Tecnica per help desk remoto

Guida scritta da Stefano Coletta (Creator) il 5 ottobre 2003
Contattatemi a creator@mindcreations.com o visitando http://www.mindcreations.com

In breve

Una soluzione multipiattaforma, sicura, versatile e soprattutto libera per gestire completamente un computer remoto dall'esterno di una rete privata (con NAT) o una rete protetta (che usa solo firewall con regole in ingresso).

Peculiarità

- Elude ogni regola di firewall in ingresso (necessita della sola porta 22/tcp aperta in uscita)
- Molto difficile spiare il traffico o intromettersi nelle comunicazioni:
    - Il traffico VNC è cifrato in modo sicuro attraverso SSH (nessuna trasmissione in chiaro)
    - Autenticazione tripla: un login per ogni client ssh e un login VNC per accedere al PC da gestire.
    - TightVNC accetta solo connessioni originate dal computer stesso
- Permette la gestione remota anche in ambienti di rete con NAT
- Realizzato interamente con software libero ed open source
- Indipendente dalla piattaforma (TightVNC e SSH girano su quasi tutti i sistemi operativi)
- Abbastanza veloce (può beneficiare dalla compressione SSH e degli algoritmi di ottimizzazione di TightVNC)
- Non c'è bisogno di sapere l'indirizzo IP del PC da gestire
- Non c'è bisogno di comunicare l'indirizzo IP del PC che gestisce al PC da gestire
- Flessibile: non importa dove tu sia, il PC da gestire può essere raggiunto sempre, non importa neanche dove è connesso, puoi raggiungerlo senza modifiche alle configurazioni.

Perchè ho bisogno di questa roba?

Molto spesso le persone esperte in informatica vengono tediate dai principianti riguardo problemi comuni sul proprio PC anche se sono di semplice risoluzione. La situazione più tipica è quella di doversi spostare dalla propria scrivania/abitazione per arrivare alla loro scrivania/abitazione per mostrargli come risolvere il loro problema. Di solito è necessario vedere la schermata del loro PC, dando un'occhiata qua e la cercando di capire quale misterioso e insolito problema li affligge (dal loro punto di vista ovviamente ☺). A volte si riesce a risolvere il problema parlando al telefono oppure inviando email dettagliate… ma sapete bene quanto è difficile per un principiante essere guidati in questo modo… così, alla fine, dovete recarvi da loro e risolvere il problema impegnando il vostro tempo e mettendo a dura prova la vostra pazienza.

Se siete uno dei tanti che si trova in questa situazione la mia tecnica potrà tornarvi utile per rimanere comodamente al vostro posto e risolvere lo stesso il problema, come se foste lì.

Di cosa ho bisogno: noto ai più come "Requisiti"

1) Del client di TightVNC per voi e il server TightVNC installato sul PC da gestire
2) Di un server ssh pubblico raggiungibile da voi e dal vostro amico/cliente/collega.
3) Del client ssh Putty (o un altro che preferite) per voi e per il PC da gestire

Le cattive notizie

- Non è così semplice da installare per i principianti (suvvia, un minimo di sforzo se si vuole essere aiutati!)
- Non funziona quando esistono delle regole in uscita sul firewall perimetrale per uno dei due computer (il vostro e quello da gestire): scenario abbastanza raro e presente solo in reti ad alta sicurezza (banche, enti governativi, difesa, e simili)

Come funziona

Guardate la prossima immagine per comprendere meglio i passi seguenti.

0) Il PC gestito esegue il server TightVNC.

1) Il PC gestito stabilisce una sessione ssh (viola) al Server SSH (IP pubblico, porta 22/tcp)

2) Il client SSH crea un tunnel ssh inverso (rosso) dal Server SSH (127.0.0.1) al PC gestito (127.0.0.1) per le porte 5800 e 5900 utilizzando il protocollo TCP (chiamate da ora in avanti "Porte VNC"). A questo punto il Server SSH può connettere se stesso (da localhost) alle porte VNC locali al PC gestito.

3) Il PC che gestisce stabilisce una sessione ssh (blu) al Server SSH (allo stesso modo del PC gestito)

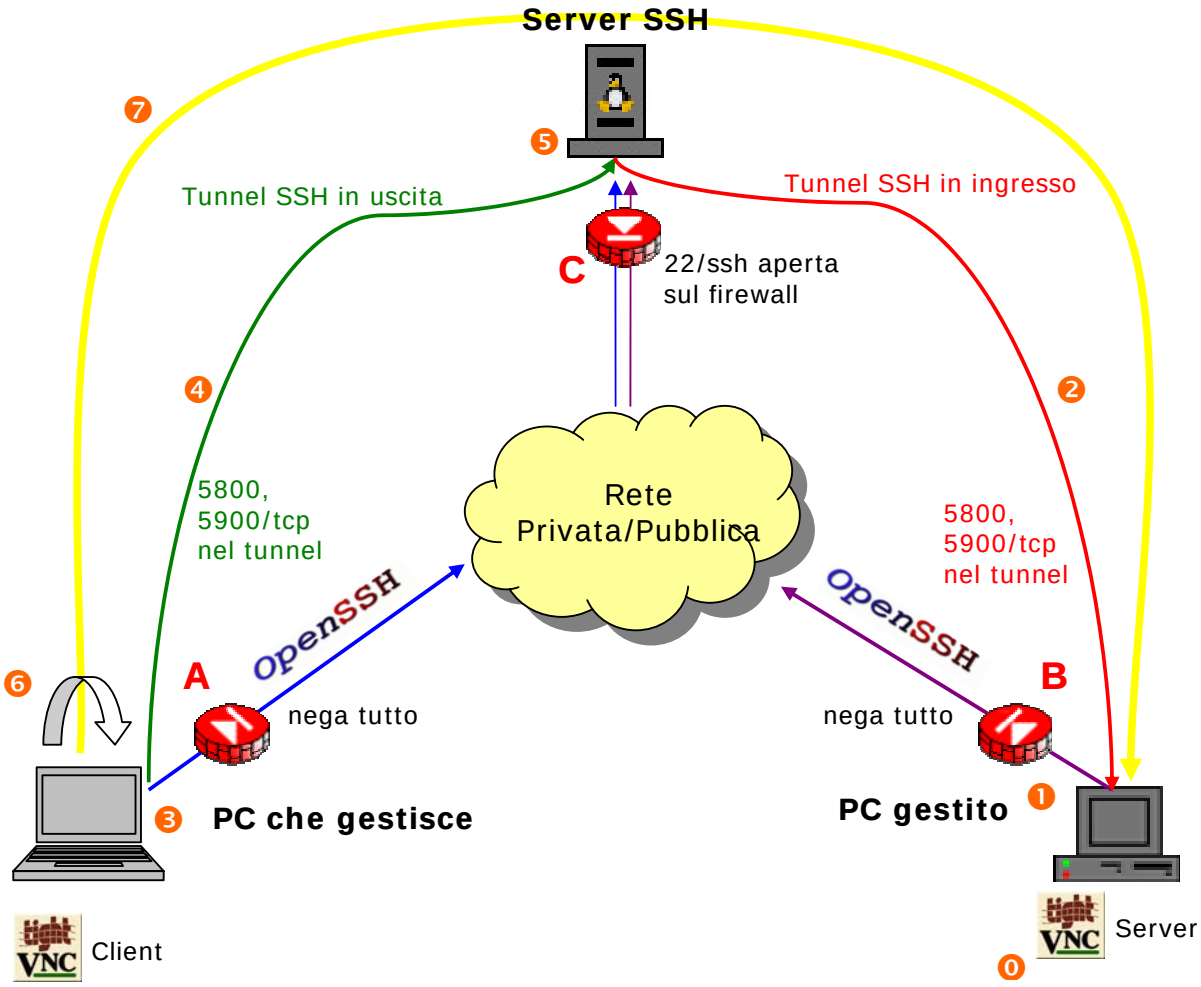
4) Il client SSH crea un tunnel ssh diretto (verde) dal PC che gestisce (127.0.0.1) al Server SSH (127.0.0.1) per le porte VNC. A questo punto il PC che gestisce può connettere se stesso da localhost alle porte VNC del Server SSH.

5) Ora, come per magia, i due tunnel SSH vengono automaticamente connessi insieme sul Server SSH permettendo al traffico di transitare dal PC che gestisce al PC gestito (verde + rosso).

6) Il PC che gestisce esegue il client TightVNC specificando come destinazione “localhost”.

7) Il PC che gestisce ora può controllare il PC gestito per mezzo del client TightVNC passando in un doppio tunnel SSH ☺ (giallo)

Diagramma dei flussi



Come vengono elusi i firewall ed il NAT?

Se guardate attentamente l'immagine precedente noterete tre firewall (A, B e C) e due reti con NAT (dietro il firewall A e B). Questo scenario è la situazione peggiore che possiate incontrare.

I firewall A e B sono configurati per negare l'accesso a qualsiasi pacchetto in ingresso, mentre il firewall C permette il transito in ingresso solo per la porta 22/tcp. Questo significa che nessuno può contattare direttamente i PC dalla rete esterna ad entrambi i firewall. Con il protocollo ssh si possono creare dei tunnel: sono proprio questi a realizzare il cosiddetto "passaggio" sfruttando una sola porta aperta (22/tcp) sul Server SSH realizzando un ponte.

Quando il PC gestito si connette al Server SSH e crea il primo tunnel inverso, effettivamente apre la porta 5800 e 5900 usando il protocollo TCP per connessioni provenienti dal Server SSH. Le porte non vengono (ovviamente) realmente aperte sul firewall B ma semplicemente rigirate al PC gestito utilizzando il tunnel inverso evidenziato in rosso. La cosa più difficile è fatta, il primo NAT con il firewall B sono elusi.

A questo punto il PC che gestisce si connette al Server SSH creando un altro tunnel, diretto, che effettivamente apre la porta 5800 e 5900 utilizzando il protocollo TCP per connessioni provenienti dal PC che gestisce. Come prima, anche queste porte non vengono realmente aperte sul firewall C ma semplicemente instradate al Server SSH per mezzo del tunnel ssh in verde. A questo punto anche il firewall C è eluso.

Da questo momento in poi, le connessioni che originano dal PC che gestisce destinate all'IP 127.0.0.1 porta 5800/tcp (il client VNC per esempio) vengono automaticamente instradate al Server SSH sulla porta 5800.
Sul Server SSH abbiamo già un altro tunnel aperto che sta realizzando una connessione inversa e quindi di fatto sta instradando i pacchetti verso la porta 5800/tcp dell'IP 127.0.0.1 del Server SSH. Le porte dei tunnel che si "incontrano" sul Server SSH sono, di fatto, le stesse. ☺
Il secondo tunnel (quello rosso) instrada i pacchetti alla porta 5800/tcp del PC gestito arrivando, infine, al socket in ascolto del server TightVNC.

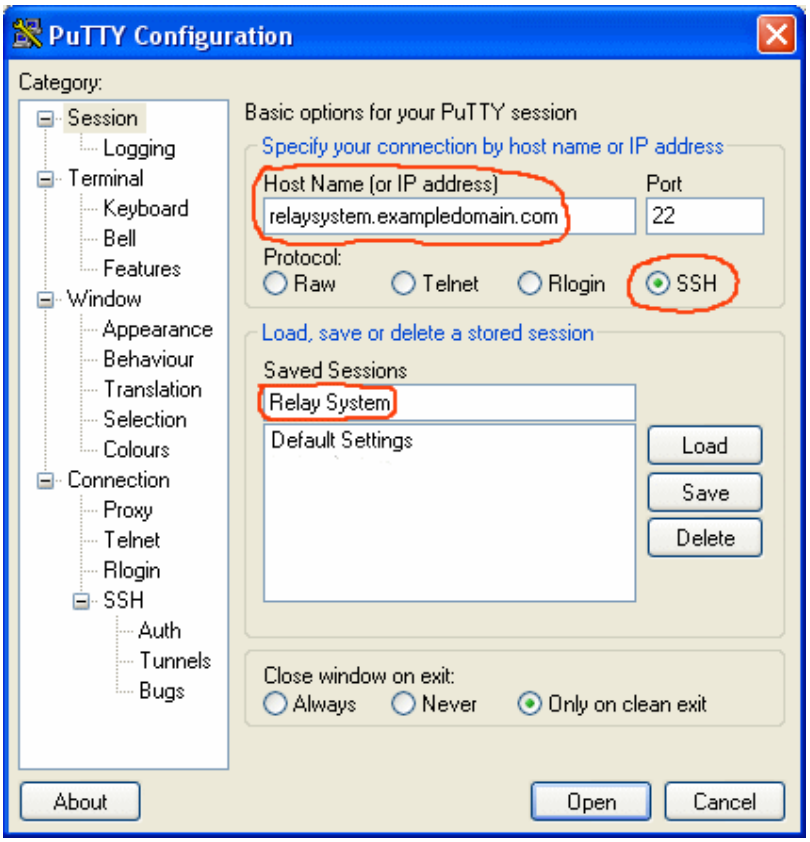
Come ci si poteva aspettare, la linea gialla rappresenta la connessione diretta che abbiamo virtualmente realizzato utilizzando il Server SSH come ponte, che in questo caso funge da "terra franca" per entrambe le parti (i PC appunto).

Istruzioni passo passo

Seguite le istruzioni per configurare entrambi i PC (quello gestito e quello che gestisce)

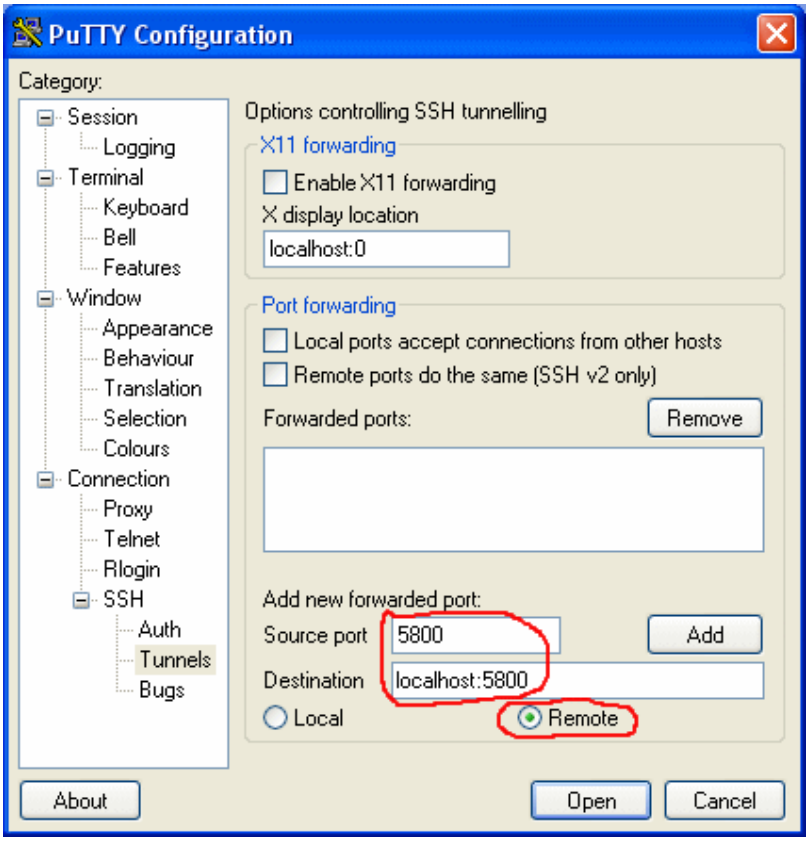
PC gestito

1) Prelevate TightVNC da http://www.tightvnc.org
2) Eseguite il setup di TightVNC e seguite le istruzioni a video. Lasciate le impostazioni di default come vengono presentate.
3) Prelevate Putty da http://www.chiark.greenend.org.uk/~sgtatham/putty/
4) Putty non richiede installazione, quindi lanciatelo, è un semplice file eseguibile.
   Appare la seguente schermata:



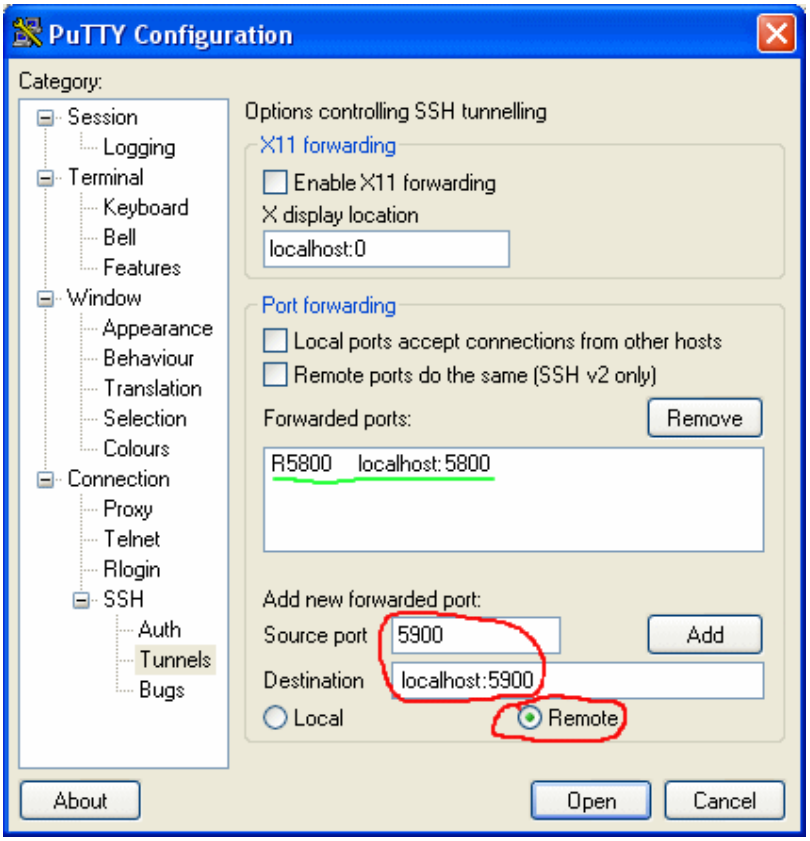
5) Riempite i campi come indicato dai cerchi rossi; sostituite relaysystem.exampledomain.com con l'indirizzo reale del Server SSH che state utilizzando e poi fate click su **Save**.

6) Ora fate click su **Tunnels** options sotto la categoria Connection/SSH, appare la schermata seguente:

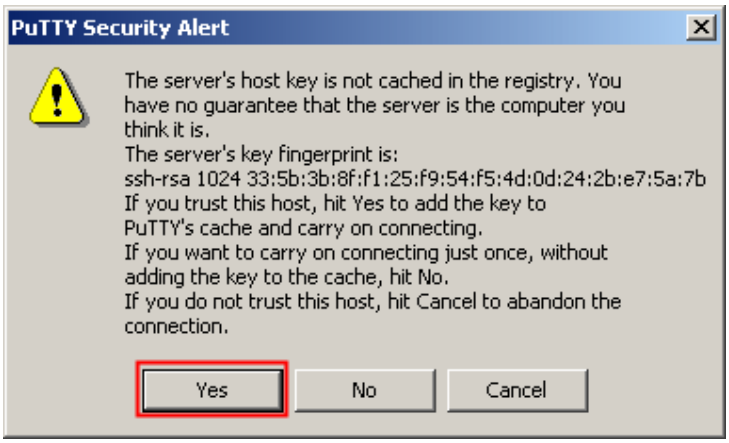


7) Riempite i campi come indicato dai cerchi rossi e fate click su **Add**.

8) Ripetete lo stesso per la porta 5900 come evidenziato nell'immagine successiva e fate click su **Add**. Notate che la porta precedente è stata aggiunta (verde sottolineata).

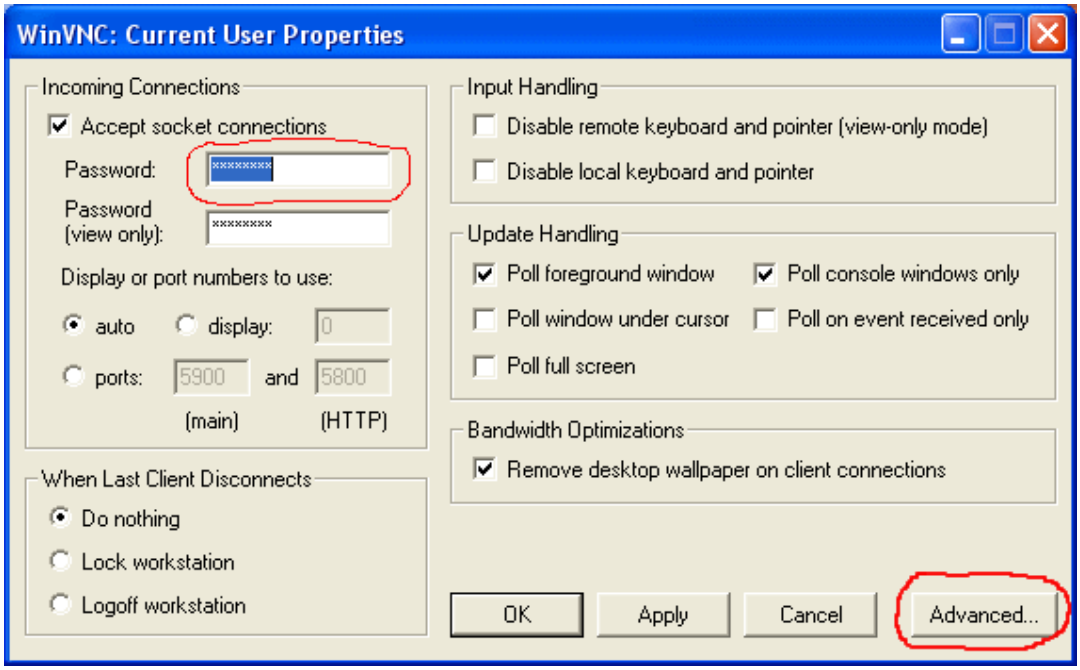


9) **Per continuare avete bisogno di un accesso valido sul Server SSH.** Ora fate click su **Open.** Dopo pochi secondi una finestra simile alla seguente vi chiederà di accettare la chiave del Server SSH remoto.

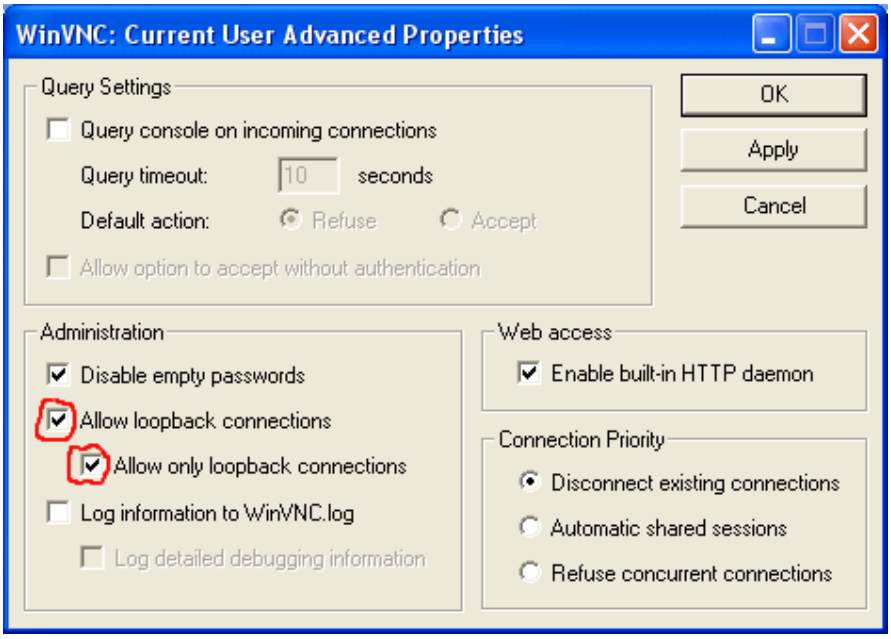


10) Fate click su YES e nella finestra successive digitate username e password. La parte di ssh è finalmente completa. ☺

11) Eseguite il server TightVNC e configuratelo per adattarsi alle vostre esigenze facendo click con il pulsante destro del mouse sulla sua icona nella system tray. Selezionate quindi **Properties**.



12) Specificate una password per permettere le connessioni al vostro PC e fate click su **Advanced**: sarà visualizzata la prossima schermata.



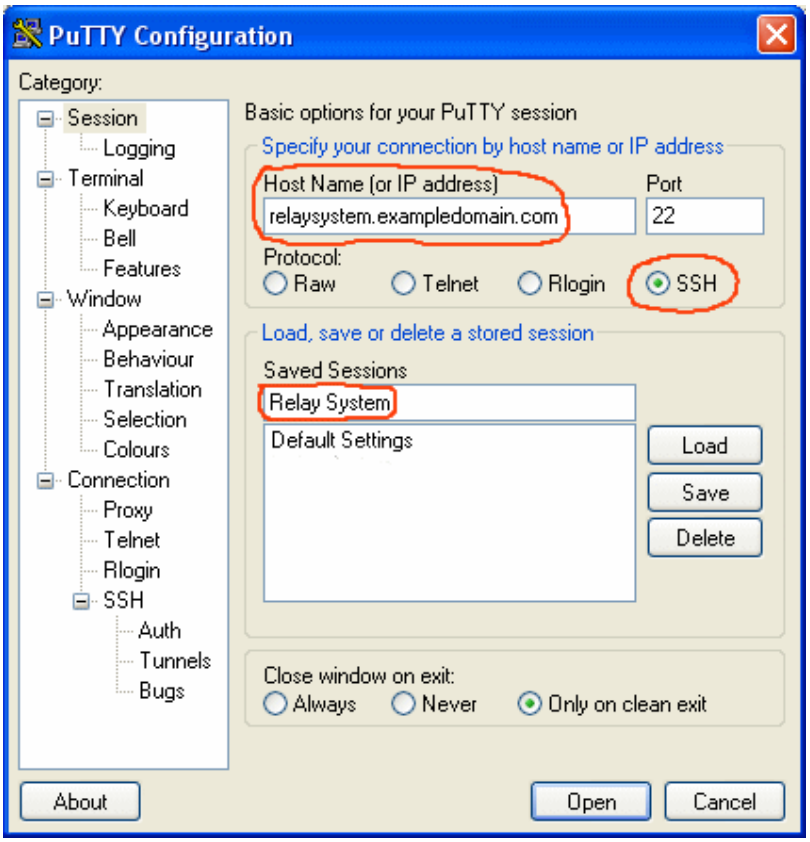
13) Spuntate “Allow loopback connections” e “Allow only loopback connections” poi fate click su **OK** per chiudere la finestra e **OK** per la precedente.

14) Avete finito! Ora dovete solo attendere l’aiuto di qualcuno dal PC che gestisce. Noterete che il puntatore del mouse comincia a muoversi per lo schermo quando il PC che gestisce si connette al vostro PC.

NOTA: per utilizzare nuovamente il sistema è necessario collegarsi al Server SSH e lanciare il server TightVNC. Le configurazioni vengono salvate e quindi non dovrete più preoccuparvi di modificarle.

