strongSwan - Issue #2916

more specific conn (rightid) not selected

10.02.2019 12:36 - Florian K

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.7.1	**Resolution:**	Duplicate

Description

I have roadwarriors that shall establish a VPN connection using IKEv2 and Windows 10. (That works already.) I am using pfSense 2.4.4 - but because pfSense writes the config files as I would expect, I came here to look for help...
`ipsec --version` outputs "FreeBSD strongSwan U5.7.1/K11.2-RELEASE-p6"

The Problem: I want to assign most of my roadwarriors an IP of 192.168.6.0/24 - the remaining ones shall geht 192.168.7.0/24. (In order to apply different firewall rules)

Unfortunately this does not work. My test-client always gets a 192.168.6.x IP.

ipsec.conf:

```
# This file is automatically generated. Do not edit
config setup
        uniqueids = yes

conn bypasslan
        leftsubnet = 10.8.0.0/16
        rightsubnet = 10.8.0.0/16
        authby = never
        type = passthrough
        auto = route

conn con-mobile
        fragmentation = yes
        keyexchange = ikev2
        reauth = yes
        forceencaps = no
        mobike = yes

        rekey = yes
        installpolicy = yes
        type = tunnel
        dpdaction = clear
        dpddelay = 10s
        dpdtimeout = 60s
        auto = add
        left = 145.REMOVED...
        right = %any
        leftid = fqdn:test.REMOVED
        ikelifetime = 28800s
        lifetime = 3600s
        rightsourceip = 192.168.6.0/24
        rightdns = 10.8.1.11
        ike = aes256-sha384-ecp384!
        esp = aes256-sha256-ecp384,aes256-sha384-ecp384!
        eap_identity=%any
        leftauth=pubkey
        rightauth=eap-mschapv2
        leftcert=/var/etc/ipsec/ipsec.d/certs/cert-1.crt
        leftsendcert=always
        leftsubnet = 10.8.0.0/16
```

```
conn mobile-1
        also = con-mobile
        eap_identity = "foo@bar.com"
        rightsourceip = 192.168.7.0/24
        rightid = "foo@bar.com"
```

As I understand the answer on https://serverfault.com/questions/709228/when-and-with-which-parameters-does-strongswan-select-a-connection Strongswan should re-evaluate which conn to use after it authenticated the rightid. However, I can't find anything in the logs that it tries to do that. Even with CFG logging at maximum. On first connect, it selects con-mobile (which is correct at that moment) - and then it sticks to it forever.

How can I get it to use "mobile-1"? Thank you!

