SmoothWall Support : Setting up **Greenbow** VPN Client
Wednesday, January 5, 2005

Greenbow VPN client, può essere scaricato da http://www.thegreenbow.com per essere utilizzato per connettere **SmoothWall Corporate Server 3** con il modulo **SmoothTunnel 3.1** installato.

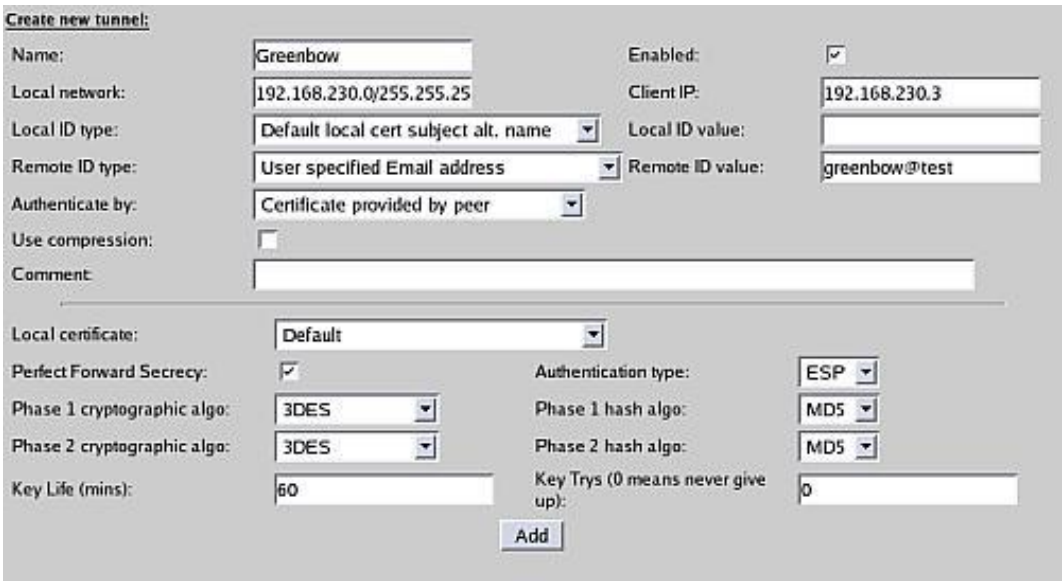
Preparazione alla configurazione di un Road warrior:

Greenbow VPN client necessita del certificate CA e di un certiicato creato appositamento per esso.
È altresì necessario configurare una connessione Road warrior nell'interfaccia di SmoothTunnel.
L'esempio seguente utilizzerà i valori sotto elencati:

IP esterno di SmoothTunnel:	192.168.72.236
IP Subnet dietro SmoothTunnel:	192.168.230.0/255.255.255.0
IP del client Road Warrior quando connesso:	192.168.230.3
ID type+value per il certficato SmoothTunnel:	DNS: greenbow.test
ID type+value per il certificate Greenbow :	EMAIL: greenbow@test

Configurazione della connessione di SmoothTunnel IPSEC Road Warrior.

Creare un certificato per il client **Greenbow**. Una volta fatto passare alla configurazione della connessione **Greenbow**. Segue uno screenshot della configurazione con i dati citati sopra.

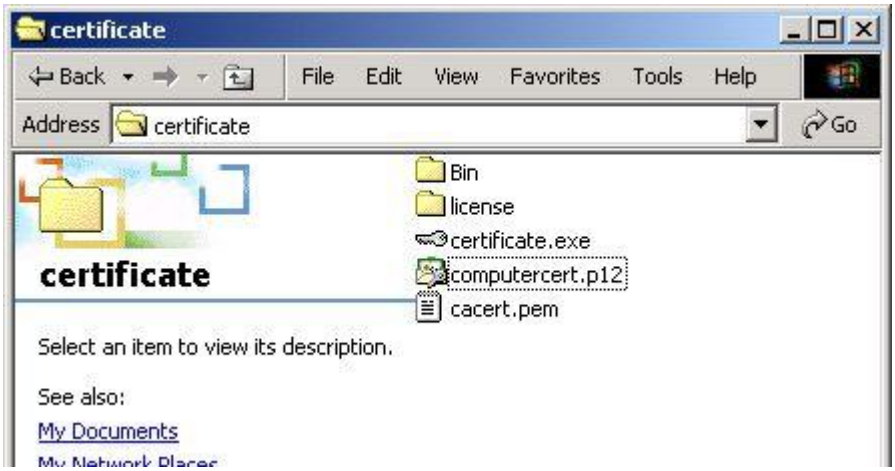


Questa configurazione è il modo standard per le Road warrior in IPSEC. Questa configurazione può essere utilizzata anche per SSH Sentinel, Safenet Softremote e Greenbow.
Notare il "Local" e il "Remote" ID Type e relativo valore. L'ID type remoto e il valore sono inseriti mentre l'ID locale e il suo valore saranno ricavati automaticamente dal certificato selezionato nella pagina di "global".

Preparazione del client Greenbow.

Dopo l'installazione di GreenBow VPN Client, sarà necessario recuperare da SmoothTUnnel il CA e il certificato creato appositamente per Greenbow . Esportare quindi dalla sezione SmoothTunnel il CA in formato PEM ed esportare il certificato per GreenBow come PKCS#12. Affinchè Greenbow possa utilizzare il PKCS#12 risulterà necessario convertirlo in formato PEM. Sul sito Greenbow è disponibile gratuitamente un programma che effettua tale conversione: http://www.thegreenbow.com/vpn_tool.html . Scaricare l'utility e scompattarla in una cartella sul desktop, dopodichè spostare il CA ("cacert.pem") e il certificato PKCS#12 ("computercert.p12") nella stessa cartella sul desktop.

Il contenuto della cartella dovrebbe risultare pressapoco:

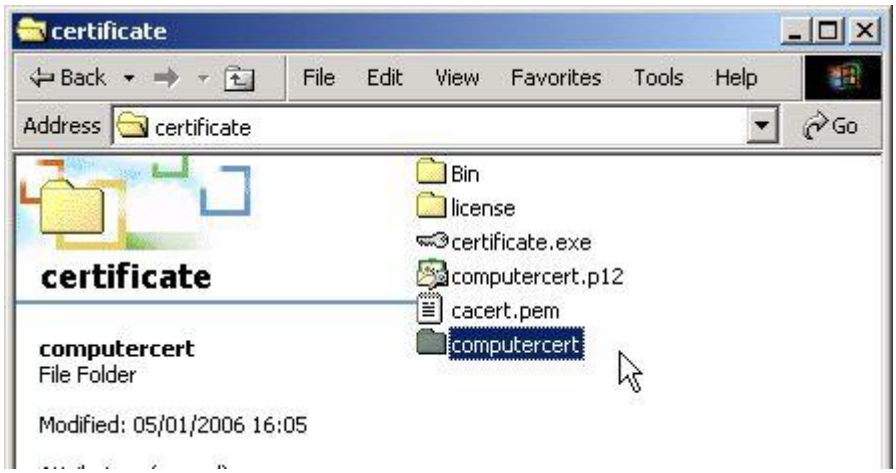


I file necessari sono: "*certificate.exe*", "*computercert.p12*" e "*cacert.pem*"

Lanciare"*certificate.exe"* e apparirà questa schermata:

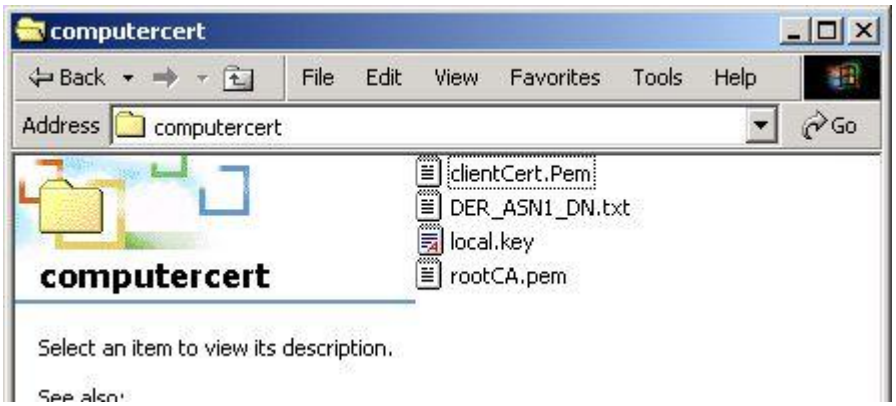
Click su "Select a new p12 certificate" e scegliere "*computercert.p12*" esportato da **SmoothTunnel**.
Inserire la password del p12 quando sarà richiesta.
Un messaggio di conferma apparirà.
Quindi fare click sul bottone "close".

Dopo la conversione del certificate il contenuto della cartella risulterà:



Si noti una nuova cartella chiamata "*computercert*".

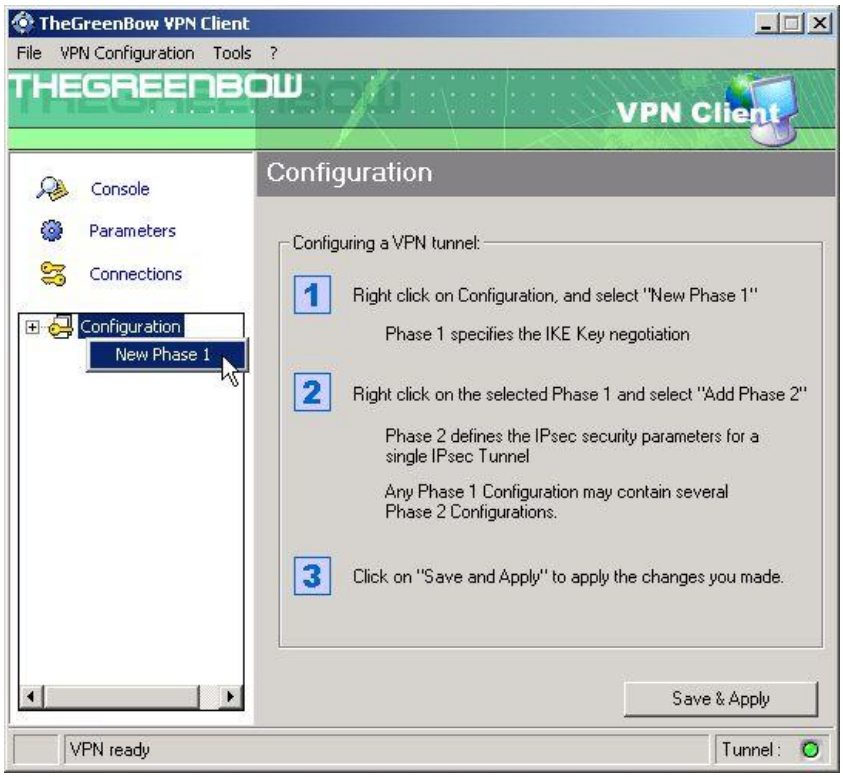
Aprendo la cartella "*computercert*" saranno presenti I seguenti file:



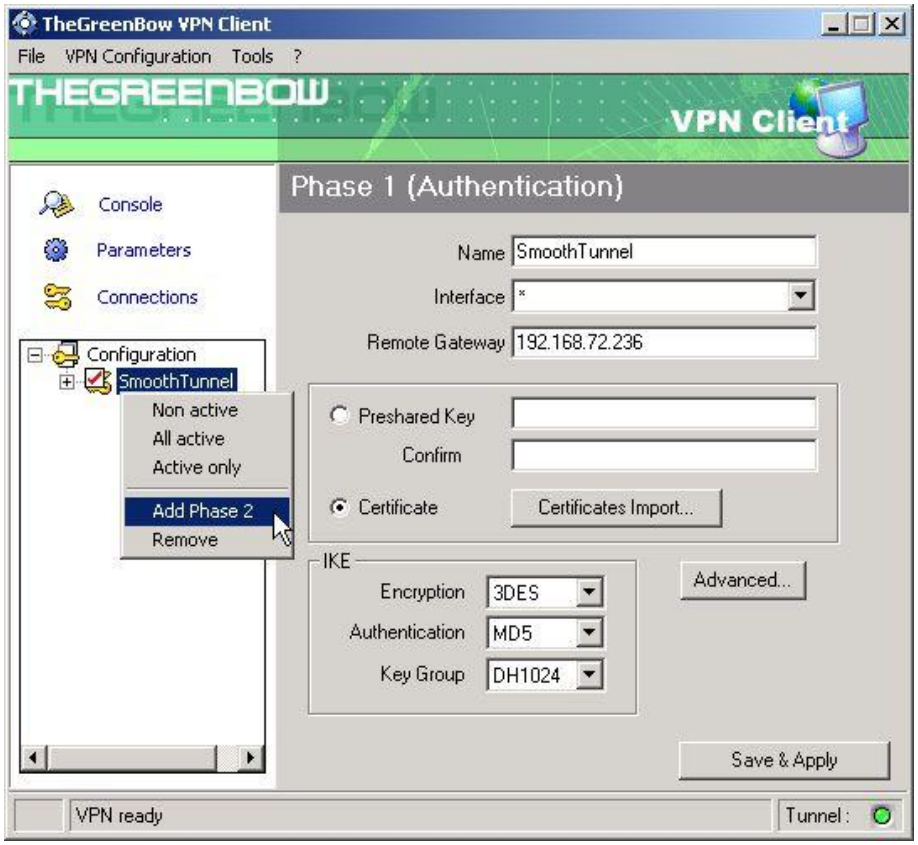
I file necessari da questa cartella sono: "clientCert.pem" e "local.key" files. Il file "rootCA.pem" non sarà utilizzato. Utilizzare il "cacert.pem" esportato da **SmoothTunnel**. Una buona idea è rinominare questi file con nomi rilevanti come: "*GreenbowAtTest.pem*", "*GreenbowAtTest.key*" and "*GreenbowAtTestCA.pem*"

Configurazione di Greenbow VPN client:

Lanciare Greenbow VPN client e cliccare col tasto destroy su "*configuration*" per aggiungere una "phase 1":



Una volta aggiunta, rinominarla in "*SmoothTunnel*".:



Inserire l'ip esterno di SmoothTunnel oppure l' host name nel campo "Remote Gateway".

Selezionare "*Certificate*".

Selezionare l'appropriato IKE encryption. Dovrà combaciare con con quanto settato in **SmoothTunnel**. Selezionare il valore più alto disponibile in "key group".

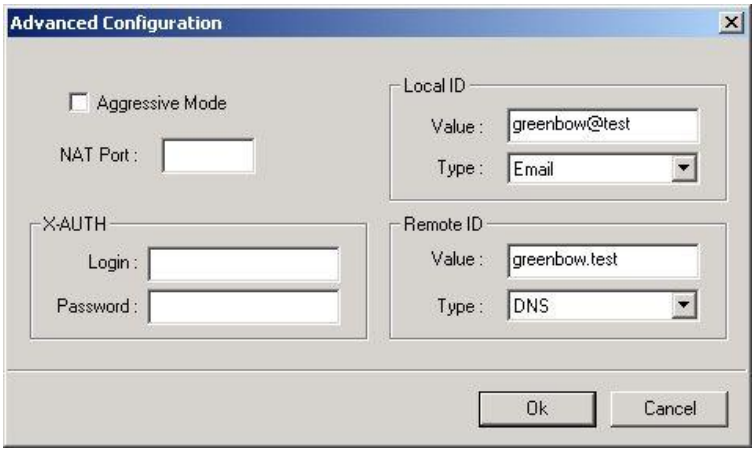
Prima di configurare la "phase 2" diamo uno sguardo ai certificati importati.

Fare click su "Certificates Import", apparirà questa maschera:

Il certificato di root (CA)"*cacert.pem*" o "*GreenbowAtTestCA.pem*".

Il certificate client "*clientCert.pem*" o "*GreenbowAtTest.pem*".

La chiave private "*local.key*" o "*GreenbowAtTest.key*".

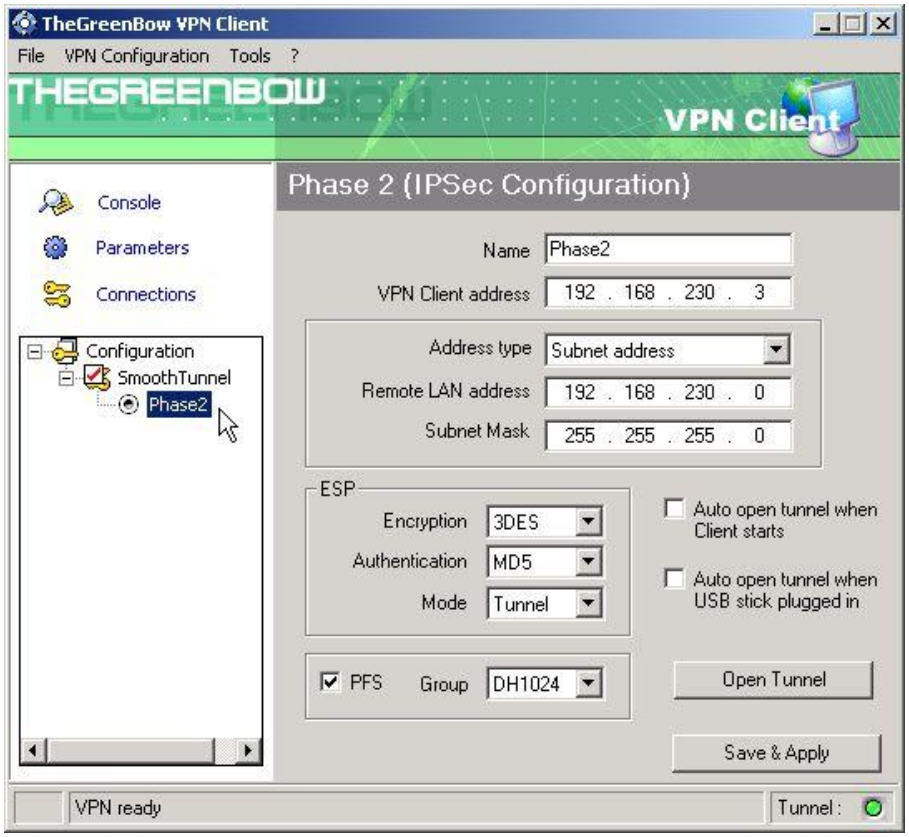


Fare click su "advanced button" e settare "ID type" e "values":

"Local ID" sarà il valore corrispondente utilizzato nel certificate "*GreenbowAtTest*". In questo caso di tipo "email" con il valore "*greenbow@test*"

"Remote ID" sarà il valore corrispondente per il certificato usato in SmoothTunnel. In questo caso il nome DNS, "*greenbow.test*"

A questo punto aggiungere una “phase 2” alla connessione **SmoothTunnel**. Tasto destro del mouse su **SmoothTunnel** in **Greenbow** e selezionare “Add Phase 2”. Dopodichè visualizzare la schermata “new phase 2”:



Cambiare i valori in modo appropriato:

Inserire l’indirizzo IP del VPN client allocato al momento della connessione a **SmoothTunnel** nel campo *“VPN Client address”*.

Inserire le informazioni relative alla rete/maschera di rete nei campi successivi.

Nella sezione **ESP**, selezionare il valore corrispondente alla “phase 2 “ settato in **SmoothTunnel**.

PFS sta per “Perfect Forward Secrecy” e deve essere selezionato in entrambi. (Client e **SmoothTunnel)**.

Click “*Save & Apply*” e cliccare su “*Open Tunnel*”. Nella console dovreste vedere un connessione effettuata con successo: