strongSwan - Issue #1183

EAP-MSCHAPv2 Win7 - EAP key found only on second try

28.10.2015 16:32 - Marcel Müller

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.3.3	**Resolution:**	No change required

Description

Hello,

I'm using strongSwan 5.3.3 successfully with Win7 Machine Certificates and I'm now trying to implement auth via MSCHAPv2 as well. This works fine on every second try. When starting the connection strongswan logs no EAP key found for hosts '%any' - '%any' - then windows wants to confirm the credentials (which I just accept) and then the connection gets established. Any idea why it looks for an EAP key with "%any" in the first try?

Thanks in advance!

Log:

```
Oct 28 16:24:45 30[IKE] <69> 172.31.2.80 is initiating an IKE_SA
Oct 28 16:24:45 30[IKE] <69> sending cert request for "<ServerCert>"
Oct 28 16:24:45 44[IKE] <69> received cert request for "<ServerCert>"
Oct 28 16:24:45 44[IKE] <69> received 47 cert requests for an unknown ca
Oct 28 16:24:45 44[CFG] <69> looking for peer configs matching 172.31.1.5[%any]...172.31.2.80[172.
31.2.80]
Oct 28 16:24:45 44[CFG] <client1|69> selected peer config 'client1'
Oct 28 16:24:45 44[IKE] <client1|69> using configured EAP-Identity client1
Oct 28 16:24:45 44[IKE] <client1|69> initiating EAP_MSCHAPV2 method (id 0xA5)
Oct 28 16:24:45 44[IKE] <client1|69> peer supports MOBIKE
Oct 28 16:24:45 44[IKE] <client1|69> authentication of '<Hostname>' (myself) with RSA signature su
ccessful
Oct 28 16:24:45 44[IKE] <client1|69> sending end entity cert "<ServerCert>"
Oct 28 16:24:45 17[IKE] <client1|69> no EAP key found for hosts '%any' - '%any'
Oct 28 16:24:45 17[IKE] <client1|69> EAP-MS-CHAPv2 verification failed, retry (1)
Oct 28 16:24:49 01[IKE] <client1|69> EAP method EAP_MSCHAPV2 succeeded, MSK established
Oct 28 16:24:49 34[IKE] <client1|69> authentication of '172.31.2.80' with EAP successful
Oct 28 16:24:49 34[IKE] <client1|69> authentication of '<Hostname>' (myself) with EAP
Oct 28 16:24:49 34[IKE] <client1|69> IKE_SA client1[69] established between 172.31.1.5[<Hostname>]
...172.31.2.80[172.31.2.80]
Oct 28 16:24:49 34[IKE] <client1|69> peer requested virtual IP %any
Oct 28 16:24:49 34[CFG] <client1|69> reassigning offline lease to 'client1'
Oct 28 16:24:49 34[IKE] <client1|69> assigning virtual IP 172.31.11.1 to peer 'client1'
Oct 28 16:24:49 34[IKE] <client1|69> peer requested virtual IP %any6
Oct 28 16:24:49 34[IKE] <client1|69> no virtual IP found for %any6 requested by 'client1'
Oct 28 16:24:49 34[IKE] <client1|69> CHILD_SA client1{56} established with SPIs ca6516bc_i 79822fb
a_o and TS 172.31.0.0/16 === 172.31.11.1/32
```

Config:

```
conn %default
        keyexchange=ikev1
        auto=ignore
        left=%defaultroute
        leftupdown = /root/custom_updown
        dpdaction=clear

conn win7machine
        leftcert=serverCert2014.pem
```

```
        leftsubnet=172.31.0.0/16
        right=%any
        rightsourceip=172.31.11.0/24
        keyexchange=ikev2
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        rekey=no

conn win7chap
        also=win7machine
        dpddelay=300s
        leftauth=pubkey
        leftid=<hostname>
        rightauth=eap-mschapv2

conn client1
        also=win7chap
        eap_identity="client1"
        auto=add
```

ipsec statusall

```
     client1:  %any...%any  IKEv2, dpddelay=300s
     client1:   local:  [<hostname>] uses public key authentication
     client1:    cert:  "<ServerCert>"
     client1:   remote: uses EAP_MSCHAPV2 authentication with EAP identity 'client1'
     client1:   child:  172.31.0.0/16 === dynamic TUNNEL, dpdaction=clear
```

Related issues:

Related to Feature #1057: conn switching based on eap identity	**New**	**06.08.2015**

History

#1 - 28.10.2015 16:38 - Tobias Brunner

- Status changed from New to Feedback

eap_identity="client1"

This is probably the problem. I guess Windows expects an EAP-Identity exchange so you have to configure *eap_identity=%identity*. Matching connections based on *eap_identity* is currently not possible anyway (see #1057 and related tickets).

#2 - 28.10.2015 21:34 - Marcel Müller

Hello Tobias,

ah I see. Didn't realise that *%identity* and *%any* (as stated in Win7EapMultipleConfig) are the same in this case. Also I needed to add the eap_identity plugin to my installation. I added a comment to the wiki page Windows7 for case B and C.
Thanks for your help, everything is working great now!

#3 - 29.10.2015 15:23 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

You're welcome.

#4 - 28.09.2018 11:24 - Tobias Brunner

- Related to Feature #1057: conn switching based on eap identity added