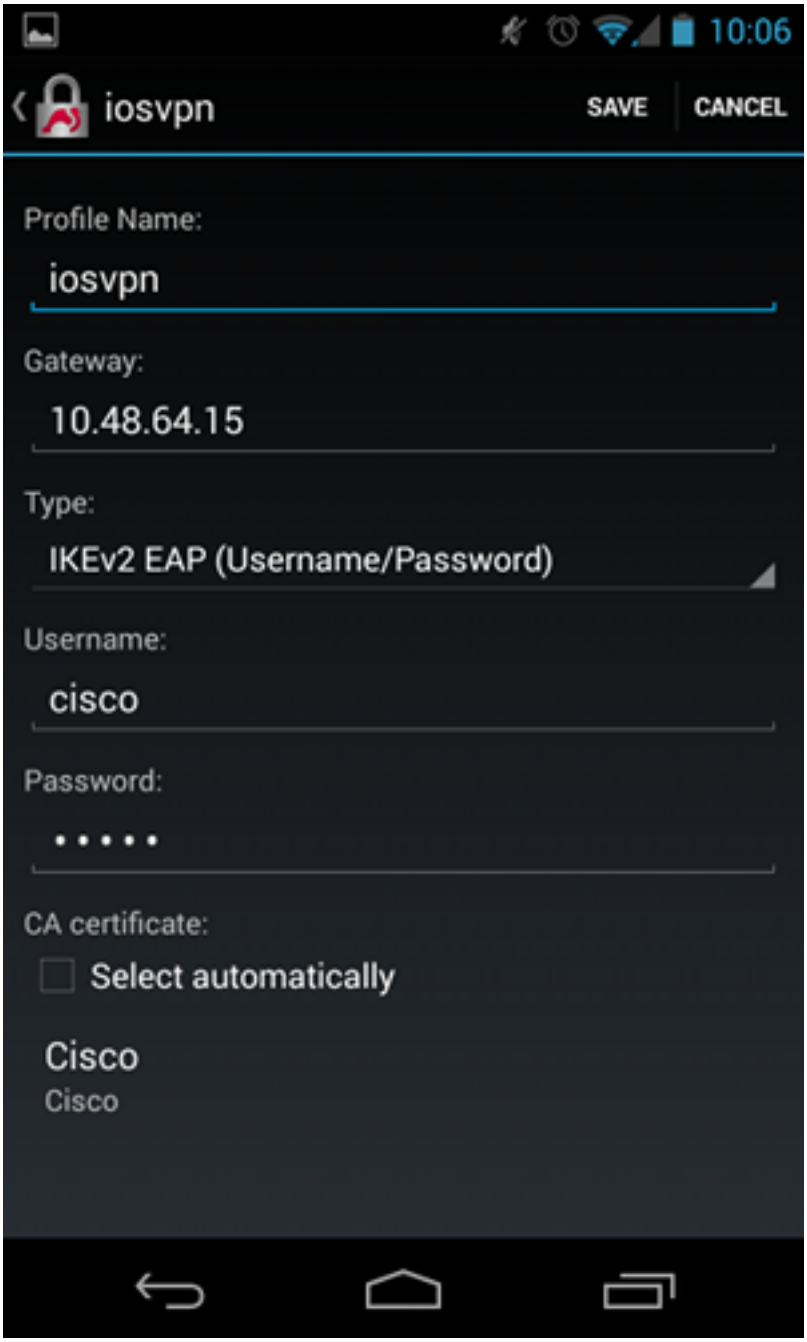
```
crypto ipsec profile PROF
 set transform-set 3DES-MD5
 set ikev2-profile PROF

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 認証用の Android 設定

Android の strongSwan には、EAP を設定する必要があります。

1. 自動証明書選択を無効にします。無効にしないと、100 以上の CERT_REQ が 3 番目のパケットで送信されます。

2. 前の手順でインポートした特定の証明書（CA）を選択します。ユーザ名とパスワードは AAA サーバと同じにする必要があります。



EAP 認証テスト

Cisco IOS ソフトウェアでの EAP の認証に最も重要なデバッグを次に示します。分かりやすくするために、ほとんどの出力が省略されています。

```
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
```

Android の口グを次に示します。

```
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)
```

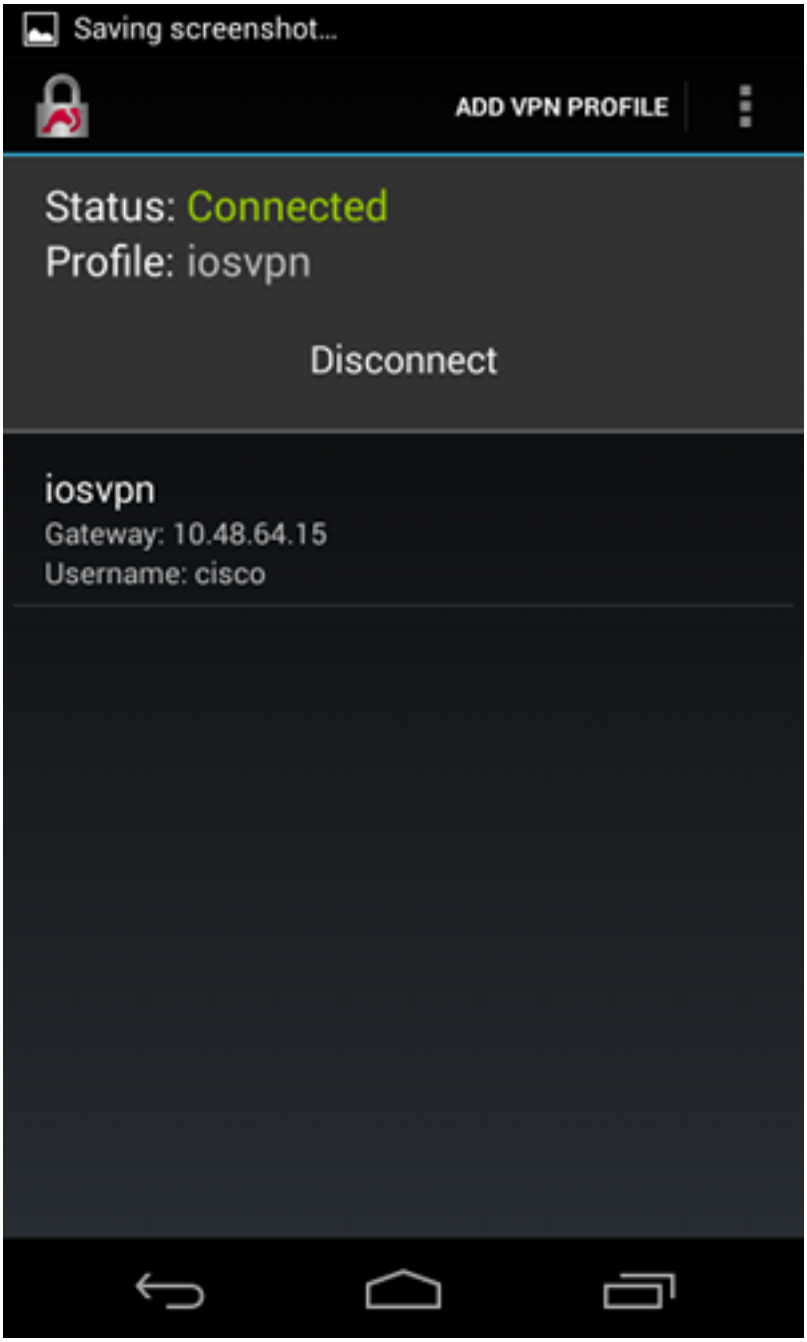
```
09[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(76 bytes)
09[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/TLS ]
