IKEv2 от Android strongSwan до Cisco IOS с EAP и Аутентификацией RSA

Содержание

Введение

Этот документ описывает, как настроить мобильную версию strongSwan для доступа к Шлюзу VPN программного обеспечения Cisco IOS по протоколу второй версии протокола Internet Key Exchange (IKEv2).

Представлены три примера:

- Телефон на базе Android с strongSwan, который соединяется со Шлюзом VPN программного обеспечения Cisco IOS с Расширяемым протоколом аутентификации - Профиль сообщения 5 (EAP-MD5) аутентификация.

- Телефон на базе Android с strongSwan, который соединяется со Шлюзом VPN программного обеспечения Cisco IOS с проверкой подлинности сертификата (RSA).
- Телефон на базе Android с strongSwan, который соединяется со Шлюзом VPN программного обеспечения Cisco IOS позади Технологии NAT. Существует требование для имения двух x509 Альтернативных имен субъекта расширений в сертификате Шлюза VPN.

Программное обеспечение Cisco IOS и strongSwan ограничения также включены.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации OpenSSL
- Базовые знания о конфигурации интерфейса командной строки (CLI) программного обеспечения Cisco IOS
- Базовые знания о IKEv2

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Android 4.0 или позже с strongSwan
- Cisco IOS Software Release 15.3T или позже
- Платформа Cisco Identity Services Engine (ISE) программное обеспечение, Версия 1.1.4 и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

> **Примечания:**
>
> Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**
>
> Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Схема сети

Android strongSwan устанавливает туннель IKEv2 со шлюзом программного обеспечения Cisco IOS для доступа к внутренним сетям надежно.

Хранилище сертификатов

Сертификаты являются предпосылкой и для основанной на EAP и для основанной на RSA аутентификации.

В сценарии Аутентификации eap сертификат необходим только на Шлюзе VPN. Клиент соединяется с программным обеспечением Cisco IOS только, когда программное обеспечение представляет сертификат, подписанный Центром сертификации (CA), которому доверяют на Android. Сеанс EAP тогда начинает для клиента аутентифицироваться на программном обеспечении Cisco IOS.

Для основанной на RSA аутентификации обе оконечных точки должны иметь корректный сертификат.

Когда IP-адрес используется в качестве peer-ID, существуют дополнительные требования для сертификата. Android strongSwan проверяет, включен ли IP-адрес Шлюза VPN в x509 дополнительное Альтернативное имя субъекта. В противном случае Android отбрасывает соединение; это - полезный прием, а также рекомендация RFC 6125.

OpenSSL используется в качестве CA, потому что программное обеспечение Cisco IOS имеет ограничение: это не может генерировать сертификаты с расширением, которое включает IP-адрес. Все сертификаты генерируются OpenSSL и импортируются в Android и программное обеспечение Cisco IOS.

В программном обеспечении Cisco IOS команда **подчиненного названия alt** может использоваться для создания расширения, которое включает IP-адрес, но команда работает только с подписанными сертификатами. Идентификатор ошибки Cisco CSCui44783, "способность к PKI ENH IOS генерировать CSR с расширением подчиненного названия alt", является запросом на расширение, чтобы позволить программному обеспечению Cisco IOS генерировать расширение для всех типов регистраций.

Это - пример команд, которые генерируют CA:

```
#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 является файлом конфигурации. Расширение CA должно быть установлено в 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
```

Команды, которые генерируют сертификат, подобны для программного обеспечения Cisco IOS и Android. Данный пример предполагает, что уже существует CA, используемый для подписания сертификата:

```
#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 является файлом конфигурации. Альтернативное расширение Имени субъекта является настройкой ключа. В данном примере установлено в False расширение CA:

```
[ 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
```

Сертификат должен генерироваться и для программного обеспечения Cisco IOS и для Android.

IP-адрес 10.48.64.15 принадлежит шлюзу программного обеспечения Cisco IOS. При генерации сертификата для программного обеспечения Cisco IOS удостоверьтесь, что subjectAltName установлен в 10.48.64.15. Android проверяет сертификат, полученный от программного обеспечения Cisco IOS, и пытается найти его IP-адрес в subjectAltName.

ПО Cisco IOS)

Программному обеспечению Cisco IOS нужно было установить корректный сертификат и для основанной на RSA и для основанной на EAP аутентификации.

pfx файл (который является контейнером pkcs12) для программного обеспечения Cisco IOS может быть импортирован:

```
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.
```

Используйте show crypto pki certificates многословная команда, чтобы проверить, что успешно выполнился импорт:

```
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

Для основанной на EAP аутентификации Andorid должен иметь просто корректный установленный сертификат CA.

Для основанной на RSA аутентификации Andorid должен иметь и сертификат CA и его собственный установленный сертификат.

Эта процедура описывает, как установить оба сертификата:

1. Передайте pfx файл по электронной почте и откройте его.

2. Предоставьте пароль, который использовался, когда генерировался pfx файл.

3. Предоставьте название для импортированного сертификата.

4. Перейдите к**> Security Параметров настройки> Учетные данные, которым Доверяют**, для проверки установки сертификатов. Новый сертификат должен появиться в пользовательском хранилище:

На этом этапе сертификат пользователя, а также сертификат CA установлен. pfx файл является контейнером pkcs12 и с сертификатом пользователя и с сертификатом CA.

Когда сертификаты импортированы, Android имеет точные требования. Например, для сертификата CA, который будет импортирован успешно, Android требует, чтобы x509v3 дополнительное Основное ограничение CA было установлено в True. Таким образом, когда вы генерируете CA или используете ваш собственный CA, важно проверить, что это имеет правильный номер:

```
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>
```

Аутентификация EAP

Конфигурация программного обеспечения Cisco IOS для аутентификации eap

IKEv2 позволяет использование стека протоколов EAP для выполнения проверки подлинности пользователя. Шлюз VPN предоставляет себе сертификат. Как только клиент полагает, что сертификат, клиент отвечает на идентичность запроса EAP от шлюза. Программное обеспечение Cisco IOS использует ту идентичность и передает сообщение Запроса RADIUS к аутентификации, авторизации и учету (AAA), и сеанс EAP-MD5 установлен между соискателем (Android) и сервером проверки подлинности (Access Control Server [ACS] или ISE).

После успешной аутентификации EAP-MD5, как обозначено Радиусом - Принимают сообщение, программное обеспечение Cisco IOS использует режим конфигурации, чтобы выдвинуть IP-адрес клиенту и продолжить согласование селектора трафика.

Заметьте, что Android передал IKEID=cisco (согласно конфигурации). Этот IKEID, полученный на соответствиях программного обеспечения Cisco IOS 'ikev2, представляет 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
```

Конфигурация Android для аутентификации eap

Android strongSwan нужно было настроить EAP:

1. Отключите автоматический выбор сертификата; иначе, 100 или больше CERT_REQ передаются в третьем пакете.

2. Выберите определенный сертификат (CA), который был импортирован в предыдущем шаге; имя пользователя и пароль должно совпасть с на AAA-сервере.

Тест аутентификации eap

В программном обеспечении Cisco IOS это самые важные отладки для Аутентификации eap. Выходные данные Most были опущены для ясности:

```
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
```

Журналы Android указывают:

```
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
```

Данный пример показывает, как проверить статус на программном обеспечении Cisco IOS:

```
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
```

Эти данные показывают, как проверить статус на Android:

Аутентификация RSA

Конфигурация программного обеспечения Cisco IOS для аутентификации RSA

На аутентификации Ривест-Шамир-Адлемена (RSA) Android передает сертификат для аутентификации на программном обеспечении Cisco IOS. Именно поэтому карта сертификата, которая связывает тот трафик с определенным профилем IKEv2, необходима. Пользовательская Аутентификация eap не требуется.

Это - пример того, как установлена аутентификация RSA для удаленного узла:

```
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
```

Конфигурация Android для аутентификации RSA

Учетные данные пользователя были заменены сертификатом пользователя:

Тест аутентификации RSA

В программном обеспечении Cisco IOS это самые важные отладки для аутентификации RSA. Выходные данные Most были опущены для ясности:

```
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
```

Журналы Android указывают:

```
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
```

В программном обеспечении Cisco IOS RSA используется и для подписания и для проверки; в предыдущем сценарии EAP использовался для проверки:

```
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
```

Проверка статуса на Android подобна этому в предыдущем сценарии.

Шлюз VPN Позади NAT - strongSwan и Ограничения программного обеспечения Cisco IOS

Данный пример объясняет ограничение strongSwan Проверок сертификата.

Предположите, что IP-адрес Шлюза VPN программного обеспечения Cisco IOS статически преобразован от 172.16.1. От 1 до 10. 147.25.80. Аутентификация eap используется.

Предположите также, что сертификат программного обеспечения Cisco IOS имеет Альтернативное имя субъекта и для 172.16.1.1 и для 10.147.25.80.

После успешной Аутентификации eap Android выполняет проверку и пытается найти IP-адрес узла, который использовался в конфигурации Android (10.147.25.80) в расширении Альтернативного имени субъекта. Сбои проверки:

Журналы указывают:

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

Сбой произошел, потому что Android может только для чтения первое расширение Альтернативного имени субъекта (172.16.1.1).

Теперь, предположите, что сертификат программного обеспечения Cisco IOS имеет оба адреса в Альтернативном имени субъекта, но в обратном порядке: 10.147.25.80 и 172.16.1.1. Android выполняет проверку, когда это получает IKEID, который является IP-адресом Шлюза VPN (172.16.1.1) в третьем пакете:

Теперь журнал показывает:

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

Таким образом, когда Android получает IKEID, он должен найти IKEID в Альтернативном имени субъекта и может использовать только первый IP-адрес.

> **Примечание:** В Аутентификации eap IKEID, передаваемым программным обеспечением Cisco IOS, является IP-адрес по умолчанию. В аутентификации RSA IKEID является DN сертификата по умолчанию. Используйте **команду identity** под профилем ikev2 для изменения этих значений вручную.

Проверка

Проверка и процедуры проверки доступны в примерах конфигурации.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

strongSwan CA Множественный CERT_REQ

Когда значением сертификата на strongSwan является Автоматический выбор (по умолчанию), Android передает CERT_REQ за всеми надежными сертификатами в локальном хранилище в третьем пакете. Программное обеспечение Cisco IOS могло бы отбросить запрос, потому что это распознает большое число запросов сертификата как Атака типа отказ в обслуживании:

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

Точка начала туннеля на DVTI

Несмотря на то, что довольно распространено установить точку начала туннеля в виртуальном туннельном интерфейсе (VTI), необязательно здесь. Предположите**, что команда tunnel source** находится под динамическим VTI (DVTI):

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

После аутентификации, если программное обеспечение Cisco IOS пытается создать интерфейс виртуального доступа, который клонирован от виртуального шаблона, он возвращает ошибку:

```
*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
```

Спустя две секунды после сбоя, программное обеспечение Cisco IOS получает ретранслируемый IKE_AUTH от Android. Тот пакет отброшен.

Ошибки программного обеспечения Cisco IOS и запросы на расширение

- Идентификатор ошибки Cisco CSCui46418, "IP-адрес IOS Ikev2, передаваемый как идентичность за аутентификацией RSA".
  Этот дефект не является проблемой, целый strongSwan видит корректное Альтернативное имя субъекта (IP-адрес), когда это ищет IKEID в сертификате для выполнения проверки.
- CSCui44976 Идентификатора ошибки Cisco, "PKI IOS неправильно отобразил

дополнительное Альтернативное имя субъекта X509v3".
Этот дефект происходит только, когда существуют несколько IP - адресовы в Альтернативном имени субъекта. Только последний IP-адрес отображен, но это не влияет на certificate usage. Целый сертификат передан и обработан правильно.

- Идентификатор ошибки Cisco CSCui44783, "способность к PKI ENH IOS генерировать CSR с расширением подчиненного названия alt".
- CSCui44335 Идентификатора ошибки Cisco, "отобразился Сертификат ENH ASA x509 расширения".

Дополнительные сведения

- Cisco IOS 15.3 руководств конфигурации VPN
- Cisco IOS 15.3 Справочников по командам
- Руководство конфигурации VPN Flex Cisco IOS
- Cisco Systems – техническая поддержка и документация