strongSwan - Issue #3417

No ping on StrongSwan IPSec in HMAC-SHA256, ping works in HMAC-SHA1

20.04.2020 12:02 - Ayman Bahouth

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Noel Kuntze</td>
</tr>
<tr>
<td>Category</td>
<td>configuration</td>
</tr>
<tr>
<td>Affected version</td>
<td>5.8.4</td>
</tr>
<tr>
<td>Resolution</td>
<td>No change required</td>
</tr>
</tbody>
</table>

**Description**

I have the following situation:

I set up an IPSec tunnel between Ubuntu and Embedded Linux system according to the configuration below. I start IPSec and a tunnel established successfully with HMAC-SHA256 authentication, but 'ping' does not work in both ways (left-2-right and right-2-left). HMAC-SHA384/512 doesn't work either.

If I change the authentication method to SHA1, the ping works just fine.

```
# cat /etc/strongswan.conf
charon {
    filelog {
        # since 5.7.0 the path to the log file has to be specified in a separate setting if it contains dots,
        # use an arbitrary name without dots for the section instead of the one given here
        charon-debug-log {
            # this setting is required with 5.7.0 and newer if the path contains dots
            path = /var/log/charon_debug.log
            time_format = %a, %Y-%m-%d %R
        }
        default = 2
        mgr = 0
        net = 1
        enc = 1
        asn = 1
        job = 1
        ike_name = yes
        append = no
        flush_line = yes
    }
}
load = random nonce aes shal sha256 pem pkcs1 curve25519 gmp x509 curl revocation hmac stroke kernel-netlink socket-default updown
multiple_authentification = no

# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration
config setup
    charondebug="all"
    uniqueids=yes
    strictcrlpolicy=no
conn %default
cnn tunnel
    left=192.168.1.3
    right=192.168.1.1
    ike=aes256-sha2_256-modp1024!
    ah=sha256
    keyingtries=0
    ikelifetime=1h
```
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=restart
authby=secret
auto=start
keyexchange=ikev2
type=transport

# cat /etc/ipsec.secrets
192.168.1.3 192.168.1.1 : PSK 'test12345'

# ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.1, Linux 4.19.72, mips64):
  uptime: 93 seconds, since Jan 01 18:27:08 1970
  malloc: sbrk 2654208, mmap 0, used 339824, free 2314384
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon random nonce aes sha1 sha2 pem pkcs1 curve25519 gmp x509 revocation hmac
  stroke kernel-netlink socket-default updown
Listening IP addresses:
  192.168.1.3
Connections:
  tunnel: 192.168.1.3...192.168.1.1 IKEv2, dpddelay=30s
  tunnel: local: [192.168.1.3] uses pre-shared key authentication
  tunnel: remote: [192.168.1.1] uses pre-shared key authentication
  tunnel: child: dynamic >>> dynamic TRANSPORT, dpdaction=restart
Security Associations (1 up, 0 connecting):
  tunnel[]: ESTABLISHED 93 seconds ago, 192.168.1.3[192.168.1.3]...192.168.1.1[192.168.1.1]
  tunnel[]: IKEv2 SPIs: 3a0582084fcd1d9b_i* 9d8dcd5f66126a18_r, pre-shared key reauthentication in 39 minutes
  tunnel[]: IKE proposal: AES_CBC_256/HMAC_SHA2_256/128/PRF_HMAC_SHA2_256/MODP_1024
  tunnel[]: INSTALLED, TRANSPORT, reqid 1, AH SPIs: c5fafa44_i c4574271_o
  tunnel[]: HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 7 hours
  tunnel[]: 192.168.1.3/32 === 192.168.1.1/32

# ip xfrm state
src 192.168.1.3 dst 192.168.1.1
  proto ah spi 0xc4574271 reqid 1 mode transport
  replay-window 0 flag align4
  auth-trunc hmac(sha256) 0x59aabf790413ccfcb9f7305b503270d50ab55a6d3780c5db00ec44894a927bac128
  anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
  sel src 192.168.1.3/32 dst 192.168.1.1/32
src 192.168.1.1 dst 192.168.1.3
  proto ah spi 0xc5fafa44 reqid 1 mode transport
  replay-window 32 flag align4
  auth-trunc hmac(sha256) 0x15dd2781d6885c1310e1d0649c0e87a31746189d804841bc203b500e8d8bad128
  anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
  sel src 192.168.1.1/32 dst 192.168.1.3/32

# cat /var/log/charon_debug.log
Thu, 2020-01-01 18:36:00[DMN] Starting IKE charon daemon (strongSwan 5.8.1, Linux 4.19.72, mips64)
Thu, 2020-01-01 18:36:00[LIB] 0x00000000[LIB] Starting IKE charon daemon (strongSwan 5.8.1, Linux 4.19.72, mips64)
Thu, 2020-01-01 18:36:00[LIB] plugin 'random': loaded successfully
Thu, 2020-01-01 18:36:00[LIB] plugin 'nonce': loaded successfully
Thu, 1970-01-01 18:36 00[LIB] plugin 'socket-default': loaded successfully
Thu, 1970-01-01 18:36 00[LIB] plugin 'updown': loaded successfully
Thu, 1970-01-01 18:36 00[NET] could not open socket: Address family not supported by protocol
Thu, 1970-01-01 18:36 00[NET] could not open IPv6 socket, IPv6 disabled
Thu, 1970-01-01 18:36 00[KNL] known interfaces and IP addresses:
    lo
        127.0.0.1
    eth0
    192.168.1.3
Thu, 1970-01-01 18:36 00[KNL] received netlink error: Address family not supported by protocol (124)
Thu, 1970-01-01 18:36 00[KNL] unable to create IPv6 routing table rule
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY:ECDSA in plugin 'pem' has unmet dependency: PRIVKEY:ECDSA
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY:DSA in plugin 'pem' has unmet dependency: PRIVKEY:DSA
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY:BLISS in plugin 'pem' has unmet dependency: PRIVKEY:BLISS
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY:ECDSA in plugin 'pem' has unmet dependency: PUBKEY:ECDSA
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY:DSA in plugin 'pem' has unmet dependency: PUBKEY:DSA
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY:BLISS in plugin 'pem' has unmet dependency: PUBKEY:BLISS
Thu, 1970-01-01 18:36 00[LIB] feature CERT_DECODE:PGP in plugin 'pem' has unmet dependency: CERT_DECODE:PGP
Thu, 1970-01-01 18:36 00[LIB] feature CERT_DECODE:OCSP_REQUEST in plugin 'pem' has unmet dependency: CERT_DECODE:OCSP_REQUEST
Thu, 1970-01-01 18:36 00[LIB] feature CERT_DECODE:PUBKEY in plugin 'pem' has unmet dependency: CERT_DECODE:PUBKEY
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_224 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_224
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_256 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_256
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_384 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_384
Thu, 1970-01-01 18:36 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA512 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_512
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_224 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_224
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_256 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_256
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_384 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_384
Thu, 1970-01-01 18:36 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA512 in plugin 'gmp' has unmet dependency: HASHER:HASH_SHA3_512
Thu, 1970-01-01 18:36 00[LIB] feature PRF:PRF_HMAC_MD5 in plugin 'hmac' has unmet dependency: HASHER:HASH_MD5
Thu, 1970-01-01 18:36 00[LIB] feature SIGNER:HMAC_MD5_96 in plugin 'hmac' has unmet dependency: HASHER:HASH_MD5
Thu, 1970-01-01 18:36 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Thu, 1970-01-01 18:36 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Thu, 1970-01-01 18:36 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
Thu, 1970-01-01 18:36 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Thu, 1970-01-01 18:36 00[CFG] loading crls from '/etc/ipsec.d/crls'
Thu, 1970-01-01 18:36 00[CFG] loading secrets from '/etc/ipsec.secrets'
Thu, 1970-01-01 18:36 00[CFG] loaded IKE secret for 192.168.1.3 192.168.1.1
Thu, 1970-01-01 18:36 00[LIB] loaded plugins: charon random nonce aes shal sha2 pem pkcs1 curve25519 gmp
x509 revocation hmac stroke kernel-netlink socket-default updown
Thu, 1970-01-01 18:36 00 [LIB] unable to load 23 plugin features (23 due to unmet dependencies)
Thu, 1970-01-01 18:36 00 [JOB] spawning 16 worker threads
Thu, 1970-01-01 18:36 01 [LIB] created thread 01 [601]
Thu, 1970-01-01 18:36 02 [LIB] created thread 02 [602]
Thu, 1970-01-01 18:36 03 [LIB] created thread 03 [603]
Thu, 1970-01-01 18:36 04 [LIB] created thread 04 [604]
Thu, 1970-01-01 18:36 05 [LIB] created thread 05 [605]
Thu, 1970-01-01 18:36 06 [LIB] created thread 06 [606]
Thu, 1970-01-01 18:36 07 [LIB] created thread 07 [607]
Thu, 1970-01-01 18:36 08 [LIB] created thread 08 [608]
Thu, 1970-01-01 18:36 09 [LIB] created thread 09 [609]
Thu, 1970-01-01 18:36 10 [LIB] created thread 10 [610]
Thu, 1970-01-01 18:36 15 [LIB] created thread 15 [615]
Thu, 1970-01-01 18:36 16 [LIB] created thread 16 [616]
Thu, 1970-01-01 18:36 05 [CFG] received stroke: add connection 'tunnel'
Thu, 1970-01-01 18:36 05 [CFG] conn tunnel
Thu, 1970-01-01 18:36 05 [CFG] left=192.168.1.3
Thu, 1970-01-01 18:36 05 [CFG] leftauth=psk
Thu, 1970-01-01 18:36 05 [CFG] right=192.168.1.1
Thu, 1970-01-01 18:36 05 [CFG] rightauth=psk
Thu, 1970-01-01 18:36 05 [CFG] ike=aes256-sha2_256-modp1024!
Thu, 1970-01-01 18:36 05 [CFG] ah=sha256
Thu, 1970-01-01 18:36 05 [CFG] dpddelay=30
Thu, 1970-01-01 18:36 05 [CFG] dpdtimeout=120
Thu, 1970-01-01 18:36 05 [CFG] dpdaction=3
Thu, 1970-01-01 18:36 05 [CFG] sha256_96=no
Thu, 1970-01-01 18:36 05 [CFG] mediation=no
Thu, 1970-01-01 18:36 05 [CFG] keyexchange=ikev2
Thu, 1970-01-01 18:36 05 [KNL] 192.168.1.1 is not a local address or the interface is down
Thu, 1970-01-01 18:36 07 [CFG] received stroke: initiate 'tunnel'
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_VENDOR task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_INIT task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_NATD task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_CERT_PRE task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_AUTH task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_CERT_POST task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_CONFIG task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_AUTH_LIFETIME task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing IKE_MOBIKE task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> queueing CHILD_CREATE task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating new tasks
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_VENDOR task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_INIT task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_NATD task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_CERT_PRE task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_AUTH task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_CERT_POST task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_CONFIG task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating CHILD_CREATE task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_AUTH_LIFETIME task
Thu, 1970-01-01 18:36 07 [IKE] <tunnel|1> activating IKE_MOBIKE task
Thu, 1970-01-01 18:36 07 [LIB] <tunnel|1> size of DH secret exponent: 1022 bits
Thu, 1970-01-01 18:36 07 [CFG] <tunnel|1> sending supported signature hash algorithms: sha256 sha384 sha512 identity
Thu, 1970-01-01 18:36 09[ENC] <tunnel|1> parsed IKE_SA_INIT response 0 [ SA KE No(NATD_S_IP) N(NATD_D_IP) CERTREQ N(HASH_ALG) ]
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> received SIGNATURE_HASH_ALGORITHMS notify
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> selecting proposal:
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> proposal matches
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> received proposals: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/1024
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> received supported signature hash algorithms: sha256 sha384 sha512
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> received 1 cert requests for an unknown ca
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> reinitiating already active tasks
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> IKE_CERT_PRE task
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> IKE_AUTH task
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> proposing traffic selectors for us:
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> proposing traffic selectors for other:
Thu, 1970-01-01 18:36 09[CFG] <tunnel|1> 192.168.1.1/32
Thu, 1970-01-01 18:36 09[IKE] <tunnel|1> establishing CHILD_SA tunnel{1}
Thu, 1970-01-01 18:36 09[KNL] <tunnel|1> got SPI c393c2aa
Thu, 1970-01-01 18:36 09[ENC] <tunnel|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Thu, 1970-01-01 18:36 10[ENC] <tunnel|1> parsed IKE_AUTH response 1 [ IDr AUTH N(USE_TRANSP) SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP) N(ADD_4_ADDR) ]
Thu, 1970-01-01 18:36 10[IKE] <tunnel|1> authentication of '192.168.1.3' (myself) with pre-shared key successful
Thu, 1970-01-01 18:36 10[IKE] <tunnel|1> scheduling reauthentication in 2740s
Thu, 1970-01-01 18:36 10[CFG] <tunnel|1> selecting proposal:
Thu, 1970-01-01 18:36 10[CFG] <tunnel|1> proposal matches
Thu, 1970-01-01 18:36 10[CFG] <tunnel|1> selecting traffic selectors for us:
Thu, 1970-01-01 18:36 10[CFG] <tunnel|1> selecting traffic selectors for other:
Thu, 1970-01-01 18:36 10[CHD] <tunnel|1> using HMAC_SHA2_256_128 for integrity
Thu, 1970-01-01 18:36 10[CHD] <tunnel|1> adding inbound AH SA
Thu, 1970-01-01 18:36 10[CHD] <tunnel|1> SPI 0xc393c2aa, src 192.168.1.1 dst 192.168.1.3
Thu, 1970-01-01 18:36 10[KNL] <tunnel|1> adding SAD entry with SPI c393c2aa and reqid (1)
Thu, 1970-01-01 18:36 10[KNL] <tunnel|1> using integrity algorithm HMAC_SHA2_256_128 with key size 256
Thu, 1970-01-01 18:36 10 [KNL] <tunnel|1> using replay window of 32 packets
Thu, 1970-01-01 18:36 10 [KNL] <tunnel|1> HW offload: no
Thu, 1970-01-01 18:36 10 [CHD] <tunnel|1> adding outbound AH SA
Thu, 1970-01-01 18:36 10 [KNL] <tunnel|1> adding SAD entry with SPI c73405d0 and reqid {1}
Thu, 1970-01-01 18:36 10 [KNL] <tunnel|1> using integrity algorithm HMAC_SHA2_256_128 with key size 256
Thu, 1970-01-01 18:36 10 [KNL] <tunnel|1> using replay window of 0 packets
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> CHILD_SA tunnel{1} established with SPIs c393c2aa_i c73405d0_o and TS 192.168.1.1/32 === 192.168.1.3/32
Thu, 1970-01-01 18:36 10 [CHD] <tunnel|1> CHILD_SA tunnel{1} state change: INSTALLING => INSTALLED
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> received AUTH_LIFETIME of 3012s, scheduling reauthentication in 2472s
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> peer supports MOBIKE
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> got additional MOBIKE peer address: 10.185.176.111
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> activating new tasks
Thu, 1970-01-01 18:36 10 [IKE] <tunnel|1> nothing to initiate

History
#1 - 20.04.2020 12:50 - Noel Kuntze
- Category set to configuration
- Status changed from New to Feedback
- Assignee set to Noel Kuntze

The peer probably uses the draft version of HMAC-SHA256, which uses 96 bit truncation. You can switch to that version specifically by setting sha256_96=yes in the conn.

#2 - 20.04.2020 13:12 - Ayman Bahouth
Noel Kuntze wrote:

The peer probably uses the draft version of HMAC-SHA256, which uses 96 bit truncation. You can switch to that version specifically by setting sha256_96=yes in the conn.

I'm sure it's not the sha256_96 configuration because IPSec manual configuration (HMAC-SHA256) works fine. I also tried it sha256_96=yes, it doesn't work.

#3 - 20.04.2020 13:29 - Noel Kuntze
Did you restart the daemon or what did you do? Also, does /proc/net/xfrm_stat exist? If so, please provide its output after you tested it.

#4 - 20.04.2020 14:01 - Ayman Bahouth
Noel Kuntze wrote:

Did you restart the daemon or what did you do? Also, does /proc/net/xfrm_stat exist? If so, please provide its output after you tested it.

Yes, I restarted the daemon.
/proc/net/xfrm_stat does not exist.

#5 - 20.04.2020 14:02 - Noel Kuntze
Okay, then there's no way to figure out what exactly the problem is from the kernel's point of view. Sorry.

#6 - 20.04.2020 14:17 - Ayman Bahouth
I enabled XFRM_STATS in linux kernel config:

```bash
# cat /proc/net/xfrm_stat
XfrmInError 0
XfrmInBufferSize 0
XfrmInHdrError 0
```
XfrmInNoStates 0
XfrmInStateProtoError 3
XfrmInStateModeError 0
XfrmInStateSeqError 0
XfrmInStateExpired 0
XfrmInStateMismatch 0
XfrmInStateInvalid 0
XfrmInTmplMismatch 0
XfrmInNoPols 0
XfrmInPolBlock 0
XfrmInPolError 0
XfrmOutError 0
XfrmOutBundleGenError 0
XfrmOutBundleCheckError 0
XfrmOutNoStates 0
XfrmOutStateProtoError 0
XfrmOutStateModeError 0
XfrmOutStateSeqError 0
XfrmOutStateExpired 0
XfrmOutPolBlock 0
XfrmOutPolDead 0
XfrmOutPolError 0
XfrmFwdHdrError 0
XfrmOutStateInvalid 0
XfrmAcquireError 0

#7 - 20.04.2020 16:21 - Noel Kuntze

XfrmInStateProtoError 3

From https://github.com/torvalds/linux/blob/master/Documentation/networking/xfrm_proc.txt:

XfrmInStateProtoError:
  Transformation protocol specific error
e.g. SA key is wrong

-> https://github.com/torvalds/linux/blob/master/net/xfrm/xfrm_input.c#L507

Looks like crypto generally fails. You can dump the AH traffic with tcpdump, save the keys and SPIs from the SAD, put that all in wireshark and check what it says about that. It might be able to tell you a little bit more than the kernel possibly logs (which as you can see by the linked code isn't all that much).

#8 - 21.04.2020 17:51 - Ayman Bahouth

Noel Kuntze wrote:

XfrmInStateProtoError 3

From https://github.com/torvalds/linux/blob/master/Documentation/networking/xfrm_proc.txt:

[...]
-> https://github.com/torvalds/linux/blob/master/net/xfrm/xfrm_input.c#L507

Looks like crypto generally fails. You can dump the AH traffic with tcpdump, save the keys and SPIs from the SAD, put that all in wireshark and check what it says about that. It might be able to tell you a little bit more than the kernel possibly logs (which as you can see by the linked code isn't all that much).

Thanks a lot for your help.
I changed "ah=sha256" to "ah=sha2_256" and it worked.
I managed to make it work with "sha256_96=yes".

#9 - 21.04.2020 17:57 - Noel Kuntze

- Status changed from Feedback to Closed
- Resolution set to No change required

Great!