strongSwan - Issue #2822

Configure StrongSwan for NetworkManager Ubuntu client

13.11.2018 12:30 - smina would

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.7.1	**Resolution:**	No change required

Description

I configured a StronSwan to connect workstations on Windows or MacOS. Unfortunately, I can't find the right configuration for Ubuntu NetworkManager. Yet the configuration for Windows seems perfect for that. Can you tell me where is my mistake.

ipsec.conf:

```
config setup
    strictcrlpolicy=no
    uniqueids = no
    charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2,  mgr 2"

conn %default
    keyexchange=ikev2
    mobike=yes
    rightfirewall=yes
    leftupdown=/etc/ipsec.d/up_influxdb.sh
    dpdaction=clear
    dpddelay=300s
    dpdtimeout=400s
    fragmentation=yes
    rekey=no
    left=%any
    leftsubnet=0.0.0.0/0
    rightsourceip=192.168.90.0/25
    rightauth=eap-mschapv2
    eap_identity=%any
    ike=aes256-sha256-modp1024,aes256-sha256-modp2048!
    forceencaps = yes

conn iOS
    auto=add
    leftauth=psk
    leftid=svpn.domaine.fr
    right=%any
    rightid=svpn-client
    rightsendcert=never
    esp=aes256-sha256-modp2048!

conn win7
    leftauth=pubkey
    leftcert=server.crt
    leftid=svpn.domaine.fr
    rightid=%any
    right=%any
    esp=aes256-sha1!
    auto=add
```

Logs :

```
Nov 13 12:14:28 svpn charon: 03[NET] received packet: from 172.18.207.162[37937] to 192.168.244.10
7[500]
Nov 13 12:14:28 svpn charon: 03[NET] waiting for data on sockets
Nov 13 12:14:28 svpn charon: 11[MGR] checkout IKEv2 SA by message with SPIs a3a6ec61caf1cb36_i 000
```

```
0000000000000_r
Nov 13 12:14:28 svpn charon: 11[MGR] created IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn charon: 11[NET] received packet: from 172.18.207.162[37937] to 192.168.244.10
7[500] (334 bytes)
Nov 13 12:14:28 svpn charon: 11[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D
_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Nov 13 12:14:28 svpn charon: 11[CFG] looking for an ike config for 192.168.244.107...172.18.207.16
2
Nov 13 12:14:28 svpn charon: 11[CFG]   candidate: %any...%any, prio 28
Nov 13 12:14:28 svpn charon: 11[CFG]   candidate: %any...%any, prio 28
Nov 13 12:14:28 svpn charon: 11[CFG] found matching ike config: %any...%any with prio 28
Nov 13 12:14:28 svpn charon: 11[IKE] 172.18.207.162 is initiating an IKE_SA
Nov 13 12:14:28 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[500] to 172.18.207.1
62[37937]
Nov 13 12:14:28 svpn ipsec[447]: 08[MGR] checkin IKE_SA (unnamed)[68]
Nov 13 12:14:28 svpn ipsec[447]: 08[MGR] checkin of IKE_SA successful
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] received packet: from 172.18.207.162[34448] to 192.168.24
4.107[4500]
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkout IKEv2 SA by message with SPIs dd18f89f8b611e52_i
 4a9b12f9bc29569a_r
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] IKE_SA (unnamed)[68] successfully checked out
Nov 13 12:14:28 svpn ipsec[447]: 11[NET] received packet: from 172.18.207.162[34448] to 192.168.24
4.107[4500] (432 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 11[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr CPRQ(
ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)
]
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] looking for peer configs matching 192.168.244.107[C=FR, S
T=France, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr]..
.172.18.207.162[usertest]
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] no matching peer config found
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] processing INTERNAL_IP4_ADDRESS attribute
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] processing INTERNAL_IP4_DNS attribute
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] processing INTERNAL_IP4_NBNS attribute
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] peer supports MOBIKE
Nov 13 12:14:28 svpn ipsec[447]: 11[ENC] generating IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Nov 13 12:14:28 svpn ipsec[447]: 11[NET] sending packet: from 192.168.244.107[4500] to 172.18.207.
162[34448] (80 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkin and destroy IKE_SA (unnamed)[68]
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] IKE_SA (unnamed)[68] state change: CONNECTING => DESTROYI
NG
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkin and destroy of IKE_SA successful
Nov 13 12:14:28 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.207.
162[34448]
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] received packet: from 172.18.207.162[37937] to 192.168.24
4.107[500]
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkout IKEv2 SA by message with SPIs a3a6ec61caf1cb36_i
 0000000000000000_r
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] created IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn ipsec[447]: 11[NET] received packet: from 172.18.207.162[37937] to 192.168.24
4.107[500] (334 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 11[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NA
TD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] looking for an ike config for 192.168.244.107...172.18.20
7.162
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG]   candidate: %any...%any, prio 28
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG]   candidate: %any...%any, prio 28
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] found matching ike config: %any...%any with prio 28
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] 172.18.207.162 is initiating an IKE_SA
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] IKE_SA (unnamed)[69] state change: CREATED => CONNECTING
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] selecting proposal:
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG]   proposal matches
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] received proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF
_HMAC_SHA2_256/MODP_1024
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/P
RF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
```

```
Nov 13 12:14:28 svpn ipsec[447]: 11[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_
HMAC_SHA2_256/MODP_1024
Nov 13 12:14:28 svpn ipsec[447]: 11[IKE] remote host is behind NAT
Nov 13 12:14:28 svpn ipsec[447]: 11[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
 N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Nov 13 12:14:28 svpn ipsec[447]: 11[NET] sending packet: from 192.168.244.107[500] to 172.18.207.1
62[37937] (336 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkin IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn ipsec[447]: 11[MGR] checkin of IKE_SA successful
Nov 13 12:14:28 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[500] to 172.18.207.1
62[37937]
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] received packet: from 172.18.207.162[34448] to 192.168.24
4.107[4500]
Nov 13 12:14:28 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 13 12:14:28 svpn ipsec[447]: 13[MGR] checkout IKEv2 SA by message with SPIs a3a6ec61caf1cb36_i
 0e89b2c2ed92853a_r
Nov 13 12:14:28 svpn ipsec[447]: 13[MGR] IKE_SA (unnamed)[69] successfully checked out
Nov 13 12:14:28 svpn ipsec[447]: 13[NET] received packet: from 172.18.207.162[34448] to 192.168.24
4.107[4500] (432 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 13[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr CPRQ(
ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)
 ]
Nov 13 12:14:28 svpn ipsec[447]: 13[CFG] looking for peer configs matching 192.168.244.107[C=FR, S
T=France, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr]..
.172.18.207.162[usertest]
Nov 13 12:14:28 svpn ipsec[447]: 13[CFG] no matching peer config found
Nov 13 12:14:28 svpn ipsec[447]: 13[IKE] processing INTERNAL_IP4_ADDRESS attribute
Nov 13 12:14:28 svpn ipsec[447]: 13[IKE] processing INTERNAL_IP4_DNS attribute
Nov 13 12:14:28 svpn ipsec[447]: 13[IKE] processing INTERNAL_IP4_NBNS attribute
Nov 13 12:14:28 svpn ipsec[447]: 13[IKE] peer supports MOBIKE
Nov 13 12:14:28 svpn ipsec[447]: 13[ENC] generating IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Nov 13 12:14:28 svpn charon: 11[IKE] IKE_SA (unnamed)[69] state change: CREATED => CONNECTING
Nov 13 12:14:28 svpn ipsec[447]: 13[NET] sending packet: from 192.168.244.107[4500] to 172.18.207.
162[34448] (80 bytes)
Nov 13 12:14:28 svpn ipsec[447]: 13[MGR] checkin and destroy IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn charon: 11[CFG] selecting proposal:
Nov 13 12:14:28 svpn charon: 11[CFG]   proposal matches
Nov 13 12:14:28 svpn charon: 11[CFG] received proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMA
C_SHA2_256/MODP_1024
Nov 13 12:14:28 svpn charon: 11[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_H
MAC_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
Nov 13 12:14:28 svpn charon: 11[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC
_SHA2_256/MODP_1024
Nov 13 12:14:28 svpn charon: 11[IKE] remote host is behind NAT
Nov 13 12:14:28 svpn charon: 11[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(N
ATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Nov 13 12:14:28 svpn charon: 11[NET] sending packet: from 192.168.244.107[500] to 172.18.207.162[3
7937] (336 bytes)
Nov 13 12:14:28 svpn charon: 11[MGR] checkin IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn charon: 11[MGR] checkin of IKE_SA successful
Nov 13 12:14:28 svpn charon: 04[NET] sending packet: from 192.168.244.107[500] to 172.18.207.162[3
7937]
Nov 13 12:14:28 svpn charon: 03[NET] received packet: from 172.18.207.162[34448] to 192.168.244.10
7[4500]
Nov 13 12:14:28 svpn charon: 03[NET] waiting for data on sockets
Nov 13 12:14:28 svpn charon: 13[MGR] checkout IKEv2 SA by message with SPIs a3a6ec61caf1cb36_i 0e8
9b2c2ed92853a_r
Nov 13 12:14:28 svpn charon: 13[MGR] IKE_SA (unnamed)[69] successfully checked out
Nov 13 12:14:28 svpn charon: 13[NET] received packet: from 172.18.207.162[34448] to 192.168.244.10
7[4500] (432 bytes)
Nov 13 12:14:28 svpn charon: 13[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr CPRQ(ADDR
 DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Nov 13 12:14:28 svpn charon: 13[CFG] looking for peer configs matching 192.168.244.107[C=FR, ST=Fr
ance, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr]...172
.18.207.162[usertest]
Nov 13 12:14:28 svpn charon: 13[CFG] no matching peer config found
Nov 13 12:14:28 svpn charon: 13[IKE] processing INTERNAL_IP4_ADDRESS attribute
```

```
Nov 13 12:14:28 svpn charon: 13[IKE] processing INTERNAL_IP4_DNS attribute
Nov 13 12:14:28 svpn charon: 13[IKE] processing INTERNAL_IP4_NBNS attribute
Nov 13 12:14:28 svpn charon: 13[IKE] peer supports MOBIKE
Nov 13 12:14:28 svpn charon: 13[ENC] generating IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Nov 13 12:14:28 svpn charon: 13[NET] sending packet: from 192.168.244.107[4500] to 172.18.207.162[
34448] (80 bytes)
Nov 13 12:14:28 svpn charon: 13[MGR] checkin and destroy IKE_SA (unnamed)[69]
Nov 13 12:14:28 svpn charon: 13[IKE] IKE_SA (unnamed)[69] state change: CONNECTING => DESTROYING
Nov 13 12:14:28 svpn charon: 13[MGR] checkin and destroy of IKE_SA successful
Nov 13 12:14:28 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.207.162[
34448]
```

