Alternative clients for VPN access

Warning: for these alternative clients, no support can be provided by “Divisione ISI”.

Linux with Network Manager (like Ubuntu, Debian)

AnyConnect compatible connection method

NOTE: instructions were made on an Italian language system, images and English translations could be not accurate. Feel free to write us corrections.

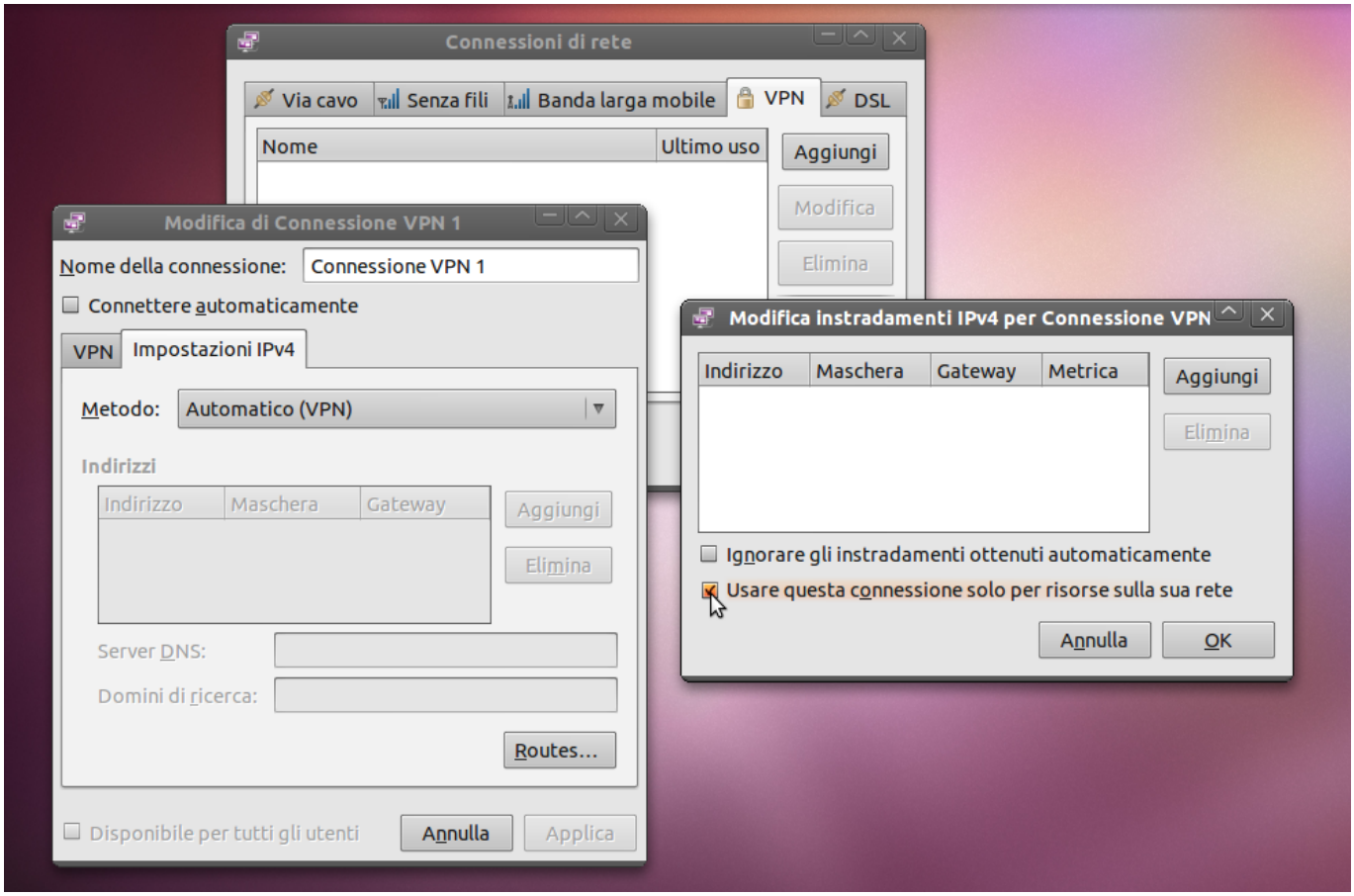
These instructions are verified on a Ubuntu 10.10 installation.

As an alternative to the official Cisco client, the package *openconnect* can be used and integrated in the Network Manager with the package *network-manager-openconnect* (install with the preferred package manager). Sometimes a logout/login or a reboot is required to enable correctly the component.

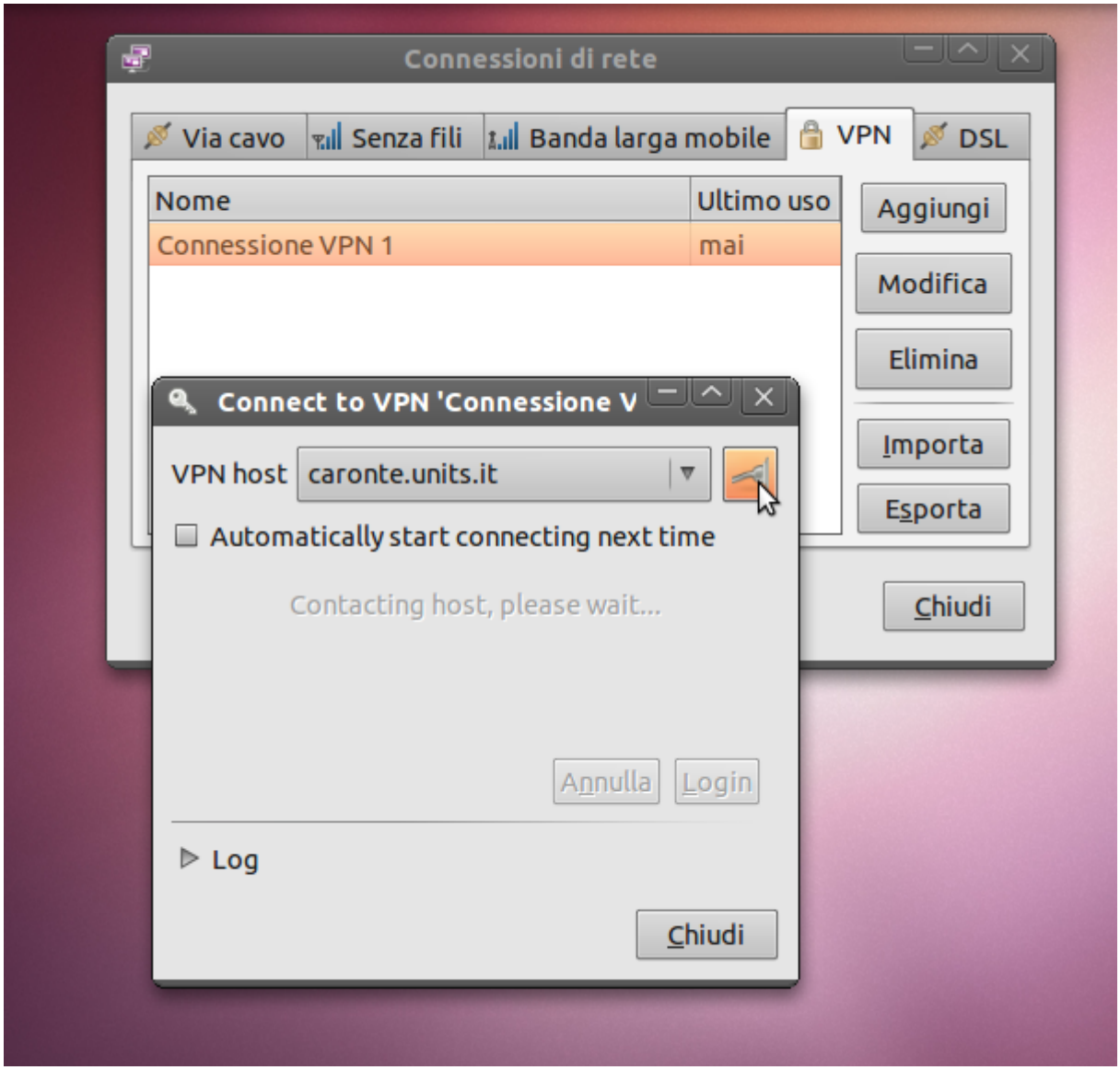
At this point in the connection manager window of the *Network Manager* (right click on the Network Manager icon in the menu bar → Manage connections…), in the *VPN* tab is possible to create the connection pressing “Add…” button.

1) In the window that will appear, select the type “Cisco AnyConnect compatible VPN” and press “Create…”:

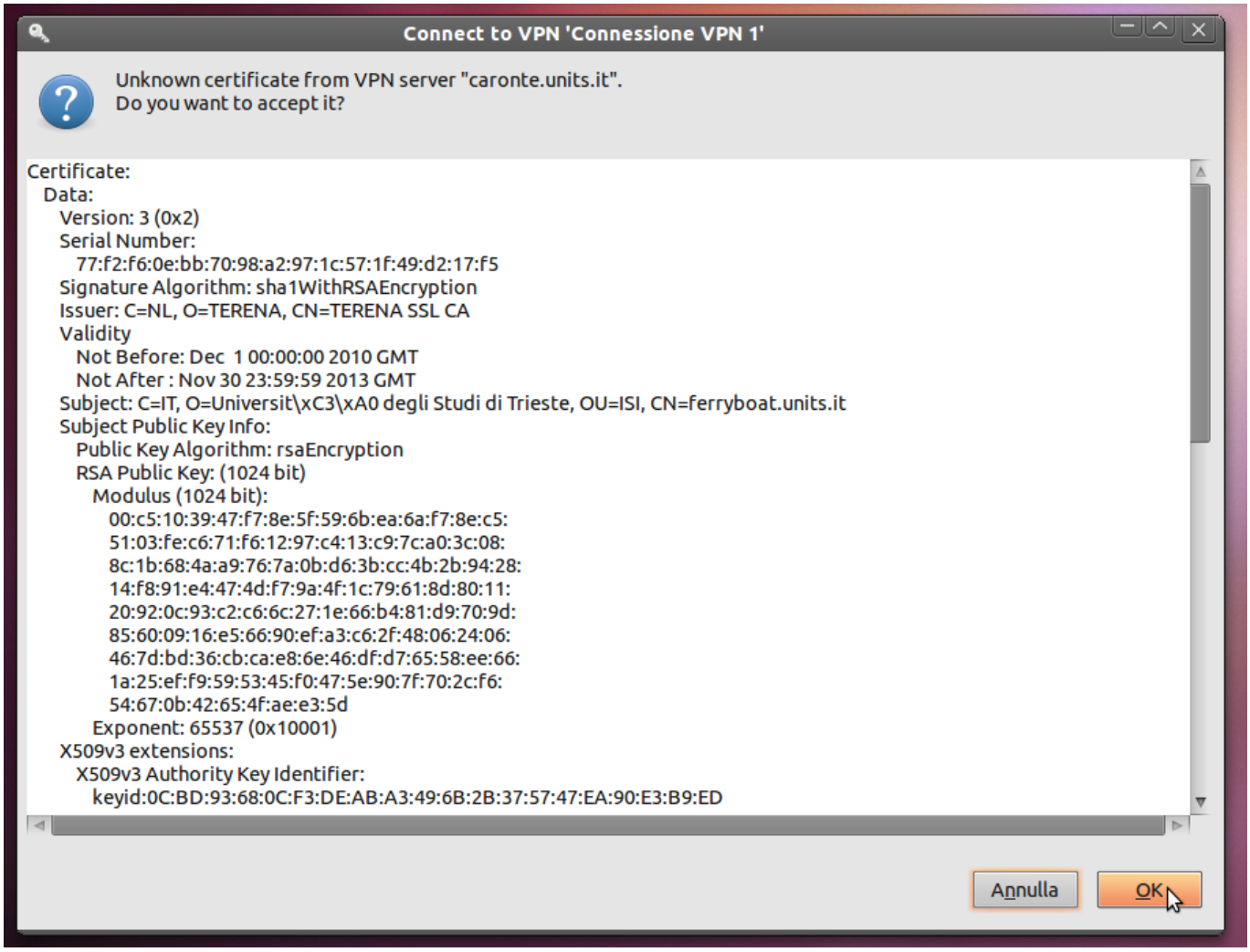
2) In the options, write *caronte.units.it* in the “Gateway” field, while on the “IPv4 settings” tab press the “Routes…” button and verify that the voice “Use this connection only for resources on its network” is checked:



3) At this point, left click on the Network Manager icon on the menu bar, select “VPN connections” and then the newly created connection; the login window will appear, press the button next to the “VPN Host” *caronte.units.it* field to start the first connection:



4) Now you will be asked to accept server's certificate (this will happen only on the first connection!):



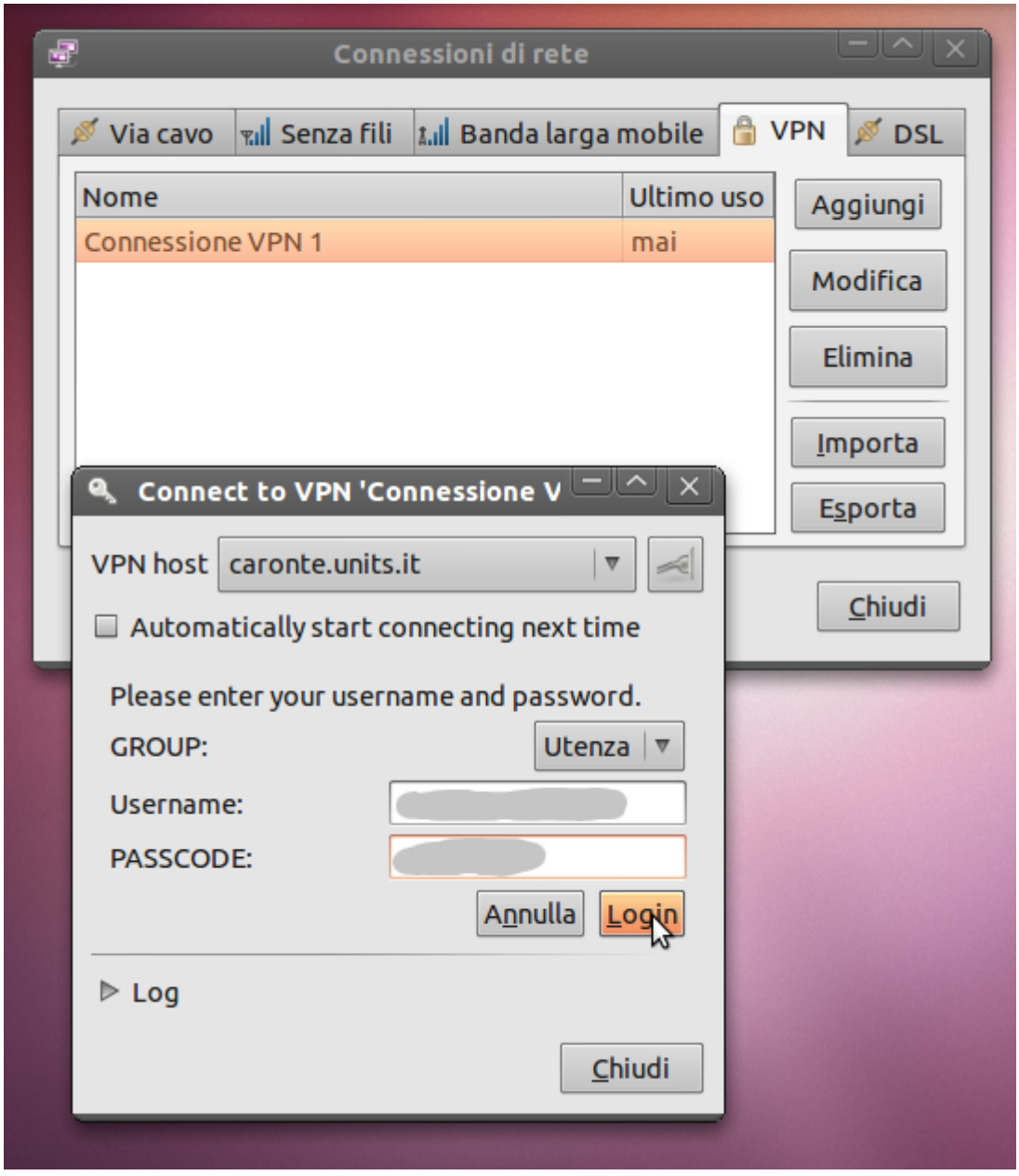
5) Verify that it is the correct one, verifying at least the green fields:

WARNING! be sure to view this instruction page through an *https* connection, to be reasonably sure that this instructions are not fake!
If the certificate does not correspond, it is possible that someone is trying to intercept the connection: stop this procedure and please contact the network administrators to point out the problem.

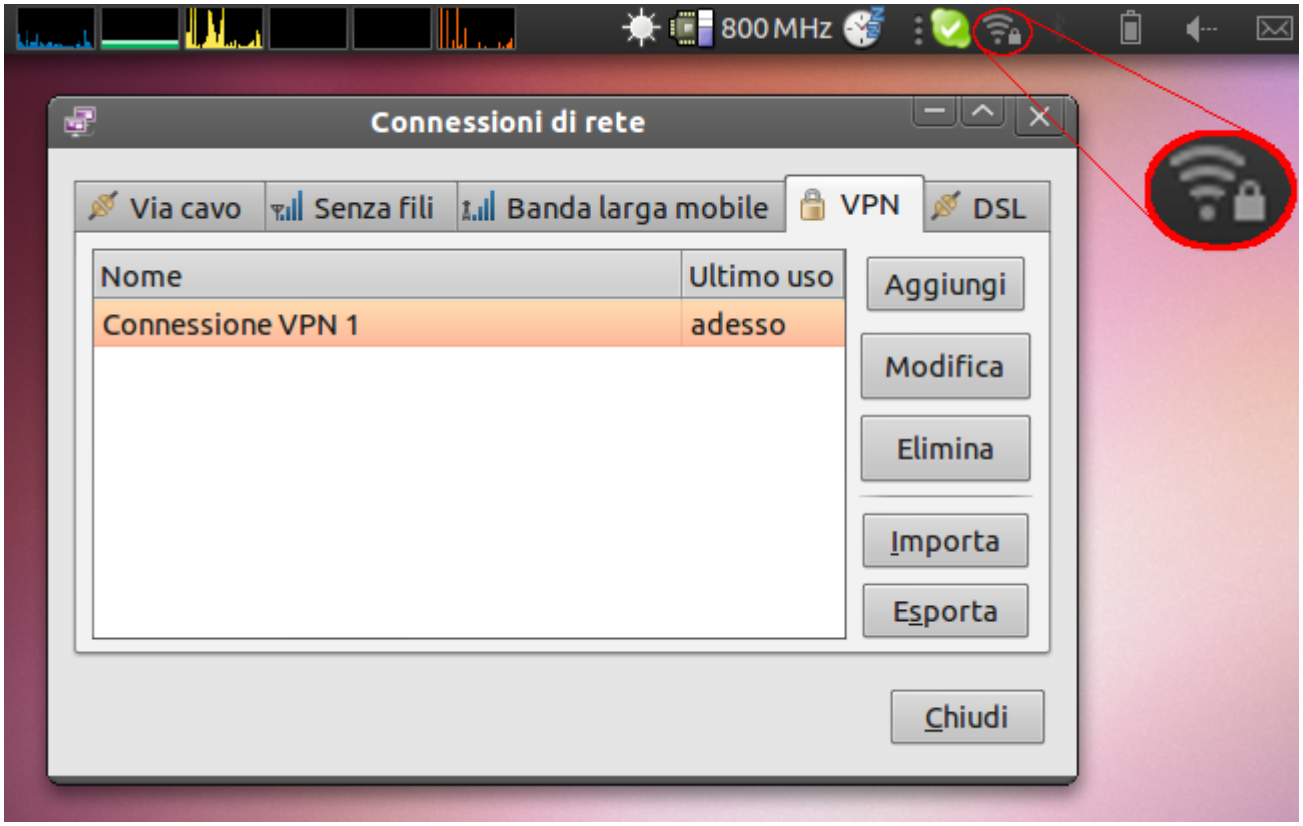
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            77:f2:f6:0e:bb:70:98:a2:97:1c:57:1f:49:d2:17:f5
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=NL, O=TERENA, CN=TERENA SSL CA
        Validity
            Not Before: Dec  1 00:00:00 2010 GMT
            Not After : Nov 30 23:59:59 2013 GMT
        Subject: C=IT, O=Universit\xC3\xA0 degli Studi di Trieste, OU=ISI, CN=ferryboat.units.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c5:10:39:47:f7:8e:5f:59:6b:ea:6a:f7:8e:c5:
                    51:03:fe:c6:71:f6:12:97:c4:13:c9:7c:a0:3c:08:
                    8c:1b:68:4a:a9:76:7a:0b:d6:3b:cc:4b:2b:94:28:
                    14:f8:91:e4:47:4d:f7:9a:4f:1c:79:61:8d:80:11:
                    20:92:0c:93:c2:c6:6c:27:1e:66:b4:81:d9:70:9d:
                    85:60:09:16:e5:66:90:ef:a3:c6:2f:48:06:24:06:
                    46:7d:bd:36:cb:ca:e8:6e:46:df:d7:65:58:ee:66:
                    1a:25:ef:f9:59:53:45:f0:47:5e:90:7f:70:2c:f6:
                    54:67:0b:42:65:4f:ae:e3:5d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:0C:BD:93:68:0C:F3:DE:AB:A3:49:6B:2B:37:57:47:EA:90:E3:B9:ED

            X509v3 Subject Key Identifier:
                36:B4:ED:07:DD:FB:FF:15:02:79:C7:2F:65:AA:34:28:15:D5:B1:B8
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.6449.1.2.2.29

            X509v3 CRL Distribution Points:
                URI:http://crl.tcs.terena.org/TERENASSLCA.crl

            Authority Information Access:
                CA Issuers - URI:http://crt.tcs.terena.org/TERENASSLCA.crt
                OCSP - URI:http://ocsp.tcs.terena.org

            X509v3 Subject Alternative Name:
                DNS:ferryboat.units.it, DNS:caronte.units.it, DNS:vpn.units.it
    Signature Algorithm: sha1WithRSAEncryption
        a9:41:be:87:c5:1f:4d:b1:30:3e:61:ff:12:13:bb:c7:19:5c:
        17:ac:e4:d8:e3:45:b7:79:39:64:a6:81:f3:45:ee:e9:c3:39:
        0e:71:bd:ac:72:60:9e:2d:ef:ef:07:c7:89:bd:74:dd:3f:da:
        78:66:f9:fa:8a:44:8c:99:d1:d0:ca:fe:8c:37:f2:fc:10:6e:
        c4:55:66:b8:3f:cc:16:a9:db:ea:3b:9f:85:55:98:45:88:ac:
        ef:75:fd:7e:8b:f0:98:eb:28:94:67:7e:14:ae:3f:6b:1c:08:
        47:9f:b8:b1:d8:33:5c:19:5e:c8:91:ca:8e:f7:a7:92:b5:01:
        3d:7a:5c:83:1a:d7:df:80:0d:a7:f2:6c:1b:f2:f6:76:7c:c6:
        43:cf:a5:56:f1:04:4e:7f:2f:ef:fc:28:f1:f2:2d:7d:56:7c:
        2a:24:46:fd:ef:63:bd:c8:f2:8b:cd:e0:41:97:cd:6c:3d:11:
        32:a1:80:b0:de:87:3a:06:8e:2d:40:5b:99:a6:1c:59:18:b5:
        58:75:86:05:43:b5:88:21:91:a7:da:b9:0b:e4:b7:14:61:83:
        77:51:2b:72:fd:00:ca:4c:2e:97:7c:d8:8f:c1:19:6b:b3:2b:
        0f:b1:39:20:2b:8c:da:93:65:28:43:01:4f:6c:9f:da:12:11:
        51:78:8e:57
```

6) Now the client tries to connect without letting you specify the *username* and *password*, so the connection will fail:

7) Start the connection again as done at point 3), this time your credentials will be asked for: write them complete with *domain* informations and do the *login*.



8) At this point the VPN connection should be working correctly: the activation will be confirmed by the appearance of a small padlock next to the Network Manager icon on the menu bar:



Have a good work!