Hi,

I have a tomato firmware on my Asus RT-N16 router and Strongswan installed from Entware. While connecting with IPSec to Dlink DI-824VUP+ I see the following errors in LOG:

Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] invalid SPI length in IKE proposal
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] PROPOSAL_SUBSTRUCTURE verification failed
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] SECURITY_ASSOCIATION_V1 payload verification failed
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[IKE] message verification failed
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] generating INFORMATIONAL_V1 request 2202842332 [ N(PLD_MAL) ]
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[IKE] ID_PROT request with message ID 0 processing failed

Tested IPSec connection with the other router Linksys WRV200, both routers connect to it successfully.

Here is my ipsec.conf:

```conf
config setup
    charondebug=all

conn %default
    ikelifetime=60
    keylife=480
    keyingtries=3
    keyexchange=ikev1
    authby=psk
    auth=esp
    ike=des-md5-modp1024
    esp=des-md5-modp1024

conn sheffapollo
    left=asus_ip
    leftsubnet=192.168.1.0/24
    leftid=asus_ip
    leftfirewall=yes
    right=dlink_ip
    rightsubnet=192.168.0.0/24
    rightid=dlink_ip
```

Associated revisions

Revision a30e0001 - 31.03.2014 14:32 - Tobias Brunner
ikev1: Accept SPI size of any length <= 16 in ISAKMP proposal

Fixes #533.
#1 - 28.02.2014 09:05 - Tobias Brunner

- Subject changed from Invalis SPI length to Invalid SPI length when connecting with D-Link DI-824VUP+
- Description updated
- Category set to interoperability
- Status changed from New to Feedback
- Assignee set to Tobias Brunner

Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] invalid SPI length in IKE proposal
Feb 26 18:03:31 apollo-router daemon.info syslog: 13[ENC] PROPOSAL_SUBSTRUCTURE verification failed

Well, this sounds like the D-Link router sends invalid data. Could you increase the log level for the enc log group, and post the log, so we can see what the other peer actually sends?

Tested IPSec connection with the other router Linksys WRV200, both routers connect to it successfully.

What do you mean? Did you successfully connect the Linksys router to the D-Link router? Or to strongSwan?

#2 - 01.03.2014 16:51 - Valentino Moscow

- File spi log.txt added

Thank you for support.
Log is attached.

Yes, D-Link and Strongswan connected to Linksys with no problem.

#3 - 03.03.2014 14:10 - Tobias Brunner

- Tracker changed from Issue to Bug
- Target version set to 5.1.3

Thanks for the log. Let's have a look at the proposal sent by the D-Link router:

Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing PROPOSAL_SUBSTRUCTURE_V1 payload, 48 bytes left
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing payload from => 48 bytes 0x436bd8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] 0: 00 00 00 30 01 01 04 01 03 00 00 10 00 00 00 2 4 ...0 ...........
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] 16: 01 01 00 00 80 01 00 01 80 02 00 01 80 03 00 01
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] 32: 80 04 00 02 80 0B 00 01 00 0C 00 04 00 00 70 8 0 ...........
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 0 U_INT_8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 0
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 1 RESERVED_BYTE
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 0
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 2 PAYLOAD_LENGTH
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 3 U_INT_8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 1
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 4 U_INT_8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 1
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 5 SPI_SIZE
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 4
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 6 U_INT_8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 1
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] parsing rule 7 SPI
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] => 4 bytes 0x437bf8
Mar 1 19:42:52 apollo-router daemon.info syslog: 12[ENC] 0: 03 00 00 10

As can be seen, the protocol ID is 1 (rule 4), which is ISAKMP/IKE. But the SPI size is set to 4 instead of either 8, which is the actual length of an
ISAKMP SPI, or 0, which it must be for the initial IKE_SA with IKEv2 (and which strongSwan uses for IKEv1 too).

Now it's interesting that in RFC 2408, section 3.5 there is the following note:

In the case of ISAKMP, the Initiator and Responder cookie pair from the ISAKMP Header is the ISAKMP SPI, therefore, the SPI Size is irrelevant and MAY be from zero (0) to sixteen (16). If the SPI Size is non-zero, the content of the SPI field MUST be ignored.

So using an SPI size of 4 is actually valid, while still not making much sense. Anyway, I pushed a fix (d040eea7) for this to the ikev1-spi-size branch of our repository. Let me know if it works for you.

#4 - 03.03.2014 15:51 - Valentino Moscow
Thank you for the answer.
But how do I apply this patch? I'm noob with this technology and linux. Can you help me with it or i need to wait for a new version?

#5 - 03.03.2014 16:41 - Tobias Brunner

But how do I apply this patch? I'm noob with this technology and linux. Can you help me with it or i need to wait for a new version?

Usually, you can simply build strongSwan from sources and just apply the patch first. But that's not so easy with embedded platforms, as you have to cross-compile the code.

Unfortunately, I don't really know Entware. But there is a short description of how to compile your own package with links to more detailed instructions. Basically you need to setup the build environment (Entware/OpenWrt Buildroot), then modify the existing strongSwan package (Entware already adds a patch to the original Openwrt package - see packages/strongswan in the Entware sources - so similarly you could add this one), then build the package and install the new version. Hopefully, the Entware/OpenWrt community can help you, if you encounter any problems.

#6 - 03.03.2014 20:53 - Valentino Moscow
Will this patch be included in new version of StrongSwan?

#7 - 04.03.2014 08:34 - Tobias Brunner

Will this patch be included in new version of StrongSwan?

Sure, but the next release isn't due until a few months. And apparently it takes quite a while until OpenWrt will include a new release (there were three since 5.0.4, two with security fixes).

#8 - 31.03.2014 14:34 - Tobias Brunner
- Status changed from Feedback to Closed
- Resolution set to Fixed

Files
spi log.txt 26.8 KB 01.03.2014 Valentino Moscow