Issues

digest algorithm too weak

```
error=CA signature digest algorithm too weak:
```

Solution: upgrade server CA to use at least SHA256

Workaround:

client.conf

```
# to work around the cert too weak issue
tls-cipher "DEFAULT:@SECLEVEL=0"
```

And from man 3 SSL_CTX_set_security_level:

```
Level 0

    Everything is permitted. This retains compatibility with previous
versions of OpenSSL.

Level 1

    The security level corresponds to a minimum of 80 bits of security. Any
parameters offering below 80 bits of security are excluded. As a result RSA,
DSA and DH keys shorter than 1024 bits and ECC keys shorter than 160 bits
are prohibited. All export cipher suites are prohibited since they all offer
less than 80 bits of security. SSL version 2 is prohibited. Any cipher suite
using MD5 for the MAC is also prohibited.
```

/sbin/resolvconf: 31: kill: Operation not permitted

```
/sbin/resolvconf: 31: kill: Operation not permitted
```

Reason: openresolv: resolvconf fails if called from openvpn during system start with "kill: Operation not permitted"

Problematic script: `/lib/resolvconf/libc.d/avahi-daemon`

IP packet with unknown IP version=15 seen

LZO compression is disabled on server but used on client.

Solution:

explicitly disable `comp-lzo no` on server.