strongSwan - Issue #1071

Fails to match connection profile when specifying eap identity

17.08.2015 23:58 - Roger Skjetlein

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	libcharon		
Affected version:	5.1.2	**Resolution:**	Duplicate

Description

Hi,

when connection profile that follows %default profile contains eap_identity with userid the profile fails to match and the authentication towards radius with eap mschapv2 fails despite the credentials are correct. When adding a connection profile straight after the %default profile that do not contain any matches and strongswan choses to try the next, the matching works.

Unsuccessfull login:

```
Aug 17 23:39:52 adm-vpn1-t charon: 08[IKE] sending cert request for "nnnn"
Aug 17 23:39:52 adm-vpn1-t charon: 08[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_I
P) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
Aug 17 23:39:52 adm-vpn1-t charon: 08[NET] sending packet: from nnn[500] to nnn[500] (333 bytes)
Aug 17 23:39:52 adm-vpn1-t charon: 09[NET] received packet: from nnnn[38632] to nnn[4500] (1076 by
tes)
Aug 17 23:39:52 adm-vpn1-t charon: 09[ENC] parsed IKE_AUTH request 1 [ IDi CERTREQ N(MOBIKE_SUP) C
PRQ(ADDR DNS NBNS SRV) SA TSi TSr ]
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] received 42 cert requests for an unknown ca
Aug 17 23:39:52 adm-vpn1-t charon: 09[CFG] looking for peer configs matching nnn[%any]...nnn[10.0.
0.20]
Aug 17 23:39:52 adm-vpn1-t charon: 09[CFG] selected peer config 'roger'
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] using configured EAP-Identity roger
Aug 17 23:39:52 adm-vpn1-t charon: 09[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:39:52 adm-vpn1-t charon: 09[CFG] received RADIUS Access-Challenge from server 'primary'
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] initiating EAP_MD5 method (id 0x01)
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] peer supports MOBIKE
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] authentication of 'nnnn' (myself) with RSA signature su
ccessful
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] sending end entity cert "nnnn"
Aug 17 23:39:52 adm-vpn1-t charon: 09[IKE] sending issuer cert "nnn"
Aug 17 23:39:52 adm-vpn1-t charon: 09[ENC] generating IKE_AUTH response 1 [ IDr CERT CERT AUTH EAP
/REQ/MD5 ]
Aug 17 23:39:52 adm-vpn1-t charon: 09[NET] sending packet: from nnn[4500] to nnn[38632] (2636 byte
s)
Aug 17 23:39:52 adm-vpn1-t charon: 10[NET] received packet: from nnnn[38632] to nnn[4500] (68 byte
s)
Aug 17 23:39:52 adm-vpn1-t charon: 10[ENC] parsed IKE_AUTH request 2 [ EAP/RES/NAK ]
Aug 17 23:39:52 adm-vpn1-t charon: 10[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:39:52 adm-vpn1-t charon: 10[CFG] received RADIUS Access-Challenge from server 'primary'
Aug 17 23:39:52 adm-vpn1-t charon: 10[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Aug 17 23:39:52 adm-vpn1-t charon: 10[NET] sending packet: from nnn[4500] to nnn[38632] (92 bytes)
Aug 17 23:39:52 adm-vpn1-t charon: 16[NET] received packet: from nnn[38632] to nnn[4500] (124 byte
s)
Aug 17 23:39:52 adm-vpn1-t charon: 16[ENC] parsed IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Aug 17 23:39:52 adm-vpn1-t charon: 16[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:39:53 adm-vpn1-t charon: 11[MGR] ignoring request with ID 3, already processing
Aug 17 23:39:53 adm-vpn1-t charon: 16[CFG] received RADIUS Access-Reject from server 'primary'
Aug 17 23:39:53 adm-vpn1-t charon: 16[IKE] RADIUS authentication of 'roger' failed
Aug 17 23:39:53 adm-vpn1-t charon: 16[IKE] EAP method EAP_MSCHAPV2 failed for peer 10.0.0.20
Aug 17 23:39:53 adm-vpn1-t charon: 16[ENC] generating IKE_AUTH response 3 [ EAP/FAIL ]
Aug 17 23:39:53 adm-vpn1-t charon: 16[NET] sending packet: from 91.203.117.210[4500] to 212.251.20
8.51[38632] (68 bytes)
```