If I understand correctly, leftid does not fit. But I didn't find the right configuration.

History

#1 - 13.11.2018 15:34 - Tobias Brunner

- Category changed from networkmanager (charon-nm) to configuration

- Status changed from New to Feedback

> If I understand correctly, leftid does not fit. But I didn't find the right configuration.

Correct, the client proposes the full subject DN of the certificate, while you configured a FQDN. The NM backend proposes this only if you configure the server certificate instead of a CA certificate (if a CA certificate is configured, or the system's CA certificates are used, the client will propose the hostname/IP address configured in the NM GUI).

So either change the server config (don't set *leftid* so it defaults to the subject DN of the certificate), or configure a CA certificate and not the server certificate in the NM client.

What's a bit strange is that the client sends a remote identity in the first place. That shouldn't be the case since 5.0.1, so either you use a very old version on the client or something doesn't work correctly.

#2 - 13.11.2018 15:56 - smina would

I am using a CA Certificate, the one used for windows (which works) and which is also in /etc/ipsec.d/cacerts/

My config :

Client :
- Ubuntu 18.10
- strongSwan 5.6.3 (from "swanctl --version" command)

Server :
- Debian 9.5
- strongSwan U5.5.1/K4.9.0-8-amd64 (ipsec version)

#3 - 13.11.2018 15:59 - Tobias Brunner

Then something is going wrong on your client.

#4 - 13.11.2018 16:02 - smina would

> So either change the server config (don't set leftid so it defaults to the subject DN of the certificate)

I removed leftid but the problem is the same

#5 - 13.11.2018 16:05 - Tobias Brunner

> > So either change the server config (don't set leftid so it defaults to the subject DN of the certificate)
>
> I removed leftid but the problem is the same

Please provide more information listed on HelpRequests (status output, logs of both ends, etc.).