09[IKE] server requested EAP_TLS authentication (id 0x59)
09[IKE] EAP method not supported, sending EAP_NAK
09[ENC] generating IKE_AUTH request 3 [ EAP/RES/NAK ]
09[NET] 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
```

この例は、Cisco IOS ソフトウェアの状態を確認する方法を示します。

```
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
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
```

次の図は、Android の状態を確認する方法を示します。


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

RSA 認証

RSA 認証用の Cisco IOS ソフトウェア設定

Rivest-Shamir-Adleman (RSA) の認証では、Android は、Cisco IOS ソフトウェアへの認証を行うために証明書を送信します。このため、そのトラフィックを特定の IKEv2 プロファイルにバインドする証明書マップが必要です。ユーザ EAP 認証は不要です。

リモート ピアの RSA 認証を設定する方法の例を次に示します。

```
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 認証用の Android 設定

ユーザ クレデンシャルは、ユーザ証明書に置き換えられています。

RSA 認証テスト

Cisco IOS ソフトウェアでの RSA の認証に最も重要なデバッグを次に示します。分かりやすくするために、ほとんどの出力が省略されています。

```
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
```

Android のログを次に示します。

```
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 ソフトウェアでは、署名および確認に RSA が使用されます。前のシナリオでは、確認に EAP が使用されました。

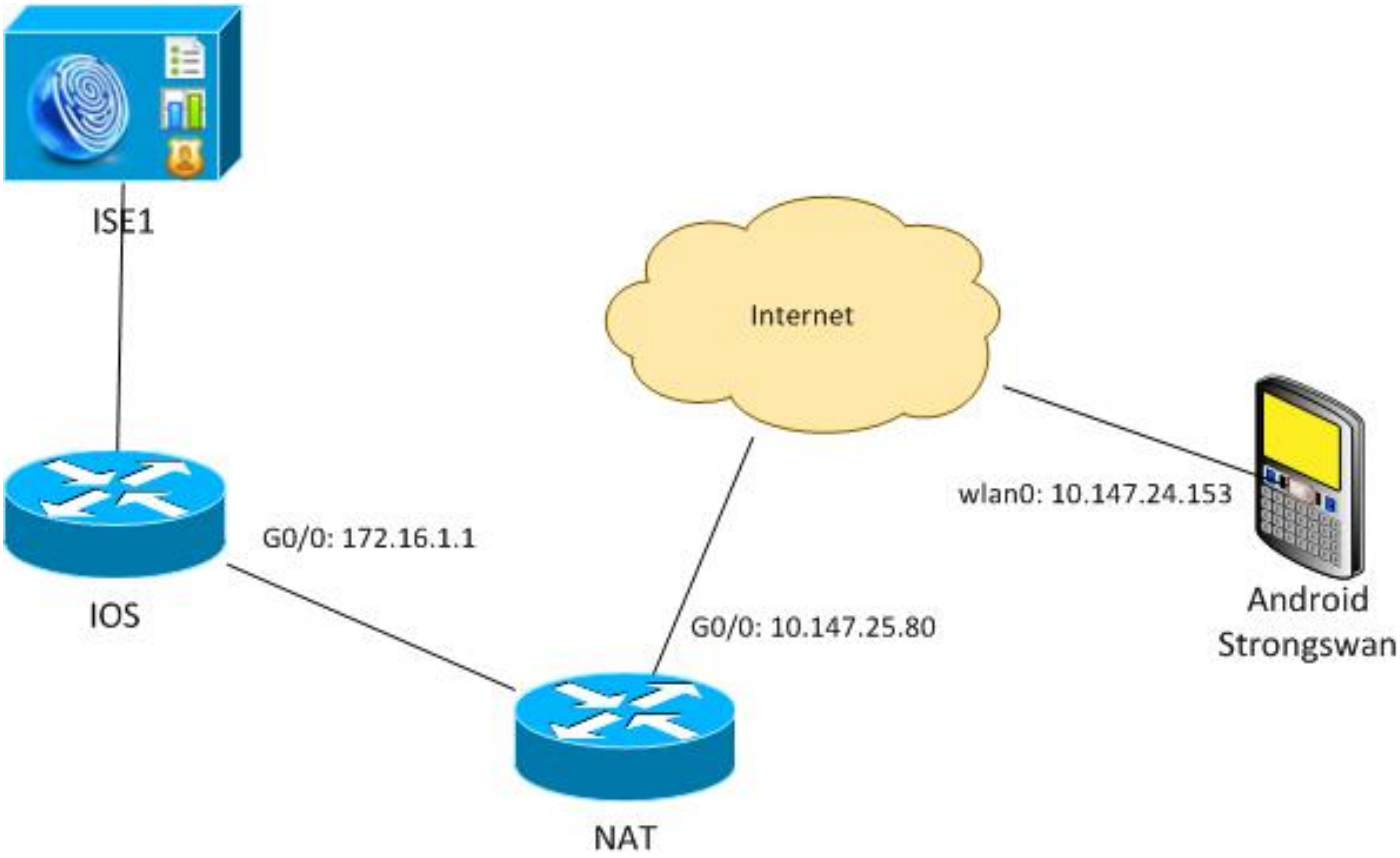
```
BSAN-2900-1#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/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
```

Android の状態の確認は、前のシナリオと同様です。

NAT の背後にある VPN ゲートウェイ - strongSwan および Cisco IOS ソフトウェアの制限

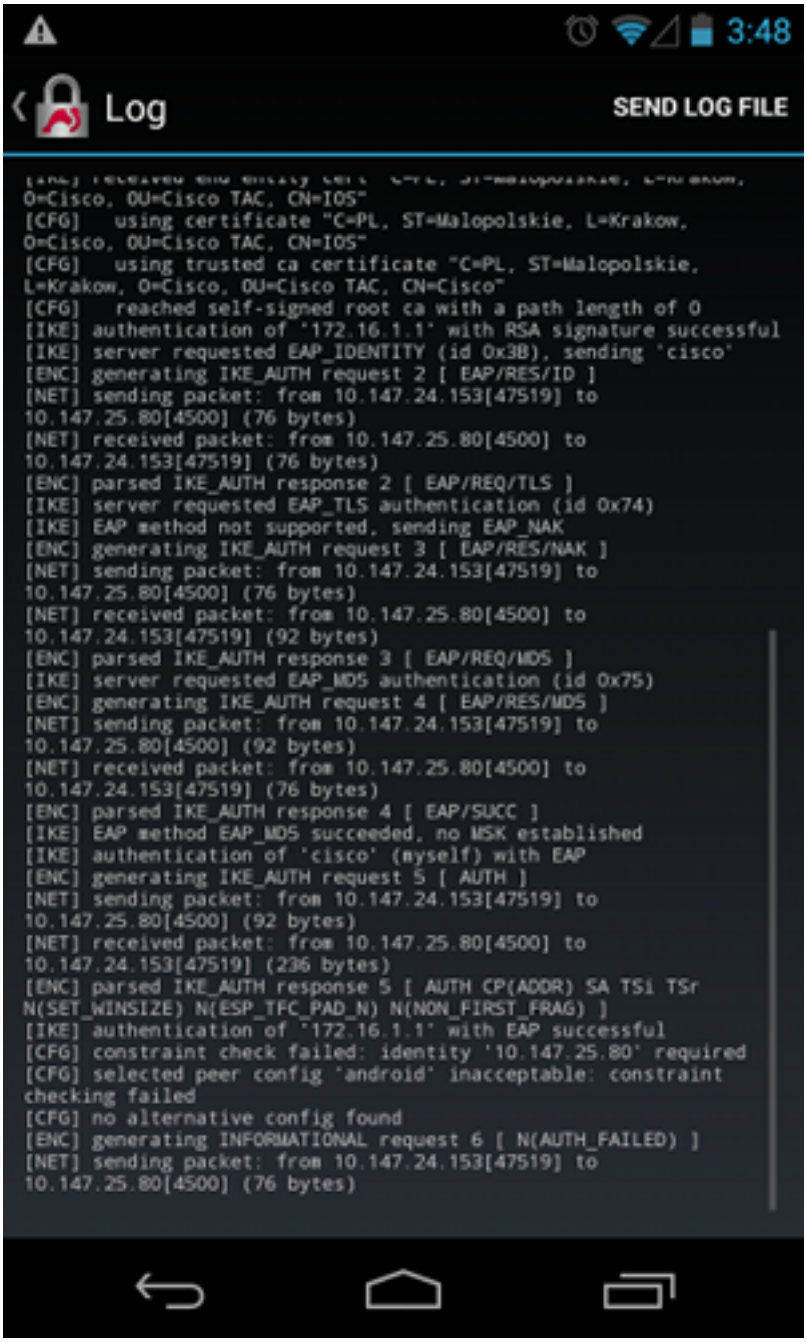
この例では、strongSwan 証明書確認の制限について説明します。

Cisco IOSソフトウェアのVPNゲートウェイのIPアドレスが172.16.1.1から10.147.25.80に静的に変換されていると仮定します。EAP認証が使用されます。



Cisco IOS ソフトウェアに 172.16.1.1 と 10.147.25.80 の両方の Subject Alternative Name があることを前提としています。