Successfull login:

```
Aug 17 23:40:34 adm-vpn1-t charon: 11[IKE] sending issuer cert "nnnnn"
Aug 17 23:40:34 adm-vpn1-t charon: 11[ENC] generating IKE_AUTH response 1 [ IDr CERT CERT AUTH EAP
/REQ/ID ]
Aug 17 23:40:34 adm-vpn1-t charon: 11[NET] sending packet: from nnnn[4500] to nnn[38632] (2620 byt
es)
Aug 17 23:40:34 adm-vpn1-t charon: 12[NET] received packet: from nnnn[38632] to nnnn[4500] (76 byt
es)
Aug 17 23:40:34 adm-vpn1-t charon: 12[ENC] parsed IKE_AUTH request 2 [ EAP/RES/ID ]
Aug 17 23:40:34 adm-vpn1-t charon: 12[IKE] received EAP identity 'testbruker'
Aug 17 23:40:34 adm-vpn1-t charon: 12[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 12[CFG] received RADIUS Access-Challenge from server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 12[IKE] initiating EAP_MD5 method (id 0x01)
Aug 17 23:40:34 adm-vpn1-t charon: 12[ENC] generating IKE_AUTH response 2 [ EAP/REQ/MD5 ]
Aug 17 23:40:34 adm-vpn1-t charon: 12[NET] sending packet: from nnnn[4500] to nnnn[38632] (84 byte
s)
Aug 17 23:40:34 adm-vpn1-t charon: 16[NET] received packet: from nnnn[38632] to nnn[4500] (68 byte
s)
Aug 17 23:40:34 adm-vpn1-t charon: 16[ENC] parsed IKE_AUTH request 3 [ EAP/RES/NAK ]
Aug 17 23:40:34 adm-vpn1-t charon: 16[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 16[CFG] received RADIUS Access-Challenge from server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 16[ENC] generating IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Aug 17 23:40:34 adm-vpn1-t charon: 16[NET] sending packet: from nnnn[4500] to nnn[38632] (100 byte
s)
Aug 17 23:40:34 adm-vpn1-t charon: 04[NET] received packet: from nnnn[38632] to nnnn[4500] (132 by
tes)
Aug 17 23:40:34 adm-vpn1-t charon: 04[ENC] parsed IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Aug 17 23:40:34 adm-vpn1-t charon: 04[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 04[CFG] received RADIUS Access-Challenge from server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 04[ENC] generating IKE_AUTH response 4 [ EAP/REQ/MSCHAPV2 ]
Aug 17 23:40:34 adm-vpn1-t charon: 04[NET] sending packet: from nnnn[4500] to nnnn[38632] (108 byt
es)
Aug 17 23:40:34 adm-vpn1-t charon: 15[NET] received packet: from nnnnnn[38632] to nnnn[4500] (68 b
ytes)
Aug 17 23:40:34 adm-vpn1-t charon: 15[ENC] parsed IKE_AUTH request 5 [ EAP/RES/MSCHAPV2 ]
Aug 17 23:40:34 adm-vpn1-t charon: 15[CFG] sending RADIUS Access-Request to server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 15[CFG] received RADIUS Access-Accept from server 'primary'
Aug 17 23:40:34 adm-vpn1-t charon: 15[IKE] RADIUS authentication of 'testbruker' successful
Aug 17 23:40:34 adm-vpn1-t charon: 15[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Aug 17 23:40:34 adm-vpn1-t charon: 15[ENC] generating IKE_AUTH response 5 [ EAP/SUCC ]
Aug 17 23:40:34 adm-vpn1-t charon: 15[NET] sending packet: from nnnn[4500] to nnnnnn[38632] (68 by
tes)
Aug 17 23:40:34 adm-vpn1-t charon: 06[NET] received packet: from nnn[38632] to nnn[4500] (84 bytes
)
Aug 17 23:40:34 adm-vpn1-t charon: 06[ENC] parsed IKE_AUTH request 6 [ AUTH ]
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] authentication of '10.0.0.20' with EAP successful
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] constraint check failed: group membership to 'finnesikk
e' required
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] selected peer config 'dummy' inacceptable: non-matching
 authentication done
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] switching to peer config 'roger'
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] constraint check failed: EAP identity 'roger' required
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] selected peer config 'roger' inacceptable: non-matching
 authentication done
Aug 17 23:40:34 adm-vpn1-t charon: 06[CFG] switching to peer config 'testbruker'
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] authentication of 'vpn-test.bch.no' (myself) with EAP
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] IKE_SA testbruker[1] established between nnnn[nnnn]...n
nnnn[nnn]
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] scheduling reauthentication in 27888s
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] maximum IKE_SA lifetime 28428s
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] peer requested virtual IP %any
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] assigning virtual IP 10.0.0.10 to peer 'testbruker'
Aug 17 23:40:34 adm-vpn1-t charon: 06[IKE] CHILD_SA testbruker{1} established with SPIs c3f4ff2e_i
 6b5a1fa6_o and TS 6.6.6.4/30 10.220.0.0/16 === 10.0.0.10/32
Aug 17 23:40:34 adm-vpn1-t charon: 06[ENC] generating IKE_AUTH response 6 [ AUTH CPRP(ADDR) SA TSi
```

```
 TSr N(AUTH_LFT) N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
Aug 17 23:40:34 adm-vpn1-t charon: 06[NET] sending packet: from nnnnn[4500] to nnnnn[38632] (236 b
ytes)
```

The configuration:

```
conn %default
        fragmentation = yes
        keyexchange = ikev2
        reauth = yes
        forceencaps = yes
        mobike = yes
        rekey = yes
        installpolicy = yes
        type = tunnel
        dpdaction = clear
        dpddelay = 10s
        dpdtimeout = 60s
        auto = add
        left = nnn
        right = %any
        leftid = nnn
        compress = yes
        ikelifetime = 28800s
        lifetime = 3600s
        rightsourceip = 10.221.100.0/22
        ike = 3des-sha1-modp1024
    esp = aes256-sha1,aes192-sha1,aes128-sha1
    eap_identity = %identity
        leftauth = pubkey
    rightauth = eap-radius
    #    rightauth=eap-mschapv2
        leftcert=/etc/ipsec.d/certs/nnn
    # Apple devices do not request certificate so we need to push it
    leftsendcert = always
        leftsubnet = nnn
    leftdns = nnn

*# fails EAP matching witout this entry
conn dummy
        rightgroups = finnesikke
        leftsubnet = 255.255.255.255/32
*
conn roger
        eap_identity = roger
        leftsubnet = 5.5.5.5/30
        rightsourceip = %radius

conn testbruker
    eap_identity = testbruker
    leftsubnet = 6.6.6.6/30,10.220.0.0/16
    rightsourceip = %radius

conn test
    eap_identity = test
    leftsubnet = 7.7.7.7/30
```

Related issues:

Is duplicate of Feature #1057: conn switching based on eap identity	**New**	**06.08.2015**

History

#1 - 18.08.2015 03:17 - Noel Kuntze

Hello Roger,

Matching conns based on the eap_identity is not supported, because it is non-trivial to implement.

Please see issue #628 for details.

Regards,
Noel Kuntze

#2 - 18.08.2015 10:51 - Tobias Brunner

- Tracker changed from Bug to Issue

- Description updated

- Category set to libcharon

- Status changed from New to Closed

- Resolution set to Duplicate

#3 - 18.08.2015 10:52 - Tobias Brunner

- Is duplicate of Feature #1057: conn switching based on eap identity added

#4 - 18.08.2015 14:27 - Roger Skjetlein

We will work around the limitation (despite it apparently works) by assigning one user per group and create one connection profile for each group. We will script the creation of profiles (policies).

#5 - 18.08.2015 14:49 - Tobias Brunner

> We will work around the limitation (despite it apparently works) by assigning one user per group and create one connection profile for each group. We will script the creation of profiles (policies).

The reason it works with the dummy config is the *eap_identity=%identity* setting inherited from *conn %default*, which causes the daemon to do an EAP-Identity exchange. This is not the case for configs that set *eap_identity* to a specific value. No identity is exchanged in that case, the configured one is just assumed and sent to the RADIUS server as EAP-Identity. So if the username in the EAP-MSCHAPv2 exchange doesn't match this identity it might cause the authentication to fail (check the RADIUS server log to see the actual reason). Perhaps the RADIUS server initiates an EAP-Identity exchange if you enable *charon.plugins.eap-radius.eap_start*, which might make it work without the dummy config.