#6 - 13.11.2018 16:19 - smina would

ipsec statusall :

```
Status of IKE charon daemon (strongSwan 5.5.1, Linux 4.9.0-8-amd64, x86_64):
  uptime: 3 days, since Nov 10 07:35:08 2018
  malloc: sbrk 2715648, mmap 0, used 737776, free 1977872
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aesni aes rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkey pkcs1 pkc
s7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve soc
ket-default connmark farp stroke updown eap-identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-radius eap-tls e
ap-ttls eap-tnc xauth-generic xauth-eap xauth-pam tnc-tnccs dhcp lookip error-notify certexpire led addrblock
unity
Virtual IP pools (size/online/offline):
  192.168.90.0/25: 126/3/17
Listening IP addresses:
  192.168.244.107
Connections:
         iOS:  %any...%any  IKEv2, dpddelay=300s
         iOS:   local:  [svpn.domaine.fr] uses pre-shared key authentication
         iOS:   remote: [svpn-client] uses EAP_MSCHAPV2 authentication with EAP identity '%any'
         iOS:   child:  0.0.0.0/0 === dynamic TUNNEL, dpdaction=clear
        win7:  %any...%any  IKEv2, dpddelay=300s
        win7:   local:  [svpn.domaine.fr] uses public key authentication
        win7:    cert:  "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr,
E=assistance@domaine.fr"
        win7:   remote: uses EAP_MSCHAPV2 authentication with EAP identity '%any'
        win7:   child:  0.0.0.0/0 === dynamic TUNNEL, dpdaction=clear
Security Associations (3 up, 0 connecting):
        win7[75]: ESTABLISHED 3 minutes ago, 192.168.244.107[svpn.domaine.fr]...172.18.237.39[172.18.237.39]
        win7[75]: Remote EAP identity: suser
        win7[75]: IKEv2 SPIs: 0e79099949c89fac_i 23508df707cb3094_r*, rekeying disabled
        win7[75]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
        win7{142}:  INSTALLED, TUNNEL, reqid 51, ESP in UDP SPIs: c9777862_i 23f3aece_o
        win7{142}:  AES_CBC_256/HMAC_SHA1_96, 25744 bytes_i (158 pkts, 14s ago), 35204 bytes_o (118 pkts, 14s
ago), rekeying disabled
        win7{142}:   0.0.0.0/0 === 192.168.90.19/32
        win7[73]: ESTABLISHED 43 minutes ago, 192.168.244.107[svpn.domaine.fr]...172.17.1.168[172.18.237.94]
        win7[73]: Remote EAP identity: guser
        win7[73]: IKEv2 SPIs: d960bce31a861066_i 400a8496479085f6_r*, rekeying disabled
        win7[73]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
        win7{141}:  INSTALLED, TUNNEL, reqid 44, ESP in UDP SPIs: c087afa5_i bc8fba4e_o
        win7{141}:  AES_CBC_256/HMAC_SHA1_96, 1650281 bytes_i (12038 pkts, 1s ago), 16166801 bytes_o (16041 pk
ts, 5s ago), rekeying disabled
        win7{141}:   0.0.0.0/0 === 192.168.90.20/32
         iOS[72]: ESTABLISHED 103 minutes ago, 192.168.244.107[svpn.domaine.fr]...172.18.205.183[svpn-client]
         iOS[72]: Remote EAP identity: vuser
         iOS[72]: IKEv2 SPIs: 96a77b87f64f98f0_i f6c1af329be6e03e_r*, rekeying disabled
         iOS[72]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
         iOS{140}:  INSTALLED, TUNNEL, reqid 50, ESP in UDP SPIs: cfd0c1c5_i 06374851_o
         iOS{140}:  AES_CBC_256/HMAC_SHA2_256_128, 80458894 bytes_i (1492411 pkts, 7s ago), 4458142527 bytes_o
 (3189818 pkts, 7s ago), rekeying disabled
         iOS{140}:   0.0.0.0/0 === 192.168.90.16/32
```

client log is coming...

#7 - 13.11.2018 16:22 - Tobias Brunner

> I removed leftid but the problem is the same

That's clearly not the case:

```
Connections:
...
        win7:   local:  [svpn.domaine.fr] uses public key authentication
...
```

#8 - 13.11.2018 16:29 - smina would

> I removed leftid but the problem is the same
>
> That's clearly not the case:

in prod, I put the old conf (with leftid).

Client log :

```
Nov 13 16:21:19 cri-port3-sabe NetworkManager[877]: <info>  [1542122479.7194] audit: op="connection-activate"
uuid="fd33d9c9-80bc-4805-b541-3fc1c4ca1321" name="VPN 2" pid=2298 uid=1000 result="success"
Nov 13 16:21:19 cri-port3-sabe NetworkManager[877]: <info>  [1542122479.7281] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: Saw the service appear; activating connection
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <info>  [1542122480.0999] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN connection: (ConnectInteractive) reply received
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[CFG] received initiate for NetworkManager connection VPN 2
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[CFG] using gateway certificate, identity 'C=FR, ST=France, L=PARI
S, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr'
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[IKE] initiating IKE_SA VPN 2[30] to 192.168.244.107
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(N
ATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[NET] sending packet: from 172.18.239.138[37937] to 192.168.244.10
7[500] (334 bytes)
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <info>  [1542122480.1023] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN plugin: state changed: starting (3)
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[NET] received packet: from 192.168.244.107[500] to 172.18.239.138
[37937] (336 bytes)
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD
_D_IP) N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[IKE] remote host is behind NAT
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[IKE] establishing CHILD_SA VPN 2{30}
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr CPRQ
(ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Nov 13 16:21:20 cri-port3-sabe charon-nm: 13[NET] sending packet: from 172.18.239.138[34448] to 192.168.244.10
7[4500] (432 bytes)
Nov 13 16:21:20 cri-port3-sabe charon-nm: 16[NET] received packet: from 192.168.244.107[4500] to 172.18.239.13
8[34448] (80 bytes)
Nov 13 16:21:20 cri-port3-sabe charon-nm: 16[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
Nov 13 16:21:20 cri-port3-sabe charon-nm: 16[IKE] received AUTHENTICATION_FAILED notify error
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <warn>  [1542122480.1114] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN plugin: failed: connect-failed (1)
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <warn>  [1542122480.1114] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN plugin: failed: connect-failed (1)
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <info>  [1542122480.1115] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN plugin: state changed: stopping (5)
Nov 13 16:21:20 cri-port3-sabe NetworkManager[877]: <info>  [1542122480.1115] vpn-connection[0x55ff2c91a7a0,fd
33d9c9-80bc-4805-b541-3fc1c4ca1321,"VPN 2",0]: VPN plugin: state changed: stopped (6)
```

#9 - 13.11.2018 16:35 - Tobias Brunner

> I removed leftid but the problem is the same
>
> That's clearly not the case:
>
> in prod, I put the old conf (with leftid).

Then why post useless output that doesn't reflect the actual config?

The client log confirms that you are **not** using a CA certificate but the certificate of the server:

```
...
Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[CFG] using gateway certificate, identity 'C=FR, ST=France, L=PARI
S, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr'
...
```

I also saw that the remote identity (IDr payload) is sent if that's the case (it is not sent if a CA certificate is configured).

#10 - 13.11.2018 16:58 - smina would

> Then why post useless output that doesn't reflect the actual config?

All logs posted reflect the actual config. I only tested without leftid.

> The client log confirms that you are not using a CA certificate but the certificate of the server

really? I just tested the client with what I think is the server certificate (and without leftid again), the server say :

```
authentication of 'C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=assi
stance@domaine.fr' (myself) with RSA_EMSA_PKCS1_SHA2_384 successful
...
IKE_SA checkout not successful
```

IKE_SA checkout is another problem...

I think I really use the CA, maybe i'am wrong. to get it, I executed this command

```
openssl genrsa -des3 -out ca.key 4096
openssl req -new -key ca.key -out ca.csr
openssl x509 -req -days 3650 -in ca.csr -signkey ca.key -out ca.crt
```

Thank you for your help

#11 - 13.11.2018 17:17 - Tobias Brunner

> > Then why post useless output that doesn't reflect the actual config?
>
> All logs posted reflect the actual config. I only tested without leftid.

The status output above is definitely not from a run without *leftid* as it clearly shows the FQDN as identity.

> > The client log confirms that you are not using a CA certificate but the certificate of the server
>
> really? I just tested the client with what I think is the server certificate (and without leftid again), the server say :
>
> ```
> authentication of 'C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=
> assistance@domaine.fr' (myself) with RSA_EMSA_PKCS1_SHA2_384 successful
> ```

If that's the subject DN of server certificate then I don't know what certificate you configured on the client, because it's not a CA certificate (otherwise you'd see a different log message, along the lines of using CA certificate, gateway identity ...) and apparently also not the actual server certificate as the identity clearly doesn't match:

> ```
> Nov 13 16:21:20 cri-port3-sabe charon-nm: 05[CFG] using gateway certificate, identity 'C=FR, ST=France, L=
> PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr'
> ```

This will obviously result in the same error seen in the original log as the identity sent by the client won't match the identity used by server:

```
C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=assistance@domaine.fr
C=FR, ST=France, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr
                                                                                     ~~~~~~~~~~~~~~~~~
```

So make sure you configure the correct certificate on the client (preferably a CA certificate).

