IKEv2从Android strongSwan到具有EAP和RSA身份验证的Cisco IOS

目录

简介
先决条件
要求
使用的组件
配置
网络图
证书注册
Cisco IOS 软件
Android
EAP 身份验证
用于EAP身份验证的Cisco IOS软件配置
EAP身份验证的Android配置
EAP身份验证测试
RSA身份验证
用于RSA身份验证的Cisco IOS软件配置
RSA身份验证的Android配置
RSA身份验证测试
NAT背后的VPN网关 — strongSwan和Cisco IOS软件限制
验证
故障排除
strongSwan CA多CERT_REQ
DVTI上的隧道源
Cisco IOS软件错误和增强请求
相关信息

简介

本文档介绍如何配置strongSwan的移动版本，以便通过互联网密钥交换版本2(IKEv2)协议访问Cisco IOS®软件VPN网关。

给出了三个示例：

- 具有strongSwan的Android电话，该StrongSwan通过可扩展身份验证协议 — 消息摘要5(EAP-MD5)身份验证连接到Cisco IOS软件VPN网关。
- 具有strongSwan的Android电话，通过证书身份验证(RSA)连接到Cisco IOS软件VPN网关。
- 具有strongSwan的Android电话，连接到网络地址转换(NAT)后的Cisco IOS软件VPN网关。 在

VPN网关证书中要求有两个x509扩展主题备用名称。
还包括Cisco IOS软件和strongSwan限制。

先决条件

要求

Cisco 建议您了解以下主题：

- OpenSSL配置的基本知识
- Cisco IOS软件命令行界面(CLI)配置的基本知识
- IKEv2的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

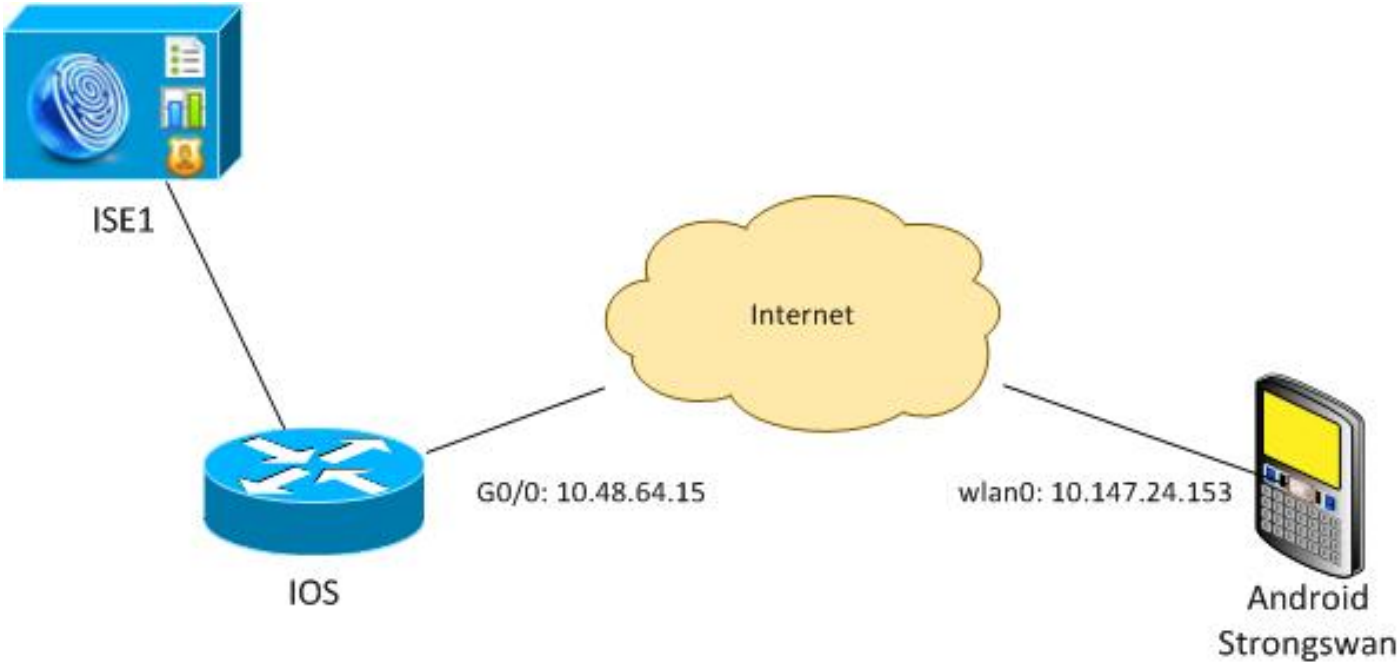
- Android 4.0或更高版本（使用strongSwan）
- Cisco IOS软件版本15.3T或更高版本
- 思科身份服务引擎(ISE)软件，版本1.1.4及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

> **注意：**
>
> 命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。
>
> 使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

网络图



Android strongSwan使用Cisco IOS软件网关建立IKEv2隧道，以安全访问内部网络。

证书注册

证书是基于EAP和基于RSA的身份验证的先决条件。

在EAP身份验证场景中，仅VPN网关需要证书。仅当软件提供由Android上受信任的证书颁发机构(CA)签名的证书时，客户端才连接到Cisco IOS软件。然后，EAP会话将启动，以便客户端向Cisco IOS软件进行身份验证。

对于基于RSA的身份验证，两个终端都必须具有正确的证书。

当IP地址用作对等ID时，对证书有其他要求。Android strongSwan验证VPN网关的IP地址是否包含在x509分机主题备用名称中。否则，Android会断开连接；这是一个良好的实践，也是RFC 6125的建议。

OpenSSL用作CA，因为Cisco IOS软件有以下限制：它无法生成扩展包含IP地址的证书。所有证书都由OpenSSL生成，并导入到Android和Cisco IOS软件。

在Cisco IOS软件中，**subject-alt-name**命令可用于创建包含IP地址的扩展，但该命令仅适用于自签名证书。Cisco Bug ID CSCui44783，“IOS ENH PKI cability to generate CSR with subject-alt-name extension”（IOS ENH PKI能力生成带有主题alt-name扩展的CSR）是允许Cisco IOS软件生成所有类型注册的扩展的增强请求。

以下是生成CA的命令示例：

```
#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是配置文件。CA分机应设置为TRUE:

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

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

生成证书的命令与Cisco IOS软件和Android非常相似。本示例假设已有CA用于签署证书：

```
#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是配置文件。“备用主题名称”分机是键设置。在本例中，CA扩展设置为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
```

应为Cisco IOS软件和Android生成证书。

IP地址10.48.64.15属于Cisco IOS软件网关。为Cisco IOS软件生成证书时，请确保

subjectAltName设置为10.48.64.15。Android验证从Cisco IOS软件接收的证书并尝试在subjectAltName中查找其IP地址。

Cisco IOS 软件

Cisco IOS软件需要为基于RSA和基于EAP的身份验证安装正确的证书。

可以导入Cisco IOS软件的pfx文件（pkcs12容器）：

```
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.
```

使用**show crypto pki certificates verbose命令**验证导入是否成功：

