OPENVPN

Mini – Howto

di installazione e configurazione

Roberto Massa
robimassa@gmail.com

OPENVPN 2.10 su sistema operativo OPENBSD vrs. 4.7

Configurazione di un VPN server per l'accesso client con autenticazione tramite certificato

Di seguito è descritta l'installazione e la configurazione di OpenVPN su un sistema OpenBSD che opera da Firewall e che deve consentire l'accesso alla rete interna ad utenti esterni all'azienda.

Si è scelto il sistema operativo OpenBSD per la grande affidabilità e sicurezza che lo contraddistinguono e nondimeno per la "leggerezza" in termini di risorse HW richieste.

La configurazione proposta ricalca una installazione attiva su un Firewall che interconnette 3 reti esterne con la rete aziendale e con il servizio di OPENVPN per l'accesso remoto.

OpenVPN, è disponibile pacchettizzato per OpenBSD nella versione 2.1 ed è anch'esso estremamente flessibile e "leggero".

Per quanto riguarda l'autenticazione in ingresso, le possibilità offerte da OpenVPN sono molteplici; in questa "guida" si è scelto di utilizzare il metodo a certificati protetti da password con gestione delle revoche direttamente dalla CA del server/firewall.

Tramite la revoca è possibile bloccare l'accesso alla rete aziendale, qualora vengano meno le necessità di connessione da parte di un utente al quale si era rilasciato precedentemente un certificato per l'accesso.

I pacchetti necessari alla nostra installazione sono due

- Openvpn-2.1.0.tgz
- Lzo2-2.03.tgz

che sono entrambi scaricabili dal sito OPENVPN al link
ftp://ftp.openbsd.org/pub/OpenBSD/4.7/packages/i386/.

Il primo pacchetto è OPENvpn vero e proprio, già compilato e pronto per essere configurato secondo i nostri scopi, mentre il secondo contiene una serie di librerie per la compressione e ottimizzazione del traffico al fine di rendere più veloce la comunicazione VPN tra client e server.

In queste note si assume che il sistema operativo sia già installato e funzionante.
Scaricati i due pacchetti è utile salvarli in una cartella di appoggio, dalla quale, con il comando:

- ***Pkg_add openvpn-2.1.0.tgz***

viene installato il primo pacchetto (openvpn) e contemporaneamente richiamata l'installazione del secondo.
Con pochi passi abbiamo installato il software per creare il sistema di accesso in VPN.

Se dal prompt comandi si digita *openvpn --help* si ottiene la lista delle opzioni di gestione.

Attivazione e configurazione della CA per la gestione dei certificati

Come già detto questa installazione si basa sull'utilizzo di certificati per le autenticazioni in ingresso e per la cifratura del traffico.
OpenVPN dispone, al suo interno, di tutto l'ambiente necessario, ossia di una CA in grado di emettere certificati e revocarli.
A tale scopo si utilizza easy-rsa già fornita con i pacchetti OPENVPN installati.
Tutti i files di configurazione e di gestione li troveremo in (usr/local/share/examples/openvpn/easy-rsa/2.0).
Per poter impostare l'ambiente sarà quindi sufficiente creare due cartelle in /etc e più precisamente: *openvpn, e al di sotto easy-rsa.*

- Mkdir /etc/openvpn
- Mkdir /etc/openvn/easy-rsa

Potremmo semplicemente usare i files dalla posizione in cui andiamo a prelevarli, ma a fronte di un aggiornamento del pacchetto OpenVPN questi verrebbero sovrascritti; da ora in poi ***/etc/openvpn*** diventerà la posizione per tutti i files di configurazione necessari al funzionamento del sistema.

- ***Cp –R /usr/local/share/examples/openvpn/easy-rsa/2.0/* /etc/openvpn/easy-rsa***

Tutti i comandi che seguiranno saranno eseguiti direttamente da questa cartella

Nella cartella easy-rsa è contenuto il file vars che contiene le variabili necessarie alla configurazione della CA; è necessario aprirlo e modificarne i valori di default contenuti, con i valori personalizzati che ci servono.