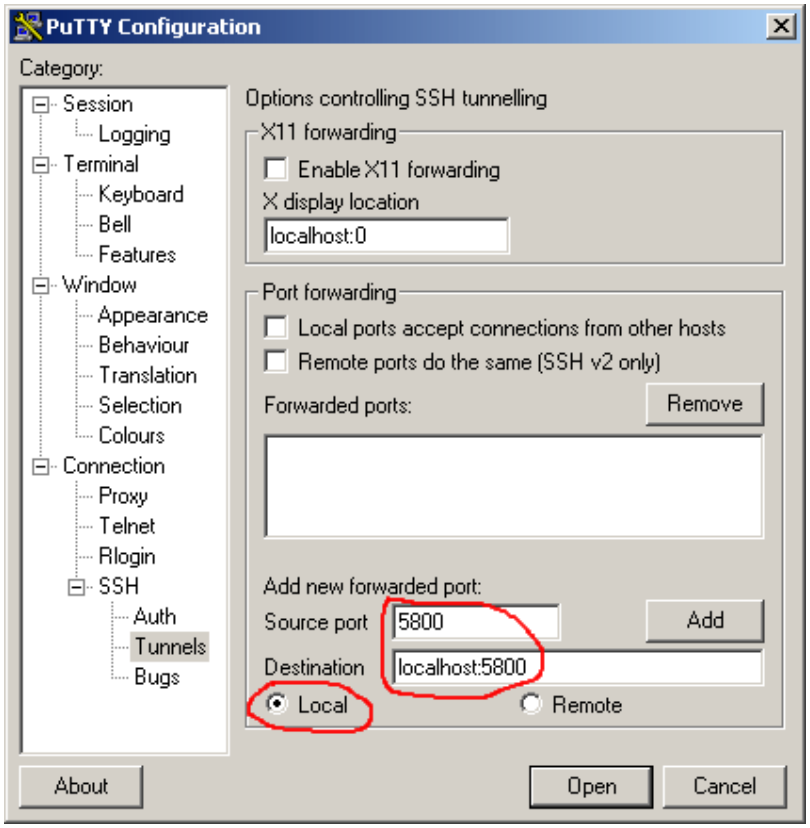
PC che gestisce

1) Prelevate TightVNC da http://www.tightvnc.org
2) Eseguite il setup di TightVNC e seguite le istruzioni a video. Lasciate le impostazioni di default come vengono presentate.
3) Prelevate Putty da http://www.chiark.greenend.org.uk/~sgtatham/putty/
4) Putty non richiede installazione, quindi lanciatelo, è un semplice file eseguibile.
   Appare la seguente schermata:

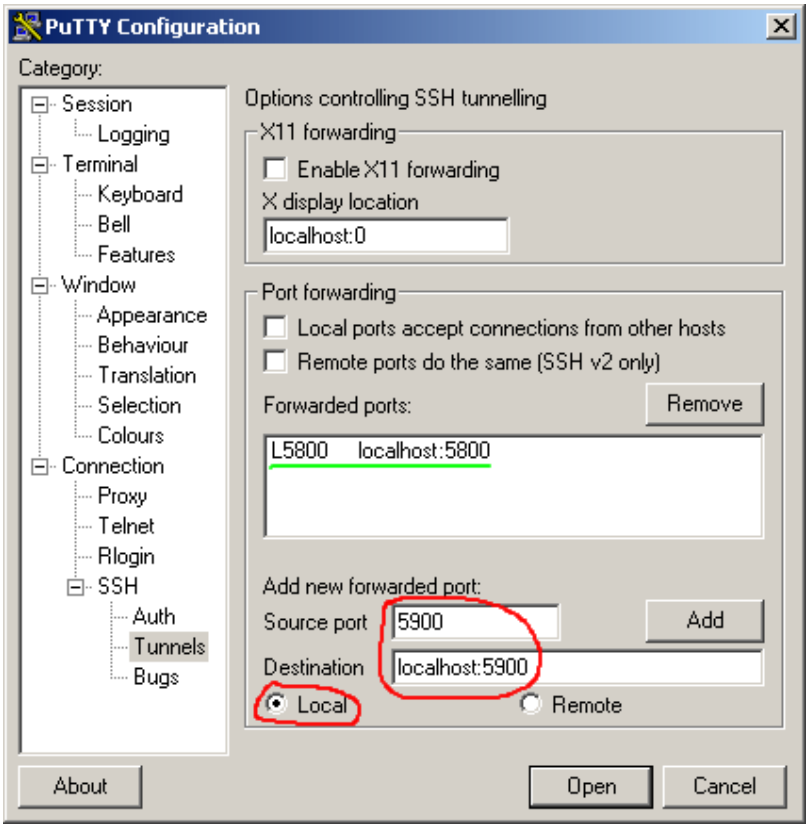


5) Riempite i campi come indicato dai cerchi rossi; sostituite relaysystem.exampledomain.com con l'indirizzo reale del Server SSH che state utilizzando e poi fate click su **Save**.

