strongSwan - Issue #3431

Authentication fail and no matching peer config found !!

29.04.2020 08:47 - ray chao

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	No feedback

Description

i am trying to connect the client and the server my configuration is :

```
# ipsec.secrets - strongSwan Client IPsec secrets file:
: RSA /mnt/log/key_file/DUT2.p12

#ipsec.conf -  strongSwan VPN client IPsec Configuration file:
config setup
conn test2
 aggressive=no
 leftsendcert=always
 rightsendcert=always
 leftcert=/mnt/log/cer_file/DUT2.p12
 authby=rsasig
 left=10.10.10.13
 right=10.10.10.10
 leftsubnet=192.168.128.254/24
 rightsubnet=192.168.127.254/24
 leftid=10.10.10.13
 rightid=10.10.10.10
 type=tunnel
 esp=aes128-sha2_256-modp2048
 rekeymargin=9m
 rekeyfuzz=100%
 keyingtries=%forever
 keyexchange=ikev1
 ikelifetime=1h
 keylife=0m
 ike=aes128-sha2_256-modp2048
 auto=start
 dpddelay=30
 dpdtimeout=120
 dpdaction=hold
conn any_wan0
 left=10.10.10.13
 leftsourceip=10.10.10.13
 right=%any

#####################################


# ipsec.secrets - strongSwan Client IPsec secrets file:
: RSA /mnt/log/key_file/DUT1.p12

config setup
conn test
 aggressive=no
 leftsendcert=always
 rightsendcert=always
 leftcert=/mnt/log/cer_file/DUT1.p12
 authby=rsasig
 left=10.10.10.10
```

```
 right=10.10.10.13
 leftsubnet=192.168.127.254/24
 rightsubnet=192.168.128.254/24
 leftid=10.10.10.10
 rightid=10.10.10.13
 type=tunnel
 esp=aes128-sha2_256-modp2048
 rekeymargin=9m
 rekeyfuzz=100%
 keyingtries=%forever
 keyexchange=ikev1
 ikelifetime=1h
 keylife=180m
 ike=aes128-sha2_256-modp2048
 auto=add
 dpddelay=30
 dpdtimeout=120
 dpdaction=hold
conn any_wan0
 left=10.10.10.10
 leftsourceip=10.10.10.10
 right=%any
```

I got this result in both peers:

The Client Side:

```
2020-04-29T06:38:14+0000 00[DMN] Starting IKE charon daemon (strongSwan 5.8.1, Linux 4.14.76-15.0.
0, aarch64)
2020-04-29T06:38:14+0000 00[CFG] PKCS11 module '<name>' lacks library path
2020-04-29T06:38:14+0000 00[KNL] received netlink error: Address family not supported by protocol
(97)
2020-04-29T06:38:14+0000 00[KNL] unable to create IPv6 routing table rule
2020-04-29T06:38:14+0000 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
2020-04-29T06:38:14+0000 00[CFG]   loaded ca certificate "O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei@m
oxa.com" from '/etc/ipsec.d/cacerts/MOXARootCA.crt'
2020-04-29T06:38:14+0000 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
2020-04-29T06:38:14+0000 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
2020-04-29T06:38:14+0000 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
2020-04-29T06:38:14+0000 00[CFG] loading crls from '/etc/ipsec.d/crls'
2020-04-29T06:38:14+0000 00[CFG] loading secrets from '/etc/ipsec.secrets'
2020-04-29T06:38:14+0000 00[CFG]   loaded RSA private key from '/mnt/log/key_file/DUT2.p12'
2020-04-29T06:38:14+0000 00[LIB] loaded plugins: charon pkcs11 aes des rc2 sha2 sha1 md5 mgf1 rand
om nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem af-alg
fips-prf gmp curve25519 xcbc cmac hmac attr kernel-netlink resolve socket-default stroke vici updo
wn xauth-generic led counters
2020-04-29T06:38:14+0000 00[JOB] spawning 16 worker threads
2020-04-29T06:38:14+0000 05[CFG] received stroke: add connection 'test2'
2020-04-29T06:38:14+0000 05[CFG]   loaded certificate "CN=DUT2" from '/mnt/log/cer_file/DUT2.p12'
2020-04-29T06:38:14+0000 05[CFG]   id '10.10.10.13' not confirmed by certificate, defaulting to 'C
N=DUT2'
2020-04-29T06:38:14+0000 05[CFG] added configuration 'test2'
2020-04-29T06:38:14+0000 08[CFG] received stroke: initiate 'test2'
2020-04-29T06:38:14+0000 08[IKE] initiating Main Mode IKE_SA test2[1] to 10.10.10.10
2020-04-29T06:38:14+0000 08[ENC] generating ID_PROT request 0 [ SA V V V V V ]
2020-04-29T06:38:14+0000 08[NET] sending packet: from 10.10.10.13[500] to 10.10.10.10[500] (216 by
tes)
2020-04-29T06:38:14+0000 09[NET] received packet: from 10.10.10.10[500] to 10.10.10.13[500] (160 b
ytes)
2020-04-29T06:38:14+0000 09[ENC] parsed ID_PROT response 0 [ SA V V V V ]
2020-04-29T06:38:14+0000 09[IKE] received XAuth vendor ID
2020-04-29T06:38:14+0000 09[IKE] received DPD vendor ID
2020-04-29T06:38:14+0000 09[IKE] received FRAGMENTATION vendor ID
2020-04-29T06:38:14+0000 09[IKE] received NAT-T (RFC 3947) vendor ID
2020-04-29T06:38:14+0000 09[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA
2_256/MODP_2048
```

```
2020-04-29T06:38:14+0000 09[ENC] generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
2020-04-29T06:38:14+0000 09[NET] sending packet: from 10.10.10.13[500] to 10.10.10.10[500] (396 by
tes)
2020-04-29T06:38:14+0000 10[NET] received packet: from 10.10.10.10[500] to 10.10.10.13[500] (484 b
ytes)
2020-04-29T06:38:14+0000 10[ENC] parsed ID_PROT response 0 [ KE No CERTREQ NAT-D NAT-D ]
2020-04-29T06:38:14+0000 10[IKE] received cert request for 'O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei
@moxa.com'
2020-04-29T06:38:14+0000 10[IKE] sending cert request for "O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei@
moxa.com"
2020-04-29T06:38:14+0000 10[IKE] authentication of 'CN=DUT2' (myself) successful
2020-04-29T06:38:14+0000 10[IKE] sending end entity cert "CN=DUT2"
2020-04-29T06:38:14+0000 10[ENC] generating ID_PROT request 0 [ ID CERT SIG CERTREQ N(INITIAL_CONT
ACT) ]
2020-04-29T06:38:14+0000 10[NET] sending packet: from 10.10.10.13[500] to 10.10.10.10[500] (1180 b
ytes)
2020-04-29T06:38:14+0000 11[NET] received packet: from 10.10.10.10[500] to 10.10.10.13[500] (108 b
ytes)
2020-04-29T06:38:14+0000 11[ENC] parsed INFORMATIONAL_V1 request 123206683 [ HASH N(AUTH_FAILED) ]
2020-04-29T06:38:14+0000 11[IKE] received AUTHENTICATION_FAILED error notify
```

The server side:

```
2020-04-29T06:36:59+0000 00[DMN] Starting IKE charon daemon (strongSwan 5.8.1, Linux 4.14.76-15.0.
0, aarch64)
2020-04-29T06:36:59+0000 00[CFG] PKCS11 module '<name>' lacks library path
2020-04-29T06:36:59+0000 00[KNL] received netlink error: Address family not supported by protocol
(97)
2020-04-29T06:36:59+0000 00[KNL] unable to create IPv6 routing table rule
2020-04-29T06:36:59+0000 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
2020-04-29T06:36:59+0000 00[CFG]   loaded ca certificate "O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei@m
oxa.com" from '/etc/ipsec.d/cacerts/MOXARootCA.crt'
2020-04-29T06:36:59+0000 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
2020-04-29T06:36:59+0000 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
2020-04-29T06:36:59+0000 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
2020-04-29T06:36:59+0000 00[CFG] loading crls from '/etc/ipsec.d/crls'
2020-04-29T06:36:59+0000 00[CFG] loading secrets from '/etc/ipsec.secrets'
2020-04-29T06:36:59+0000 00[CFG]   loaded RSA private key from '/mnt/log/key_file/DUT1.p12'
2020-04-29T06:36:59+0000 00[LIB] loaded plugins: charon pkcs11 aes des rc2 sha2 sha1 md5 mgf1 rand
om nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem af-alg
fips-prf gmp curve25519 xcbc cmac hmac attr kernel-netlink resolve socket-default stroke vici updo
wn xauth-generic led counters
2020-04-29T06:36:59+0000 00[JOB] spawning 16 worker threads
2020-04-29T06:36:59+0000 05[CFG] received stroke: add connection 'test'
2020-04-29T06:36:59+0000 05[CFG]   loaded certificate "CN=DUT1" from '/mnt/log/cer_file/DUT1.p12'
2020-04-29T06:36:59+0000 05[CFG]   id '10.10.10.10' not confirmed by certificate, defaulting to 'C
N=DUT1'
2020-04-29T06:36:59+0000 05[CFG] added configuration 'test'
2020-04-29T06:37:00+0000 07[NET] received packet: from 10.10.10.13[500] to 10.10.10.10[500] (216 b
ytes)
2020-04-29T06:37:00+0000 07[ENC] parsed ID_PROT request 0 [ SA V V V V V ]
2020-04-29T06:37:00+0000 07[IKE] received XAuth vendor ID
2020-04-29T06:37:00+0000 07[IKE] received DPD vendor ID
2020-04-29T06:37:00+0000 07[IKE] received FRAGMENTATION vendor ID
2020-04-29T06:37:00+0000 07[IKE] received NAT-T (RFC 3947) vendor ID
2020-04-29T06:37:00+0000 07[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
2020-04-29T06:37:00+0000 07[IKE] 10.10.10.13 is initiating a Main Mode IKE_SA
2020-04-29T06:37:00+0000 07[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA
2_256/MODP_2048
2020-04-29T06:37:00+0000 07[ENC] generating ID_PROT response 0 [ SA V V V V ]
2020-04-29T06:37:00+0000 07[NET] sending packet: from 10.10.10.10[500] to 10.10.10.13[500] (160 by
tes)
2020-04-29T06:37:00+0000 08[NET] received packet: from 10.10.10.13[500] to 10.10.10.10[500] (396 b
ytes)
2020-04-29T06:37:00+0000 08[ENC] parsed ID_PROT request 0 [ KE No NAT-D NAT-D ]
2020-04-29T06:37:00+0000 08[IKE] sending cert request for "O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei@
moxa.com"
```

```
2020-04-29T06:37:00+0000 08[ENC] generating ID_PROT response 0 [ KE No CERTREQ NAT-D NAT-D ]
2020-04-29T06:37:00+0000 08[NET] sending packet: from 10.10.10.10[500] to 10.10.10.13[500] (484 by
tes)
2020-04-29T06:37:00+0000 09[NET] received packet: from 10.10.10.13[500] to 10.10.10.10[500] (1180
bytes)
2020-04-29T06:37:00+0000 09[ENC] parsed ID_PROT request 0 [ ID CERT SIG CERTREQ N(INITIAL_CONTACT)
 ]
2020-04-29T06:37:00+0000 09[IKE] received cert request for 'O=MOXA, OU=NET, CN=MOXAHTTPtest, E=iei
@moxa.com'
2020-04-29T06:37:00+0000 09[IKE] received end entity cert "CN=DUT2"
2020-04-29T06:37:00+0000 09[CFG] looking for RSA signature peer configs matching 10.10.10.10...10.
10.10.13[CN=DUT2]
2020-04-29T06:37:00+0000 09[IKE] no peer config found
2020-04-29T06:37:00+0000 09[ENC] generating INFORMATIONAL_V1 request 123206683 [ HASH N(AUTH_FAILE
D) ]
2020-04-29T06:37:00+0000 09[NET] sending packet: from 10.10.10.10[500] to 10.10.10.13[500] (108 by
tes)
```

I can't recognize where the fail is!! and why it is written in the log file that " no peer config found " .

History

#1 - 29.04.2020 14:56 - Tobias Brunner

- Status changed from New to Feedback

First, why would you use IKEv1 between two strongSwan hosts? Just NO, use IKEv2!

> and why it is written in the log file that " no peer config found " .

It says so right there:

```
2020-04-29T06:37:00+0000 09[CFG] looking for RSA signature peer configs matching 10.10.10.10...10.10.10.13
[CN=DUT2]
2020-04-29T06:37:00+0000 09[IKE] no peer config found
```

You configured *rightid=10.10.10.13*, which obviously doesn't match *CN=DUT2*. The reason why your configured identities are no good can be seen in both logs. For example, on the client:

```
2020-04-29T06:38:14+0000 05[CFG]   id '10.10.10.13' not confirmed by certificate, defaulting to 'CN=DUT2'
```

So either add the IPs as SAN to the certificates, or change the configs.

#2 - 30.04.2020 10:58 - ray chao

Yse,i change server side *rightid="CN=DUT2"* and client side *right="CN=DUT1"* can establish success.
But,I want to use a CA Certificate and i copy this certificate to /etc/ipsec.d/cacerts/caCert.crt
(**holds the CA certificate which issued** and signed all peer certificates, gets loaded automatically.)

In this description that strongswan will automatically load CA certificate.

I can use the following config establish with CA certificate on openswan.

```
conn test
 leftsendcert=always
 rightsendcert=always
 leftcert=/mnt/log1/cer_file/DUT1.p12
 authby=rsasig
 type=tunnel
 auth=esp
 esp=aes128-sha2_256
 rekeymargin=9m
 rekeyfuzz=100%
 keyexchange=ike
 ikelifetime=1h
 keylife=480m
 ike=aes128-sha2_256-modp2048
 auto=add
```

I can't realize why must assign rightid in ipsec.conf at strongswan, if i want to use the ca certificate authentication,
Are there need another set when using x.590 with ca?

I following the https://www.strongswan.org/docs/readme4.htm#section_4.3
4.3 Configuring the peer side using CA certificates

```
When the IP address of a peer is known to be stable, it can be specified as well. This entry is mandatory when
 the strongSwan host wants to act as the initiator of an IPSec connection.

conn sun
     right=192.168.0.2
     rightid=@sun.strongswan.org

conn carol
     right=192.168.0.100
     rightid=carol@strongswan.org

conn dave
     right=192.168.0.200
     rightid="C=CH, O=Linux strongSwan, CN=dave@strongswan.org"

conn venus
     right=192.168.0.50

In the last example the ID types  FQDN, USER_FQDN, DER_ASN1_DN and IPV4_ADDR, respectively, were used. Of cour
se all connection definitions presented so far have included the lines in the conn %defaults section, comprisi
ng among others a left and leftcert entry,.
```

#3 - 30.04.2020 15:46 - Tobias Brunner

> I can use the following config establish with CA certificate on openswan.

Not relevant at all as other than the basic structure of the legacy ipsec.conf file, the two project have nothing in common.

> I can't realize why must assign rightid in ipsec.conf at strongswan, if i want to use the ca certificate authentication,
> Are there need another set when using x.590 with ca?

Doesn't matter if you configure a CA certificate or the end-entity certificates directly. The configured remote identity has to be confirmed by the peer's certificate (if no identity is configured, the IP address is used, so that would have to be contained in the certificate as SAN).

> I following the https://www.strongswan.org/docs/readme4.htm#section_4.3

That's very old (there is even a huge warning), better refer to UsableExamples.

#4 - 11.05.2020 13:41 - ray chao

Tobias Brunner wrote:

> > I can't realize why must assign rightid in ipsec.conf at strongswan, if i want to use the ca certificate authentication,
> > Are there need another set when using x.590 with ca?
>
> Doesn't matter if you configure a CA certificate or the end-entity certificates directly. The configured remote identity has to be confirmed by the peer's certificate (if no identity is configured, the IP address is used, so that would have to be contained in the certificate as SAN).

So,if i use IP address as remote identity,Is the only way the IP address that would have to be contained in the certificate as SAN?
Example:

```
 leftid=10.10.10.13
 rightid=10.10.10.10
```

DUT1.p12

```
Certificate:
    Data:
        Version: 3 (0x2)
```

```
        Serial Number: 3 (0x3)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=MOXA, OU=NET, CN=MOXAHTTPtest/emailAddress=iei@moxa.com
        Validity
            Not Before: Dec  6 08:20:00 2018 GMT
            Not After : Dec  6 08:20:00 2023 GMT
        Subject: CN=DUT1
```

##
DUT2.p12

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=MOXA, OU=NET, CN=MOXAHTTPtest/emailAddress=iei@moxa.com
        Validity
            Not Before: Dec  6 08:23:00 2018 GMT
            Not After : Dec  6 08:23:00 2023 GMT
        Subject: CN=DUT2
```

MOXARootCA.crt

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=MOXA, OU=NET, CN=MOXAHTTPtest/emailAddress=iei@moxa.com
        Validity
            Not Before: Dec  6 05:32:00 2018 GMT
            Not After : Dec  6 05:32:00 2028 GMT
        Subject: O=MOXA, OU=NET, CN=MOXAHTTPtest/emailAddress=iei@moxa.com
        Subject Public Key Info:
```

The error message:

```
2020-04-29T06:37:00+0000 09[CFG] looking for RSA signature peer configs matching 10.10.10.10...10.10.10.13[CN=
DUT2]
2020-04-29T06:37:00+0000 09[IKE] no peer config found
...
2020-04-29T06:38:14+0000 05[CFG]   id '10.10.10.13' not confirmed by certificate, defaulting to 'CN=DUT2'
```

Does this error message mean that the file with CN=DUT2 config cannot be found?
So, I need to add rightid = DUT2 in ipsec.conf.

If i want use IP address as remote identity,is it possible to add CN=DUT2 by loading DUT2.p12 files?

#5 - 11.05.2020 13:50 - Tobias Brunner

> So,if i use IP address as remote identity,Is the only way the IP address that would have to be contained in the certificate as SAN?

Yes, as I said, the identity you want to use has to be contained in the certificate.

> Does this error message mean that the file with CN=DUT2 config cannot be found?

Not directly. But did you try to load the remote certificate with *rightcert*?

> So, I need to add rightid = DUT2 in ipsec.conf.

Unless *DUT2* is a SAN in the certificate, you'd have to configure the full subject DN (i.e. "CN=DUT2" in this example) for a match.

> If i want use IP address as remote identity,is it possible to add CN=DUT2 by loading DUT2.p12 files?

Not sure what you mean.

#6 - 25.09.2020 11:39 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback