strongSwan - Issue #1290

IPsec tunnel connection strongswan - opeswan (IKEv1, PSK)

01.02.2016 14:59 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	interoperability		
Affected version:	5.3.5	**Resolution:**	No change required

Description

Hello,

I need a connection beetween strongswan (5.3.5) and openswan (2.6.43). Strongswan is an initiator and openswan is an responder. But openswan rejects conncetion with following messages:

```
2016-02-01 15:05:34 pluto[8902]: packet from 10.40.30.240:500: received Vendor ID payload [XAUTH]
2016-02-01 15:05:34 pluto[8902]: packet from 10.40.30.240:500: received Vendor ID payload [Dead Pe
er Detection]
2016-02-01 15:05:34 pluto[8902]: packet from 10.40.30.240:500: received Vendor ID payload [RFC 394
7] method set to=115
2016-02-01 15:05:34 pluto[8902]: packet from 10.40.30.240:500: received Vendor ID payload [draft-i
etf-ipsec-nat-t-ike-02_n] meth=106, but already using method 115
2016-02-01 15:05:34 pluto[8902]: packet from 10.40.30.240:500: initial Main Mode message received
on 10.40.30.242:500 but no connection has been authorized with policy=PSK+XAUTH
```

strongswan's ipsec.conf:

```
conn ipsec1
         leftid="10.40.30.240"
         rightid="10.40.30.242"
         authby=psk
         leftauth=psk
         rightauth=psk
         ikelifetime=3600
         keylife=3600
         rekeymargin=540
         rekeyfuzz=100%
         type=tunnel
         esp=aes128-sha1,3des-sha1
         keyexchange=ikev1
         right=10.40.30.242
         left=10.40.30.240
         leftsubnet=192.168.1.0/24
         rightsubnet=192.168.100.0/24
         auto=start
         leftfirewall=yes
```

I think that problem is that strongswan sends XAUTH even though XAUTH is not set up in config file.
When openswan is initiator and strongswan responder (auto=add) tunnel is succesfully estabilished.

Thank you for any suggestions

History

#1 - 01.02.2016 15:14 - Jiri Zendulka

Openswan's ipsec status:

"ipsec1": 192.168.100.0/24===10.40.30.242[+S?C]...%any[+S?C]===192.168.1.0/24; unrouted; eroute owner: #0
"ipsec1": myip=unset; hisip=unset; myup=/etc/scripts/updown; hisup=/etc/scripts/updown;
"ipsec1": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec1": policy: PSK+ENCRYPT+TUNNEL; prio: 24,24; interface: eth1;
"ipsec1": debug: raw+crypt+parsing+emitting+control+lifecycle+klips+dns+oppo+controlmore+pfkey+nattraversal+x509+dpd+oppoinfo

"ipsec1":   newest ISAKMP SA: #0; newest IPsec SA: #0;

#2 - 01.02.2016 15:17 - Tobias Brunner

- Description updated

- Category set to interoperability

- Status changed from New to Feedback

> I think that problem is that strongswan sends XAUTH even though XAUTH is not set up in config file.

You could try increasing the log level or look at the initial packet in Wireshark to see what authentication method strongSwan actually proposes. But there should be no reason for it to propose XAuth (so the authentication method should be 1 and not 65001). Maybe Openswan is thrown off by the XAUTH vendor ID (which, I guess, does not technically have to be sent when XAuth is not used, but it should also not be the reason for any errors).

#3 - 04.02.2016 10:23 - Jiri Zendulka

- File ipsec added

Hi Tobias,

I attacched a file with initial packets from strongswan. It looks there is an XAUTH part in these packets...

#4 - 04.02.2016 11:57 - Tobias Brunner

- File disable-xauth-vendor-id.patch added

> I attacched a file with initial packets from strongswan. It looks there is an XAUTH part in these packets...

Thanks. That's only the XAuth vendor ID, the authentication method in all transforms of the SA payload is PSK. But as I mentioned, maybe that vendor ID is actually a problem for Openswan.

If you don't use XAuth for any other connections you could try disabling sending the vendor ID in the code with the attached patch.

#5 - 04.02.2016 13:17 - Jiri Zendulka

It works. Many thanks.

#6 - 04.02.2016 14:30 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

#7 - 18.05.2016 10:09 - Jiri Zendulka

Hi Tobias,

May I used xauth-eap plugin with ikev2 with that disable-xauth-vendor-id.patch? The patch concerns ikev1 xauth only? I need compatiblity with openswan but I would need xauth-eap plugin for ikev2 for another customer too. To be honest I am little bit confused about xauth. I thought that xauth works with ikev1 only and it is "obsolete" nowadays. But I heard xauth with eap can used with ikev2 and it is used. I found on strongswan's website that ikev2 can use many kind of eap method...

Many thanks.

#8 - 18.05.2016 12:00 - Tobias Brunner

> To be honest I am little bit confused about xauth. I thought that xauth works with ikev1 only and it is "obsolete" nowadays. But I heard xauth with eap can used with ikev2 and it is used. I found on strongswan's website that ikev2 can use many kind of eap method...

Yes, XAuth is only for IKEv1. And the xauth-eap plugin is an XAuth provider that uses an EAP method to verify the credentials provided by IKEv1/XAuth clients. So you don't use it with IKEv2 but with IKEv1. This could be useful if you e.g. have a RADIUS server that authenticates IKEv2 clients with EAP-MD5 (they just use plain EAP via eap-radius plugin). The *xauth-eap* plugin allows reusing this infrastructure for IKEv1, that is, the

XAuth credentials are passed by the *xauth-eap* plugin to the RADIUS server via *eap-radius* plugin (the *eap-radius* plugin now also provides its own simple XAuth backend, which is not based on EAP).

Files

ipsec	1.82 KB	04.02.2016	Jiri Zendulka
disable-xauth-vendor-id.patch	563 Bytes	04.02.2016	Tobias Brunner