IKEv2 von Android strongWechsel zu Cisco IOS mit EAP- und RSA-Authentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die mobile Version von strongSwan so konfiguriert wird, dass der Zugriff auf ein Cisco IOS® Software-VPN-Gateway über das Internet Key Exchange Version 2 (IKEv2)-Protokoll möglich ist.

Es werden drei Beispiele vorgestellt:

- Android-Telefon mit strongSwan, das über Extensible Authentication Protocol - Message Digest 5 (EAP-MD5)-Authentifizierung mit dem VPN-Gateway der Cisco IOS-Software verbunden ist.

- Android-Telefon mit strongSwan, das mit dem VPN-Gateway der Cisco IOS-Software über eine Zertifikatsauthentifizierung (RSA) verbunden ist.
- Android-Telefon mit strongSwan, das mit dem VPN-Gateway der Cisco IOS-Software hinter Network Address Translation (NAT) verbunden ist. Im VPN-Gateway-Zertifikat müssen zwei x509-Erweiterungen mit dem Betreffalternativen-Namen vorhanden sein.

Cisco IOS-Software und strongSwan-Beschränkungen sind ebenfalls enthalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der OpenSSL-Konfiguration
- Grundkenntnisse der Konfiguration der Cisco IOS Software Command Line Interface (CLI)
- Grundkenntnisse von IKEv2

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

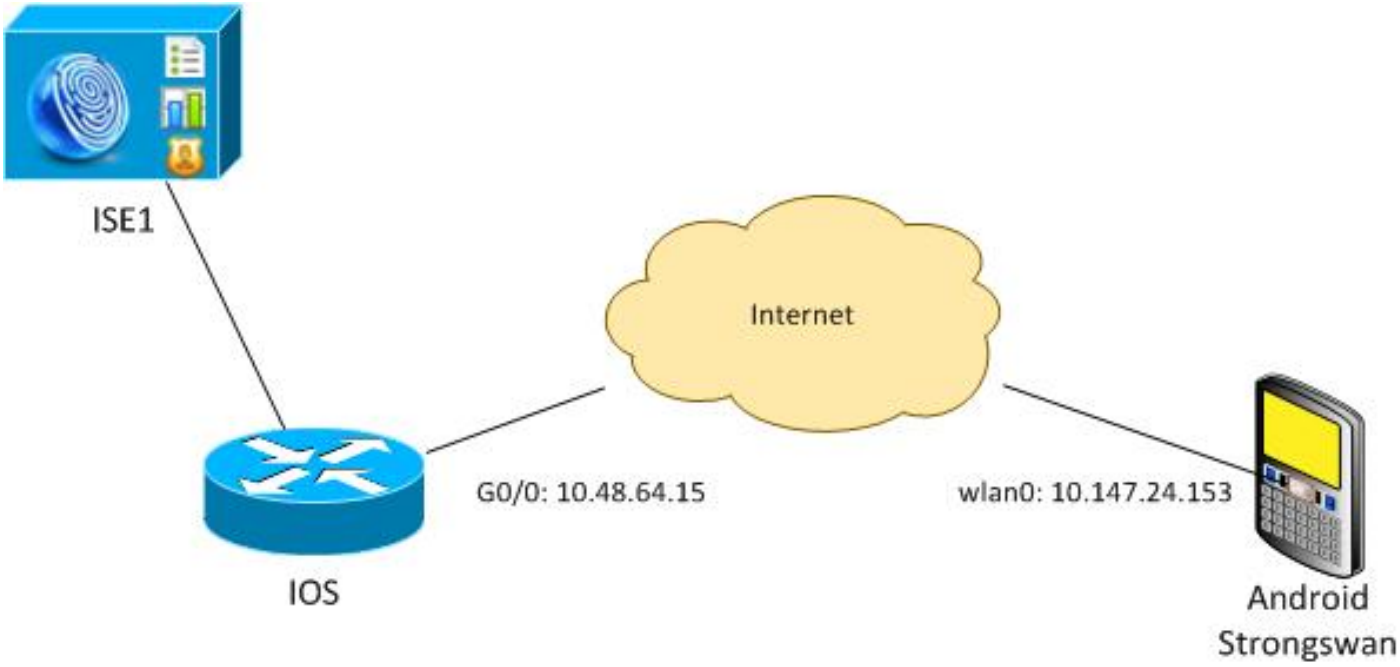
- Android 4.0 oder höher mit strongSwan
- Cisco IOS Software Release 15.3T oder höher
- Cisco Identity Services Engine (ISE)-Software, Version 1.1.4 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

> **Hinweise**:
>
> Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.
>
> Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

Netzwerkdiagramm



Android strongSwan stellt einen IKEv2-Tunnel mit einem Cisco IOS-Software-Gateway her, um sicher auf interne Netzwerke zuzugreifen.

Zertifikatsregistrierung

Zertifikate sind eine Voraussetzung für die EAP- und die RSA-basierte Authentifizierung.

Im EAP-Authentifizierungsszenario ist ein Zertifikat nur für das VPN-Gateway erforderlich. Der Client stellt nur dann eine Verbindung zur Cisco IOS-Software her, wenn die Software ein Zertifikat vorlegt, das von einer Zertifizierungsstelle (Certificate Authority, CA) signiert wurde, die bei Android als vertrauenswürdig gilt. Anschließend wird eine EAP-Sitzung gestartet, in der der Client sich bei der Cisco IOS-Software authentifizieren kann.

Für die RSA-basierte Authentifizierung müssen beide Endpunkte über ein korrektes Zertifikat verfügen.

Wenn eine IP-Adresse als Peer-ID verwendet wird, gibt es zusätzliche Anforderungen für das Zertifikat. Android strongSwan überprüft, ob die IP-Adresse des VPN-Gateways in der Erweiterung x509 unter "Subject Alternative Name" (Alternativer Name des Betreibers) enthalten ist. Wenn nicht, verwirft Android die Verbindung. Dies ist eine gute Praxis und eine Empfehlung von RFC 6125.