#12 - 15.11.2018 09:29 - smina would

Hi Tobias,

here are logs of a connection from a windows :

```
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[500] to 192.168.244.107[500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] checkout IKEv2 SA by message with SPIs 7e883131ec26b9a5_i c426da54b43
```

```
efd9c_r
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] IKE_SA checkout not successful
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.204.46[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] checkout IKEv2 SA by message with SPIs 7e883131ec26b9a5_i c426da54b43
efd9c_r
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] IKE_SA checkout not successful
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.204.46[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] checkout IKEv2 SA by message with SPIs 7e883131ec26b9a5_i c426da54b43
efd9c_r
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] IKE_SA checkout not successful
Nov 15 09:22:23 svpn ipsec[447]: 06[MGR] checkout IKEv2 SA with SPIs 89c482f172a899e4_i 0e37b3ceeecc6e6f_r
Nov 15 09:22:23 svpn ipsec[447]: 06[MGR] IKE_SA iOS-IKEV2[138] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 06[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 in
Nov 15 09:22:23 svpn ipsec[447]: 06[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 fwd
Nov 15 09:22:23 svpn ipsec[447]: 06[MGR] checkin IKE_SA iOS-IKEV2[138]
Nov 15 09:22:23 svpn ipsec[447]: 06[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] checkout IKEv2 SA with SPIs 7e883131ec26b9a5_i c426da54b43efd9c_r
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] IKE_SA checkout not successful
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] checkout IKEv2 SA with SPIs 89c482f172a899e4_i 0e37b3ceeecc6e6f_r
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] IKE_SA iOS-IKEV2[138] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 15[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 in
Nov 15 09:22:23 svpn ipsec[447]: 15[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 fwd
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] checkin IKE_SA iOS-IKEV2[138]
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.204.5[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] checkout IKEv2 SA by message with SPIs 89c482f172a899e4_i 0e37b3ceeec
c6e6f_r
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] IKE_SA iOS-IKEV2[138] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 10[NET] received packet: from 172.18.204.5[4500] to 192.168.244.107[4500] (80
 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 10[ENC] parsed INFORMATIONAL request 8 [ ]
Nov 15 09:22:23 svpn ipsec[447]: 10[ENC] generating INFORMATIONAL response 8 [ ]
Nov 15 09:22:23 svpn ipsec[447]: 10[NET] sending packet: from 192.168.244.107[4500] to 172.18.204.5[4500] (80
bytes)
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] checkin IKE_SA iOS-IKEV2[138]
Nov 15 09:22:23 svpn ipsec[447]: 10[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.204.5[4500]
Nov 15 09:22:23 svpn charon: 14[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i 000000000000000
0_r
Nov 15 09:22:23 svpn ipsec[447]: 13[MGR] checkout IKEv2 SA with SPIs 89c482f172a899e4_i 0e37b3ceeecc6e6f_r
Nov 15 09:22:23 svpn ipsec[447]: 13[MGR] IKE_SA iOS-IKEV2[138] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 13[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 in
Nov 15 09:22:23 svpn ipsec[447]: 13[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 fwd
Nov 15 09:22:23 svpn ipsec[447]: 13[MGR] checkin IKE_SA iOS-IKEV2[138]
Nov 15 09:22:23 svpn ipsec[447]: 13[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkout IKEv2 SA with SPIs 89c482f172a899e4_i 0e37b3ceeecc6e6f_r
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] IKE_SA iOS-IKEV2[138] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 14[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 in
Nov 15 09:22:23 svpn ipsec[447]: 14[KNL] querying policy 192.168.90.10/32 === 0.0.0.0/0 fwd
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkin IKE_SA iOS-IKEV2[138]
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[500] to 192.168.244.107[500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i 00000000000
00000_r
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] created IKE_SA (unnamed)[139]
Nov 15 09:22:23 svpn ipsec[447]: 14[NET] received packet: from 172.18.195.212[500] to 192.168.244.107[500] (52
8 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 14[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] looking for an ike config for 192.168.244.107...172.18.195.212
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   candidate: %any...%any, prio 28
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   candidate: %any...%any, prio 28
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] found matching ike config: %any...%any with prio 28
Nov 15 09:22:23 svpn ipsec[447]: 14[IKE] 172.18.195.212 is initiating an IKE_SA
Nov 15 09:22:23 svpn ipsec[447]: 14[IKE] IKE_SA (unnamed)[139] state change: CREATED => CONNECTING
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   no acceptable PSEUDO_RANDOM_FUNCTION found
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] selecting proposal:
```

```
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG]   proposal matches
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] received proposals: IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_
1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_384_192/PRF_HMAC_S
HA2_384/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024
Nov 15 09:22:23 svpn charon: 14[MGR] created IKE_SA (unnamed)[139]
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2
_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
Nov 15 09:22:23 svpn ipsec[447]: 14[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_25
6/MODP_1024
Nov 15 09:22:23 svpn ipsec[447]: 14[IKE] faking NAT situation to enforce UDP encapsulation
Nov 15 09:22:23 svpn ipsec[447]: 14[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP
) N(MULT_AUTH) ]
Nov 15 09:22:23 svpn ipsec[447]: 14[NET] sending packet: from 192.168.244.107[500] to 172.18.195.212[500] (312
 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkin IKE_SA (unnamed)[139]
Nov 15 09:22:23 svpn ipsec[447]: 14[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[500] to 172.18.195.212[500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13a
d2a36_r
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] IKE_SA (unnamed)[139] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 08[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (
848 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 08[ENC] parsed IKE_AUTH request 1 [ IDi CERTREQ N(MOBIKE_SUP) CPRQ(ADDR DNS N
BNS SRV ADDR6 DNS6 SRV6) SA TSi TSr ]
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 0e:ac:82:60:40:56:27:
97:e5:25:13:fc:2a:e1:0a:53:95:59:e4:a4
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid dd:bc:bd:86:9c:3f:07:
ed:40:e3:1b:08:ef:ce:c4:d1:88:cd:3b:15
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 4a:5c:75:22:aa:46:bf:
a4:08:9d:39:97:4e:bd:b4:a3:60:f7:a0:1d
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 6a:47:a2:67:c9:2e:2f:
19:68:8b:9b:86:61:66:95:ed:c1:2c:13:00
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 01:f0:33:4c:1a:a1:d9:
ee:5b:7b:a9:de:43:bc:02:7d:57:09:33:fb
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 88:a9:5a:ef:c0:84:fc:
13:74:41:6b:b1:63:32:c2:cf:92:59:bb:3b
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 34:4f:30:2d:25:69:31:
91:ea:f7:73:5c:ab:f5:86:8d:37:82:40:ec
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 3e:df:29:0c:c1:f5:cc:
73:2c:eb:3d:24:e1:7e:52:da:bd:27:e2:f0
Nov 15 09:22:23 svpn charon: 14[NET] received packet: from 172.18.195.212[500] to 192.168.244.107[500] (528 by
tes)
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid af:29:98:f0:ce:45:1f:
d3:f0:40:c5:5c:15:2f:ef:46:b6:ff:df:59
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid da:ed:64:74:14:9c:14:
3c:ab:dd:99:a9:bd:5b:28:4d:8b:3c:c9:d8
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 86:26:cb:1b:c5:54:b3:
9f:bd:6b:ed:63:7f:b9:89:a9:80:f1:f4:8a
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid a8:e3:02:96:70:a6:8b:
57:eb:ec:ef:cc:29:4e:91:74:9a:d4:92:38
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 30:a4:e6:4f:de:76:8a:
fc:ed:5a:90:84:28:30:46:79:2c:29:15:70
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 48:e6:68:f9:2b:d2:b2:
95:d7:47:d8:23:20:10:4f:33:98:90:9f:d4
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 87:db:d4:5f:b0:92:8d:
4e:1d:f8:15:67:e7:f2:ab:af:d6:2b:67:75
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid d5:2e:13:c1:ab:e3:49:
da:e8:b4:95:94:ef:7c:38:43:60:64:66:bd
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 59:79:12:de:61:75:d6:
6f:c4:23:b7:77:13:74:c7:96:de:6f:88:72
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 6c:ca:bd:7d:b4:7e:94:
a5:75:99:01:b6:a7:df:d4:5d:1c:09:1c:cc
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid a5:06:8a:78:cf:84:bd:
74:32:dd:58:f9:65:eb:3a:55:e7:c7:80:dc
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid e2:7f:7b:d8:77:d5:df:
9e:0a:3f:9e:b4:cb:0e:2e:a9:ef:db:69:77
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid b1:81:08:1a:19:a4:c0:
94:1f:fa:e8:95:28:c1:24:c9:9b:34:ac:c7
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 21:0f:2c:89:f7:c4:cd:
5d:1b:82:5e:38:d6:c6:59:3b:a6:93:75:ae
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 23:4b:71:25:56:13:e1:
30:dd:e3:42:69:c9:cc:30:d4:6f:08:41:e0
```

```
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 68:33:0e:61:35:85:21:
59:29:83:a3:c8:d2:d2:e1:40:6e:7a:b3:c1
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received cert request for unknown ca with keyid 4f:9c:7d:21:79:9c:ad:
0e:d8:b9:0c:57:9f:1a:02:99:e7:90:f3:87
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] received 25 cert requests for an unknown ca
Nov 15 09:22:23 svpn charon: 14[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
Nov 15 09:22:23 svpn ipsec[447]: 08[CFG] looking for peer configs matching 192.168.244.107[%any]...172.18.195.
212[172.18.195.212]
Nov 15 09:22:23 svpn ipsec[447]: 08[CFG]   candidate "win7", match: 1/1/28 (me/other/ike)
Nov 15 09:22:23 svpn charon: 14[CFG] looking for an ike config for 192.168.244.107...172.18.195.212
Nov 15 09:22:23 svpn charon: 14[CFG]   candidate: %any...%any, prio 28
Nov 15 09:22:23 svpn charon: 14[CFG]   candidate: %any...%any, prio 28
Nov 15 09:22:23 svpn charon: 14[CFG] found matching ike config: %any...%any with prio 28
Nov 15 09:22:23 svpn charon: 14[IKE] 172.18.195.212 is initiating an IKE_SA
Nov 15 09:22:23 svpn charon: 14[IKE] IKE_SA (unnamed)[139] state change: CREATED => CONNECTING
Nov 15 09:22:23 svpn charon: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn charon: 14[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Nov 15 09:22:23 svpn charon: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn charon: 14[CFG]   no acceptable PSEUDO_RANDOM_FUNCTION found
Nov 15 09:22:23 svpn charon: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn charon: 14[CFG]   no acceptable ENCRYPTION_ALGORITHM found
Nov 15 09:22:23 svpn charon: 14[CFG] selecting proposal:
Nov 15 09:22:23 svpn charon: 14[CFG]   proposal matches
Nov 15 09:22:23 svpn charon: 14[CFG] received proposals: IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IK
E:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_384_192/PRF_HMAC_SHA2_
384/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024
Nov 15 09:22:23 svpn charon: 14[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256
/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
Nov 15 09:22:23 svpn charon: 14[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MO
DP_1024
Nov 15 09:22:23 svpn charon: 14[IKE] faking NAT situation to enforce UDP encapsulation
Nov 15 09:22:23 svpn charon: 14[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(
MULT_AUTH) ]
Nov 15 09:22:23 svpn charon: 14[NET] sending packet: from 192.168.244.107[500] to 172.18.195.212[500] (312 byt
es)
Nov 15 09:22:23 svpn charon: 14[MGR] checkin IKE_SA (unnamed)[139]
Nov 15 09:22:23 svpn charon: 14[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[500] to 172.18.195.212[500]
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn charon: 08[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13ad2a3
6_r
Nov 15 09:22:23 svpn charon: 08[MGR] IKE_SA (unnamed)[139] successfully checked out
Nov 15 09:22:23 svpn charon: 08[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (848
bytes)
Nov 15 09:22:23 svpn charon: 08[ENC] parsed IKE_AUTH request 1 [ IDi CERTREQ N(MOBIKE_SUP) CPRQ(ADDR DNS NBNS
SRV ADDR6 DNS6 SRV6) SA TSi TSr ]
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 0e:ac:82:60:40:56:27:97:e
5:25:13:fc:2a:e1:0a:53:95:59:e4:a4
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid dd:bc:bd:86:9c:3f:07:ed:4
0:e3:1b:08:ef:ce:c4:d1:88:cd:3b:15
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 4a:5c:75:22:aa:46:bf:a4:0
8:9d:39:97:4e:bd:b4:a3:60:f7:a0:1d
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 6a:47:a2:67:c9:2e:2f:19:6
8:8b:9b:86:61:66:95:ed:c1:2c:13:00
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 01:f0:33:4c:1a:a1:d9:ee:5
b:7b:a9:de:43:bc:02:7d:57:09:33:fb
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 88:a9:5a:ef:c0:84:fc:13:7
4:41:6b:b1:63:32:c2:cf:92:59:bb:3b
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 34:4f:30:2d:25:69:31:91:e
a:f7:73:5c:ab:f5:86:8d:37:82:40:ec
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 3e:df:29:0c:c1:f5:cc:73:2
c:eb:3d:24:e1:7e:52:da:bd:27:e2:f0
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid af:29:98:f0:ce:45:1f:d3:f
0:40:c5:5c:15:2f:ef:46:b6:ff:df:59
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid da:ed:64:74:14:9c:14:3c:a
b:dd:99:a9:bd:5b:28:4d:8b:3c:c9:d8
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 86:26:cb:1b:c5:54:b3:9f:b
d:6b:ed:63:7f:b9:89:a9:80:f1:f4:8a
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid a8:e3:02:96:70:a6:8b:57:e
b:ec:ef:cc:29:4e:91:74:9a:d4:92:38
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 30:a4:e6:4f:de:76:8a:fc:e
d:5a:90:84:28:30:46:79:2c:29:15:70
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 48:e6:68:f9:2b:d2:b2:95:d
```

```
7:47:d8:23:20:10:4f:33:98:90:9f:d4
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 87:db:d4:5f:b0:92:8d:4e:1
d:f8:15:67:e7:f2:ab:af:d6:2b:67:75
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid d5:2e:13:c1:ab:e3:49:da:e
8:b4:95:94:ef:7c:38:43:60:64:66:bd
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 59:79:12:de:61:75:d6:6f:c
4:23:b7:77:13:74:c7:96:de:6f:88:72
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 6c:ca:bd:7d:b4:7e:94:a5:7
5:99:01:b6:a7:df:d4:5d:1c:09:1c:cc
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid a5:06:8a:78:cf:84:bd:74:3
2:dd:58:f9:65:eb:3a:55:e7:c7:80:dc
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid e2:7f:7b:d8:77:d5:df:9e:0
a:3f:9e:b4:cb:0e:2e:a9:ef:db:69:77
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid b1:81:08:1a:19:a4:c0:94:1
f:fa:e8:95:28:c1:24:c9:9b:34:ac:c7