- **vi /etc/openvpn/easy-rsa/vars**

qui di seguito sono riportati i valori modificati usati per l'installazione di test

```
export EASY_RSA="/etc/openvpn/easy-rsa"
export KEY_CONFIG="/etc/openvpn/easy-rsa/openssl.cnf"

export KEY_COUNTRY=IT
export KEY_PROVINCE=CN
export KEY_CITY=Cuneo
export KEY_ORG="Openvpn-test"
export KEY_EMAIL=prova@openvpn.test.it
```

Per continuare l'installazione e la configurazione della CA è necessario a questo punto lanciare il seguente comando dalla cartella /etc/easy-rsa

- ***. ./vars && ./clean-all*** *(n.b. I punti sono separati da uno spazio)*

Sono due comandi concatenati: il primo (./vars) imposta le variabili ambiente secondo la personalizzazione descritta sopra, il secondo (./clean-all), esegue un reset totale dell'ambiente eliminando tutti i files generati in precedenza. Questo comando genera anche, all'interno di easy-rsa la cartella keys, questa cartella conterrà tutti i files necessari al funzionamento della CA ed anche i files relativi ai certificati di volta in volta generati

NOTA BENE Nel caso successivamente a questa fase di installazione, si debbano nuovamente rilasciare certificati client o revocarli , sarà sufficiente lanciare soltanto il comando

- ***. ./vars***

Prima di ogni altro comando relativo alla gestione della CA.

Una volta impostato l'ambiente con le informazioni necessarie, procediamo con la creazione vera e propria della "Certification Authority"

- ***./build-ca***

Questo è l'output a seguito del comando build-ca; da notare che tutte le opzioni proposte contengono il default impostato nel file VARS ad eccezione della richiesta per Common Name che dovremo necessariamente fornire e che sarà il nome univoco per la nostra CA.
Qui di seguito è riportato l'output del comando

```
Generating a 1024 bit RSA private key
……++++++
……..++++++
writing new private key to 'ca.key'
——
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
——
Country Name (2 letter code) [IT]:
State or Province Name (full name) [CN]:
Locality Name (eg, city) [Cuneo]:
Organization Name (eg, company) [Openvpn-test]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Openvpn-test CA]:
Name []:
Email Address [prova@openvpn.test.it]:
```

Terminata la creazione della CA dovremo procedere alla creazione delle varie chiavi server e client

- ***./build-key-server*** "***server-test"*** (dove server-test sarà il nome del nostro server)

L'esecuzione di questo comando genererà un output molto simile a quello visto in precedenza.
Dovremo confermare con YES le due richieste finali di :

- **Sign the certificate** e
- **1 of 1 certificate requests certified, commit?**

(tralasceremo la richiesta di fornire la challenge password"
Abbiamo così generato le chiavi server che OpenVPN userà per avviarsi e per attivare i tunnel cifrati con i vari client che accederanno.

Dovremo ancora fare generare i parametri Diffie-Hellmann che vengono utilizzati per lo scambio iniziale delle chiavi

- ***./build-dh***

Questo comando, richiede un tempo di esecuzione più lungo rispetto ai precedenti.

procederemo ora con la generazione dei certificati per i vari utenti che dovranno accedere alla rete. Come già anticipato, i certificati saranno generati protetti da password, ma se per ragioni diverse da quelle esposte dovessimo utilizzare certificati standard (senza protezione di accesso con password) sarà sufficiente il comando ./build-key

- **./build-key-pass "nome_utente"**

```
# ./build-key-pass robimassa
Generating a 1024 bit RSA private key
.....++++++
.........++++++
writing new private key to 'robimassa.key'
Enter PEM pass phrase: DIGITARE QUI LA PASSWORD A PROTEZIONE DEL CERTIFICATO
Verifying - Enter PEM pass phrase: DIGITARE QUI LA PASSWORD A PROTEZIONE DEL CERTIFICATO
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [IT]:
State or Province Name (full name) [CN]:
Locality Name (eg, city) [Cuneo]:
Organization Name (eg, company) [Openvpn-test]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [robimassa]:
Name []:
Email Address [prova@openvpn.test.it]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'IT'
stateOrProvinceName   :PRINTABLE:'CN'
localityName          :PRINTABLE:'Cuneo'
organizationName      :PRINTABLE:'Openvpn-test'
commonName            :PRINTABLE:'robimassa'
emailAddress          :IA5STRING:'prova@openvpn.test.it'
Certificate is to be certified until May 28 22:17:34 2020 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Configurazione di OPENVPN lato SERVER

Terminata la configurazione della CA e la generazione dei relativi certificati, è necessario definire il file di configurazione di OPENVPN che chiameremo OPENVPN.CONF e posizioneremo in /etc/openvpn; naturalmente il file può avere anche un altro nome (come vedremo più avanti si modificherà il processo di startup del sistema per attivare al boot il servizio OPENVPN con il file di configurazione voluto).

Tale file consente una molteplicità di possibili parametri di configurazione a seconda delle funzioni attivate, ma in questo documento si analizzeranno soltanto le opzioni effettivamente implementate.

Openvpn.conf

```
* port    9999
* proto   udp
* local   80.81.82.83
* dev     tun0
* ca      /etc/openvpn/easy-rsa/keys/ca.crt
* cert    /etc/openvpn/easy-rsa/keys/serveropenvpn.crt
* key     /etc/openvpn/easy-rsa/keys/serveropenvpn.key
* dh      /etc/openvpn/easy-rsa/keys/dh1024.pem
* mode    server
* server  172.16.0.0 255.255.255.0
* push "route 192.168.0.0 255.255.255.0"
* ifconfig-pool-persist   ipp.txt
* keepalive       10 120
* comp-lzo
* user _openvpn
* group _openvpn
* persist-key
* persist-tun
* verb 5
* crl-verify /certificati_revocati/crl.pem
* daemon
```

Descrizione delle direttive usate nel file opevpn.conf lato SERVER

PORT definisce il n° di porta sul quale il servizio rimane in ascolto.

PROTO definisce il protocollo TCP/UDP su cui OPENVPN opera.

LOCAL definisce l'indirizzo ip sul quale attivarsi e deve corrispondere all'indirizzo di un'interfaccia. Se non dichiarato, un ip OPENVPN si attiva in ascolto su tutte le interfacce.

DEV è il tipo dell'interfaccia TUN/TAP virtuale connessa al servizio OPENVPN che viene attivata. TUN0 in caso di interfaccia di tipo routed, TAP0 se l'interfaccia virtuale è di tipo bridged.
http://www.openvpn.net/index.php/documentation/faq.html (fornisce una esauriente spiegazione su quando è utile un tipo di interfaccia di tipo TUN oppure TAP, in generale per reti tcp/ip e buona norma, utilizzare il TUN)

CA,CERT,KEY,DH sono i files dei certificati generati precedentemente e che vengono utilizzati dal demone OPENVPN per la definizione del canale cifrato con i vari client.

MODE impone ad OPENVPN di operare in modalità server.

SERVER 172.16.0.0. 255.255.255.0 sarà la classe di indirizzi che verrà utilizzata per le connessioni client e sulla quale il server assegnerà un indirizzo alla interfaccia TUN0

PUSH "route 192.168.0.0 255.255.255.0" è la rete che viene pubblicata ai client in connessione VPN, solitamente la rete interna. In alternativa la direttiva PUSH-REDIRECT-GATEWAY imposta sul client il server OPENVPN come default gateway; è comunque possibile dichiarare più route in push.

IFCONFIG-POOL-PERSIST è il file nel quale openvpn tiene traccia dell'abbinamento certificato_client-ip in modo da riassegnare sempre lo stesso ip allo stesso client. Questa funzione è molto utile quando esiste la necessita, tramite PF, di filtrare in traffico consentendo ai vari utenti accessi su porzioni differenti della rete interna.

KEEPALIVE 10 120 è usata per determinare lo stato della connessione con il client; a questo scopo viene eseguito un ping ogni 10 secondi e, se per 120 secondi non si ottengono risposte, si assume che la connessione sia persa.

COMP-LZO: con questa direttiva si attiva l'uso delle librerie di compressione installate con il pacchetto in fase di attivazione del servizio.

USER e GROUP definiscono l'utente ed il gruppo con cui il demone openvpn "gira" sul sistema.

VERB 5 è il livello di verbosità dei log; di default con questa configurazione i log sono salvati in /var/log/messages, i livelli vanno da 0 a 9, intendendo con 9 il livello massimo.

CRL-VERIFY è la direttiva che impone ad OPENVPN di verificare la CRL, ossia la lista dei certificati revocati prima di consentire l'accesso.

DAEMON istruisce openvpn per essere eseguito in modalità di servizio, daemon appunto.

Definizioni delle regole per il FIREWALL PF

A questo punto, l'ambiente operativo per consentire ad OPENVPN di funzionare è stato definito; considerato che il nostro sistema opera come firewall con funzioni di protezione tra la rete interna ed internet, avremo anche precedentemente definito alcune regole di filtro nel file PF.CONF.
Ci limiteremo qui ad analizzare le poche regole da attivare in PF.CONF al fine di permettere al traffico entrante dalla VPN di raggiungere la rete interna.

```
#accesso alla porta 9999 UDP da tutta le rete internet sull'ip pubblico
pass in on fxp1 proto udp from any to $ip_internet port 9999

#tutto il traffico tcp  ed icmp può transitare dalla rete della VPN alla LAN
pass in on tun0 proto tcp from $lan_vpn to $lan_interna keep state
pass in on tun0 proto icmp from $lan_vpn to $lan_interna keep state

#tutto il traffico icmp e tcp dalla rete interna può transitare verso la VPN
pass out on $interna_if proto tcp from any to $lan_interna keep state
pass out on $interna_if proto icmp from any to $lan_interna keep state
```

Queste regole nel firewall consentiranno al traffico della VPN di entrare correttamente sulle interfacce; si noti che le dichiarazioni di: **$lan_interna**, **$ip_internet**, **$lan_vpn**, **$interna_if**, **fxp1** sono valori che cambiano a seconda delle installazioni e delle modalità con cui sono dichiarate le costanti ed i nomi delle interfacce.
Si sono riportate queste righe a solo titolo di esempio delle azioni da compiere anche sul Firewall affinché tutto funzioni correttamente, non è oggetto di questa guida la configurazione del firewall PF su OPENBSD..

Accesso diversificato per utenti alla rete interna

Come già accennato tramite il file ipp.txt è possibile mantenere fisso l'indirizzo assegnato da OPENVPN ad un determinato utente che esegue l'accesso; per fare ciò e sufficiente all'interno del file ipp.txt scrivere il nome del certificato/utente ed il relativo ip da assegnare separati da virgola.
Va tenuto in considerazione il fatto che OPENVPN assegna per ogni certificato all'interno del file ipp.txt una rete di due HOST (quattro indirizzi totali) e l'indirizzo specificato nel file ipp.txt corrisponde all'ip di rete.
Queste reti sono porzioni della rete definita alla voce SERVER nel file openvpn.conf

Per esempio se si vuole assegnare ad ogni connessione dell'utente, che ha il certificato con nome "**utente1"**, l'indirizzo ip 172.16.0.26 dovremo dichiarare nel file ipp.txt la seguente riga
.

utente1,172.16.0.24

Il client che effettua la connessione si vedrà assegnato l'indirizzo 172.16.0.26 che appartiene alla rete 172.16.0.24 con subnet 255.255.255.252

Questo è l'output del comando ipconfig sul client; si noti che viene riportato un servizio DHCP all'indirizzo 172.16.0.25.

Scheda Ethernet VPN_Sito1:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : TAP-Win32 Adapter V8
Indirizzo fisico. . . . . : 00-FF-5B-1A-FD-46
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IP. . . . . : **172.16.0.26**
Subnet mask . . . . . : **255.255.255.252**
Gateway predefinito . . . . . :
Server DHCP . . . . . : 172.16.0.25
Lease ottenuto. . . . . : mercoledì 9 luglio 2008 0.29.18
Scadenza lease . . . . . : giovedì 9 luglio 2009 0.29.18

una eventuale impostazione errata all'interno del file ipp.txt viene automaticamente corretta da OPENVPN in fase di avvio e viene assegnato l'ip di rete più vicino a quello impostato erroneamente.

A questo punto agendo sulle regole di PF analogamente a quanto fatto prima, potremo definire con estrema precisione cosa gli utenti esterni possono fare all'interno della rete.

pass in quick on tun0 proto tcp from $client1 to $server_mail keep state

Questa regola (puramente esemplificativa) consente all'utente che si presenta con l'ip definito in $client1 di raggiungere solo e soltanto l'ip del $server_mail

Attivazione del servizio OPENVPN a boot time

A questo punto della configurazione si deve fare sì che l'avvio di OPENVPN sia a boot time, altrimenti dopo l'avvio del sistema è necessario avviare a mano il demone OPENVPN

Per fare eseguire ad OPENBSD il servizio OPENVPN è necessario agire sul file **/etc/rc.local** (dove sarà sufficiente inserire queste poche righe di configurazione).

```
if [ -x /usr/local/sbin/openvpn ]; then
        echo -n 'Openvpn Start'
        /usr/local/sbin/openvpn --config /etc/openvpn/openvpn.conf > /dev/null 2>&1
fi
```

In grassetto è riportata la direttiva –-config seguita dal percorso e nome del file di configurazione che, come detto in precedenza, può avere un nome diverso ed essere collocato in una posizione diversa.

Revoca di certificati

Una caratteristica della configurazione descritta è la possibilità di revocare i certificati rilasciati, al fine di impedire l'accesso ai client che non ne hanno più titolo.
L'elenco dei certificati revocati di default, viene generato nella cartella "keys", la stessa già vista in precedenza.
Ogni volta che si deve revocare un certificato è sufficiente lanciare il comando **./revoke-full** seguito dal nome del certificato: il file di revoca viene aggiornato con le informazioni sulla variazione effettuata, il file contenente l'elenco avrà nome **crl.pem**

Se si vuole consultare la lista delle revoche effettuate è sufficiente eseguire il comando
./list-crl crl.pem: la lista viene riportata a video con i numeri seriali dei vari certificati; per risalire al nome del certificato vero e proprio è necessario aprire il file index.txt (sempre contenuto nella cartella keys) ed individuare la riga corrispondente al seriale del certificato, sulla stessa riga sono riportate le informazioni sul nome file del certificato revocato.

Il demone OPENVPN, viene fatto girare sul sistema con privilegi ridotti e perciò, non ha i permessi di accesso per leggere il file crl.pem nel punto in cui viene creato di default, è necessario copiare a mano dopo ogni revoca questo file in una posizione in cui il servizio OPENVPN possa leggerlo.
In alternativa con una piccola modifica si istruisce lo script revoke-full per eseguirne la copia dopo ogni esecuzione

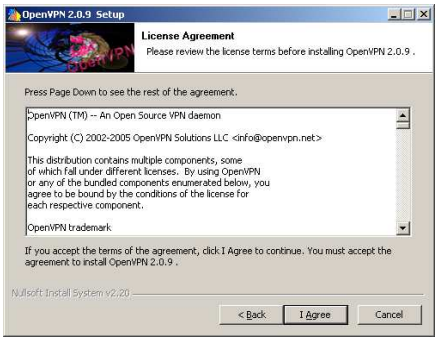
file revoke per la revoca dei certificati

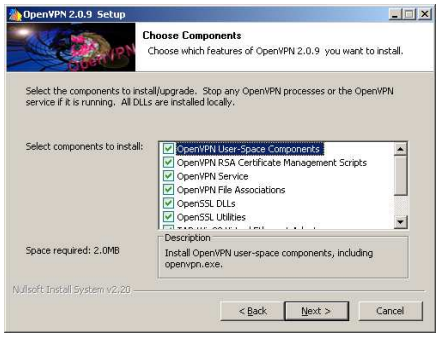
Modifica del file revoke-full per ottenere la copia del file crl.pem dalla cartella KEYS dove l'utente con cui "gira" Openvpn non ha permessi in un percorso differente a sola lettura.

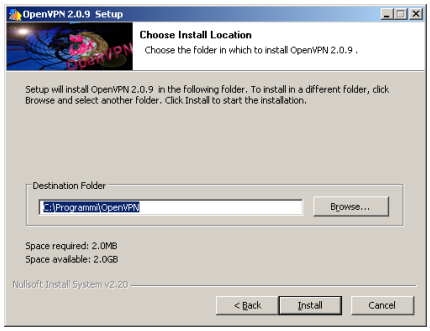
```
#!/bin/sh

# revoke a certificate, regenerate CRL,
# and verify revocation

CRL="crl.pem"
RT="revoke-test.pem"
CRL_OVPN="/certificati_revocati/" #posizione dove copiare il file crl.pem relativo alla revoca dei certificati

if [ $# -ne 1 ]; then
    echo "usage: revoke-full <cert-name-base>";
    exit 1
fi

if [ "$KEY_DIR" ]; then
    cd "$KEY_DIR"
    rm -f "$RT"

    # set defaults
    export KEY_CN=""
    export KEY_OU=""
    export KEY_NAME=""

    # revoke key and generate a new CRL
    $OPENSSL ca -revoke "$1.crt" -config "$KEY_CONFIG"

    # generate a new CRL -- try to be compatible with
    # intermediate PKIs
    $OPENSSL ca -gencrl -out "$CRL" -config "$KEY_CONFIG"
    if [ -e export-ca.crt ]; then
        cat export-ca.crt "$CRL" >"$RT"
    else
        cat ca.crt "$CRL" >"$RT"
    fi

    # verify the revocation
    $OPENSSL verify -CAfile "$RT" -crl_check "$1.crt"
    cp $CRL $CRL_OVPN
else
    echo 'Please source the vars script first (i.e. "source ./vars")'
    echo 'Make sure you have edited it to reflect your configuration.'
fi
```

Installazione e configurazione del Client (Windows)

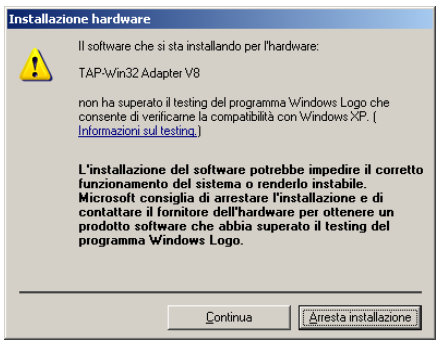
Sempre sul sito Openvpn.net nella sezione "downloads" si può scaricare il file .exe per l'installazione della componente client e server su windows (da notare che tutto il sistema descritto sopra può funzionare come server di accesso anche installato su sistemi Microsoft)
A questo punto è sufficiente lanciarlo e seguire i passi di installazione,

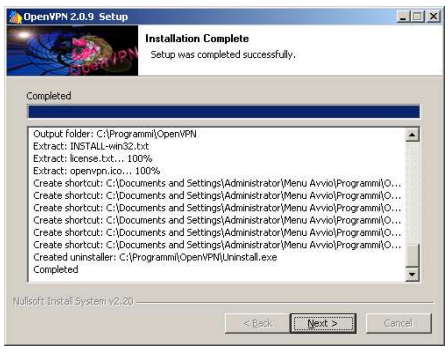






Durante l'installazione viene creato un device di rete che ha come driver
"TAP-Win32 Adapter V8 #1"; tale device verrà utilizzato ed attivato dal sistema all'avvio della sessione VPN.
Nelle risorse di rete vedremo visualizzata una nuova scheda di rete con cavo disconnesso.





Il file di configurazione della VPN client è posto in **c:\programmi\openvpn\.** A questo punto è sufficiente modificare il file openvpn.conf secondo le impostazioni desiderate, per poter avviare i servizi client.

Prima però è necessario copiare dal server OPENVPN i files necessari al funzionamento, ovvero il certificato relativo alla CA (ca.crt) ed i due files generati precedentemente.

Il file openvpn.conf lato client, nel caso dell'esempio descritto in questo documento, ha le seguenti impostazioni.

```
client
remote 80.81.82.83
proto udp
port 9999
dev tun
dev-node VPN_1
comp-lzo
ca C:\\Programmi\\OpenVPN\\ ca.crt
cert C:\\Programmi\\OpenVPN\\nome_utente.crt
key C:\\Programmi\\OpenVPN\\nome_utente.key
```

i files **nome_utente.crt**, **nome_utente.key** e **ca.crt**, sono i files generati in precedenza e dovranno fisicamente essere copiati sul client affinché questo possa accedere correttamente alla VPN.
Potrebbe essere utile in caso di accesso a più server VPN da parte di un unico client, definire anche fisicamente una interfaccia di rete per ogni accesso. Per aggiungerne successivamente, sarà sufficiente dal menu programmi/openvpn selezionare la scelta "**Add a new TAP-Win32 virtual ethernet adapter**"; così facendo verrà creata una ulteriore scheda di rete per l'accesso VPN.
Dalle proprietà di windows è possibile rinominare la connessione e nel file di configurazione di OpenVPN riferirsi direttamente all'interfaccia voluta.

Descrizione delle direttive utilizzate nel file openvpn.conf lato CLIENT

CLIENT imposta il software per lavorare in modalità client.

REMOTE è l'ip address o il nome internet su cui e attivo il servizio OPENVPN server

PROTO e PORT definiscono la porta e protocollo sul quale il servizio server "ascolta"

DEV TUN specifica su quale tipo di interfaccia si sta operando

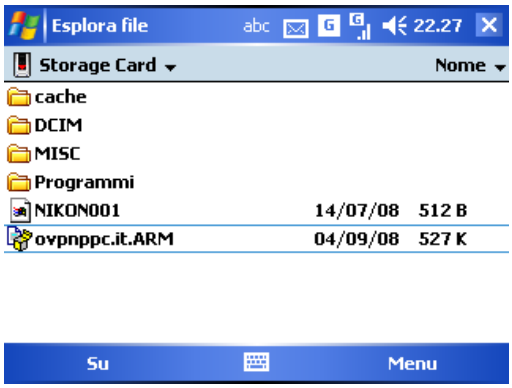
DEV-NODE: qualora localmente al pc client client si avessero diversi device di accesso, ognuno per un diverso server OPENVPN, una volta rinominate, le varie connessioni di rete su windows saranno indicate qui, con il nome dell'interfaccia da utilizzare per ogni connessione.

COMP-LZO attiva lato client la compressione.

CA, CERT, KEY sono i vari certificati rilasciati dalla ca per il client

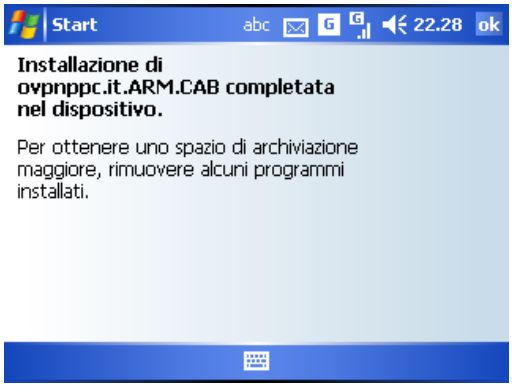
Installazione del Client (WINDOWS MOBILE)

Nella sua estrema praticità di utilizzo, OPENVPN (client) può essere facilmente installato ed utilizzato anche su dispositivi basati su sistema operativo WINDOWS MOBILE versione 5.0 o successive (gli screenshots seguenti sono della versione 5.0)
E' necessario eseguire il download del client OPENVPN al sito **http://ovpnppc.ziggurat29.com/ovpnppc-files.htm.** Da questa pagina si accede al download delle varie versioni "nazionalizzate": eseguire quello della versione italiana e, per comodità il link al file .CAB.
Effettuando questo download si dovrà poi copiare il file di installazione sul palmare e da qui, successivamente, lanciarne l'istallazione. Se si effettua il download della versione ACTIVE SYNC l'installazione sarà effettuata direttamente tramite l'utility stessa dal pc connesso tramite USB al dispositivo mobile.



Trasferito quindi il file sul palmare non avremo che da eseguirlo.

Alla richiesta della posizione in cui installare l'applicativo, dovremo scegliere quella più appropriata per la configurazione del nostro palmare, ossia sulla memoria interna al dispositivo stesso, oppure (se disponibile) la storage card.



Al termine sarà sufficiente uscire dal setup

Il desktop del palmare presenta ora in basso a destra una nuova icona; selezionandola, attiviamo la configurazione e la gestione delle connessioni VPN.

prima però è necessario copiare sul palmare, nella cartella "config" che troveremo all'interno del percorso di installazione, i certificati, generati dal server OPENVPN.

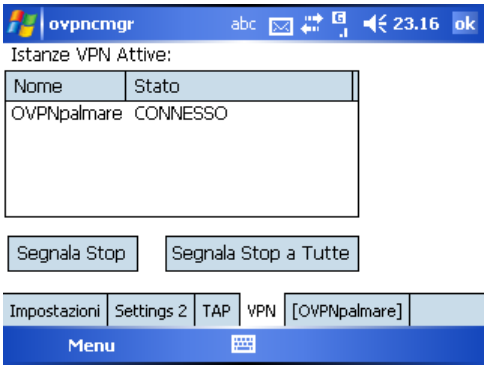
Per questo tipo di accesso non funziona il certificato protetto da password, sarà quindi necessaria la generazione di un certificato standard tramite il comando build-key.
Sempre nella cartella "config" bisognerà creare il file di testo con le specifiche della connessione; per fare ciò è utile partire dal file sample.conf, modificandolo.
Per facilitare la scrittura del file può essere utile trasferirlo sul pc, modificarlo e riportarlo sul palmare a modifiche completate.

Qui di seguito è riportato un esempio di file di configurazione utilizzato su un dispositivo mobile, è da notare che nel dichiarare il percorso dei vari file certificato non è più presente la lettera di unità C:,D: etc. presente su Windows

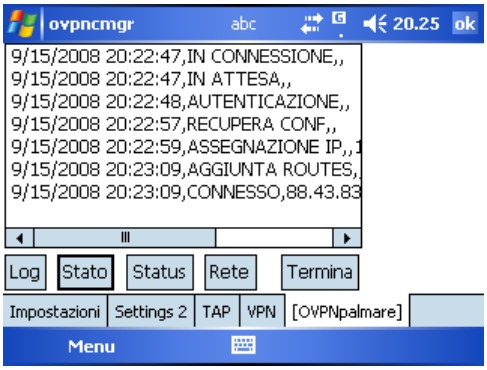
```
client
remote 80.81.82.83
port 9999
dev tun
proto udp
comp-lzo
ca \\Programmi\\OpenVPN\\config\\ca.crt
cert \\Programmi\\OpenVPN\\config\\palmare.crt
key \\Programmi\\OpenVPN\\config\\palmare.key
```

selezionando quindi l'cona relativa al client OPENVPN, e successivamente "**Avvio da Config.**" verranno visualizzati tutti i file di configurazione presenti nella cartella config. Selezionando la configurazione desiderata, si avvia la connessione.

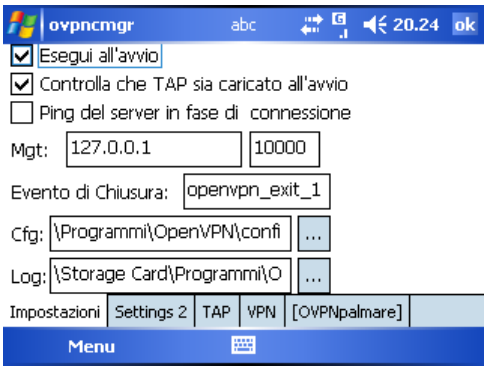
Richiamando nuovamente l'icona del client e scegliendo "**Utilità**" e successivamente "**Istanze VPN**" si accede ad un sottomenù utile per visualizzare lo stato della connessione.



Qui di fianco è riportata la connessione attivata precedentemente ed il suo stato attuale; le cartelle "**impostazioni**", "**settings**", "**TAP**" e "**VPN**" sono relative allo stato generale del client ed alle sue configurazioni.
La cartella più a destra (con il nome della connessione) è presente soltanto quando questa è attiva e ne riporta dettagliatamente le informazioni,.



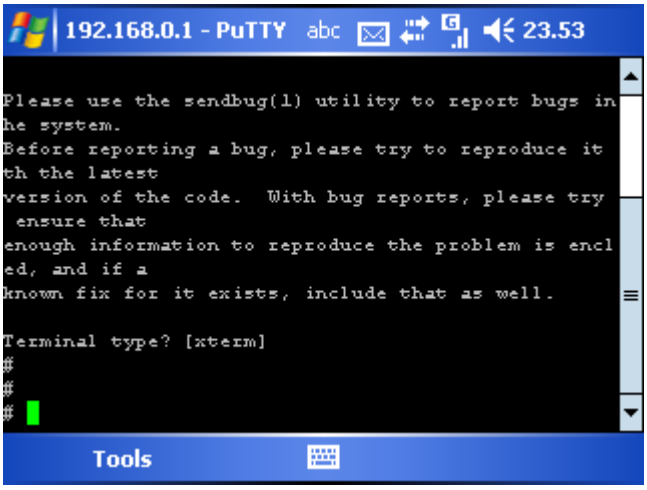
Premendo "**TERMINA**" si effettua la disconnessione dal server OPENVPN cui ci si era connessi.



La cartella "**impostazioni**" contiene i settaggi operativi del client, in particolare la posizione dei files .conf per l'accesso ai vari server OPENVPN e quella dei files di log; è bene disabilitare (in quanto di default è abilitato) il checkbox "**ping del server in fase di connessione**", altrimenti ad ogni avvio di sessione il client tenta di raggiungere il server prima con un ping e se questi, per varie ragioni, non risponde all'icmp viene riportato un messaggio che richiede se continuare o meno.

Queste note non sono esaustive. Per maggior completezza riferirsi al sito da cui si è precedentemente scaricato il client.

http://ovpnppc.ziggurat29.com/ovpnppc-usage.htm



Qui a fianco è riportato lo "screenshot" di un accesso in SSH tramite PUTTY (per windows mobile) su un server OPENBSD tramite VPN realizzata con la configurazione descritta sopra.