OpenSSL wird als CA verwendet, da die Cisco IOS-Software folgende Einschränkungen aufweist: Es kann keine Zertifikate mit einer Erweiterung generieren, die eine IP-Adresse enthält. Alle Zertifikate werden von OpenSSL generiert und in Android und die Cisco IOS-Software importiert.

In der Cisco IOS-Software kann der Befehl **subject-alt-name** verwendet werden, um eine Erweiterung mit einer IP-Adresse zu erstellen. Der Befehl funktioniert jedoch nur mit selbstsignierten Zertifikaten. Die Cisco Bug-ID CSCui44783, "IOS ENH PKI ability to generate CSR with subject-alt-name extension", ist eine Erweiterungsanforderung, mit der die Cisco IOS-Software die Erweiterung für alle Arten von Anmeldungen generieren kann.

Dies ist ein Beispiel für Befehle, die eine CA generieren:

```
#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 ist eine Konfigurationsdatei. Die CA-Erweiterung sollte auf TRUE gesetzt werden:

```
[ 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
```

Die Befehle, die ein Zertifikat generieren, sind für Cisco IOS-Software und Android sehr ähnlich. In diesem Beispiel wird davon ausgegangen, dass bereits eine CA zum Signieren des Zertifikats verwendet wird:

```
#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 ist eine Konfigurationsdatei. Die Erweiterung Alternativer Betreffname ist eine Schlüsseleinstellung. In diesem Beispiel ist die CA-Erweiterung auf FALSE festgelegt:

```
[ 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
```

Sowohl für die Cisco IOS-Software als auch für Android sollte ein Zertifikat generiert werden.

Die IP-Adresse 10.48.64.15 gehört zum Cisco IOS Software-Gateway. Wenn Sie ein Zertifikat für die Cisco IOS-Software generieren, stellen Sie sicher, dass subjectAltName auf 10.48.64.15 festgelegt ist. Android überprüft das Zertifikat, das von der Cisco IOS-Software erhalten wurde, und versucht, die IP-Adresse im BetreffAltName zu finden.

Cisco IOS-Software

Die Cisco IOS-Software muss über ein korrektes Zertifikat für die RSA- und EAP-basierte Authentifizierung verfügen.

Die PFX-Datei (ein pkcs12-Container) für die Cisco IOS-Software kann importiert werden:

```
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.
```

Verwenden Sie den Befehl **show crypto pki certificate verbose**, um zu überprüfen, ob der Import erfolgreich war:

```
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

Für die EAP-basierte Authentifizierung muss Andorid nur das richtige CA-Zertifikat installiert

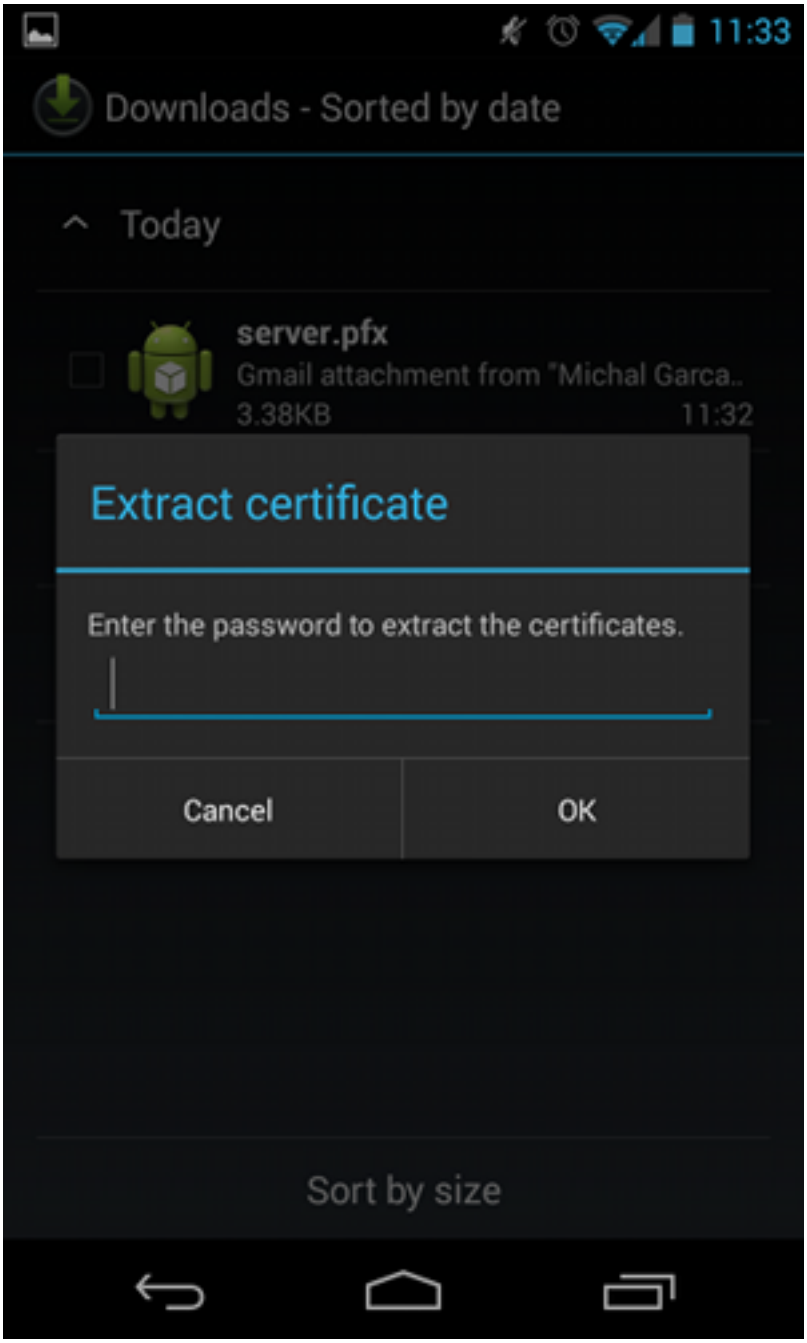
haben.

Für die RSA-basierte Authentifizierung muss Andorid sowohl das Zertifizierungsstellenzertifikat als auch das eigene Zertifikat installiert haben.

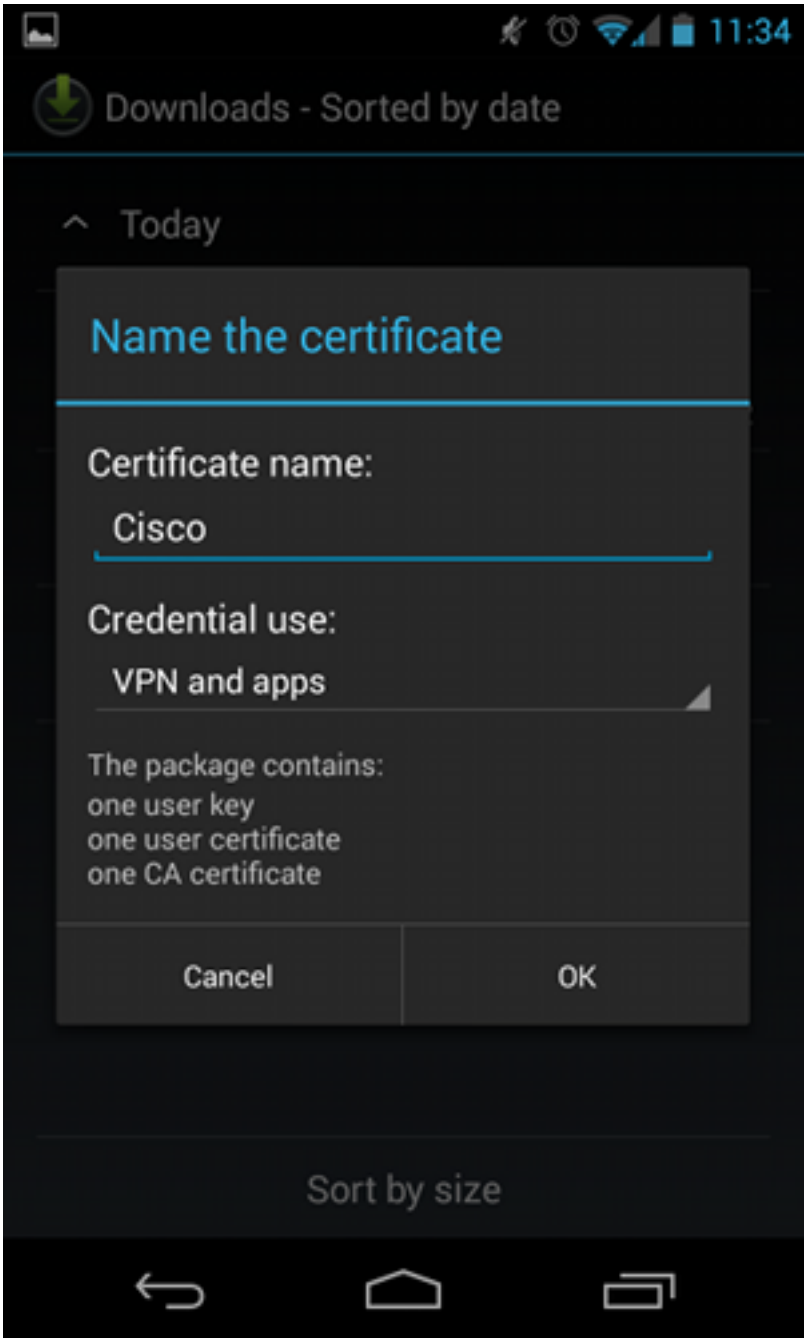
In diesem Verfahren wird beschrieben, wie Sie beide Zertifikate installieren:

1. Senden Sie die PFX-Datei per E-Mail, und öffnen Sie sie.

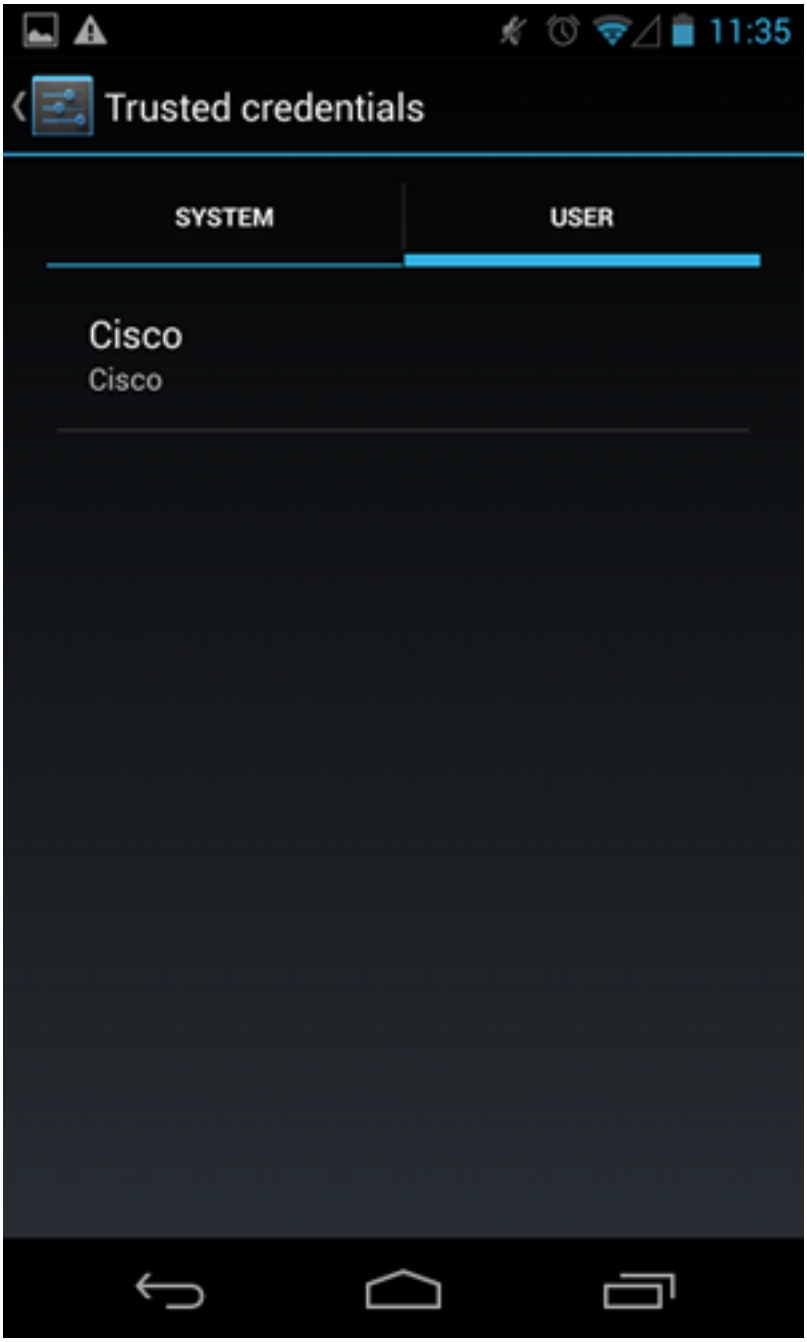
2. Geben Sie das Kennwort an, das bei der Erstellung der pfx-Datei verwendet wurde.



3. Geben Sie den Namen für das importierte Zertifikat an.



4. Navigieren Sie zu **Einstellungen > Sicherheit > Vertrauenswürdige Anmeldeinformationen**, um die Zertifikatsinstallation zu überprüfen. Das neue Zertifikat sollte im Benutzerspeicher angezeigt werden:



An diesem Punkt werden ein Benutzerzertifikat sowie ein Zertifizierungsstellenzertifikat installiert. Die pfx-Datei ist ein pkcs12-Container mit dem Benutzerzertifikat und dem Zertifizierungsstellen-Zertifikat.

Für Android gelten genaue Anforderungen, wenn Zertifikate importiert werden. Damit beispielsweise ein CA-Zertifikat erfolgreich importiert werden kann, muss die Basic Constraint CA der x509v3-Erweiterung auf TRUE gesetzt werden. Wenn Sie also eine CA generieren oder eine eigene CA verwenden, ist es wichtig, zu überprüfen, ob diese die richtige Durchwahl hat:

