Hi,

We've recently implemented the IKEv1 fragmentation option, but we are having the same issue for IKEv2 connections. Whereby a mobile device attempting to connect using a captive portal that drops IP Fragmentation packets is unable to complete a connection.

I've noticed there is an IKEv2 fragmentation branch.

We are also looking at moving to version 5.2.0, and would like to test this solution alongside it, or possibly after 5.2.0 validation. We would be connecting using the Strongswan client and certificate authentication.

Is the IKEv2 fragmentation branch acceptable for test purposes?

Is there a preferred deployment process for the IKEv2 fragmentation branch?

Is there anything we would need to be aware of before attempting to update a newly installed instance of 5.2.0 with any IKEv2 fragmentation changes?

Many Thanks

Jason

---

**History**

**#1 - 14.07.2014 16:03 - Tobias Brunner**

- Status changed from New to Feedback
- Assignee set to Tobias Brunner

  Is the IKEv2 fragmentation branch acceptable for test purposes?

Sure, I just rebased it the current master.

Is there a preferred deployment process for the IKEv2 fragmentation branch?

What do you mean?

Is there anything we would need to be aware of before attempting to update a newly installed instance of 5.2.0 with any IKEv2 fragmentation changes?

The main problem with the branch is that it is based on an Internet Draft ([draft-ietf-ipsecme-ikev2-fragmentation](https://tools.ietf.org/html/draft-ietf-ipsecme-ikev2-fragmentation)). This means IANA has not yet allocated any identifiers for the new payload/notification types. So it is not interoperable as the currently used identifiers are from the private use ranges. Of course, if you only use strongSwan clients and servers this is not an issue.

**#2 - 14.07.2014 16:43 - Jason Kershaw**

Thanks for the exceedingly quick response.

Is there a preferred deployment process for the IKEv2 fragmentation branch?

What do you mean?

I wasn't sure if the branch would need applying as a patch to an existing 5.2.0 or if it should be deployed in it own right. Apologies for any confusion I'm not particularly source code/repository conversant am afraid, one of our developers understands what's required.
At present we would only be using Strongswan clients and servers, so we'll look to implement this as soon as possible, and thanks for the information.

Cheers

Jason

#3 - 22.07.2014 15:04 - Tobias Brunner
- Tracker changed from Issue to Feature
- Category set to libcharon
- Target version set to 5.2.1

#4 - 06.08.2014 12:06 - Strongswan User
I'm experiencing issues building this branch, getting errors related to AC_LIB_PREFIX macro.

Running a "autoreconf -i" gets me through to a successful execution of "./configure <options>" but then "make" fails.

Please advise, we would like to test this branch and will only be using the strongswan client.

#5 - 06.08.2014 14:15 - Martin Willi
To build from git sources, you'll need additional build dependencies, refer to the source:HACKING file for details.

Once installed, make maintainer-clean (or check out a fresh copy of) your tree and follow the instructions.

Regards

Martin

#6 - 06.08.2014 18:59 - Lian Duan
Initial testing of the branch shows that it worked for IKEv2 fragmentation with strongswan client.

However, IKEv1 is no longer working, it shows that "encrypting encrypted payload failed, no IV generator" (Worked fine with 5.2.0)

Aug 6 18:54:12 server charon: 16[ENC] parsed ID_PROT request 0 [ SA V V V V V V V V V V V V V ]
Aug 6 18:54:12 server charon: 16[IKE] received NAT-T (RFC 3947) vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-08 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-07 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-06 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-05 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-04 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-03 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-02 vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received XAuth vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received Cisco Unity vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received FRAGMENTATION vendor ID
Aug 6 18:54:12 server charon: 16[IKE] received DPD vendor ID
Aug 6 18:54:12 server charon: 16[IKE] CLIENT_IP is initiating a Main Mode IKE_SA
Aug 6 18:54:12 server charon: 16[ENC] generating ID_PROT response 0 [ SA V V V V ]
Aug 6 18:54:12 server charon: 16[ENC] parsed ID_PROT request 0 [ KE No NAT-D NAT-D ]
Aug 6 18:54:12 server charon: 16[IKE] remote host is behind NAT
Aug 6 18:54:12 server charon: 16[IKE] sending cert request for
Aug 6 18:54:12 server charon: 16[IKE] sending cert request for
Aug 6 18:54:12 server charon: 16[IKE] sending cert request for
Aug 6 18:54:12 server charon: 16[IKE] sending cert request for
Aug 6 18:54:12 server charon: 16[IKE] generating ID_PROT response 0 [ KE No CERTREQ CERTREQ CERTREQ CERTREQ CERTREQ NAT-D NAT-D ]
Aug 6 18:54:12 server charon: 16[ENC] encrypting encrypted payload failed, no IV generator

#7 - 07.08.2014 11:07 - Strongswan User
I have installed all dependencies listed in that file but still getting errors. 5.1.3 and 5.2.0 both compiled fine on the same box and have both run fine apart from problems with IKEv2 connections so very keen to get this branch tested.

I am running on CentOS 6.5 with the following:

automake-1.11.1-4.el6.noarch
autoconf-2.63-5.1.el6.noarch
libtool-2.2.6-15.5.el6.x86_64

20.03.2020
I've seen that others are getting the same errors and it seems that Debian systems compile this branch better.

#8 - 11.08.2014 15:41 - Tobias Brunner
- File fix-message-generate.patch added

Lian Duan wrote:

However, IKEv1 is no longer working, it shows that "encrypting encrypted payload failed, no IV generator" (Worked fine with 5.2.0)

Thanks for the report. A local variable's initialization was lost in a refactoring, which caused the IKEv1 payloads to get wrapped in an IKEv2 encrypted payload. I updated the branch (rebased to the current master). You can also apply the attached patch.

Strongswan User wrote:

I have installed all dependencies listed in that file but still getting errors.

What errors?

5.1.3 and 5.2.0 both compiled fine on the same box

From the repository or from the tarball? The tarball already contains all the generated files so the external tools listed in HACKING are not required.

I've seen that others are getting the same errors and it seems that Debian systems compile this branch better.

Where did you see that? And yes, because the strongSwan devs develop on Debian/Ubuntu building on that platform is better supported.

#9 - 11.08.2014 17:54 - Strongswan User

After running `./configure --prefix=/usr --sysconfdir=/etc --enable-openssl --enable-xauth-noauth --enable-eap-radius --enable-curl`

I get some warnings:

configure: WARNING: linux/fib_rules.h: present but cannot be compiled
configure: WARNING: linux/fib_rules.h: check for missing prerequisite headers?
configure: WARNING: linux/fib_rules.h: see the Autoconf documentation
configure: WARNING: linux/fib_rules.h: section "Present But Cannot Be Compiled"
configure: WARNING: linux/fib_rules.h: proceeding with the preprocessor's result
configure: WARNING: linux/fib_rules.h: in the future, the compiler will take precedence

And after make, I get:

```
```

```
settings_parser.y:113: error: '$section' undeclared (first use in this function)
settings_parser.y:113: error: (Each undeclared identifier is reported only once for each function it appears in.)
settings_parser.y:113: error: '$setting' undeclared (first use in this function)
settings_parser.y:125: error: '$section_start' undeclared (first use in this function)
settings_parser.y:132: error: '$NAME' undeclared (first use in this function)
ssettings_parser.y:144: error: '$value' undeclared (first use in this function)
make[5]: *** [settings/settings_parser.lo] Error 1
make[5]: Leaving directory `/usr/local/bin/strongswan-5.2.0-ikev2-fragmentation.e73a803d/src/libstrongswan'
make[4]: *** [all-recursive] Error 1
make[4]: Leaving directory `/usr/local/bin/strongswan-5.2.0-ikev2-fragmentation.e73a803d/src/libstrongswan'
make[3]: *** [all] Error 2
make[3]: Leaving directory `/usr/local/bin/strongswan-5.2.0-ikev2-fragmentation.e73a803d/src/libstrongswan'
```

20.03.2020
After running 'autoconf -Wall' and 'autoupdate' to update my obsolete AC_HAVE_LIBRARY I am now getting:

configure.ac:329: error: possibly undefined macro: AC_LIB_PREFIX
If this token and others are legitimate, please use m4_pattern_allow.
See the Autoconf documentation.

Strongswan User wrote:

I get some warnings:

configure: WARNING: linux/fib_rules.h: present but cannot be compiled

Looks like additional headers are required for that check on Cent OS 6.5. I pushed a fix (b04f4040) to master and rebased the ikev2-fragmentation branch.

And after make, I get:

settings_parser.y: In function 'settings_parser_parse':
settings_parser.y:113: error: '$section' undeclared (first use in this function)

Looks like bison is too old on Cent OS 6.5. Named references were added with bison 2.5 (released in 2011). If you can't upgrade, try to build the tarball (make dist-bzip2) on a newer system and then use that to build strongSwan on your target host.

After running 'autoconf -Wall' and 'autoupdate' to update my obsolete AC_HAVE_LIBRARY I am now getting:

configure.ac:329: error: possibly undefined macro: AC_LIB_PREFIX

This macro is (usually) provided by gettext.

Built the tarball using make dist-bzip2 on CentOS 7 and then moved over to CentOS 6.5.

Thanks for the help.

Does fragmentation=yes setting need to be configured in /etc/ipsec.conf in the same way as for ikev1 connections?

I am now successfully running the branch, but not seeing anything in the logs to indicate that it is doing anything. Problems with ikev2 connections failing with retransmits remain.

Yes, the configuration is exactly the same.

I am now successfully running the branch, but not seeing anything in the logs to indicate that it is doing anything. Problems with ikev2 connections failing with retransmits remain.

Could you post the logs of both peers?

Does fragmentation=yes setting need to be configured in /etc/ipsec.conf in the same way as for ikev1 connections?

Yes, the configuration is exactly the same.
For those that get:

configure.ac:329: error: possibly undefined macro: AC_LIB_PREFIX
If this token and others are legitimate, please use m4_pattern_allow.
See the Autoconf documentation.

I stumbled upon the same issue. Installing not only gettext but also gettext-devel resolved the issue, since the AC_LIB_PREFIX macro is only available in the gettext header files.

Files

fix-message-generate.patch  471 Bytes  11.08.2014  Tobias Brunner