strongSwan - Feature #508

Add generic configuration features to charon-cmd

03.02.2014 13:04 - Yves-Alexis Perez

Status:	Closed	**Start date:**	03.02.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	charon-cmd		
Target version:	5.1.2		
Resolution:	Fixed		

Description

Hi,

right now charon-cmd is only configurable through its command line interface, and that doesn't enable ciphers configuration, which breaks some setups.

For example I use on my responder:

esp = aes128gcm16-ecp384,aes256gcm16-ecp384,aes256-sha256-ecp384,aes256-sha256-modp2048!
ike = aes256gcm16-sha256-ecp384,aes256gcm16-sha256-modp2048,aes256-sha256-modp2048!

and trying to connect gives:

```
09[IKE] peer didn't accept DH group MODP_1024, it requested ECP_384
[...]
14[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
14[IKE] received AUTHENTICATION_FAILED notify error
```

and on the responder:

```
Feb  3 12:59:52 molly charon: 04[IKE] DH group MODP_1024 inacceptable, requesting ECP_384
Feb  3 12:59:52 molly charon: 04[ENC] generating IKE_SA_INIT response 0 [ N(INVAL_KE) ]
```

(I'm not too sure why charon-cmd can't provide ECP_384)

Anyway, that's the case for ciphers but I guess other configurations options might be worth having even in charon-cmd.

Associated revisions

Revision fe40c475 - 06.02.2014 15:58 - Martin Willi

Merge branch 'cmd-proposals'

Introduce --ike/esp/ah-proposal options to offer custom proposals, and requests
an IPv6 virtual IP if an IPv6 --remote-ts is given.

Fixes #508.

History

#1 - 04.02.2014 11:02 - Martin Willi

- Category set to charon-cmd

- Assignee set to Martin Willi

Hi Yves-Alexis,

> right now charon-cmd is only configurable through its command line interface, and that doesn't enable ciphers configuration, which breaks some setups.

This has been a clear design decision: We don't want any dependency on ipsec.conf and it's parser in starter; charon-cmd should as be simple as possible.

```
09[IKE] peer didn't accept DH group MODP_1024, it requested ECP_384
[...]
14[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
14[IKE] received AUTHENTICATION_FAILED notify error
```

I don't think these two errors are directly related. Guessing a wrong DH group in IKEv2 can happen. If the proposal is acceptable, the responder should request a different group, and the initiator should retry with that group.

> I'm not too sure why charon-cmd can't provide ECP_384

charon-cmd currently uses the default IKE proposal, which includes all supported DH groups. Most like you don't have the openssl plugin loaded in charon-cmd?

> Anyway, that's the case for ciphers but I guess other configurations options might be worth having even in charon-cmd.

There is no "generic" way to add options, but it certainly might make sense to add one or the other. I'll take a closer look to what it takes to add proposal options to charon-cmd.

Regards
Martin

#2 - 04.02.2014 11:24 - Yves-Alexis Perez

Martin Willi wrote:

> Hi Yves-Alexis,
>
>> right now charon-cmd is only configurable through its command line interface, and that doesn't enable ciphers configuration, which breaks some setups.
>
> This has been a clear design decision: We don't want any dependency on ipsec.conf and it's parser in starter; charon-cmd should as be simple as possible.

Actually I've discussed with Tobias yesterday on irc and he mentionned such a possibility, that's why I added it here.

> [...]
>
> I don't think these two errors are directly related. Guessing a wrong DH group in IKEv2 can happen. If the proposal is acceptable, the responder should request a different group, and the initiator should retry with that group.

Maybe I'm confused then. But indeed it doesn't work here (maybe for other reasons), and in any case having a way to specify (hard) requirements on ciphers would be nice.

>> I'm not too sure why charon-cmd can't provide ECP_384
>
> charon-cmd currently uses the default IKE proposal, which includes all supported DH groups. Most like you don't have the openssl plugin loaded in charon-cmd?

It looks loaded here. Here's the complete log from charon-cmd:

```
00[LIB] dropped capabilities, running as uid 0, gid 0
00[DMN] Starting charon-cmd IKE client (strongSwan 5.1.1, Linux 3.12-1-amd64, x86_64)
00[LIB] loaded plugins: charon-cmd aes rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1
 pkcs7 pkcs8 pkcs12 sshkey pem openssl fips-prf gmp agent xcbc hmac gcm kernel-netlink resolve socket-default
00[LIB] unable to load 4 plugin features (4 due to unmet dependencies)
00[JOB] spawning 16 worker threads
06[IKE] initiating IKE_SA cmd[1] to <responder>
06[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
06[NET] sending packet: from 0.0.0.0[40019] to <responder>[4500] (696 bytes)
09[NET] received packet: from <responder>[4500] to <initiator>[40019] (38 bytes)
09[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
09[IKE] peer didn't accept DH group MODP_1024, it requested ECP_384
09[IKE] initiating IKE_SA cmd[1] to <responder>
09[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
09[NET] sending packet: from <initiator>[40019] to <responder>[4500] (664 bytes)
10[NET] received packet: from <responder>[4500] to <initiator>[40019] (272 bytes)
10[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH) ]
10[IKE] authentication of 'corsac' (myself) with RSA signature successful
```

```
10[IKE] establishing CHILD_SA cmd
10[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) AUTH CPRQ(ADDR DNS) SA TSi TSr N(MOBIKE_SUP) N(ADD
_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
10[NET] sending packet: from <initiator>[42547] to <responder>[4500] (547 bytes)
14[NET] received packet: from <responder>[4500] to <initiator>[42547] (65 bytes)
14[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
14[IKE] received AUTHENTICATION_FAILED notify error
```

It seems that it retries IKE_SA_INIT (maybe with ECP_384), but then again fails, not too sure why. I'll investigate, but it looks unrelated, sorry for the noise.

> > Anyway, that's the case for ciphers but I guess other configurations options might be worth having even in charon-cmd.
>
> There is no "generic" way to add options, but it certainly might make sense to add one or the other. I'll take a closer look to what it takes to add proposal options to charon-cmd.

Thanks!

#3 - 04.02.2014 11:37 - Yves-Alexis Perez

Actually, there was indeed a mistake on the responder side, but when fixing the error I still get:

On the initiator (complete log)

```
00[LIB] dropped capabilities, running as uid 0, gid 0
00[DMN] Starting charon-cmd IKE client (strongSwan 5.1.1, Linux 3.12-1-amd64, x86_64)
00[LIB] loaded plugins: charon-cmd aes rc2 sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkcs1
 pkcs7 pkcs8 pkcs12 sshkey pem openssl fips-prf gmp agent xcbc hmac gcm kernel-netlink resolve socket-default
00[LIB] unable to load 4 plugin features (4 due to unmet dependencies)
00[JOB] spawning 16 worker threads
07[IKE] initiating IKE_SA cmd[1] to <responder>
07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
07[NET] sending packet: from 0.0.0.0[33972] to <responder>[4500] (696 bytes)
09[NET] received packet: from <responder>[4500] to <initiator>[33972] (38 bytes)
09[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
09[IKE] peer didn't accept DH group MODP_1024, it requested ECP_384
09[IKE] initiating IKE_SA cmd[1] to <responder>
09[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
09[NET] sending packet: from <initiator>[33972] to <responder>[4500] (664 bytes)
05[NET] received packet: from <responder>[4500] to <initiator>[33972] (272 bytes)
05[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH) ]
05[IKE] authentication of <id> (myself) with RSA signature successful
05[IKE] establishing CHILD_SA cmd
05[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) AUTH CPRQ(ADDR DNS) SA TSi TSr N(MOBIKE_SUP) N(ADD
_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
05[NET] sending packet: from <initiator>[44363] to <responder>[4500] (547 bytes)
10[NET] received packet: from <responder>[4500] to <initiator>[44363] (501 bytes)
10[ENC] parsed IKE_AUTH response 1 [ IDr AUTH CPRP(ADDR DNS DNS6) N(AUTH_LFT) N(MOBIKE_SUP) N(ADD_4_ADDR) N(AD
D_4_ADDR) N(ADD_6_ADDR) N(NO_PROP) ]
10[CFG] no issuer certificate found for "C=FR, O=example.com, CN=hostname"
10[CFG]   using trusted certificate "C=FR, O=example.com, CN=hostname"
10[IKE] authentication of 'C=FR, O=example.com, CN=hostname' with RSA signature successful
10[IKE] IKE_SA cmd[1] established between <initiator>[<id>]...<responder>[C=FR, O=example.com, CN=hostname]
10[IKE] scheduling rekeying in 35659s
10[IKE] maximum IKE_SA lifetime 36259s
10[IKE] installing DNS server <dns1> via resolvconf
10[IKE] installing DNS server <dns2> via resolvconf
10[IKE] installing new virtual IP <ip>
10[IKE] received NO_PROPOSAL_CHOSEN notify, no CHILD_SA built
10[IKE] failed to establish CHILD_SA, keeping IKE_SA
10[IKE] received AUTH_LIFETIME of 28603s, scheduling reauthentication in 28003s
10[IKE] peer supports MOBIKE
00[IKE] deleting IKE_SA cmd[1] between <initiator>[<id>]...<responder>[C=FR, O=example.com, CN=hostname]
00[IKE] sending DELETE for IKE_SA cmd[1]
00[ENC] generating INFORMATIONAL request 2 [ D ]
00[NET] sending packet: from <initiator>[44363] to <responder>[4500] (65 bytes)
```

On the responder (excerpt)

```
Feb  4 11:27:20 <hostname> charon: 05[CFG] received proposals: ESP:AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CB
C/BLOWFISH_CBC_256/HMAC_SHA1_96/AES_XCBC_96/HMAC_MD5_96/NO_EXT_SEQ
Feb  4 11:27:20 <hostname> charon: 05[CFG] configured proposals: ESP:AES_GCM_16_128/ECP_384/NO_EXT_SEQ, ESP:AE
S_GCM_16_256/ECP_384/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA2_256_128/ECP_384/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SH
```

```
A2_256_128/MODP_2048/NO_EXT_SEQ
Feb  4 11:27:20 <hostname> charon: 05[IKE] no acceptable proposal found
Feb  4 11:27:20 <hostname> charon: 05[IKE] failed to establish CHILD_SA, keeping IKE_SA
```

So it looks like IKE ciphers eventually match, but not ESP ones: GCM is not part of the proposal, neither are HMAC_SHA2 nor any DH groups (EC_384 or MODP_2048).

Might it be worth cloning the feature request to a bug request about the “default” esp proposals in charon-cmd?

#4 - 04.02.2014 11:49 - Martin Willi

- Status changed from New to Feedback

> So it looks like IKE ciphers eventually match, but not ESP ones: GCM is not part of the proposal, neither are HMAC_SHA2 nor any DH groups (EC_384 or MODP_2048).

Because there is no proper way to ask the kernel for supported algorithms, the default is rather conservative for ESP proposals. It does not include anything missing from 2.6.x kernels, so no GCM or SHA2. Further, it does not use PFS for CHILD_SA rekeying, therefore no DH group.

Anyway, you may try the last four commits of the cmd-proposals branch. It adds (among others) an --esp-proposal option to define a custom ESP proposal; repeat the option to define multiple proposals.

http://git.strongswan.org/?p=strongswan.git;a=shortlog;h=refs/heads/cmd-proposals

Regards
Martin

#5 - 04.02.2014 14:38 - Yves-Alexis Perez

Not sure if it's related to that branch but I get an error when building:

```
make[3]: Entering directory `/home/corsac/debian/strongswan/upstream/src/libstrongswan'
\
        (cd ./asn1/ && /usr/bin/perl oid.pl)
\
         -N proposal_get_token_static -m 10 -C -G -c -t -D < \
                                       ./crypto/proposal/proposal_keywords_static.txt > crypto/proposal/propo
sal_keywords_static.c
/bin/bash: line 1: -N: command not found
make[3]: *** [crypto/proposal/proposal_keywords_static.c] Error 127
make[3]: Leaving directory `/home/corsac/debian/strongswan/upstream/src/libstrongswan'
make[2]: *** [all-recursive] Error 1
make[2]: Leaving directory `/home/corsac/debian/strongswan/upstream/src'
make[1]: *** [all-recursive] Error 1
make[1]: Leaving directory `/home/corsac/debian/strongswan/upstream'
make: *** [all] Error 2
```

I can re-type make after that, but then later I get:

```
make[4]: Entering directory `/home/corsac/debian/strongswan/upstream/src/starter'
depbase=`echo parser.o | sed 's|[^/]*$|.deps/&|;s|\.o$||'`;\
    gcc -DHAVE_CONFIG_H -I. -I../..  -I../../src/include -I../../src/libstrongswan -I../../src/libhydra -I../.
./src/stroke -DIPSEC_DIR=\"/usr/local/libexec/ipsec\" -DIPSEC_CONFDIR=\"/usr/local/etc\" -DIPSEC_PIDDIR=\"/var
/run\" -DIPSEC_EAPDIR=\"\" -DIPSEC_SCRIPT=\"ipsec\" -DDEV_RANDOM=\"/dev/random\" -DDEV_URANDOM=\"/dev/urandom\
" -DPLUGINS=\""kernel-netlink\"" -DDEBUG -DSTART_CHARON -DLOAD_WARNING -DGENERATE_SELFCERT   -g -O2 -Wall -Wno
-format -Wno-format-security -Wno-pointer-sign -include /home/corsac/debian/strongswan/upstream/config.h -MT p
arser.o -MD -MP -MF $depbase.Tpo -c -o parser.o parser.c &&\
    mv -f $depbase.Tpo $depbase.Po
/bin/bash ../../ylwrap lexer.l .c lexer.c -- :
depbase=`echo lexer.o | sed 's|[^/]*$|.deps/&|;s|\.o$||'`;\
    gcc -DHAVE_CONFIG_H -I. -I../..  -I../../src/include -I../../src/libstrongswan -I../../src/libhydra -I../.
./src/stroke -DIPSEC_DIR=\"/usr/local/libexec/ipsec\" -DIPSEC_CONFDIR=\"/usr/local/etc\" -DIPSEC_PIDDIR=\"/var
/run\" -DIPSEC_EAPDIR=\"\" -DIPSEC_SCRIPT=\"ipsec\" -DDEV_RANDOM=\"/dev/random\" -DDEV_URANDOM=\"/dev/urandom\
" -DPLUGINS=\""kernel-netlink\"" -DDEBUG -DSTART_CHARON -DLOAD_WARNING -DGENERATE_SELFCERT   -g -O2 -Wall -Wno
-format -Wno-format-security -Wno-pointer-sign -include /home/corsac/debian/strongswan/upstream/config.h -MT l
exer.o -MD -MP -MF $depbase.Tpo -c -o lexer.o lexer.c &&\
    mv -f $depbase.Tpo $depbase.Po
gcc: error: lexer.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
make[4]: *** [lexer.o] Error 4
make[4]: Leaving directory `/home/corsac/debian/strongswan/upstream/src/starter'
```

```
make[3]: *** [all] Error 2
make[3]: Leaving directory `/home/corsac/debian/strongswan/upstream/src/starter'
make[2]: *** [all-recursive] Error 1
make[2]: Leaving directory `/home/corsac/debian/strongswan/upstream/src'
make[1]: *** [all-recursive] Error 1
make[1]: Leaving directory `/home/corsac/debian/strongswan/upstream'
make: *** [all] Error 2
make  121,31s user 10,53s system 89% cpu 2:27,46 total
```

It might just be some missing deps, but as ./configure didn't detect it…

#6 - 04.02.2014 15:09 - Yves-Alexis Perez

Ok, completely unrelated, Tobias pointed me to the missing bits.

#7 - 04.02.2014 15:37 - Yves-Alexis Perez

It seems to work just fine with:

sudo -E ./src/charon-cmd/charon-cmd --host <hostname> --identity <id> --agent --cert /etc/ipsec.d/certs/hostname.der --remote-identity "C=FR, O=example.org, CN=<hostname>" --esp-proposal aes128gcm16-ecp384

(remote-identity is because I've not yet switched to a pure pubkey setup on the responder)

Many thanks for this. I guess it's a bit late for a merge for 5.1.2 but I guess it might be possible for 5.2?

#8 - 04.02.2014 15:46 - Yves-Alexis Perez

Just another quick question. Is there a way to ask for dual-stack, like (ipsec.conf syntax):

rightsubnet=0.0.0.0/0,::0/0
leftsourceip=%config4,%config6

#9 - 04.02.2014 16:51 - Martin Willi

> Many thanks for this. I guess it's a bit late for a merge for 5.1.2 but I guess it might be possible for 5.2?

As the release candidate for 5.1.2 is still pending we'll consider merging that branch.

> Is there a way to ask for dual-stack, like (ipsec.conf syntax):

By using the --remote-ts option, you could ask for both IPv4 and IPv6 connectivity (*--remote-ts 0.0.0.0/0 --remote-ts ::/0*). Up until now only an IPv4 virtual IP was requested. I've tried to fix that with the latest commit in http://git.strongswan.org/?p=strongswan.git;a=shortlog;h=refs/heads/cmd-proposals .

Regards
Martin

#10 - 04.02.2014 17:15 - Yves-Alexis Perez

Martin Willi wrote:

> > Many thanks for this. I guess it's a bit late for a merge for 5.1.2 but I guess it might be possible for 5.2?
>
> As the release candidate for 5.1.2 is still pending we'll consider merging that branch.
>
> > Is there a way to ask for dual-stack, like (ipsec.conf syntax):
>
> By using the --remote-ts option, you could ask for both IPv4 and IPv6 connectivity (*--remote-ts 0.0.0.0/0 --remote-ts ::/0*). Up until now only an IPv4 virtual IP was requested. I've tried to fix that with the latest commit in http://git.strongswan.org/?p=strongswan.git;a=shortlog;h=refs/heads/cmd-proposals .

And it seems to work fine:

```
10[IKE] CHILD_SA cmd{1} established with SPIs ca31c4bf_i c61fcb03_o and TS 192.168.0.129/32 xxxx:xxxx:xxxx:xxxx::xxxx/128 === 0.0.0.0/0 ::/0
```

Many thanks for your quick work!

#11 - 06.02.2014 16:04 - Martin Willi

- Status changed from Feedback to Closed

- Target version set to 5.1.2

- Resolution set to Fixed

> And it seems to work fine:

Thanks for testing, merged to master.

Regards
Martin