```
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-Authentifizierung

Cisco IOS Software-Konfiguration für EAP-Authentifizierung

IKEv2 ermöglicht die Verwendung eines EAP-Protokoll-Stacks für die Benutzerauthentifizierung. Das VPN-Gateway präsentiert sich mit dem Zertifikat. Sobald der Client diesem Zertifikat vertraut, antwortet der Client auf die EAP-Anforderungsidentität vom Gateway. Die Cisco IOS-Software verwendet diese Identität und sendet eine Radius-Request-Nachricht an den AAA-Server (Authentication, Authorization, Accounting). Zwischen der Komponente (Android) und dem Authentifizierungsserver (Access Control Server [ACS] oder ISE) wird eine EAP-MD5-Sitzung eingerichtet.

Nach erfolgreicher EAP-MD5-Authentifizierung, wie durch eine Radius-Accept-Nachricht angegeben, verwendet die Cisco IOS-Software den Konfigurationsmodus, um die IP-Adresse an den Client weiterzuleiten und die Datenverkehrsauswahl-Aushandlung fortzusetzen.

Beachten Sie, dass Android IKEID=cisco gesendet hat (wie konfiguriert). Diese IKEID, die in der Cisco IOS-Software empfangen wird, entspricht dem Profil "ikev2 profile 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
```

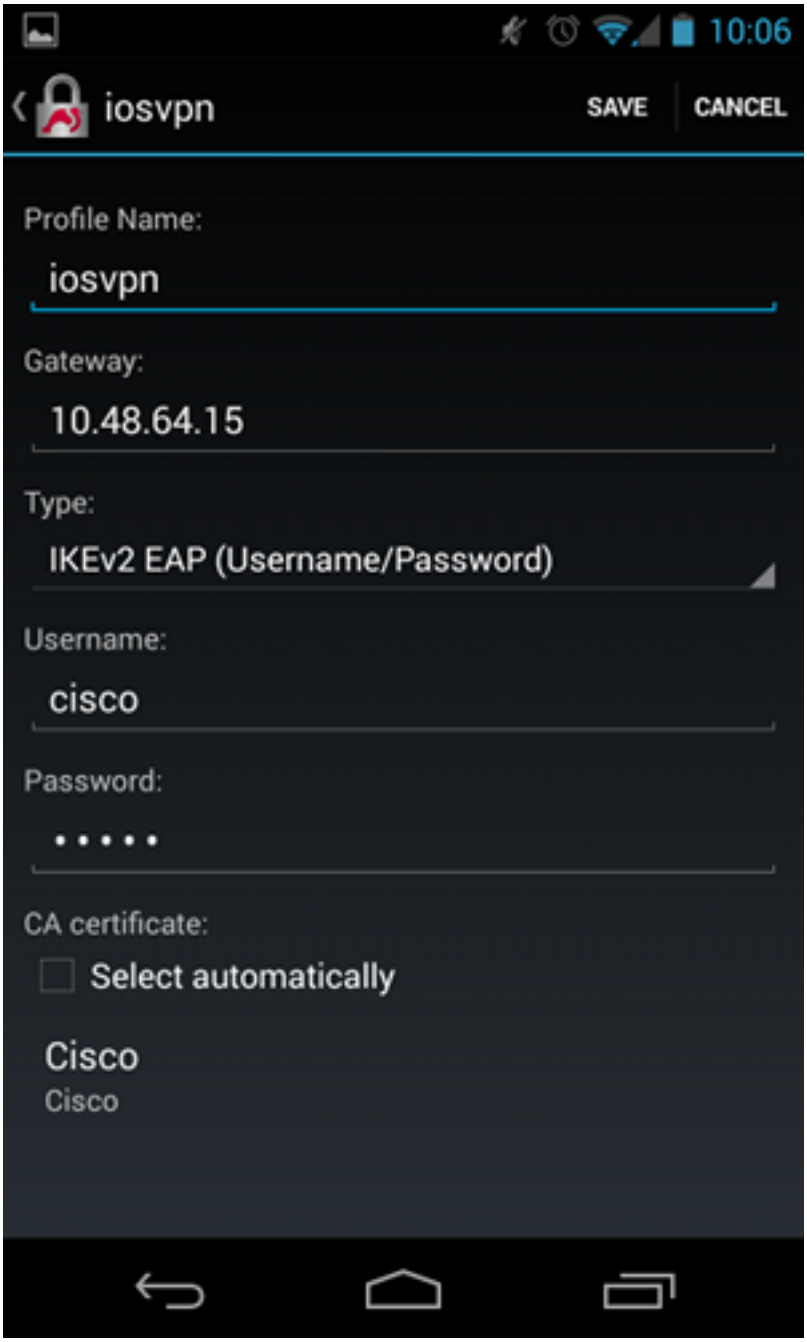
```
 mode tunnel
!
crypto ipsec profile PROF
 set transform-set 3DES-MD5
 set ikev2-profile PROF