```
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

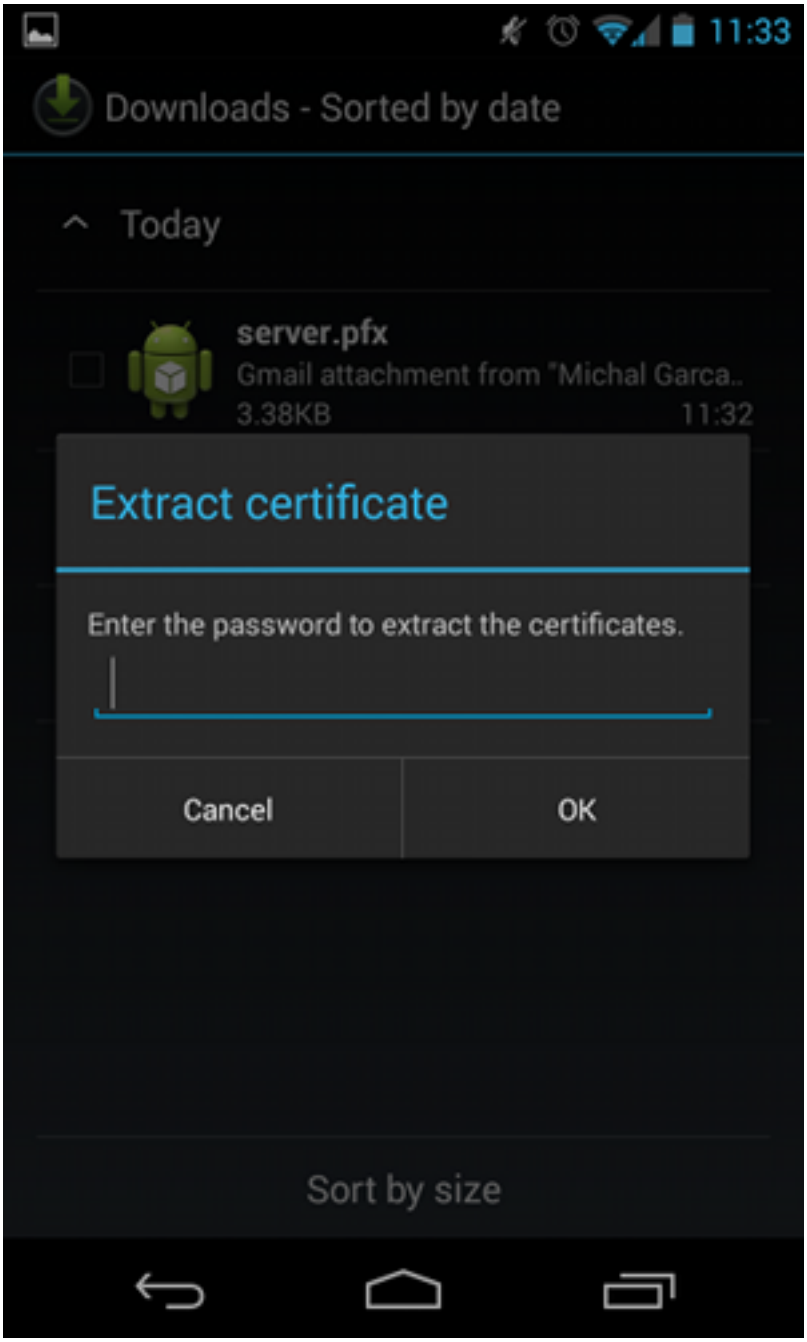
对于基于EAP的身份验证，Andorid只需安装正确的CA证书。

对于基于RSA的身份验证，Andorid需要同时安装CA证书和自己的证书。

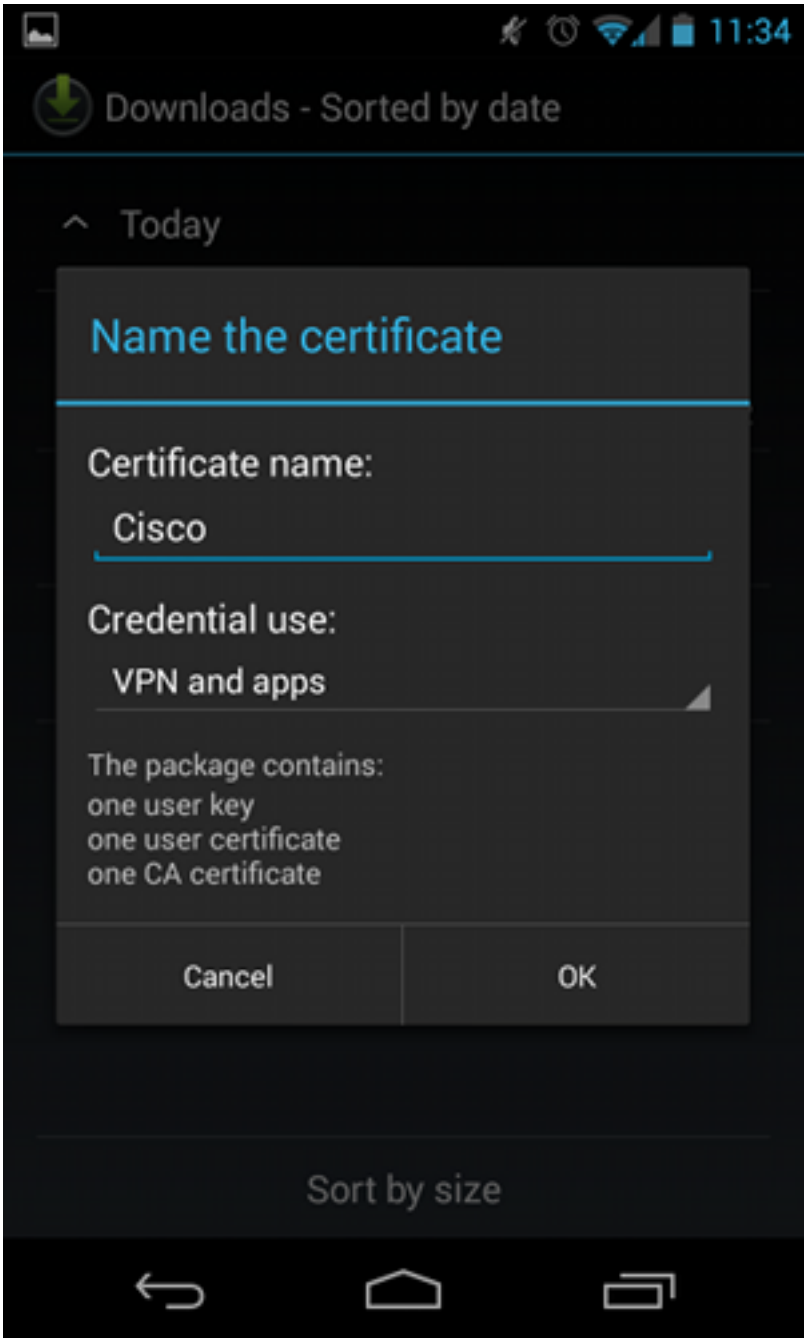
此过程介绍如何安装两个证书：

1. 通过电子邮件发送pfx文件，然后将其打开。

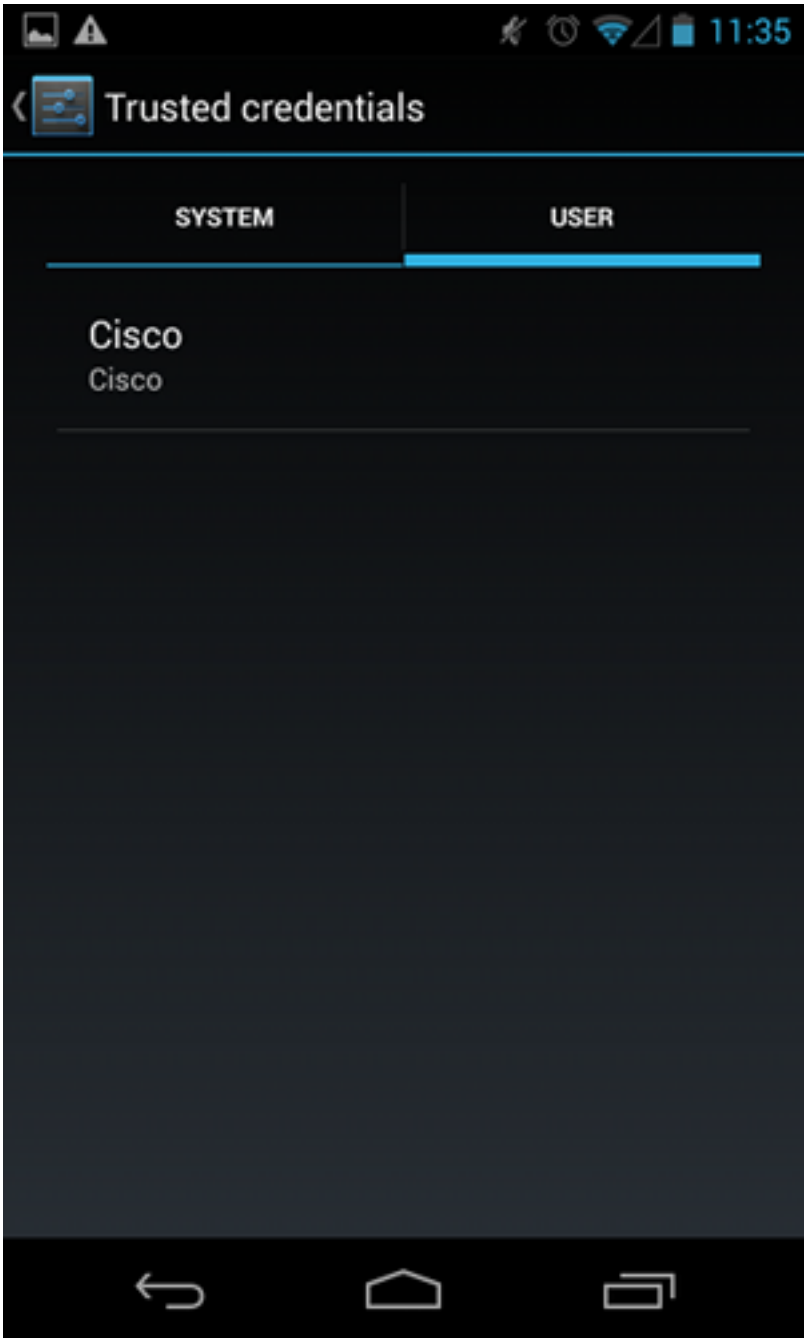
2. 提供生成pfx文件时使用的密码。



3. 提供导入的证书的名称。



4. 导航至**设置 > 安全 > 受信任凭据**以验证证书安装。新证书应显示在用户存储中：



此时，将安装用户证书和CA证书。pfx文件是包含用户证书和CA证书的pkcs12容器。

Android在导入证书时有精确要求。例如，要成功导入CA证书，Android要求将x509v3扩展基本约束CA设置为TRUE。因此，当您生成CA或使用自己的CA时，必须验证其是否具有正确的分机号：

```
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 身份验证

用于EAP身份验证的Cisco IOS软件配置