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 21:0f:2c:89:f7:c4:cd:5d:1
b:82:5e:38:d6:c6:59:3b:a6:93:75:ae
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 23:4b:71:25:56:13:e1:30:d
d:e3:42:69:c9:cc:30:d4:6f:08:41:e0
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 68:33:0e:61:35:85:21:59:2
9:83:a3:c8:d2:d2:e1:40:6e:7a:b3:c1
Nov 15 09:22:23 svpn ipsec[447]: 08[CFG] selected peer config 'win7'
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] initiating EAP_IDENTITY method (id 0x00)
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP4_ADDRESS attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP4_DNS attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP4_NBNS attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP4_SERVER attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP6_ADDRESS attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP6_DNS attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] processing INTERNAL_IP6_SERVER attribute
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] peer supports MOBIKE
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] authentication of 'svpn.domaine.fr' (myself) with RSA signature succe
ssful
Nov 15 09:22:23 svpn ipsec[447]: 08[IKE] sending end entity cert "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr,
 OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=assistance@domaine.fr"
Nov 15 09:22:23 svpn ipsec[447]: 08[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Nov 15 09:22:23 svpn ipsec[447]: 08[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (2
208 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn ipsec[447]: 08[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 05[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13a
d2a36_r
Nov 15 09:22:23 svpn ipsec[447]: 05[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 05[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (
96 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 05[ENC] parsed IKE_AUTH request 2 [ EAP/RES/ID ]
Nov 15 09:22:23 svpn ipsec[447]: 05[IKE] received EAP identity 'testuser'
Nov 15 09:22:23 svpn ipsec[447]: 05[IKE] initiating EAP_MSCHAPV2 method (id 0x28)
Nov 15 09:22:23 svpn ipsec[447]: 05[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Nov 15 09:22:23 svpn ipsec[447]: 05[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (1
12 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 05[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn ipsec[447]: 05[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13a
d2a36_r
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn charon: 08[IKE] received cert request for unknown ca with keyid 4f:9c:7d:21:79:9c:ad:0e:d
8:b9:0c:57:9f:1a:02:99:e7:90:f3:87
Nov 15 09:22:23 svpn ipsec[447]: 07[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (
144 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 07[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Nov 15 09:22:23 svpn ipsec[447]: 07[ENC] generating IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Nov 15 09:22:23 svpn ipsec[447]: 07[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (1
44 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn ipsec[447]: 07[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
```

```
Nov 15 09:22:23 svpn ipsec[447]: 12[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13a
d2a36_r
Nov 15 09:22:23 svpn ipsec[447]: 12[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 12[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (
80 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 12[ENC] parsed IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Nov 15 09:22:23 svpn ipsec[447]: 12[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Nov 15 09:22:23 svpn ipsec[447]: 12[ENC] generating IKE_AUTH response 4 [ EAP/SUCC ]
Nov 15 09:22:23 svpn ipsec[447]: 12[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (8
0 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 12[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn ipsec[447]: 12[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn ipsec[447]: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn ipsec[447]: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13a
d2a36_r
Nov 15 09:22:23 svpn ipsec[447]: 15[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn ipsec[447]: 15[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (
112 bytes)
Nov 15 09:22:23 svpn ipsec[447]: 15[ENC] parsed IKE_AUTH request 5 [ AUTH ]
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] authentication of '172.18.195.212' with EAP successful
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] authentication of 'svpn.domaine.fr' (myself) with EAP
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] IKE_SA win7[139] established between 192.168.244.107[svpn.domaine.fr]
...172.18.195.212[172.18.195.212]
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] IKE_SA win7[139] state change: CONNECTING => ESTABLISHED
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] peer requested virtual IP %any
Nov 15 09:22:23 svpn ipsec[447]: 15[CFG] assigning new lease to 'testuser'
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] assigning virtual IP 192.168.90.25 to peer 'testuser'
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] peer requested virtual IP %any6
Nov 15 09:22:23 svpn charon: 08[IKE] received 25 cert requests for an unknown ca
Nov 15 09:22:23 svpn ipsec[447]: 15[IKE] no virtual IP found for %any6 requested by 'testuser'
Nov 15 09:22:23 svpn charon: 08[CFG] looking for peer configs matching 192.168.244.107[%any]...172.18.195.212[
172.18.195.212]
Nov 15 09:22:23 svpn charon: 08[CFG]   candidate "win7", match: 1/1/28 (me/other/ike)
Nov 15 09:22:23 svpn charon: 08[CFG] selected peer config 'win7'
Nov 15 09:22:23 svpn charon: 08[IKE] initiating EAP_IDENTITY method (id 0x00)
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP4_ADDRESS attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP4_DNS attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP4_NBNS attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP4_SERVER attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP6_ADDRESS attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP6_DNS attribute
Nov 15 09:22:23 svpn charon: 08[IKE] processing INTERNAL_IP6_SERVER attribute
Nov 15 09:22:23 svpn charon: 08[IKE] peer supports MOBIKE
Nov 15 09:22:23 svpn charon: 08[IKE] authentication of 'svpn.domaine.fr' (myself) with RSA signature successfu
l
Nov 15 09:22:23 svpn charon: 08[IKE] sending end entity cert "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=
svpn.domaine.fr, CN=svpn.domaine.fr, E=assistance@domaine.fr"
Nov 15 09:22:23 svpn charon: 08[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Nov 15 09:22:23 svpn charon: 08[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (2208
bytes)
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn charon: 08[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn charon: 08[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn charon: 05[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13ad2a3
6_r
Nov 15 09:22:23 svpn charon: 05[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn charon: 05[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (96 b
ytes)
Nov 15 09:22:23 svpn charon: 05[ENC] parsed IKE_AUTH request 2 [ EAP/RES/ID ]
Nov 15 09:22:23 svpn charon: 05[IKE] received EAP identity 'testuser'
Nov 15 09:22:23 svpn charon: 05[IKE] initiating EAP_MSCHAPV2 method (id 0x28)
Nov 15 09:22:23 svpn charon: 05[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Nov 15 09:22:23 svpn charon: 05[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (112 b
ytes)
Nov 15 09:22:23 svpn charon: 05[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn charon: 05[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn charon: 07[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13ad2a3
6_r
```

```
Nov 15 09:22:23 svpn charon: 07[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn charon: 07[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (144
bytes)
Nov 15 09:22:23 svpn charon: 07[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Nov 15 09:22:23 svpn charon: 07[ENC] generating IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Nov 15 09:22:23 svpn charon: 07[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (144 b
ytes)
Nov 15 09:22:23 svpn charon: 07[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn charon: 07[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn charon: 12[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13ad2a3
6_r
Nov 15 09:22:23 svpn charon: 12[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn charon: 12[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (80 b
ytes)
Nov 15 09:22:23 svpn charon: 12[ENC] parsed IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Nov 15 09:22:23 svpn charon: 12[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Nov 15 09:22:23 svpn charon: 12[ENC] generating IKE_AUTH response 4 [ EAP/SUCC ]
Nov 15 09:22:23 svpn charon: 12[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (80 by
tes)
Nov 15 09:22:23 svpn charon: 12[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn charon: 12[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
Nov 15 09:22:23 svpn charon: 03[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500]
Nov 15 09:22:23 svpn charon: 03[NET] waiting for data on sockets
Nov 15 09:22:23 svpn charon: 15[MGR] checkout IKEv2 SA by message with SPIs d96f9c5992b8772d_i ac5fc73b13ad2a3
6_r
Nov 15 09:22:23 svpn charon: 15[MGR] IKE_SA win7[139] successfully checked out
Nov 15 09:22:23 svpn charon: 15[NET] received packet: from 172.18.195.212[4500] to 192.168.244.107[4500] (112
bytes)
Nov 15 09:22:23 svpn charon: 15[ENC] parsed IKE_AUTH request 5 [ AUTH ]
Nov 15 09:22:23 svpn charon: 15[IKE] authentication of '172.18.195.212' with EAP successful
Nov 15 09:22:23 svpn charon: 15[IKE] authentication of 'svpn.domaine.fr' (myself) with EAP
Nov 15 09:22:23 svpn charon: 15[IKE] IKE_SA win7[139] established between 192.168.244.107[svpn.domaine.fr]...1
72.18.195.212[172.18.195.212]
Nov 15 09:22:23 svpn charon: 15[IKE] IKE_SA win7[139] state change: CONNECTING => ESTABLISHED
Nov 15 09:22:23 svpn charon: 15[IKE] peer requested virtual IP %any
Nov 15 09:22:23 svpn charon: 15[CFG] assigning new lease to 'testuser'
Nov 15 09:22:23 svpn charon: 15[IKE] assigning virtual IP 192.168.90.25 to peer 'testuser'
Nov 15 09:22:23 svpn charon: 15[IKE] peer requested virtual IP %any6
Nov 15 09:22:23 svpn charon: 15[IKE] no virtual IP found for %any6 requested by 'testuser'
Nov 15 09:22:23 svpn charon: 15[IKE] building INTERNAL_IP4_DNS attribute
Nov 15 09:22:23 svpn charon: 15[IKE] building INTERNAL_IP4_DNS attribute
Nov 15 09:22:23 svpn charon: 15[CFG] looking for a child config for ::/0 0.0.0.0/0 === ::/0 0.0.0.0/0
Nov 15 09:22:23 svpn charon: 15[CFG] proposing traffic selectors for us:
Nov 15 09:22:23 svpn charon: 15[CFG]  0.0.0.0/0
Nov 15 09:22:23 svpn charon: 15[CFG] proposing traffic selectors for other:
Nov 15 09:22:23 svpn charon: 15[CFG]  192.168.90.25/32
Nov 15 09:22:23 svpn charon: 15[CFG]   candidate "win7" with prio 5+1
Nov 15 09:22:23 svpn charon: 15[CFG] found matching child config "win7" with prio 6
Nov 15 09:22:23 svpn charon: 15[CFG] selecting proposal:
Nov 15 09:22:23 svpn charon: 15[CFG]   proposal matches
Nov 15 09:22:23 svpn charon: 15[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC
/HMAC_SHA1_96/NO_EXT_SEQ
Nov 15 09:22:23 svpn charon: 15[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Nov 15 09:22:23 svpn charon: 15[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Nov 15 09:22:23 svpn charon: 15[KNL] got SPI cf61825a
Nov 15 09:22:23 svpn charon: 15[CFG] selecting traffic selectors for us:
Nov 15 09:22:23 svpn charon: 15[CFG]  config: 0.0.0.0/0, received: ::/0 => no match
Nov 15 09:22:23 svpn charon: 15[CFG]  config: 0.0.0.0/0, received: 0.0.0.0/0 => match: 0.0.0.0/0
Nov 15 09:22:23 svpn charon: 15[CFG] selecting traffic selectors for other:
Nov 15 09:22:23 svpn charon: 15[CFG]  config: 192.168.90.25/32, received: ::/0 => no match
Nov 15 09:22:23 svpn charon: 15[CFG]  config: 192.168.90.25/32, received: 0.0.0.0/0 => match: 192.168.90.25/32
Nov 15 09:22:23 svpn charon: 15[KNL] adding SAD entry with SPI cf61825a and reqid {89}
Nov 15 09:22:23 svpn charon: 15[KNL]   using encryption algorithm AES_CBC with key size 256
Nov 15 09:22:23 svpn charon: 15[KNL]   using integrity algorithm HMAC_SHA1_96 with key size 160
Nov 15 09:22:23 svpn charon: 15[KNL]   using replay window of 32 packets
Nov 15 09:22:23 svpn charon: 15[KNL] adding SAD entry with SPI 2c585479 and reqid {89}
Nov 15 09:22:23 svpn charon: 15[KNL]   using encryption algorithm AES_CBC with key size 256
Nov 15 09:22:23 svpn charon: 15[KNL]   using integrity algorithm HMAC_SHA1_96 with key size 160
Nov 15 09:22:23 svpn charon: 15[KNL]   using replay window of 0 packets
Nov 15 09:22:23 svpn charon: 15[KNL] adding policy 0.0.0.0/0 === 192.168.90.25/32 out [priority 391808, refcou
nt 1]
```

```
Nov 15 09:22:23 svpn charon: 15[KNL] adding policy 192.168.90.25/32 === 0.0.0.0/0 in [priority 391808, refcoun
t 1]
Nov 15 09:22:23 svpn charon: 15[KNL] adding policy 192.168.90.25/32 === 0.0.0.0/0 fwd [priority 391808, refcou
nt 1]
Nov 15 09:22:23 svpn charon: 15[KNL] policy 0.0.0.0/0 === 192.168.90.25/32 out already exists, increasing refc
ount
Nov 15 09:22:23 svpn charon: 15[KNL] updating policy 0.0.0.0/0 === 192.168.90.25/32 out [priority 191808, refc
ount 2]
Nov 15 09:22:23 svpn charon: 15[KNL] getting a local address in traffic selector 0.0.0.0/0
Nov 15 09:22:23 svpn charon: 15[KNL] using host %any
Nov 15 09:22:23 svpn charon: 15[KNL] getting iface name for index 2
Nov 15 09:22:23 svpn charon: 15[KNL] using 192.168.244.1 as nexthop and eth0 as dev to reach 172.18.195.212/32
Nov 15 09:22:23 svpn charon: 15[KNL] installing route: 192.168.90.25/32 via 192.168.244.1 src %any dev eth0
Nov 15 09:22:23 svpn charon: 15[KNL] getting iface index for eth0
Nov 15 09:22:23 svpn charon: 15[KNL] policy 192.168.90.25/32 === 0.0.0.0/0 in already exists, increasing refco
unt
Nov 15 09:22:23 svpn charon: 15[KNL] updating policy 192.168.90.25/32 === 0.0.0.0/0 in [priority 191808, refco
unt 2]
Nov 15 09:22:23 svpn charon: 15[KNL] policy 192.168.90.25/32 === 0.0.0.0/0 fwd already exists, increasing refc
ount
Nov 15 09:22:23 svpn charon: 15[KNL] updating policy 192.168.90.25/32 === 0.0.0.0/0 fwd [priority 191808, refc
ount 2]
Nov 15 09:22:23 svpn charon: 15[IKE] CHILD_SA win7{208} established with SPIs cf61825a_i 2c585479_o and TS 0.0
.0.0/0 === 192.168.90.25/32
Nov 15 09:22:23 svpn charon: 15[KNL] 192.168.244.107 is on interface eth0
Nov 15 09:22:23 svpn charon: 15[ENC] generating IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(MOB
IKE_SUP) N(NO_ADD_ADDR) ]
Nov 15 09:22:23 svpn charon: 15[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500] (256 b
ytes)
Nov 15 09:22:23 svpn charon: 15[MGR] checkin IKE_SA win7[139]
Nov 15 09:22:23 svpn charon: 15[MGR] checkin of IKE_SA successful
Nov 15 09:22:23 svpn charon: 04[NET] sending packet: from 192.168.244.107[4500] to 172.18.195.212[4500]
```

It's work fine. can you tell me if I'm using the CA or not?
thanks.

#13 - 15.11.2018 09:37 - Tobias Brunner

Please re-read my comments above. The problem is on your client, where you configured the wrong certificate for the gateway (you configured a non-matching end-entity/server certificate instead of a CA certificate - or at least a matching server certificate). Windows or the server log has no relevance to that.

#14 - 15.11.2018 10:42 - smina would

ok, but yet the certificate I use seems for me to be the CA. I imported this same certificate into the windows certificate authority store and this seems to fit. I will still resume the creation of certificates from scratch ...
Thank you

#15 - 15.11.2018 10:45 - Tobias Brunner

> ok, but yet the certificate I use seems for me to be the CA.

According to charon-nm it isn't a CA certificate (i.e. it doesn't have the CA basicConstraint set). Please post the certificate here if you think there is a mistake.

#16 - 15.11.2018 11:24 - smina would

thank you, but I would like to remain anonymous. Can I send it to you by mail? or can you delete the post once you've retrieved it?

#17 - 15.11.2018 11:26 - Tobias Brunner

> thank you, but I would like to remain anonymous. Can I send it to you by mail? or can you delete the post once you've retrieved it?

Sure, you can send an email, or I can delete the attachment here afterwards if you prefer that.

#18 - 15.11.2018 11:45 - Tobias Brunner

As suspected, the certificate you placed in /etc/ipsec.d/cacerts/ (and use on the client) is not a CA certificate. While it is self-signed, it's missing the cA basicConstraints flag (see section 4.2.1.9 of RFC 5280). So you should issue that certificate again, with that flag set (if you used the pki --self

command, don't forget to add --ca).

#19 - 16.11.2018 11:03 - smina would

Ok, I will create new self-signed CA. Thank you.

#20 - 06.12.2018 15:55 - smina would

I just followed the document SimpleCA to create a new CA. it's much simpler than openssl. to be sure to understand, now I need to copy the caCert.der into /etc/ipsec.d/cacerts/ and use this same file into networkManager gateway certificate field. I'am wrong?

#21 - 06.12.2018 16:02 - Tobias Brunner

Your understanding is correct.

#22 - 07.12.2018 10:08 - smina would

Server is now authenticated, but I get an EAP_IDENTITY error.

Client logs :

```
Dec  7 09:27:44 cri-port3-sabe charon-nm: 15[IKE] sending cert request for "C=FR, ST=FRANCE, L=PARIS, O=svpn-t
est.domaine.fr, OU=svpn-test.domaine.fr, CN=svpn-test.domaine.fr, E=svpn-test.domaine.fr"
Dec  7 09:27:44 cri-port3-sabe charon-nm: 15[IKE] establishing CHILD_SA VPN 1{49}
Dec  7 09:27:44 cri-port3-sabe charon-nm: 15[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ
CPRQ(ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 15[NET] sending packet: from 172.18.207.162[34448] to 192.168.244.10
9[4500] (336 bytes)
Dec  7 09:27:44 cri-port3-sabe charon-nm: 13[NET] received packet: from 192.168.244.109[4500] to 172.18.207.16
2[34448] (1236 bytes)
Dec  7 09:27:44 cri-port3-sabe charon-nm: 13[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 13[ENC] received fragment #1 of 2, waiting for complete IKE message
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[NET] received packet: from 192.168.244.109[4500] to 172.18.207.16
2[34448] (372 bytes)
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[ENC] received fragment #2 of 2, reassembling fragmented IKE messa
ge
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[IKE] received end entity cert "C=FR, ST=FRANCE, L=PARIS, O=svpn-t
est.domaine.fr, OU=svpn-test.domaine.fr, CN=svpn-test.domaine.fr, E=svpn-test.domaine.fr"
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[CFG]   using certificate "C=FR, ST=FRANCE, L=PARIS, O=svpn-test.d
omaine.fr, OU=svpn-test.domaine.fr, CN=svpn-test.domaine.fr, E=svpn-test.domaine.fr"
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[CFG]   using trusted ca certificate "C=FR, ST=FRANCE, L=PARIS, O=
svpn-test.domaine.fr, OU=svpn-test.domaine.fr, CN=svpn-test.domaine.fr, E=svpn-test.domaine.fr"
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[CFG] checking certificate status of "C=FR, ST=FRANCE, L=PARIS, O=
svpn-test.domaine.fr, OU=svpn-test.domaine.fr, CN=svpn-test.domaine.fr, E=svpn-test.domaine.fr"
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[CFG] certificate status is not available
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[CFG]   reached self-signed root ca with a path length of 0
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[IKE] authentication of 'svpn-test.domaine.fr' with RSA_EMSA_PKCS1
_SHA2_256 successful
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[IKE] server requested EAP_IDENTITY (id 0x00), sending 'username1'
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[IKE] EAP_IDENTITY not supported, sending EAP_NAK
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[ENC] generating IKE_AUTH request 2 [ EAP/RES/NAK ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 16[NET] sending packet: from 172.18.207.162[34448] to 192.168.244.10
9[4500] (80 bytes)
Dec  7 09:27:44 cri-port3-sabe charon-nm: 06[NET] received packet: from 192.168.244.109[4500] to 172.18.207.16
2[34448] (80 bytes)
Dec  7 09:27:44 cri-port3-sabe charon-nm: 06[ENC] parsed IKE_AUTH response 2 [ EAP/FAIL ]
Dec  7 09:27:44 cri-port3-sabe charon-nm: 06[IKE] received EAP_FAILURE, EAP authentication failed
Dec  7 09:27:44 cri-port3-sabe charon-nm: 06[ENC] generating INFORMATIONAL request 3 [ N(AUTH_FAILED) ]
```

what am I doing wrong?

#23 - 07.12.2018 10:09 - Tobias Brunner

You need to install the *eap-identity* plugin.

#24 - 07.12.2018 11:45 - smina would

ok! it work. Thank you Tobias.

#25 - 07.12.2018 14:00 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required