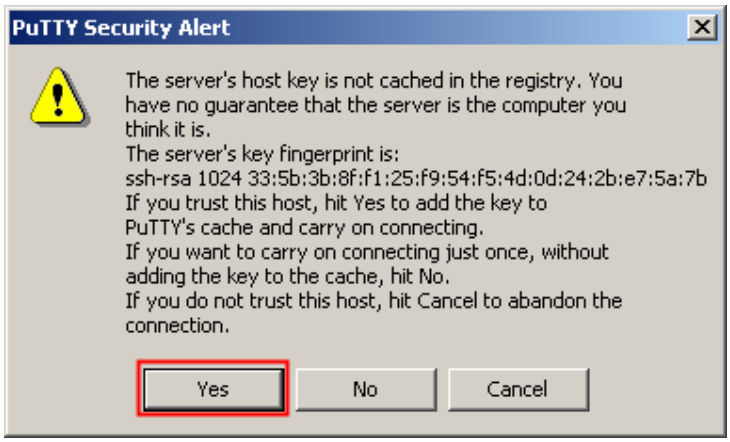
6) Ora fate click su **Tunnels** options sotto la categoria Connection/SSH, appare la schermata seguente:



7) Riempite i campi come indicato dai cerchi rossi e fate click su **Add**.
8) Ripetete lo stesso per la porta 5900 come evidenziato nell'immagine successiva e fate click su **Add**. Notate che la porta precedente è stata aggiunta (verde sottolineata).

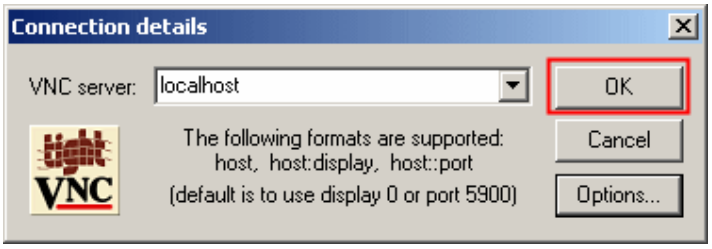


9) **Per continuare avete bisogno di un accesso valido sul Server SSH.** Ora fate click su **Open.** Dopo pochi secondi una finestra simile alla seguente vi chiederà di accettare la chiave del Server SSH remoto.

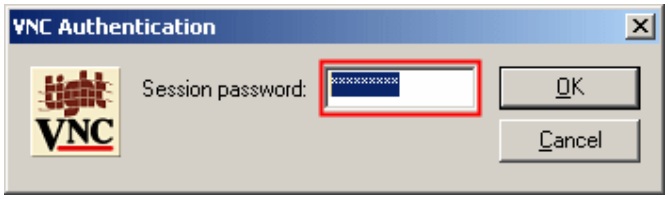


10) Fate click su YES e nella finestra successive digitate username e password. La parte di ssh è finalmente completa. ☺

11) Eseguite il cliente TightVNC (Fast compression o Best compression). Appare la schermata seguente:



12) Fate click su **OK**. Se tutto funziona ora dovreste vedere la schermata:



13) Digitate la password di TightVNC che avete impostato durante le istruzioni passo passo per la configurazione del PC gestito e fate click su **OK.** Se tutto va bene vedrete la schermata del PC gestito… e buon troubleshooting! Ora avete pieno accesso al PC gestito esattamente come se foste presso il vostro amico/cliente/collega.

Suggerimenti per la risoluzione di problemi

Se qualcosa non funziona provate a seguire questi suggerimenti.

Da un prompt dei comandi (shell) scrivete:

`netstat -an`

su entrambi i PC (quello che gestisce e quello gestito) per constatare se le due linee seguenti sono presenti nell'elenco che verrà visualizzato dopo aver premuto il tasto invio:

```
TCP    127.0.0.1:5800         0.0.0.0:0              LISTENING
TCP    127.0.0.1:5900         0.0.0.0:0              LISTENING
```

Se non lo sono, i vostri tunnel non sono stati creati da Putty.
Controllate la configurazione rileggendo la guida per constatare se i tunnel sono impostati correttamente.
Un'altra possibilità è che la funzionalità di "port-forwarding" del demone sshd del Server SSH è stata disabilitata dall'amministratore. Il solo modo che avete per sistemare questo problema è di contattare l'amministratore e chiedergli di abilitarla.

NOTA: La configurazione di default di sshd è di permettere il port-forwarding.

Se non riuscite a connettervi al Server SSH provate a raggiungerlo digitando:

`telnet ipdelserverssh 22`

sostituendo la parola **`ipdelserverssh`** con l'indirizzo IP reale del Server SSH a cui vi state connettendo.

Come risultato dovreste vedere una linea simile alla seguente:

SSH-2.0-OpenSSH_3.5p1

Questo significa che potete connettervi al Server SSH e quindi che la configurazione del firewall non è un problema.

Controllate meglio la coppia login/password che digitate ed eventualmente chiedete all'amministratore del Server SSH i parametri specifici riguardo l'autenticazione ssh.