strongSwan - Bug #289

Windows SuiteB to StrongSwan 5 quickmode fail

31.01.2013 08:34 - violet se

Status:	Closed	**Start date:**	31.01.2013
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:			
Target version:	5.0.3		
Affected version:	5.0.1	**Resolution:**	Fixed

Description

Hi,

When attempting to make a transport connection to a windows 2012 machine with the following configuration, there appears to be a bug...

Error log:
Jan 31 18:13:03 update charon: 09[MGR] check-in of IKE_SA successful.
Jan 31 18:13:03 update charon: 11[NET] received packet: from 192.168.32.252[500] to 192.168.32.20[500]
Jan 31 18:13:03 update charon: 11[NET] waiting for data on sockets
Jan 31 18:13:03 update charon: 13[MGR] checkout IKE_SA by message
Jan 31 18:13:03 update charon: 13[MGR] IKE_SA testing[1] successfully checked out
Jan 31 18:13:03 update charon: 13[NET] received packet: from 192.168.32.252[500] to 192.168.32.20[500] (108 bytes)
Jan 31 18:13:03 update charon: 13[ENC] parsed QUICK_MODE response 1171673827 [HASH N(INIT_CONTACT)]
Jan 31 18:13:03 update charon: 13[IKE] next IV for MID 1171673827 => 16 bytes @ 0x293e4000de0
Jan 31 18:13:03 update charon: 13[IKE]   0: DC EB 1A 5E C1 BA ED 4C 84 F5 3E FD A6 80 5C 2D ...^...L..>...\-
Jan 31 18:13:03 update charon: 13[IKE] received QUICK_MODE response, but expected EXCHANGE_TYPE_UNDEFINED
Jan 31 18:13:03 update charon: 13[MGR] checkin and destroy IKE_SA testing[1]
Jan 31 18:13:03 update charon: 13[IKE] IKE_SA testing[1] state change: ESTABLISHED => DESTROYING

ipsec.conf:

conn testing
left=192.168.32.20
right=192.168.32.252
leftcert=update-server.crt
rightcert=testing.crt
leftca="C=AU, ST=NSW, L=BLAH, O=BLAH, CN=TEST"
rightca=%same
leftauth=pubkey
rightauth=pubkey
ike=aes256-sha384-ecp384!
esp=aes256gcm16-ecp384!
keyexchange=ikev1
type=transport
auto=route

The quickmode connection comes up for just a moment and then it is straight away pulled offline when I get the error "Jan 31 18:13:03 update charon: 13[IKE] received QUICK_MODE response, but expected EXCHANGE_TYPE_UNDEFINED"

I have tried with 5.0.0, 5.0.1 and 5.0.2 same problem.

Associated revisions

Revision 0235914d - 11.03.2013 10:53 - Martin Willi

Ignore fourth Qick Mode message sent by Windows servers.

Initial patch by Paul Stewart, fixes #289.

History

#1 - 31.01.2013 11:30 - Martin Willi

Hi,

> 13[ENC] parsed QUICK_MODE response 1171673827 [HASH N(INIT_CONTACT)]

Can you give us a little more context when this happens? Is this received just after or during the setup of Main Mode? What messages have been exchanged previously? Is this message part of a regular Quick Mode exchange?

While it is uncommon, sending INITIAL_CONTACT in a Quick Mode is fine. But it would require a complete Quick Mode exchange with three messages, what I don't see here.

#2 - 31.01.2013 15:07 - violet se

Martin Willi wrote:

> Hi,
>
> > 13[ENC] parsed QUICK_MODE response 1171673827 [HASH N(INIT_CONTACT)]
>
> Can you give us a little more context when this happens? Is this received just after or during the setup of Main Mode? What messages have been exchanged previously? Is this message part of a regular Quick Mode exchange?
>
> While it is uncommon, sending INITIAL_CONTACT in a Quick Mode is fine. But it would require a complete Quick Mode exchange with three messages, what I don't see here.

Sorry, so, main mode appears to be setup and established properly, and then it attempts to setup quick mode, I will have to double check but I think it has sent 3 quick mode messages. On the windows side, there is a event log saying quick mode setup was successful, then another message right after that it has ended.

In a few hours I can post a longer log with all the quick mode information, and the netsh commands I used to setup the windows host.

#3 - 01.02.2013 02:55 - violet se

- File strongswanlog.txt added

Ok, so to be super clear, this is occurring when I start ipsec, and attempt to connect to the machine in the rule.

The windows machine has the following setup:

netsh advfirewall set global mainmode mmsecmethods ecdhp384:aes256-sha384

netsh advfirewall consec add rule name="Update Server" endpoint1=192.168.222.20 endpoint2=any action=RequireInRequireOut auth1=ComputerCertECDSAP384 Auth1ECDSAP384CA="C=AU, S=NSW, L=BLAH, O=BLAH, CN=TEST" qmpfs=ecdhp384 qmsecmethods=esp:aesgcm256-aesgcm256

I have attached a more complete strongswan log showing what happens.

#4 - 01.02.2013 12:32 - Martin Willi

> generating QUICK_MODE request 3504573362 [HASH SA No KE]
> parsed QUICK_MODE response 3504573362 [HASH SA KE No ID ID]
> generating QUICK_MODE request 3504573362 [HASH]
> parsed QUICK_MODE response 3504573362 [HASH N(INIT_CONTACT)]

Interesting. Seems that the Windows server extends a three message Quick Mode to a four message exchange. I don't know on which standard this is based on or what the vendor intends with it. At least in RFC2409 5.5, a Quick Mode exchanges three messages only. This is why strongSwan thinks the other implementation is misbehaving and closes the connection.

Would be interesting to know if older Windows versions use something similar. It certainly is possible to extend our state handling and accept such messages, but maybe it is just a bug in the new server (that might get fixed).

Regards
Martin

#5 - 01.02.2013 12:42 - violet se

I can confirm that the exact same thing is happening on a standard windows 8 machine, and it doesnt matter what cipher suite i pick for perfect forward secrecy/quick mode encryption, the same issue occurs.

#6 - 05.02.2013 14:57 - Andreas Steffen

I just remember that Windows 2000 set the Commit Bit in the Flags field of the ISAKMP header (http://tools.ietf.org/html/rfc2408#section-3.1) which would require a fourth Quick mode message as an acknowledgement that the third Quick mode message had been received. Pluto achieved interoperability by ignoring the Commit bit. See e.g. http://comments.gmane.org/gmane.network.freeswan.user/8735. I don't know how charon handles the Commit Bit and if this is an issue with your problem anyway.

Regards

Andreas

#7 - 05.02.2013 15:06 - Andreas Steffen

An explanation how Microsoft uses the Commit Bit in a wrong way can be found under this link
http://tools.ietf.org/html/draft-jenkins-ipsec-rekeying-01#section-2.1.4 (see point 5)

#8 - 09.03.2013 17:07 - Paul Stewart

- File strongswan-5.0.2-ignore-spurious-quick-mode_new-61e34a57dc0ed52aa738fc2f79744faaf229d817.patch added

It's likely I'm not solving the issue the "right" way, but I patched my local copy of strongswan 5.0.2 as follows, and it allows me to connect to Windows RRAS servers now. It looks for an unexpected N(INIT_CONTACT) and ignores it.

#9 - 11.03.2013 11:01 - Martin Willi

- Status changed from New to Closed

- Target version set to 5.0.3

- Resolution set to Fixed

Thanks for the patch, looks good. I've pushed a simplified version to master, see
http://git.strongswan.org/?p=strongswan.git;a=commitdiff;h=0235914d.

#10 - 06.05.2013 19:14 - Andreas Steffen

- Assignee set to Martin Willi

Files

strongswanlog.txt	37.6 KB	01.02.2013	violet se
strongswan-5.0.2-ignore-spurious-quick-mode_new-61e34a57dc0ed52aa738fc2f79744faaf229d817.patch	2.36 KB	09.03.2013	Paul Stewart