EAP 認証が成功した後、Android では、確認を実行し、Subject Alternative Name 拡張の Android 設定で使用されたピアの IP アドレス（10.147.25.80）を検索します。確認が失敗します。

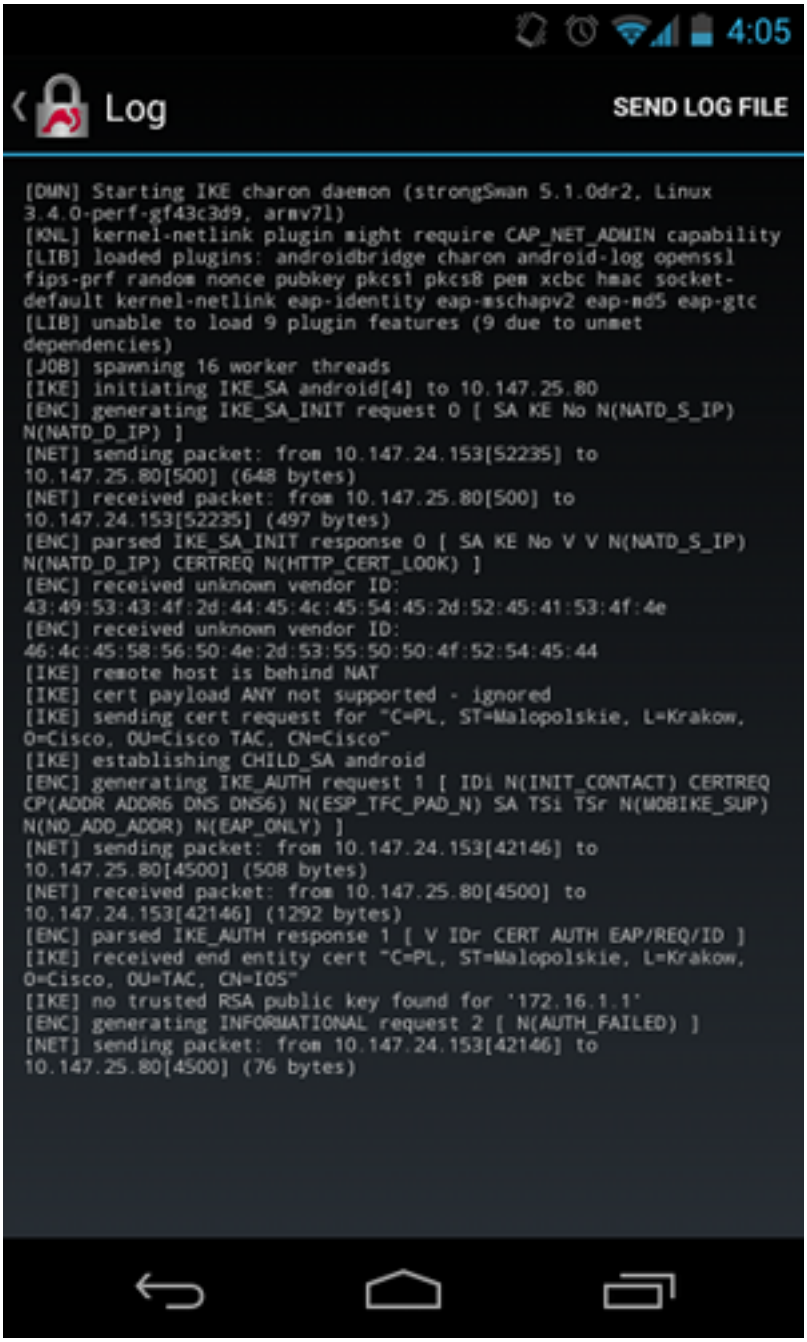


ログは次の内容を示しています。

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

Android が最初の Subject Alternative Name 拡張（172.16.1.1）しか読み取れないため、障害が発生しました。

ここでは、Cisco IOS ソフトウェア証明書の Subject Alternative Name に逆順の 2 つのアドレス10.147.25.80および172.16.1.1。Androidは、VPNゲートウェイ(172.16.1.1)のIPアドレスであるIKEIDを3番目のパケットで受信すると、検証を実行します。



ログは次の内容を示しています。

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

したがって、Android は、IKEID を受信すると、Subject Alternative Name で IKEID を検索する必要がありますが、最初の IP アドレスしか読み取れません。

> **注**：EAP 認証では、Cisco IOS ソフトウェアによって送信された IKEID がデフォルトで IP アドレスになっています。RSA 認証では、IKEID がデフォルトで証明書 DN になっています。これらの値を手動で変更するには、ikev2 プロファイルで **identity コマンドを使用します。**

確認

