

VPN Host-toLAN Facile con ZeroShell, OpenVPN e Gnome

di Giuseppe Virzi
[info_at_giuseppevirzi.it]

Scopo del documento

Lo scopo di questo breve documento è di illustrare in poche pagine come è possibile integrare il processo di connessione ad una VPN basata su OpenVPN con l'ambiente desktop Gnome di un client.

Questo documento non descrive il processo di setup del server VPN, per il quale rimando a specifiche guide che potete trovare tra la [documentazione](#) di [ZeroShell](#).

Inoltre le istruzioni che seguono permettono di loggarsi ad una VPN che utilizza l'autenticazione basata su password, senza certificati utente a chiave privata.

Gli ingredienti fondamentali per una connessione del tipo descritto sono l'indirizzo del server OpenVPN, la coppia di username e password e il certificato della CA.

Installazione del client addon per NetworkManager

Se si dispone di un sistema di pacchettizzazione, l'installazione del plugin per NetworkManager si riduce ad una singola riga di comando:

su Fedora:

```
yum install NetworkManager-vpnc NetworkManager-pptp NetworkManager-openvpn
```

su Ubuntu:

```
sudo apt-get install network-manager-openvpn-gnome
```

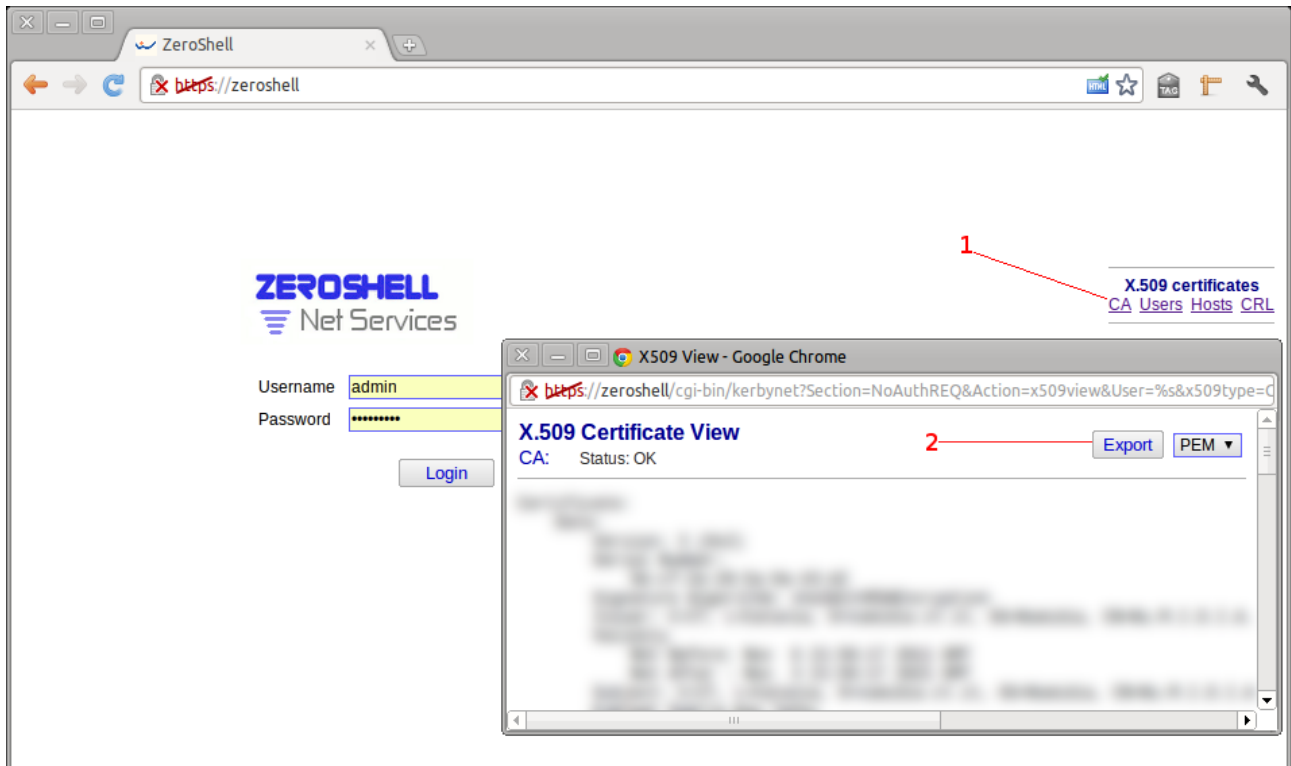
Potrebbe essere necessario riavviare la sessione per rendere effettive le modifiche. Verificare che queste siano state rese effettive cliccando con il tasto destro sull'icona del NetworkManager e poi sulla voce *"Modifica connessioni"*.

Nella scheda VPN cliccare sul tasto *"Aggiungi"*. Se nella finestra che si apre è possibile scegliere la voce OpenVPN allora l'installazione è andata a buon fine.



Ottenere il certificato della CA (ZeroShell)

Potete facilmente ottenerlo dalla schermata di login della vostra installazione di ZeroShell



Otterrete un file *.pem*. Supponiamo che esso venga salvato all'indirizzo `~/vpn/CA.pem`.