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-Konfiguration für EAP-Authentifizierung

Für Android strongSwan muss EAP konfiguriert sein:

1. Deaktivieren der automatischen Zertifikatsauswahl Andernfalls werden im dritten Paket mindestens 100 CERT_REQs gesendet.

2. Wählen Sie ein bestimmtes Zertifikat (CA) aus, das im vorherigen Schritt importiert wurde. Benutzername und Kennwort müssen mit dem auf dem AAA-Server übereinstimmen.



EAP-Authentifizierungstest

In der Cisco IOS-Software sind dies die wichtigsten Debug-Prozesse für die EAP-Authentifizierung. Die meisten Ausgaben wurden aus Gründen der Übersichtlichkeit weggelassen:

```
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
```

Die Android-Protokolle zeigen Folgendes an:

```
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)
```

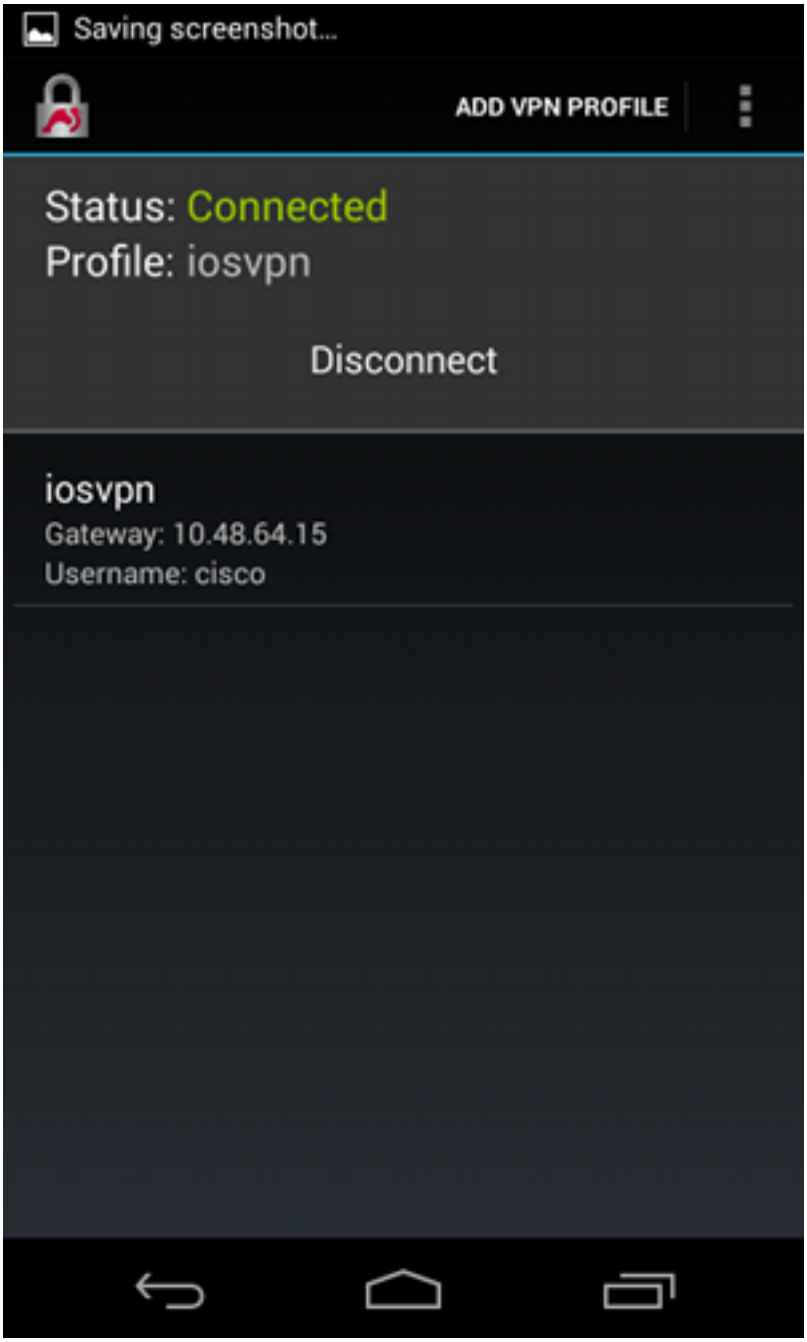
```
09[NET] received packet: from 10.48.64.15[4500] to 10.147.24.153[35564]
(76 bytes)
09[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/TLS ]
09[IKE] server requested EAP_TLS authentication (id 0x59)
09[IKE] EAP method not supported, sending EAP_NAK
09[ENC] generating IKE_AUTH request 3 [ EAP/RES/NAK ]
09[NET]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

Dieses Beispiel zeigt, wie der Status der Cisco IOS-Software überprüft wird:

```
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
```

Diese Zahlen zeigen, wie der Status auf Android überprüft wird:


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

RSA-Authentifizierung

Cisco IOS-Softwarekonfiguration für die RSA-Authentifizierung

Bei der Rivest-Shamir-Adleman (RSA)-Authentifizierung sendet Android das Zertifikat zur Authentifizierung an die Cisco IOS-Software. Aus diesem Grund wird die Zertifikatszuordnung benötigt, die den Datenverkehr an ein bestimmtes IKEv2-Profil bindet. Benutzer-EAP-Authentifizierung ist nicht erforderlich.

Dies ist ein Beispiel dafür, wie die RSA-Authentifizierung für einen Remote-Peer festgelegt wird:

```
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-Konfiguration für RSA-Authentifizierung

Benutzeranmeldeinformationen wurden durch das Benutzerzertifikat ersetzt:

RSA-Authentifizierungstest

In der Cisco IOS-Software sind dies die wichtigsten Debugger für die RSA-Authentifizierung. Die meisten Ausgaben wurden aus Gründen der Übersichtlichkeit weggelassen:

```
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
```

Die Android-Protokolle zeigen Folgendes an:

```
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 der Cisco IOS-Software wird RSA sowohl für die Signierung als auch für die Verifizierung verwendet. Im vorherigen Szenario wurde EAP zur Überprüfung verwendet:

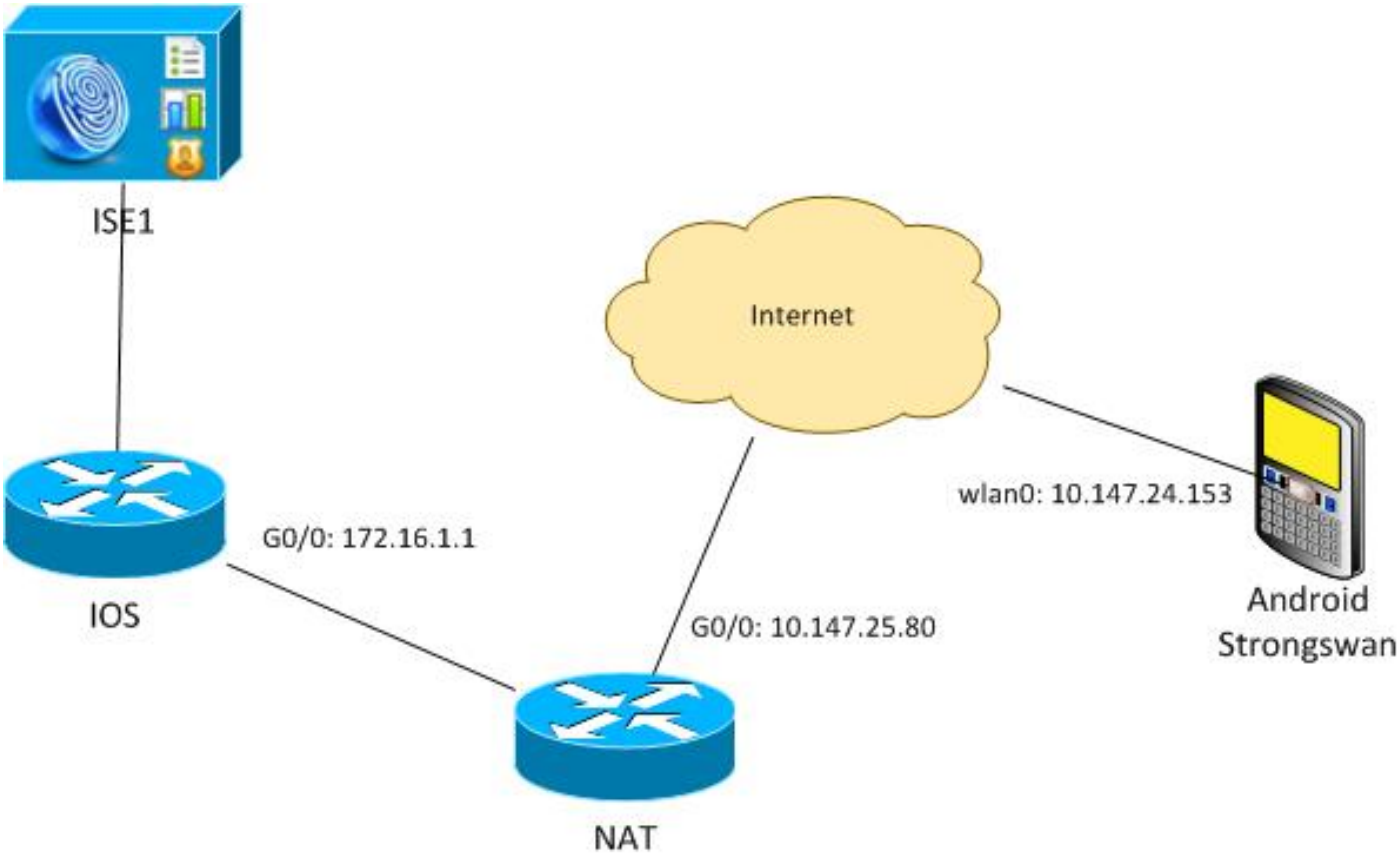
```
BSAN-2900-1#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

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
```

Die Statusüberprüfung für Android ähnelt der im vorherigen Szenario.

VPN-Gateway hinter NAT - strongSwan- und Cisco IOS-Softwarebeschränkungen

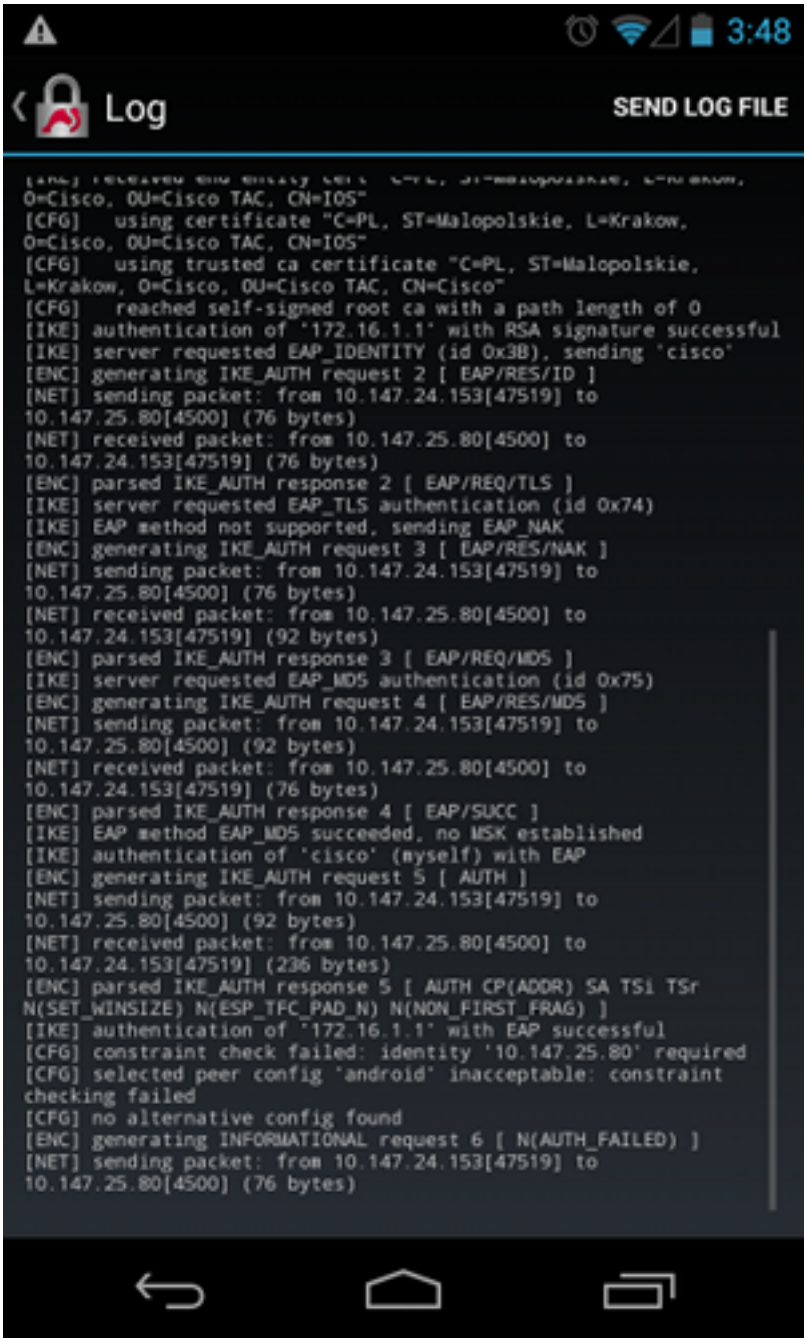
In diesem Beispiel wird eine Beschränkung der Prüfungen für das strongSwan-Zertifikat erklärt.

Nehmen Sie an, dass die IP-Adresse des VPN-Gateways der Cisco IOS-Software statisch von 172.16.1.1 in 10.147.25.80 übersetzt wird. EAP-Authentifizierung wird verwendet.



Angenommen, das Cisco IOS-Softwarezertifikat verfügt über einen Subject Alternative Name für 172.16.1.1 und 10.147.25.80.

Nach erfolgreicher EAP-Authentifizierung überprüft Android die IP-Adresse des Peers, der in der Android-Konfiguration (10.147.25.80) verwendet wurde, und versucht, die IP-Adresse des Peers in der Erweiterung Subject Alternative Name (Betreff-Alternative) zu finden. Die Überprüfung schlägt fehl:

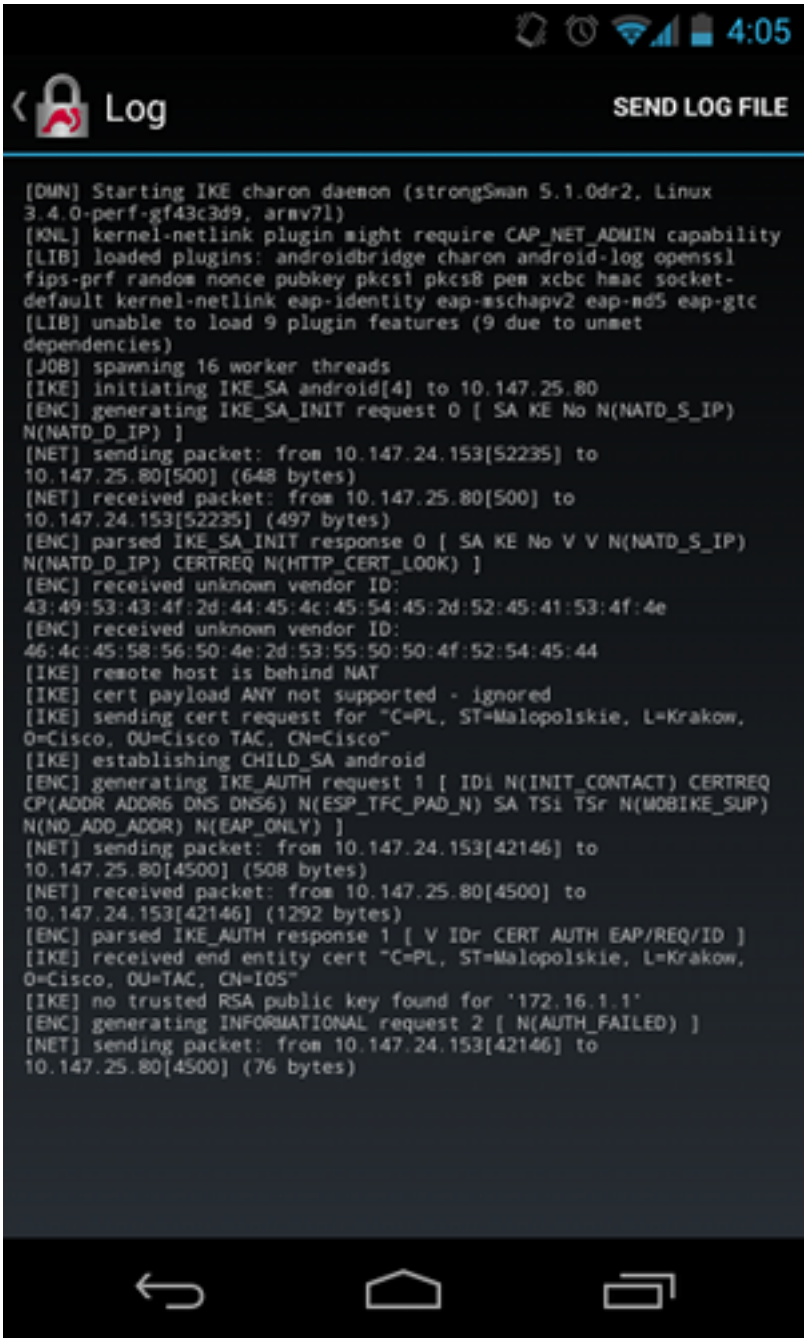


Die Protokolle zeigen Folgendes an:

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

Der Fehler ist aufgetreten, weil Android nur die erste Erweiterung "Subject Alternative Name" (Alternativer Betreff-Name) lesen kann (172.16.1.1).

Gehen Sie jetzt davon aus, dass das Cisco IOS-Softwarezertifikat beide Adressen im Betreffalternativen-Namen, aber in umgekehrter Reihenfolge hat: 10.147.25.80 und 172.16.1.1 Android führt eine Validierung durch, wenn es im dritten Paket die IKEID (die IP-Adresse des VPN-Gateways (172.16.1.1) empfängt:



Jetzt wird das Protokoll angezeigt:

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

Wenn Android die IKEID empfängt, muss es daher die IKEID im Betreff-Alternativnamen suchen und kann nur die erste IP-Adresse verwenden.

> **Hinweis**: Bei der EAP-Authentifizierung ist die von der Cisco IOS-Software gesendete IKEID standardmäßig die IP-Adresse. Bei der RSA-Authentifizierung ist IKEID standardmäßig die DN des Zertifikats. Um diese Werte manuell zu ändern, verwenden Sie den Befehl **identity** unter dem Profil ikev2.

Überprüfen

In den Konfigurationsbeispielen finden Sie Überprüfungs- und Testverfahren.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

strongSwan CA Multiple CERT_REQ

Wenn die Zertifikatseinstellung auf strongSwan die automatische Auswahl (die Standardeinstellung) lautet, sendet Android CERT_REQ für alle vertrauenswürdigen Zertifikate im lokalen Speicher im dritten Paket. Die Cisco IOS-Software kann die Anforderung verwerfen, da sie eine große Anzahl von Zertifikatsanforderungen als Denial-of-Service-Angriff erkennt:

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

Tunnelquelle auf DVTI

Es ist zwar üblich, die Tunnelquelle auf einer virtuellen Tunnelschnittstelle (VTI) festzulegen, aber hier ist dies nicht erforderlich. Angenommen, der Befehl **Tunnel-Quelle** befindet sich unter einem dynamischen VTI (DVTI):

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

Wenn die Cisco IOS-Software nach der Authentifizierung versucht, eine virtuelle Zugriffsschnittstelle zu erstellen, die aus einer virtuellen Vorlage geklont wird, wird ein Fehler zurückgegeben:

```
*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
```

Zwei Sekunden nach dem Ausfall erhält die Cisco IOS-Software eine erneute Übertragung von IKE_AUTH von Android. Dieses Paket wird verworfen.

Cisco IOS Software Bugs and Enhancement Requests

- Cisco Bug-ID CSCui46418, "IOS Ikev2 IP-Adresse, die als Identität für die RSA-Authentifizierung gesendet wird"
  Dieser Fehler ist kein Problem, solange strongSwan einen korrekten Subject Alternative Name (die IP-Adresse) sehen kann, wenn er im Zertifikat nach der IKEID sucht, um eine Überprüfung durchzuführen.

- Cisco Bug-ID CSCui44976: "IOS PKI hat den alternativen Namen der X509v3-Erweiterung falsch angezeigt."
  Dieser Fehler tritt nur auf, wenn der Betreffalternative-Name mehrere IP-Adressen enthält. Es wird nur die letzte IP-Adresse angezeigt, was sich jedoch nicht auf die Zertifikatsverwendung auswirkt. Das gesamte Zertifikat wird korrekt gesendet und verarbeitet.
- Cisco Bug-ID CSCui44783, "IOS ENH PKI ability to generate CSR with subject-alt-name extension".
- Cisco Bug ID CSCui44335, "ASA ENH Certificate x509 extensions displayed"

Zugehörige Informationen

- Cisco IOS 15.3 VPN-Konfigurationsleitfaden
- Cisco IOS 15.3 Befehlsreferenz
- Konfigurationsleitfaden für Cisco IOS Flex VPN
- Technischer Support und Dokumentation - Cisco Systems