設定例では、確認およびテストの手順を使用できます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

strongSwan CA の複数の CERT_REQ

strongSwan の証明書の設定が自動選択（デフォルト）の場合、Android は 3 番目のパケットでローカル ストアのすべての信頼できる証明書の CERT_REQ を送信します。Cisco IOS ソフトウェアは、多数の証明書要求をサービス拒否攻撃と認識するため、要求をドロップすることがあります。

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

DVTI のトンネル発信元

仮想トンネル インターフェイス（VTI）上でトンネル発信元を設定することが広く一般的に採用されていますが、ここでは不要です。ダイナミック VTI（DVTI）に tunnel source コマンドがあると仮定します。

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

認証後、Cisco IOS ソフトウェアは、仮想テンプレートからクローニングされた仮想アクセス インターフェイスを作成しようとすると、次のようにエラーが返されます。

```
*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
```

障害の 2 秒後に、Cisco IOS ソフトウェアは Android から再送信された IKE_AUTH を受信します。そのパケットはドロップされます。

Cisco IOS ソフトウェアのバグや拡張要求

- Cisco Bug ID CSCui46418、「IOS Ikev2 の IP アドレスが RSA 認証の ID として送信される（IOS Ikev2 ip address sent as identity for RSA authentication）」
  この不具合は、確認を実行するために証明書の IKEID を検索するときに strongSwan が正しい Subject Alternative Name（IP アドレス）を認識できる限りは問題になりません。
- Cisco Bug ID CSCui44976、「IOS PKI で X509v3 拡張の Subject Alternative Name が正しく表示されない（IOS PKI incorrectly displayed X509v3 extension Subject Alternative

Name ）」
この不具合が発生するのは、Subject Alternative Name に複数の IP アドレスがある場合だけです。最後の IP アドレスだけが表示されますが、証明書の使用には影響しません。証明書全体が送信され、正しく処理されます。
- Cisco Bug ID CSCui44783、「subject-alt-name 拡張で CSR を生成できる IOS ENH PKI 機能（IOS ENH PKI ability to generate CSR with subject-alt-name extension ）」
- Cisco Bug ID CSCui44335、「ASA ENH 証明書 x509 拡張が表示される」

関連情報

- Cisco IOS 15.3 VPN コンフィギュレーション ガイド
- Cisco IOS 15.3 Command Reference
- Cisco IOS Manager VPN Configuration Guide
- テクニカル サポートとドキュメント – Cisco Systems