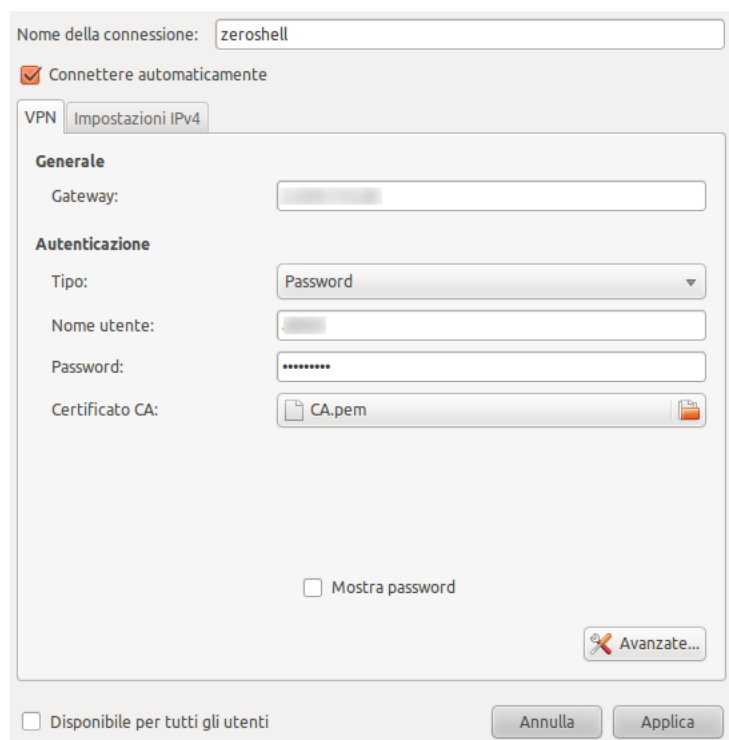
Configurazione del client VPN

Per configurare il client:

1. click destro su icona NetworkManager
2. Modifica Connessioni
3. Scheda VPN
4. Aggiungi
5. Selezionare OpenVPN
6. Crea...

Nella finestra che si aprirà inserire alla voce Gateway l'indirizzo del server VPN,

Per la voce Tipo scegliere Password e alle voci username e password inserire la coppia di credenziali impostate su ZeroShell.



Alla voce Certificato CA scegliere il file che abbiamo salvato all'indirizzo ~/vpn/CA.pem.
Cliccare poi sulla voce “Avanzate...” e riportare le impostazioni delle seguenti figure:

Generale Sicurezza Autenticazione TLS

Usare una porta gateway personalizzata: 1194

Usare un intervallo di rinegoziazione personalizzato: 0

Usare la compressione LZO

Usare una connessione TCP

Usare un device TAP

Usare una Maximum Transmission Unit (MTU) per il tunnel personalizzata: 1500

Usare una dimensione di frammento UDP personalizzata: 1300

Limitare il Maximum Segment Size (MSS) TCP del tunnel

Annulla OK

Generale Sicurezza Autenticazione TLS

Cifrario: BF-CBC

Autenticazione HMAC: SHA-1

Annulla OK

Avviare la connessione

A questo punto avviare la connessione è una operazione molto semplice. Basta cliccare con il tasto sinistro sulla icona del network manager e selezionare la voce relativa alla vostra VPN appena creata dal menu “Connessioni VPN”. La avvenuta connessione alla vostra VPN è segnalata con l'apposizione di un piccolo lucchetto all'icona del network manager. Come ulteriore verifica potete visitare il sito www.mioip.net e verificare che l'indirizzo riportato corrisponda all'indirizzo pubblico del gateway della VPN e non quello relativo al vostro gateway locale.

Troubleshooting

Se ottenete degli errori potete ottenere utili informazioni per il debug scrivendo sulla riga di comando:

```
tail -f /var/log/syslog
```

Se dopo aver avviato la connessione, tra l'output del precedente comando notate delle righe simili a questa:

```
[1297693509.445619] [nm-vpn-connection.c:844] connection_need_secrets_cb(): NeedSecrets failed: dbus-glib-error-quark Rejected send message, 1 matched rules; type="method_call", sender=":1.4" (uid=0 pid=1129 comm="NetworkManager) interface="org.freedesktop.NetworkManager.VPN.Plugin" member="NeedSecrets" error name="(unset)" requested_reply=0 destination="org.freedesktop.NetworkManager.openvpn" (uid=0 pid=8646 comm="/usr/lib/network-manager-openvpn/nm-openvpn-service"))
```

La soluzione potrebbe essere quella di abilitare anche la policy `user="at_console"` a lanciare connessioni VPN, aggiungendo al file `/etc/dbus-1/system.d/nm-openvpn-service.conf` le righe:

```
<policy user="at_console">
    <allow own="org.freedesktop.NetworkManager.openvpn"/>
    <allow send_destination="org.freedesktop.NetworkManager.openvpn"/>
</policy>
```

Potrebbe essere necessario riavviare il computer (o forse basta riavviare dbus).

Credits

Questa piccola guida è stata realizzata a seguito della riprogettazione della rete interna voluta da [Nu.M.I.D.I.A SRL](#). Tengo a ringraziare questa società per l'impegno profuso nell'uso e nella diffusione del software libero.