pfSense - Bug #9646

OpenSSL 1.1.1 does not list engines for AES-NI or BSD crypto

07/24/2019 07:25 AM - Vance Emerson

Status:	Resolved	**Start date:**	07/24/2019
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	100%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Affected Version:	2.5.x	**Affected Architecture:**	

Description

Cannot select BSD Crypto Device under OPENVPN clients - Hardware Crypto, it only has No Hardware Crypto Acceleration.

History

#1 - 07/24/2019 09:47 AM - Jim Pingle

- Subject changed from Cannot select Hardware Crypto under OPENVPN client to OpenSSL 1.1.1 does not list engines for AES-NI or BSD crypto

- Category changed from OpenVPN to Operating System

- Priority changed from Low to Normal

I can confirm this, but it is not specific to OpenVPN.

OpenSSL 1.1.1 doesn't list AES-NI or the BSD crypto dev, even on stock FreeBSD 12, with the appropriate kernel modules loaded:

```
: kldstat
Id Refs Address                Size Name
 1   32 0xffffffff80200000  3126450 kernel
 2    1 0xffffffff83327000   3aa890 zfs.ko
 3    2 0xffffffff836d2000     a4f0 opensolaris.ko
 4    1 0xffffffff83811000      fe0 cpuctl.ko
 5    1 0xffffffff83812000     7ec0 aesni.ko
 6    1 0xffffffff8381a000     3110 cryptodev.ko
 7    1 0xffffffff8381e000      b98 coretemp.ko
 8    1 0xffffffff8381f000    11308 dummynet.ko
```

```
: openssl engine -t -c
(rdrand) Intel RDRAND engine
 [RAND]
     [ available ]
(dynamic) Dynamic engine loading support
     [ unavailable ]
```

```
: openssl engine -t -c -pre DUMP_INFO
(rdrand) Intel RDRAND engine
[Failure]: DUMP_INFO
34370957312:error:260AB089:engine routines:ENGINE_ctrl_cmd_string:invalid cmd name:/build/factory-crossbuild-m
aster/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_ctrl.c:255:
 [RAND]
     [ available ]
(dynamic) Dynamic engine loading support
[Failure]: DUMP_INFO
34370957312:error:260AC089:engine routines:int_ctrl_helper:invalid cmd name:/build/factory-crossbuild-master/p
fSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_ctrl.c:87:
34370957312:error:260AB089:engine routines:ENGINE_ctrl_cmd_string:invalid cmd name:/build/factory-crossbuild-m
aster/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_ctrl.c:255:
     [ unavailable ]
```

I updated the subject to better reflect the problem.

#2 - 10/29/2019 02:36 AM - Viktor Gurov

discussion and patch in freebsd mailing list:
https://lists.freebsd.org/pipermail/freebsd-current/2018-December/072452.html

#3 - 10/29/2019 07:14 AM - Renato Botelho

- Status changed from New to Feedback

- Assignee set to Renato Botelho

- % Done changed from 0 to 100

I've cherry-picked that patch to 2.5.0. Thanks for pointing that out

#4 - 10/30/2019 03:16 PM - Renato Botelho

- Status changed from Feedback to In Progress

Patch reverted after we see problems with it applied

#5 - 10/30/2019 03:17 PM - Jim Pingle

For the sake of those Googling or searching for the error, the following message was showing up in the logs and on the console with this patch applied:

```
Could not open /dev/crypto: No such file or directory
```

#6 - 11/18/2019 12:47 AM - Ronald Schellberg

This issue caught my eye, so I enabled the devcrypto patch on my version based on 12.1. On my VM, after loading the cryptodev.ko module, i get:

```
: openssl engine -t -c -pre DUMP_INFO
(devcrypto) /dev/crypto engine
[Failure]: DUMP_INFO
34371006464:error:260AB089:engine routines:ENGINE_ctrl_cmd_string:invalid cmd name:/root/pfsense/tmp/FreeBSD-s
rc/crypto/openssl/crypto/engine/eng_ctrl.c:255:
     [ available ]
(rdrand) Intel RDRAND engine
[Failure]: DUMP_INFO
34371006464:error:260AB089:engine routines:ENGINE_ctrl_cmd_string:invalid cmd name:/root/pfsense/tmp/FreeBSD-s
rc/crypto/openssl/crypto/engine/eng_ctrl.c:255:
 [RAND]
     [ available ]
(dynamic) Dynamic engine loading support
[Failure]: DUMP_INFO
34371006464:error:260AC089:engine routines:int_ctrl_helper:invalid cmd name:/root/pfsense/tmp/FreeBSD-src/cryp
to/openssl/crypto/engine/eng_ctrl.c:87:
34371006464:error:260AB089:engine routines:ENGINE_ctrl_cmd_string:invalid cmd name:/root/pfsense/tmp/FreeBSD-s
rc/crypto/openssl/crypto/engine/eng_ctrl.c:255:
     [ unavailable ]
```

My status page indicates that --->AES-NI CPU Crypto: Yes (active)