IKEv2允许使用EAP协议栈来执行用户身份验证。VPN网关自行提供证书。一旦客户端信任该证书，客户端就会从网关响应EAP请求身份。Cisco IOS软件使用该身份并向身份验证、授权和记帐(AAA)服务器发送Radius-Request消息，并在请求方(Android)和身份验证服务器（访问控制服务器[ACS]或ISE）之间建立EAP-MD5会话。

成功进行EAP-MD5身份验证后（如Radius-Accept消息所示），Cisco IOS软件使用配置模式将IP地址推送到客户端并继续进行流量选择器协商。

请注意，Android已发送IKEID=cisco（如配置）。 Cisco IOS软件上收到的此IKEID与“ikev2配置文件PROF”匹配。

```
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

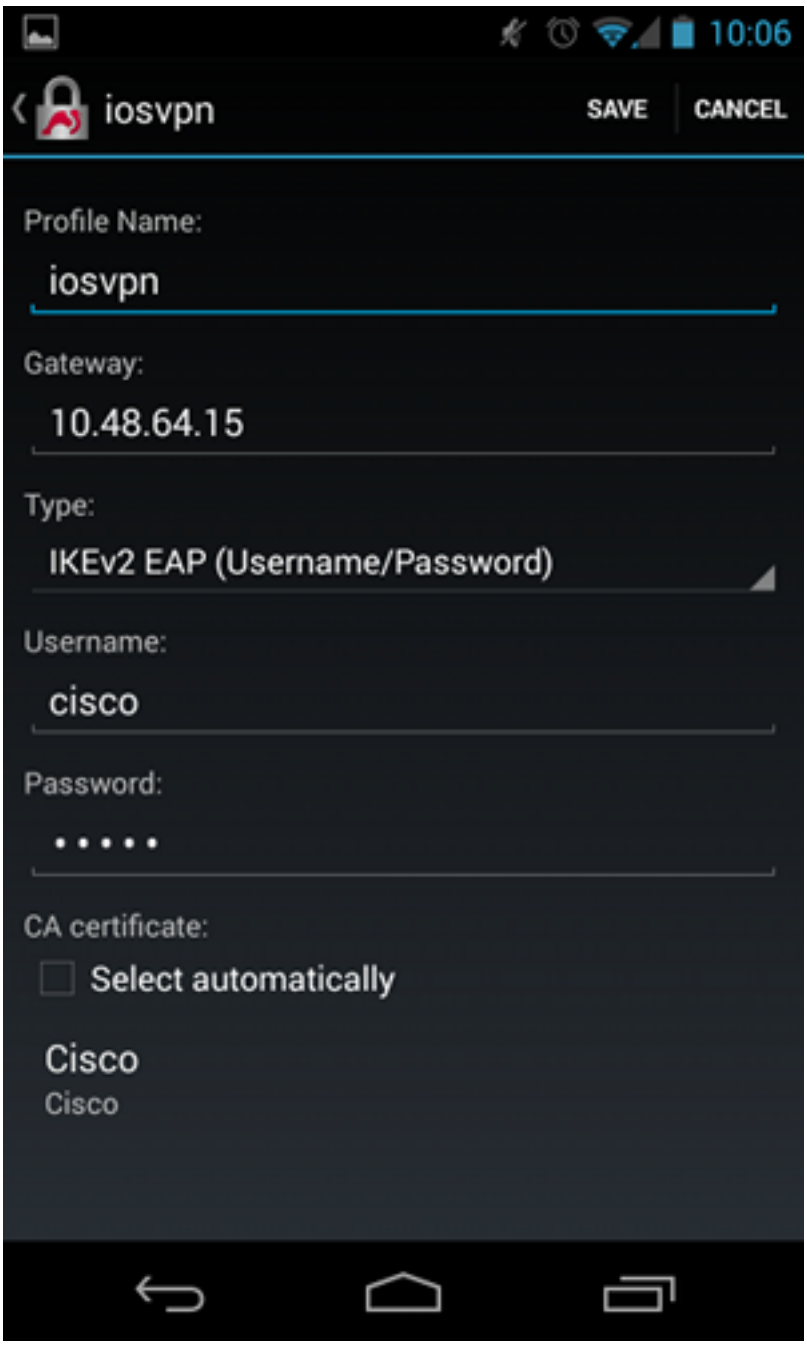
ip local pool POOL 192.168.0.1 192.168.0.10

radius-server host 10.48.66.185 key cisco
```

EAP身份验证的Android配置

Android strongSwan必须配置EAP:

1. 禁用自动证书选择；否则，在第三个数据包中发送100个或更多CERT_REQ。
2. 选择在上一步中导入的特定证书(CA);用户名和密码应与AAA服务器上的相同。



EAP身份验证测试

在Cisco IOS软件中，这些是EAP身份验证的最重要调试。为了清楚起见，大多数输出已省略：

```
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日志显示：

```
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
```

此示例显示如何验证Cisco IOS软件的状态：

```
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
```

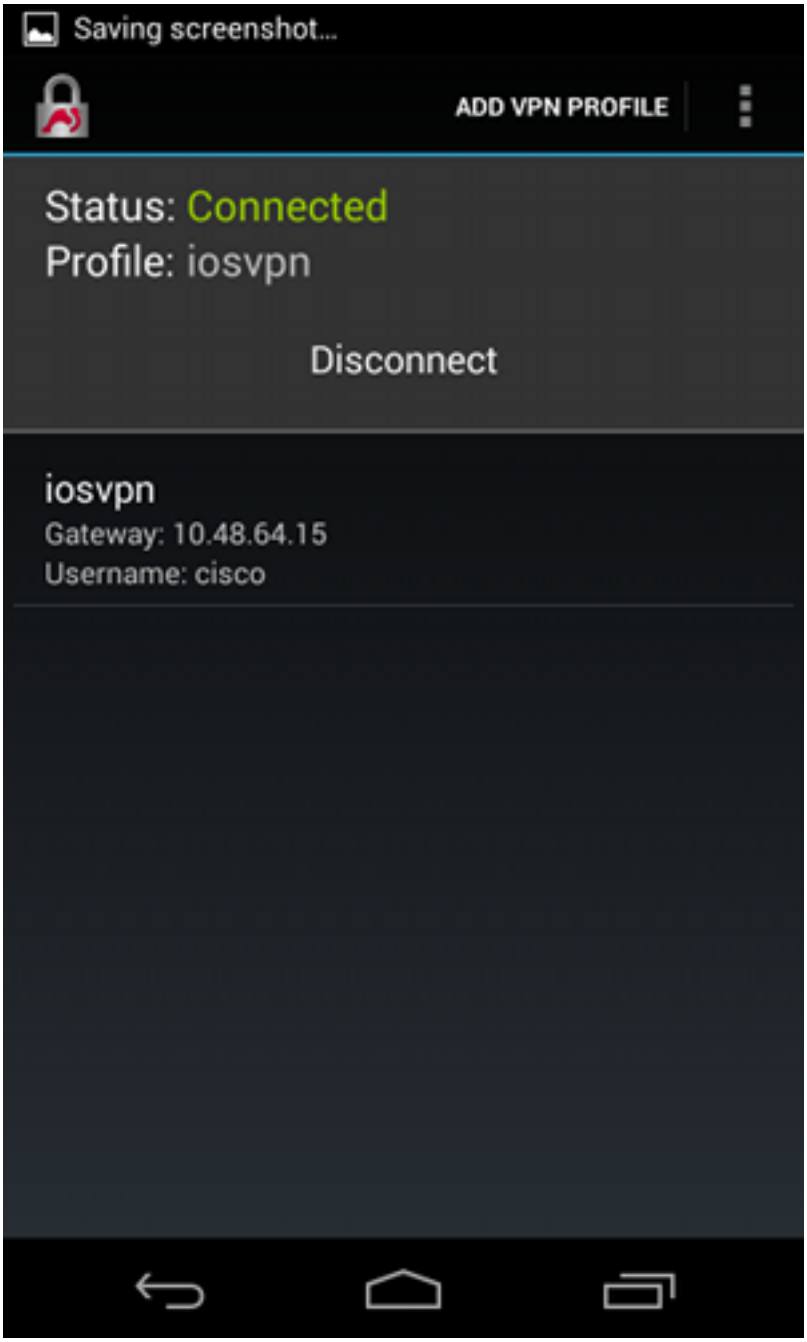
```
X - IKE Extended Authentication, F - IKE Fragmentation

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
```

下图显示了如何验证Android上的状态：


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



RSA身份验证

用于RSA身份验证的Cisco IOS软件配置

在Rivest-Shamir-Adleman(RSA)身份验证中，Android发送证书以向Cisco IOS软件进行身份验证。因此，需要将该流量绑定到特定IKEv2配置文件的证书映射。用户EAP身份验证不是必需的。

以下是如何为远程对等体设置RSA身份验证的示例：

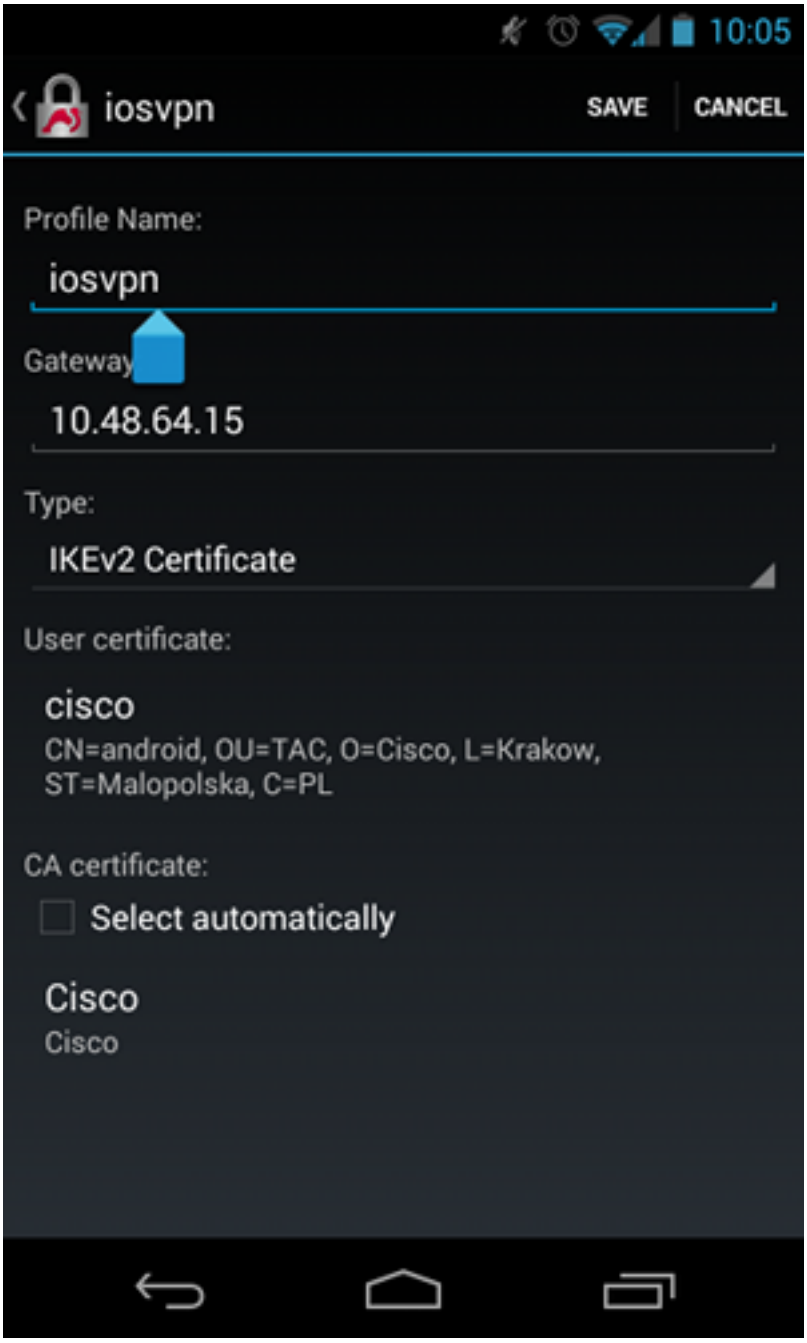
```
crypto pki certificate map CERT_MAP 10
 subject-name co android

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身份验证的Android配置

用户凭证已被用户证书替换：



RSA身份验证测试

在Cisco IOS软件中，这些是RSA身份验证的最重要调试。为了清楚起见，大多数输出已省略：

```
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日志显示：

```
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
```

在Cisco IOS软件中，RSA用于签名和验证；在上一个场景中，EAP用于验证：

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

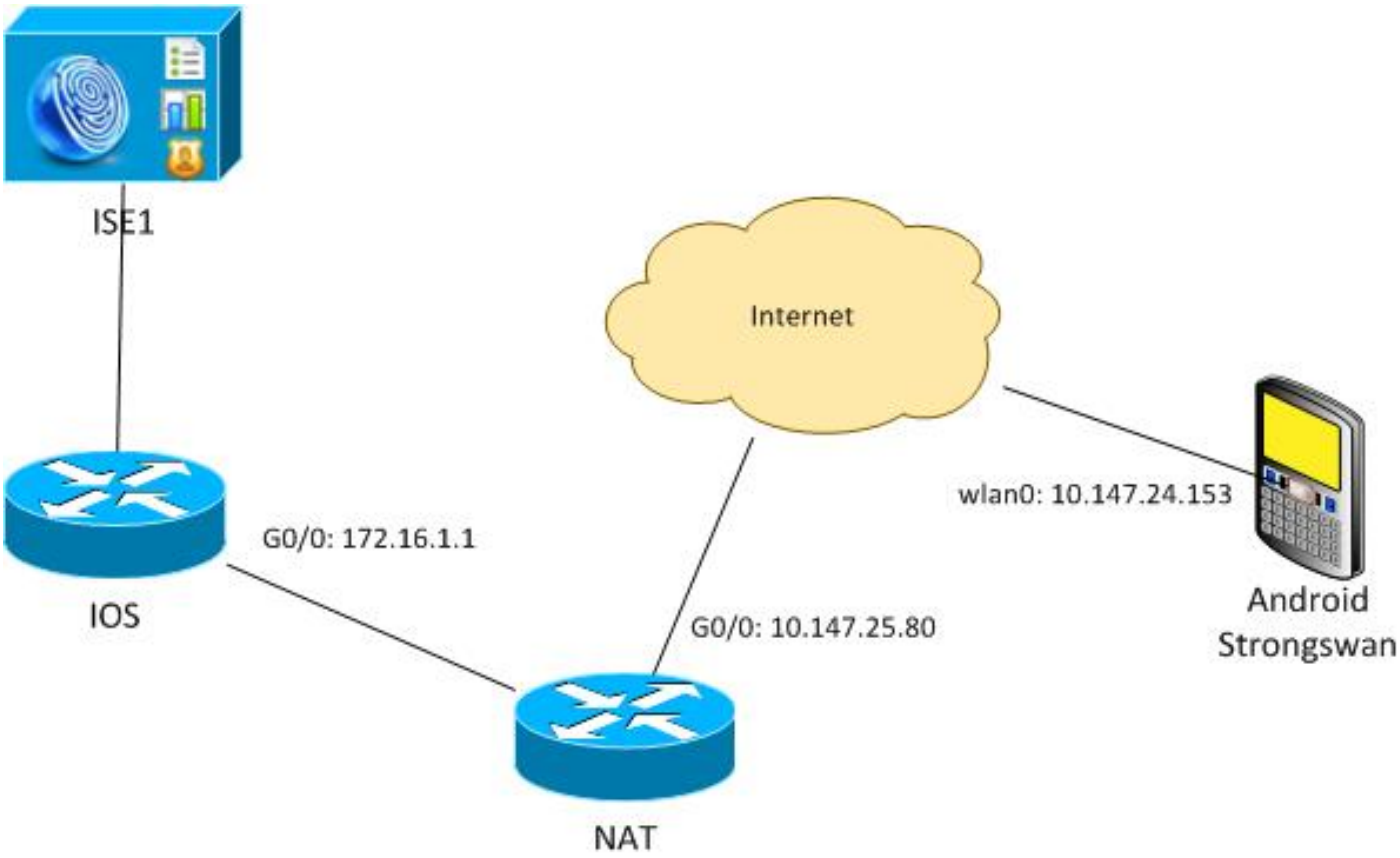
Tunnel-id Local                 Remote                fvrf/ivrf          Status
1         10.48.64.15/4500      10.147.24.153/44527   none/none          READY
     Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
     Life/Active Time: 86400/16 sec
     CE id: 1010, 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上的状态验证与上一个场景中的状态验证类似。

NAT背后的VPN网关 — strongSwan和Cisco IOS软件限制

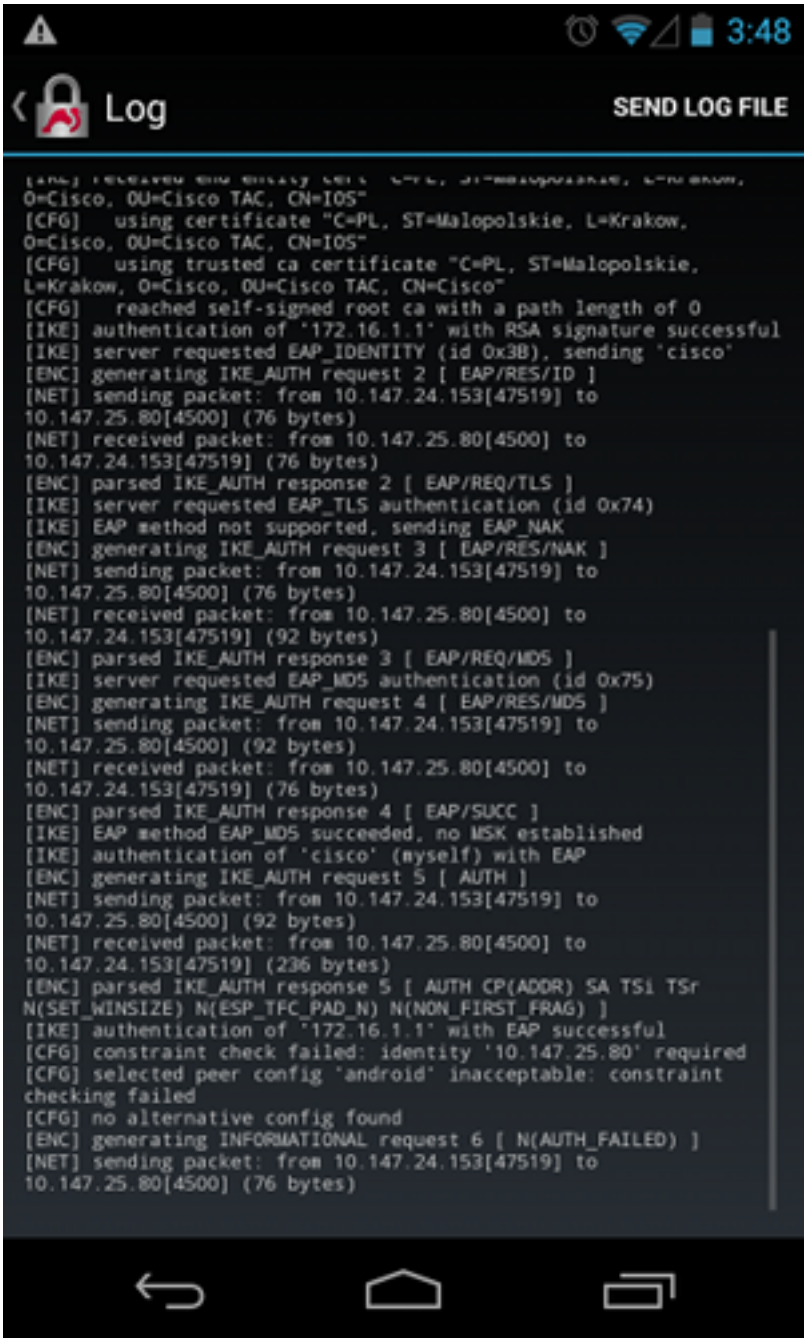
此示例解释了StrongSwan证书验证的限制。

假设Cisco IOS软件VPN网关IP地址从172.16.1.1静态转换为10.147.25.80。使用EAP身份验证。



另外，假设Cisco IOS软件证书具有172.16.1.1和10.147.25.80的使用者备用名称。

成功进行EAP身份验证后，Android将执行验证，并尝试在Subject Alternative Name扩展中查找Android配置(10.147.25.80)中使用的对等体的IP地址。验证失败：

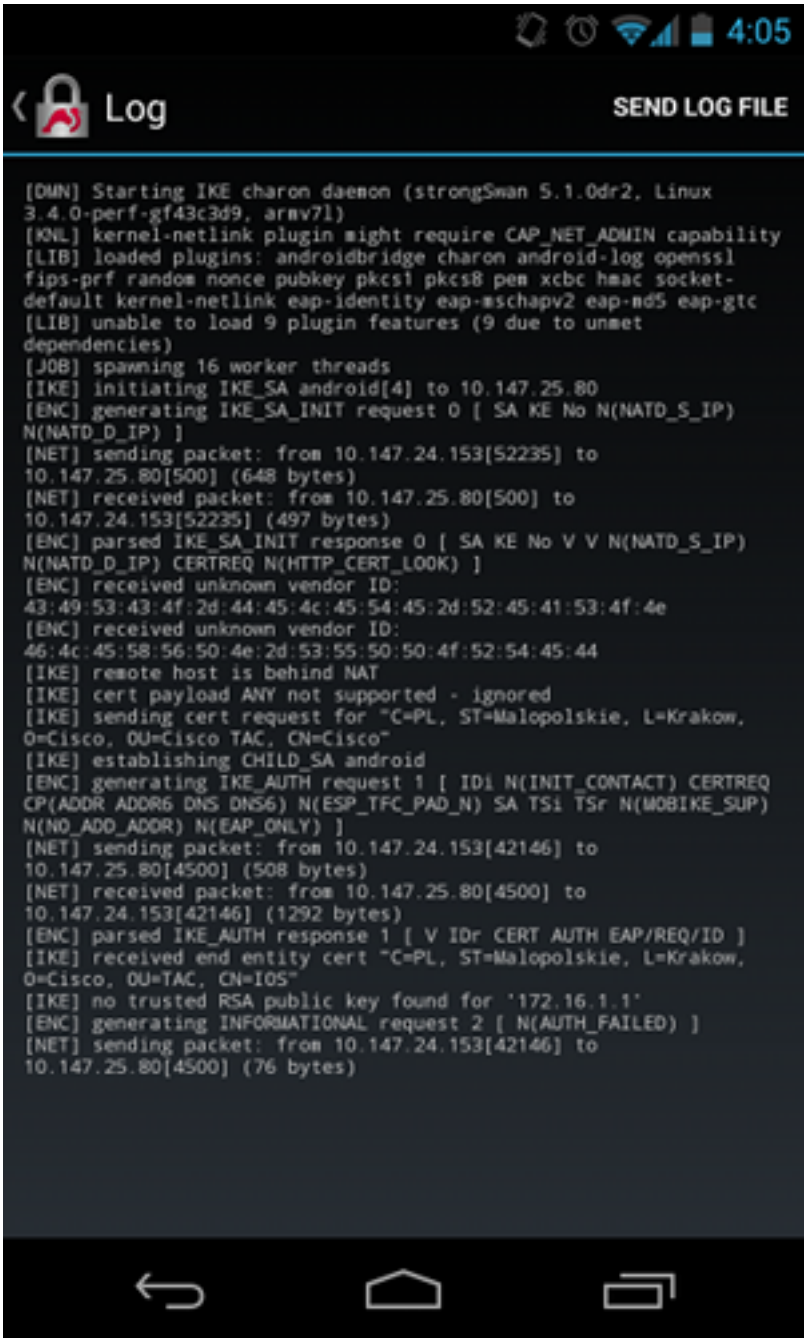


日志显示：

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

发生故障是因为Android只能读取第一个主题备用名称扩展(172.16.1.1)。

现在，假设Cisco IOS软件证书在主题备用名称中具有两个地址，但顺序相反：10.147.25.80和172.16.1.1。Android在收到第三个数据包中的IKEID(IKEID是VPN网关(172.16.1.1)的IP地址)时执行验证：



现在，日志显示：

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

因此，当Android收到IKEID时，它需要在主题备用名称中查找IKEID，并且只能使用第一个IP地址。

> **注意**：在EAP身份验证中，Cisco IOS软件发送的IKEID是默认的IP地址。在RSA身份验证中，IKEID是默认的证书DN。使用ikev2配置文件下的**identity**命令手动更改这些值。

验证

配置示例中提供了验证和测试过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

strongSwan CA多CERT_REQ

当strongSwan上的证书设置为自动选择（默认）时，Android会发送CERT_REQ，用于第三个数据包中的本地存储中的所有受信任证书。Cisco IOS软件可能会丢弃该请求，因为它将大量证书请求识别为拒绝服务攻击：

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

DVTI上的隧道源

虽然在虚拟隧道接口(VTI)上设置隧道源非常常见，但此处不必设置。假设**隧道**源命令在动态VTI(DVTI)下：

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

身份验证后，如果Cisco IOS软件尝试创建从虚拟模板克隆的虚拟访问接口，它会返回错误：

```
*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
```

故障发生两秒后，Cisco IOS软件收到来自Android的重新传输的IKE_AUTH。该数据包被丢弃。

Cisco IOS软件错误和增强请求

- Cisco Bug ID CSCui46418，“IOS Ikev2 ip address sent as identity for RSA authentication”。此Bug不是问题，只要strongSwan在证书中查找IKEID以执行验证时能看到正确的主题备用名称（IP地址）。
- Cisco Bug ID CSCui44976，“IOS PKI错误地显示了X509v3扩展主题备用名称。”仅当主题备用名称中有多个IP地址时，才会发生此错误。仅显示最后一个IP地址，但这不会影响证书的使用。整个证书已发送并正确处理。
- Cisco Bug ID CSCui44783，“IOS ENH PKI cability to generate CSR with subject-alt-name extension”。
- Cisco Bug ID CSCui44335，“ASA ENH Certificate x509 extensions displayed”。

相关信息

- Cisco IOS 15.3 VPN配置指南
- Cisco IOS 15.3命令参考
- 思科IOS Flex VPN配置指南
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。