strongSwan - Bug #1434

IKEv1/XAuth connection to Dell SonicWall appliance fails

25.04.2016 20:13 - Buddy Butterfly

Status:	Closed	**Start date:**	25.04.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.5.0		
Affected version:	5.1.2	**Resolution:**	Fixed

Description

After a lengthy session on IRC with ecdsa and Thermi (tnx for the excellent support),
we managed to migrate a configuraton from OpenSwan, which was given by the following documentation
[[
http://www.pelagodesign.com/blog/2009/05/18/ubuntu-linux-how-to-setup-a-vpn-connection-to-a-sonicwall-router-using-openswan-and-pre-shared-keys-psk/]],
to StrongSwan. Unfortunately a connection is not possible due to an error. It has
been confirmed by ecdsa that it is a bug. Please find below information on the issue.

```
OS:           Ubuntu 14.04.4 LTS
StrongSwan:   5.1.2

Configuration
-------------
# Connection to Dell SonicWall
conn sonicwall
     type=tunnel
     left=192.168.0.1

     leftsourceip=%config4
     leftid=@GroupVPN
     leftauth=psk
     leftauth2=xauth
     right=8.8.8.8
     rightsubnet=172.17.0.0/16
     rightid=@A0CBF1C56F19
     rightauth=psk
     keyexchange=ikev1
     keyingtries=0
     aggressive=yes
     auto=add
     esp=3des-sha1-modp1024!
     ike=3des-sha1-modp1024!
     xauth_identity=user1

Log
---
Apr 25 16:42:58 fridolin charon: 00[LIB] loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4
 md5 rdrand random nonce x509 revocation constraints pkcs1 pkcs7 pkcs8 pkcs12 pem openssl xcbc cma
c hmac ctr ccm gcm attr kernel-netlink resolve socket-default stroke updown eap-identity xauth-gen
eric xauth-eap xauth-noauth addrblock
Apr 25 16:42:58 fridolin charon: 00[LIB] unable to load 5 plugin features (5 due to unmet dependen
cies)
Apr 25 16:42:58 fridolin charon: 00[LIB] dropped capabilities, running as uid 0, gid 0
Apr 25 16:42:58 fridolin charon: 00[JOB] spawning 16 worker threads
Apr 25 16:42:58 fridolin charon: 06[KNL] 8.8.8.8 is not a local address or the interface is down
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing ISAKMP_VENDOR task
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing ISAKMP_CERT_PRE task
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing AGGRESSIVE_MODE task
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing ISAKMP_CERT_POST task
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing ISAKMP_NATD task
Apr 25 16:43:00 fridolin charon: 09[IKE] queueing QUICK_MODE task
```

```
Apr 25 16:43:00 fridolin charon: 09[IKE] activating new tasks
Apr 25 16:43:00 fridolin charon: 09[IKE]   activating ISAKMP_VENDOR task
Apr 25 16:43:00 fridolin charon: 09[IKE]   activating ISAKMP_CERT_PRE task
Apr 25 16:43:00 fridolin charon: 09[IKE]   activating AGGRESSIVE_MODE task
Apr 25 16:43:00 fridolin charon: 09[IKE]   activating ISAKMP_CERT_POST task
Apr 25 16:43:00 fridolin charon: 09[IKE]   activating ISAKMP_NATD task
Apr 25 16:43:00 fridolin charon: 09[IKE] sending XAuth vendor ID
Apr 25 16:43:00 fridolin charon: 09[IKE] sending DPD vendor ID
Apr 25 16:43:00 fridolin charon: 09[IKE] sending NAT-T (RFC 3947) vendor ID
Apr 25 16:43:00 fridolin charon: 09[IKE] sending draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Apr 25 16:43:00 fridolin charon: 09[IKE] initiating Aggressive Mode IKE_SA sonicwall[1] to 8.8.8.8
Apr 25 16:43:00 fridolin charon: 09[IKE] IKE_SA sonicwall[1] state change: CREATED => CONNECTING
Apr 25 16:43:00 fridolin charon: 09[ENC] generating AGGRESSIVE request 0 [ SA KE No ID V V V V ]
Apr 25 16:43:00 fridolin charon: 09[NET] sending packet: from 192.168.0.1[500] to 8.8.8.8[500] (33
6 bytes)
Apr 25 16:43:00 fridolin charon: 10[NET] received packet: from 8.8.8.8[500] to 192.168.0.1[500] (4
04 bytes)
Apr 25 16:43:00 fridolin charon: 10[ENC] parsed AGGRESSIVE response 0 [ SA KE No ID V V V NAT-D NA
T-D V V HASH ]
Apr 25 16:43:00 fridolin charon: 10[ENC] received unknown vendor ID: 10:4b:f4:93:52:2c:b2:f6
Apr 25 16:43:00 fridolin charon: 10[ENC] received unknown vendor ID: 43:36:2b:8c:20:f6:99:07
Apr 25 16:43:00 fridolin charon: 10[IKE] received NAT-T (RFC 3947) vendor ID
Apr 25 16:43:00 fridolin charon: 10[IKE] received DPD vendor ID
Apr 25 16:43:00 fridolin charon: 10[IKE] received XAuth vendor ID
Apr 25 16:43:00 fridolin charon: 10[IKE] local host is behind NAT, sending keep alives
Apr 25 16:43:00 fridolin charon: 10[IKE] reinitiating already active tasks
Apr 25 16:43:00 fridolin charon: 10[IKE]   ISAKMP_VENDOR task
Apr 25 16:43:00 fridolin charon: 10[IKE]   AGGRESSIVE_MODE task
Apr 25 16:43:00 fridolin charon: 10[IKE] queueing MODE_CONFIG task
Apr 25 16:43:00 fridolin charon: 10[ENC] generating AGGRESSIVE request 0 [ NAT-D NAT-D HASH ]
Apr 25 16:43:00 fridolin charon: 10[NET] sending packet: from 192.168.0.1[4500] to 8.8.8.8[4500] (
108 bytes)
Apr 25 16:43:00 fridolin charon: 10[IKE] activating new tasks
Apr 25 16:43:00 fridolin charon: 10[IKE] nothing to initiate
Apr 25 16:43:00 fridolin charon: 11[NET] received packet: from 8.8.8.8[4500] to 192.168.0.1[4500]
(76 bytes)
Apr 25 16:43:00 fridolin charon: 11[ENC] parsed TRANSACTION request 4164982822 [ HASH CPRQ(X_TYPE
X_USER X_PWD) ]
Apr 25 16:43:00 fridolin charon: 11[ENC] generating TRANSACTION response 4164982822 [ HASH CPRP(X_
USER X_PWD) ]
Apr 25 16:43:00 fridolin charon: 11[NET] sending packet: from 192.168.0.1[4500] to 8.8.8.8[4500] (
92 bytes)
Apr 25 16:43:00 fridolin charon: 12[NET] received packet: from 8.8.8.8[4500] to 192.168.0.1[4500]
(84 bytes)
Apr 25 16:43:00 fridolin charon: 12[ENC] parsed INFORMATIONAL_V1 request 1318178631 [ HASH N(INITI
AL_CONTACT) ]
Apr 25 16:43:00 fridolin charon: 12[IKE] configuration payload missing in XAuth request
Apr 25 16:43:00 fridolin charon: 12[IKE] IKE_SA sonicwall[1] state change: CONNECTING => DESTROYIN
G
```

A fix would be highly appreciated as I am not able to connect to SonicWall from Linux.

Associated revisions

Revision 1b4e7fe1 - 06.06.2016 13:52 - Tobias Brunner

ikev1: Queue INFORMATIONAL messages during XAuth

Some peers send an INITIAL_CONTACT notify after they received our XAuth username. The XAuth task waiting for the third XAuth message handles this incorrectly and closes the IKE_SA as no configuration payloads are contained in the message. We queue the INFORMATIONAL until the XAuth exchange is complete to avoid this issue.

Fixes #1434.

History

#1 - 26.04.2016 13:09 - Tobias Brunner

- Status changed from New to Feedback

- Assignee changed from Buddy Butterfly to Tobias Brunner

- Target version set to 5.5.0

```
Apr 25 16:43:00 fridolin charon: 12[ENC] parsed INFORMATIONAL_V1 request 1318178631 [ HASH N(INITIAL_CONTACT)
]
Apr 25 16:43:00 fridolin charon: 12[IKE] configuration payload missing in XAuth request
```

As mentioned in our discussion the problem is that the XAuth task expects the third XAuth message but gets tripped up by the INFORMATIONAL message the SonicWALL sends.

This is what happens:

```
strongSwan                                              SonicWALL
                                        <-----------    Transaction XAuth CPRQ(X_TYPE X_USER X_PWD)(41649828
22)
Transaction CPRP(X_USER X_PWD)(4164982822) ----------->   Notices that this is the first connection with a cli
ent with
                                                        that username and sends an INITIAL_CONTACT notify
XAuth task treats this as invalid third    <-----------   Informational INITIAL_CONTACT (1318178631)
Transaction message and closes the SA
Already destroyed the SA                   <-----------   Transaction XAuth CPS(X_STATUS)(4164982822)
```

I pushed a possible fix to the *1434-xauth-informational* branch of our repository.

#2 - 06.06.2016 13:54 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

#3 - 04.07.2016 15:51 - Tobias Brunner

- Subject changed from Connection to Dell SonicWall Appliance fails to IKEv1/XAuth connection to Dell SonicWall appliance fails