Running the following I get:

```
: openssl speed -engine rdrand -evp aes-128-cbc
engine "rdrand" set.
Doing aes-128-cbc for 3s on 16 size blocks: 74650924 aes-128-cbc's in 3.00s
Doing aes-128-cbc for 3s on 64 size blocks: 20569026 aes-128-cbc's in 3.10s
Doing aes-128-cbc for 3s on 256 size blocks: 5410274 aes-128-cbc's in 3.09s
Doing aes-128-cbc for 3s on 1024 size blocks: 1331442 aes-128-cbc's in 3.04s
Doing aes-128-cbc for 3s on 8192 size blocks: 158118 aes-128-cbc's in 3.05s
Doing aes-128-cbc for 3s on 16384 size blocks: 85998 aes-128-cbc's in 3.01s
OpenSSL 1.1.1d-freebsd  10 Sep 2019
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(int) aes(partial) idea(int) blowfish(ptr)
compiler: clang
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-cbc     398138.26k   424436.93k   447686.51k   448624.08k   424037.70k   468443.84k
: openssl speed -engine devcrypto -evp aes-128-cbc
engine "devcrypto" set.
Doing aes-128-cbc for 3s on 16 size blocks: 74953526 aes-128-cbc's in 3.01s
Doing aes-128-cbc for 3s on 64 size blocks: 21202916 aes-128-cbc's in 3.09s
Doing aes-128-cbc for 3s on 256 size blocks: 5184930 aes-128-cbc's in 3.01s
Doing aes-128-cbc for 3s on 1024 size blocks: 1358597 aes-128-cbc's in 3.02s
Doing aes-128-cbc for 3s on 8192 size blocks: 164037 aes-128-cbc's in 3.05s
Doing aes-128-cbc for 3s on 16384 size blocks: 82463 aes-128-cbc's in 3.00s
OpenSSL 1.1.1d-freebsd  10 Sep 2019
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(int) aes(partial) idea(int) blowfish(ptr)
compiler: clang
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-cbc     398713.82k   438621.94k   441298.15k   460139.60k   439911.15k   450357.93k
```

#7 - 11/19/2019 04:57 AM - yon Liu

https://forum.netgate.com/topic/148171/openvpn-no-option-for-aes-ni/6

openssl speed -engine rdrand -evp aes-128-gcm
invalid engine "rdrand"
34370957312:error:25066067:DSO support routines:dlfcn_load:could not load the shared library:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/dso/dso_dlfcn.c:117:filename(/usr/lib/engines/rdrand.so): Cannot open "/usr/lib/engines/rdrand.so"
34370957312:error:25070067:DSO support routines:DSO_load:could not load the shared library:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/dso/dso_lib.c:162:

34370957312:error:260B6084:engine routines:dynamic_load:dso not found:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_dyn.c:414:
34370957312:error:2606A074:engine routines:ENGINE_by_id:no such engine:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_list.c:334:id=rdrand
34370957312:error:25066067:DSO support routines:dlfcn_load:could not load the shared library:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/dso/dso_dlfcn.c:117:filename(librdrand.so): Shared object "librdrand.so" not found, required by "openssl"
34370957312:error:25070067:DSO support routines:DSO_load:could not load the shared library:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/dso/dso_lib.c:162:
34370957312:error:260B6084:engine routines:dynamic_load:dso not found:/build/ce-crossbuild-master/pfSense/tmp/FreeBSD-src/crypto/openssl/crypto/engine/eng_dyn.c:414:
Doing aes-128-gcm for 3s on 16 size blocks: 42700620 aes-128-gcm's in 3.05s
Doing aes-128-gcm for 3s on 64 size blocks: 32651171 aes-128-gcm's in 3.06s
Doing aes-128-gcm for 3s on 256 size blocks: 14878766 aes-128-gcm's in 3.04s
Doing aes-128-gcm for 3s on 1024 size blocks: 4697224 aes-128-gcm's in 3.02s
Doing aes-128-gcm for 3s on 8192 size blocks: 619970 aes-128-gcm's in 3.02s
Doing aes-128-gcm for 3s on 16384 size blocks: 309228 aes-128-gcm's in 3.01s
OpenSSL 1.1.1a-freebsd 20 Nov 2018
built on: reproducible build, date unspecified
options:bn(64,64) rc4(8x,int) des(int) aes(partial) idea(int) blowfish(ptr)
compiler: clang
The 'numbers' are in 1000s of bytes per second processed.
type 16 bytes 64 bytes 256 bytes 1024 bytes 8192 bytes 16384 bytes
aes-128-gcm 223659.51k 682342.84k 1253335.23k 1595011.77k 1679807.91k 1684410.70k

#8 - 11/19/2019 09:15 AM - Ronald Schellberg

On my beyond 2.5 version (12.1 based), the devcryto patch applied, and after the devcrypto.ko is loaded:

```
:openssl speed -engine rdrand -evp aes-128-gcm
engine "rdrand" set.
Doing aes-128-gcm for 3s on 16 size blocks: 41833147 aes-128-gcm's in 3.03s
Doing aes-128-gcm for 3s on 64 size blocks: 30990552 aes-128-gcm's in 3.01s
Doing aes-128-gcm for 3s on 256 size blocks: 16462906 aes-128-gcm's in 3.01s
Doing aes-128-gcm for 3s on 1024 size blocks: 6288923 aes-128-gcm's in 3.09s
Doing aes-128-gcm for 3s on 8192 size blocks: 1029772 aes-128-gcm's in 3.09s
Doing aes-128-gcm for 3s on 16384 size blocks: 499340 aes-128-gcm's in 3.00s
OpenSSL 1.1.1d-freebsd  10 Sep 2019
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(int) aes(partial) idea(int) blowfish(ptr)
compiler: clang
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-gcm     220810.01k   659414.55k  1401185.72k  2086839.79k  2726753.04k  2727062.19k
```

No errors reported and of course Intel AES-NI support

#9 - 10/01/2020 06:31 AM - Renato Botelho

- Status changed from In Progress to Feedback

It's working as expected on recent snapshots

#10 - 10/06/2020 10:45 AM - Steve Beaver

- Status changed from Feedback to Resolved