Relevant log entries:

```
Feb 7 22:26:38     charon          10[CFG] <3> looking for peer configs matching 145.REMOVED[%any].
..46.REMOVED[192.168.189.34]
Feb 7 22:26:38     charon          10[CFG] <3> candidate "bypasslan", match: 1/1/24 (me/other/ike)
Feb 7 22:26:38     charon          10[CFG] <3> candidate "con-mobile", match: 1/1/1052 (me/other/ik
e)
Feb 7 22:26:38     charon          10[CFG] <con-mobile|3> selected peer config 'con-mobile'
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> initiating EAP_IDENTITY method (id 0x00)
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> peer supports MOBIKE
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> authentication of 'test.REMOVED' (myself)
 with RSA signature successful
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> sending end entity cert "C=DE, O=REMOVED,
 CN=test.REMOVED"
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 1 [ IDr CERT
 AUTH EAP/REQ/ID ]
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> splitting IKE message (1560 bytes) into 2
 fragments
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 1 [ EF(1/2)
]
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 1 [ EF(2/2)
]
Feb 7 22:26:38     charon          10[NET] <con-mobile|3> sending packet: from 145.REMOVED[4500] to
 46.REMOVED[63541] (1244 bytes)
Feb 7 22:26:38     charon          10[NET] <con-mobile|3> sending packet: from 145.REMOVED[4500] to
 46.REMOVED[63541] (396 bytes)
Feb 7 22:26:38     charon          10[NET] <con-mobile|3> received packet: from 46.REMOVED[63541] t
o 145.REMOVED[4500] (104 bytes)
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> parsed IKE_AUTH request 2 [ EAP/RES/ID ]
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> received EAP identity 'foo@bar.com'
Feb 7 22:26:38     charon          10[IKE] <con-mobile|3> initiating EAP_MSCHAPV2 method (id 0x1E)
Feb 7 22:26:38     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 2 [ EAP/REQ/
MSCHAPV2 ]
Feb 7 22:26:38     charon          10[NET] <con-mobile|3> sending packet: from 145.REMOVED[4500] to
 46.REMOVED[63541] (120 bytes)
Feb 7 22:26:39     charon          10[NET] <con-mobile|3> received packet: from 46.REMOVED[63541] t
o 145.REMOVED[4500] (152 bytes)
Feb 7 22:26:39     charon          10[ENC] <con-mobile|3> parsed IKE_AUTH request 3 [ EAP/RES/MSCHA
PV2 ]
Feb 7 22:26:39     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 3 [ EAP/REQ/
MSCHAPV2 ]
Feb 7 22:26:39     charon          10[NET] <con-mobile|3> sending packet: from 145.REMOVED[4500] to
 46.REMOVED[63541] (152 bytes)
Feb 7 22:26:39     charon          10[NET] <con-mobile|3> received packet: from 46.REMOVED[63541] t
o 145.REMOVED[4500] (88 bytes)
Feb 7 22:26:39     charon          10[ENC] <con-mobile|3> parsed IKE_AUTH request 4 [ EAP/RES/MSCHA
PV2 ]
Feb 7 22:26:39     charon          10[IKE] <con-mobile|3> EAP method EAP_MSCHAPV2 succeeded, MSK es
tablished
Feb 7 22:26:39     charon          10[ENC] <con-mobile|3> generating IKE_AUTH response 4 [ EAP/SUCC
 ]
```

```
Feb 7 22:26:39     charon         10[NET] <con-mobile|3> sending packet: from 145.REMOVED[4500] to
 46.REMOVED[63541] (88 bytes)
Feb 7 22:26:39     charon         10[NET] <con-mobile|3> received packet: from 46.REMOVED[63541] t
o 145.REMOVED[4500] (136 bytes)
Feb 7 22:26:39     charon         10[ENC] <con-mobile|3> parsed IKE_AUTH request 5 [ AUTH ]
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> authentication of '192.168.189.34' with E
AP successful
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> authentication of 'test.REMOVED' (myself)
 with EAP
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> IKE_SA con-mobile[3] established between
145.REMOVED[test.REMOVED]...46.REMOVED[192.168.189.34]
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> scheduling reauthentication in 27974s
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> maximum IKE_SA lifetime 28514s
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> peer requested virtual IP %any
Feb 7 22:26:39     charon         10[CFG] <con-mobile|3> reassigning offline lease to 'foo@bar.com
'
Feb 7 22:26:39     charon         10[IKE] <con-mobile|3> assigning virtual IP 192.168.6.1 to peer
'foo@bar.com'
```

The second last line here says "reassigning offline lease" so I also just tried a brand new account. It does not change anything:

```
Feb 7 22:31:24     charon         01[CFG] <con-mobile|4> assigning new lease to 'bli@bla'
Feb 7 22:31:24     charon         01[IKE] <con-mobile|4> assigning virtual IP 192.168.6.2 to peer
'bli@bla'
```

My expectation would have been, that somewhere after "authentication of '192.168.189.34' with EAP successful" there would be another line saying "looking for peer configs matching...".
(Or maybe even already after "received EAP identity 'foo@bar.com'")
And then the "mobile-1" conn would match because it is more specific.

Related issues:

Related to Issue #2719: Windows - Different peer configs per identity	**Closed**	
Is duplicate of Feature #1057: conn switching based on eap identity	**New**	**06.08.2015**

History

#1 - 11.02.2019 10:15 - Tobias Brunner

- Category set to configuration

- Status changed from New to Closed

- Resolution set to Duplicate

#2 - 11.02.2019 10:15 - Tobias Brunner

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

#3 - 11.02.2019 10:16 - Tobias Brunner

- Related to Issue #2719: Windows - Different peer configs per identity added