CONFIGURAZIONE IPSEC POLICY IN WINDOWS 2003 SERVER

Aprire la cartella Administrative Tools posta sul Desktop

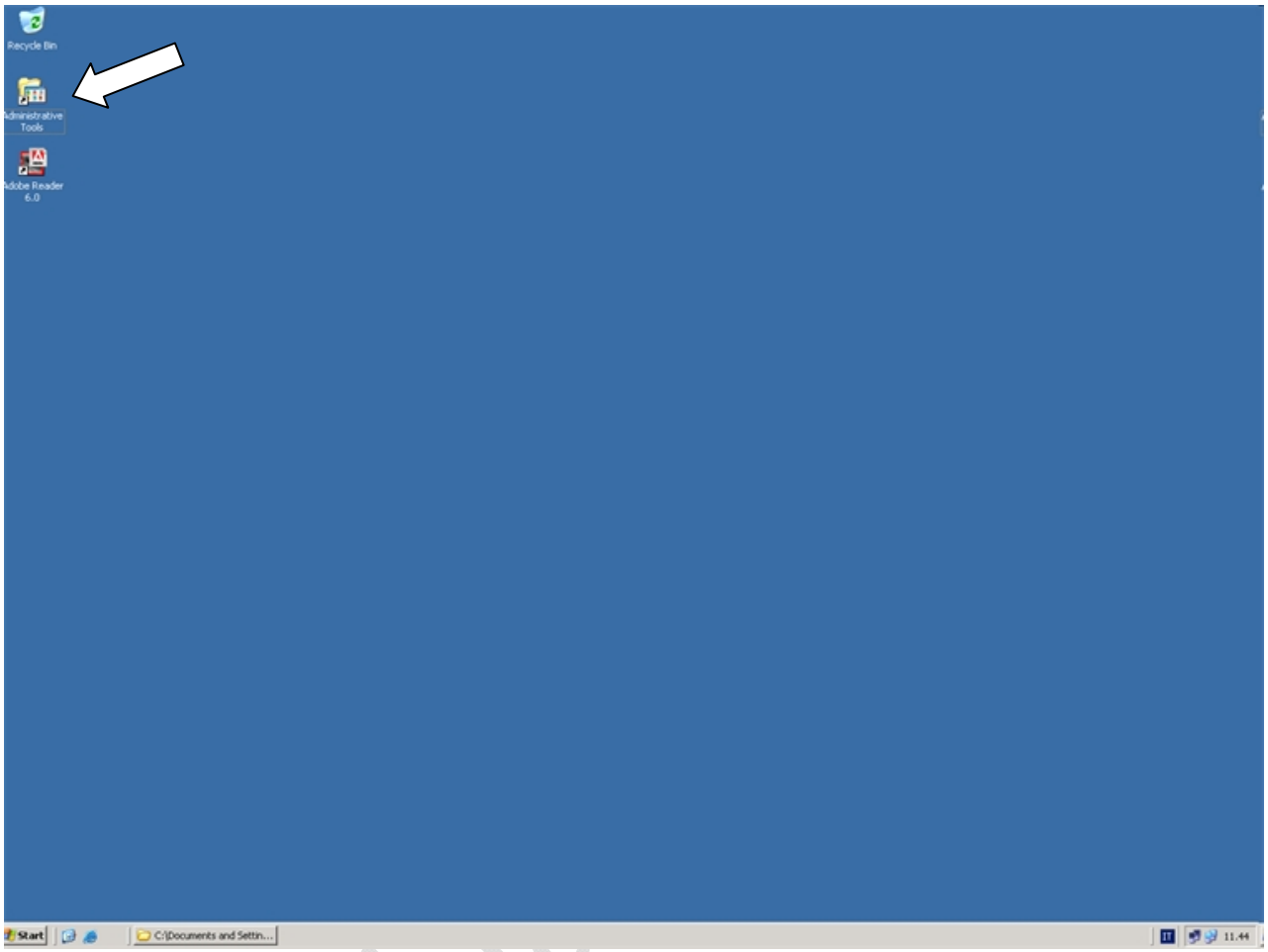

Fig.1

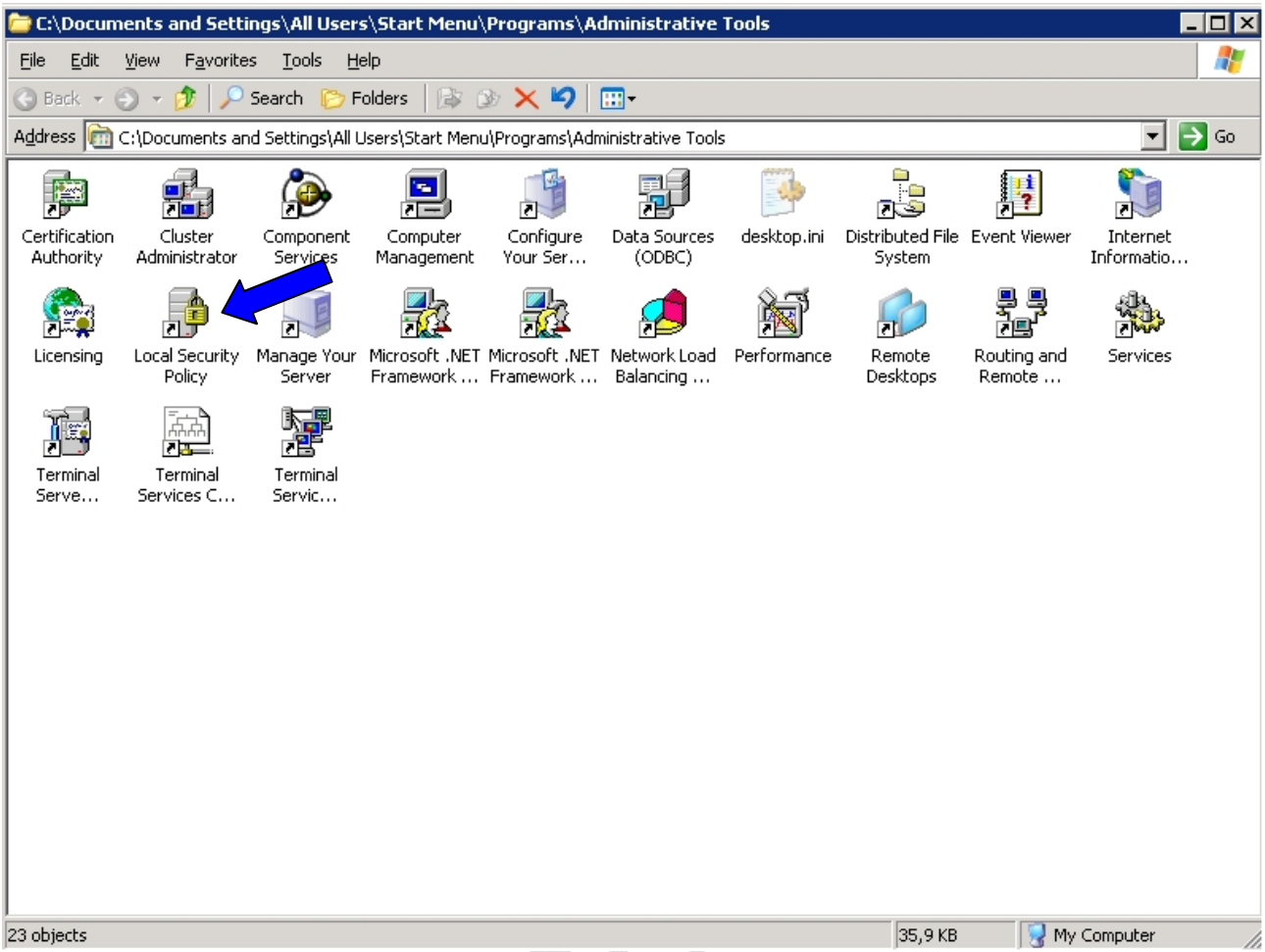

Fig.2

Cliccare su **Local Security Policing** come raffigurato in Figura 2.

Si aprirà la schermata come in Figura 3.

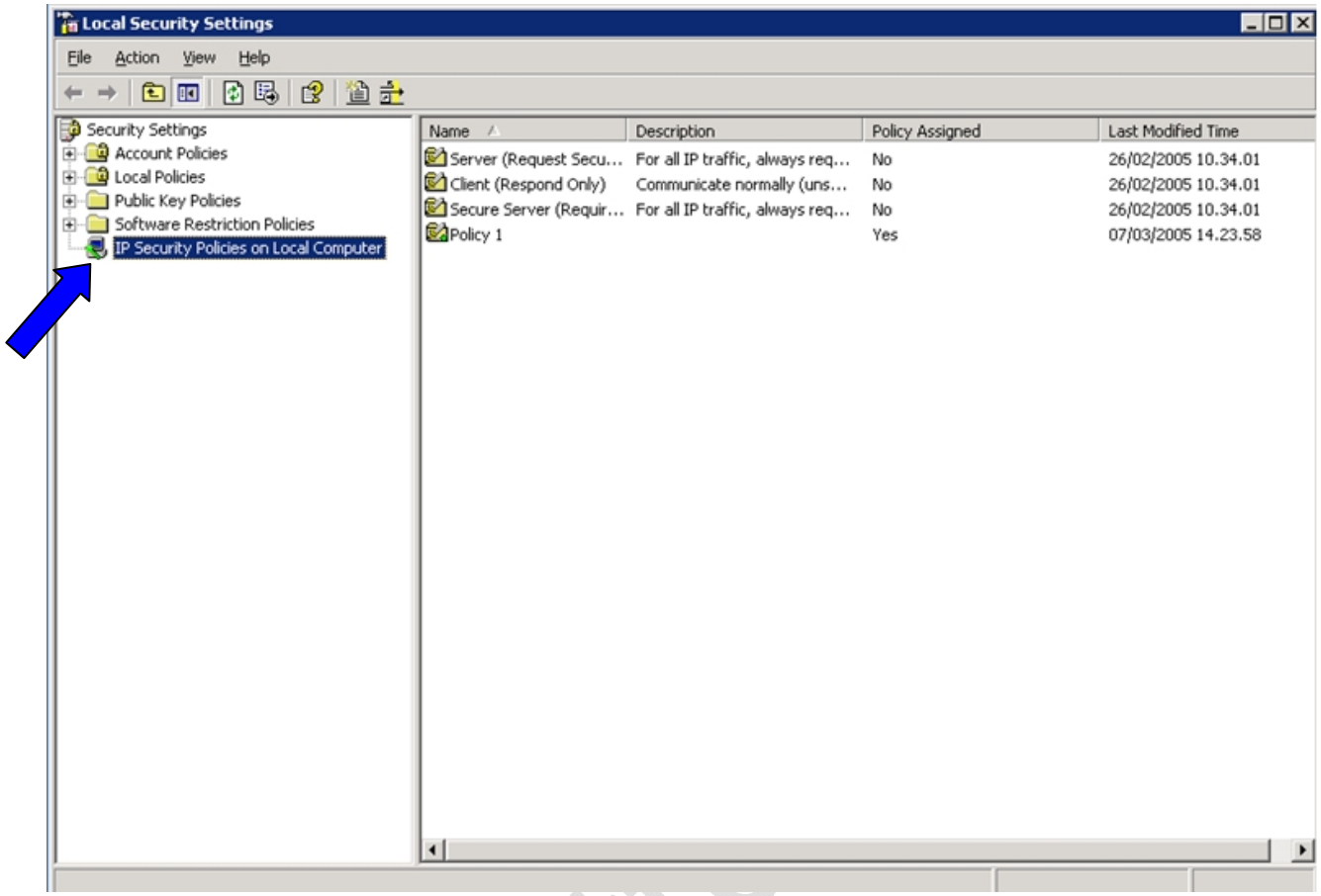

Fig.3

Clicchiamo di destro su **IP Security Policies on Local Computer** e selezioniamo **Manage IP filter lists and filter actions....** come mostrato in Figura 4.

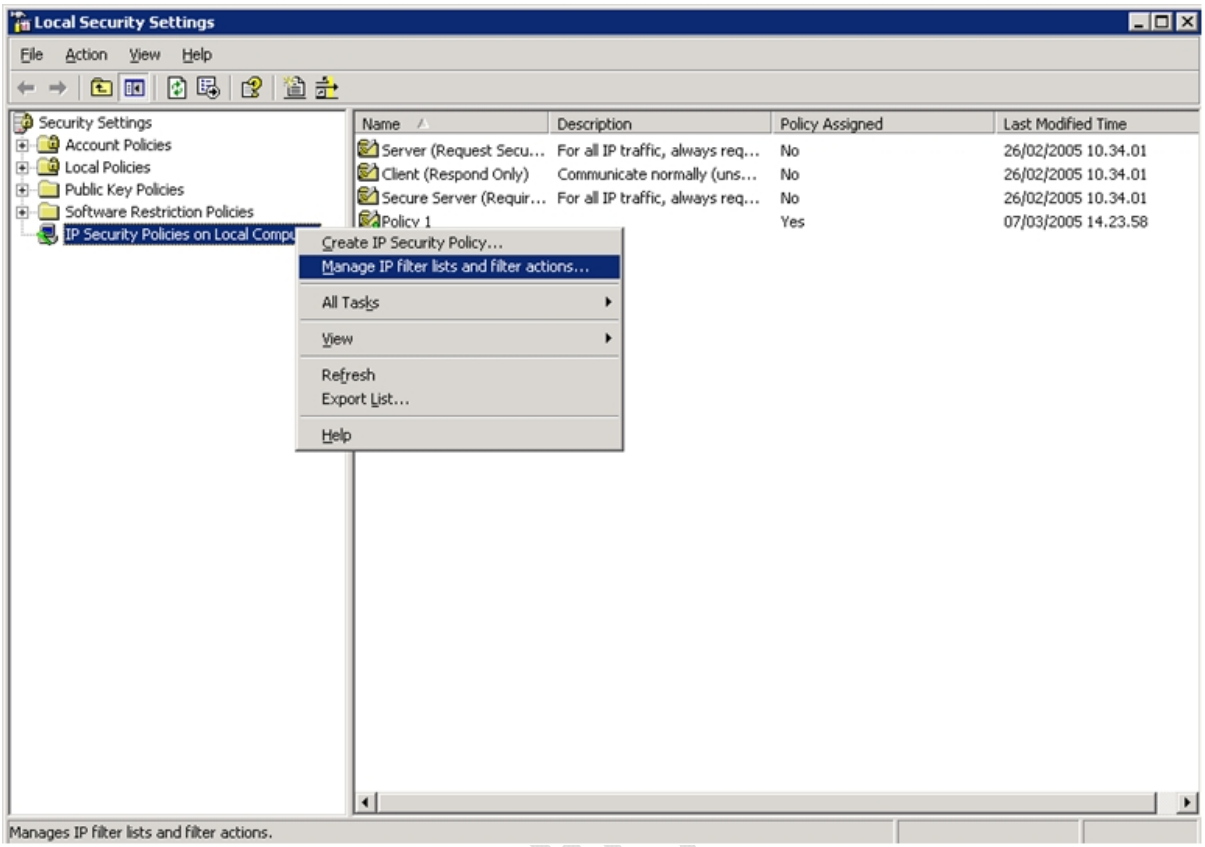

Fig.4

La prima cosa che dobbiamo fare è creare un **Filter Actions**.

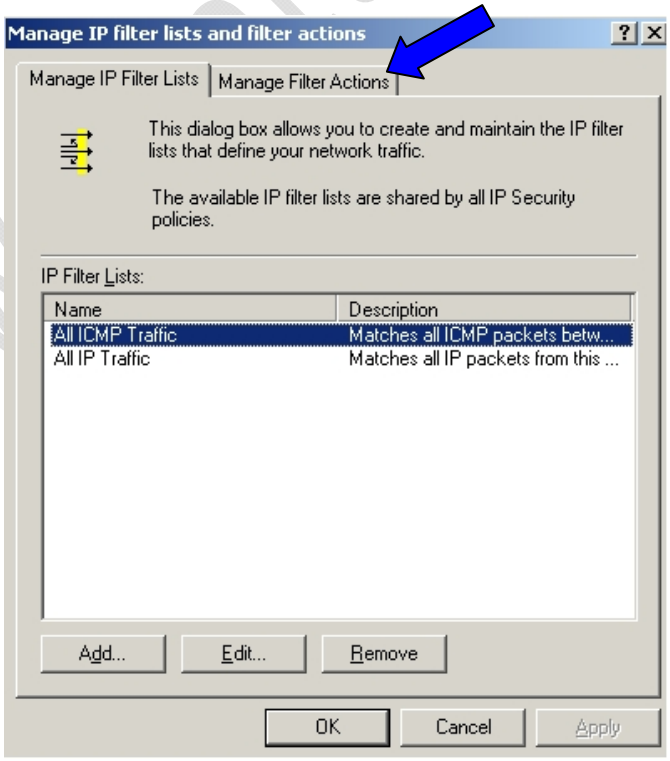

Fig.5

Quindi ci spostiamo all'interno di **Manage Filter Actions**.

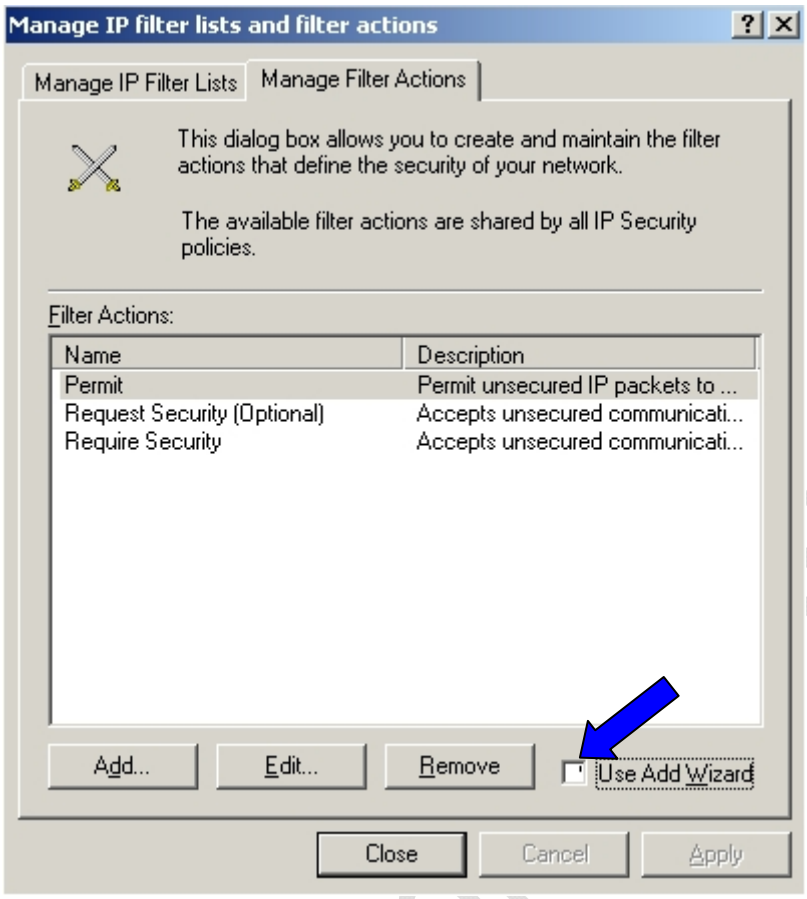

Fig.6

Qui deselezioniamo **Use Add Wizard** e clicchiamo su **Add**.

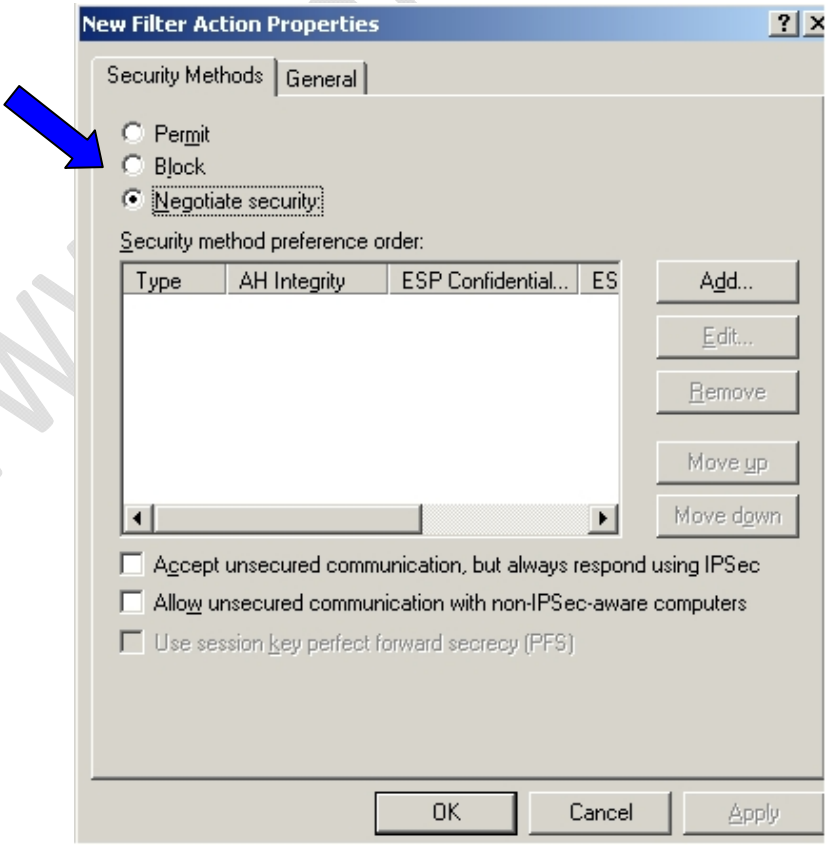

Fig.7

Quindi selezioniamo l'opzione **Block** e clicchiamo su **Apply** ottenendo un risultato come in Figura 8.

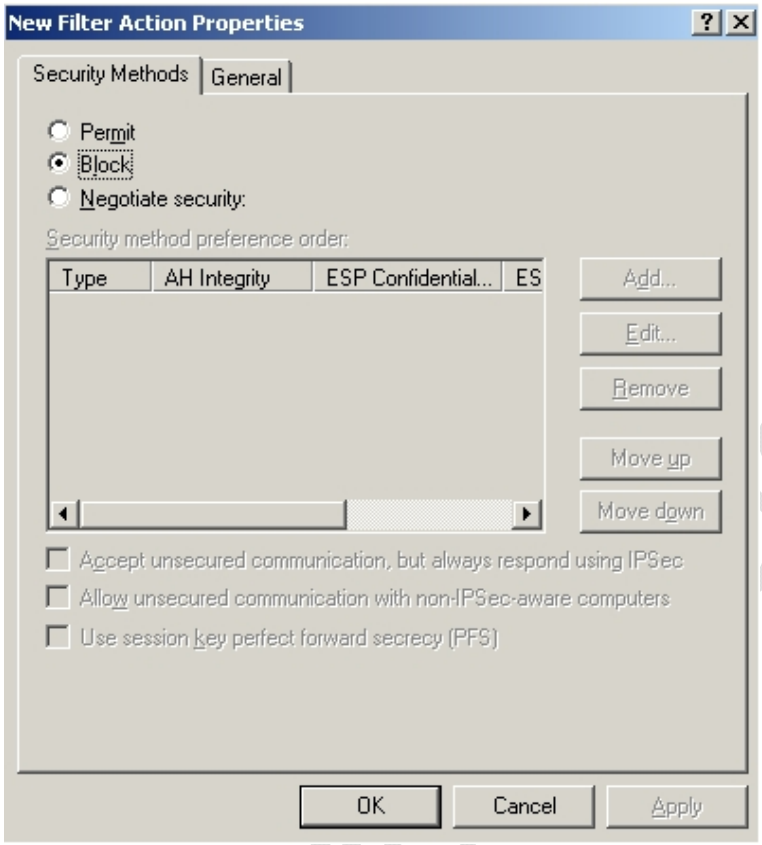

Fig.8

Poi nella sezione **General** inseriamo all'interno del campo Name **: Block**.

Clicchiamo su **Apply** (vedi Figura 9)

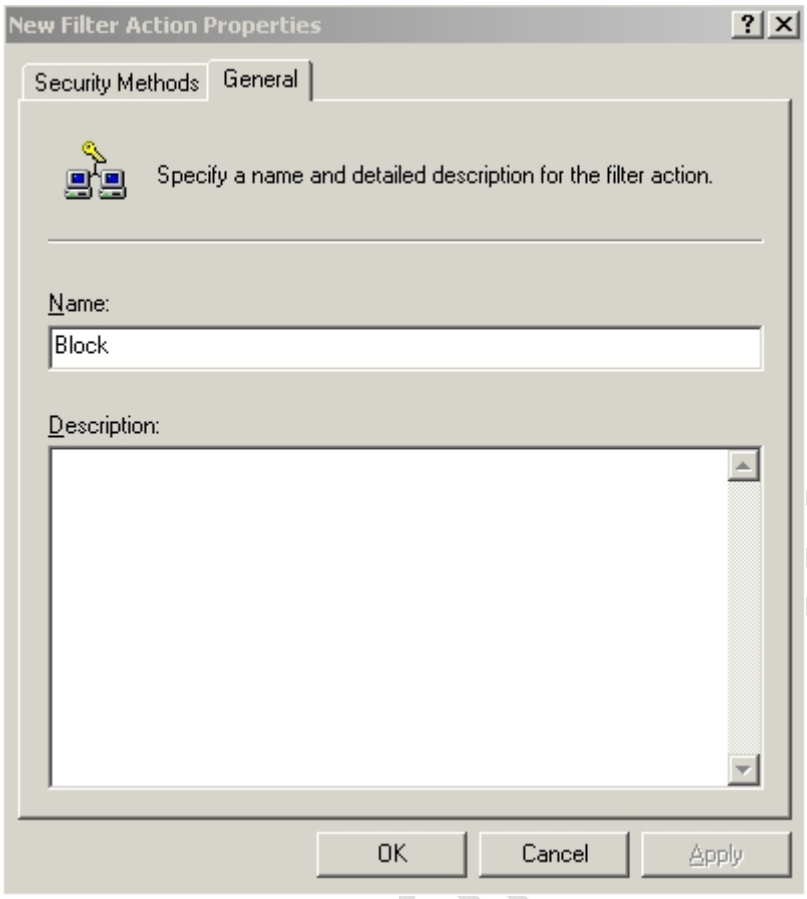

Fig.9

Quindi clicchiamo su **OK**.

Dovremmo ottenere un risultato come quello in Figura 10.

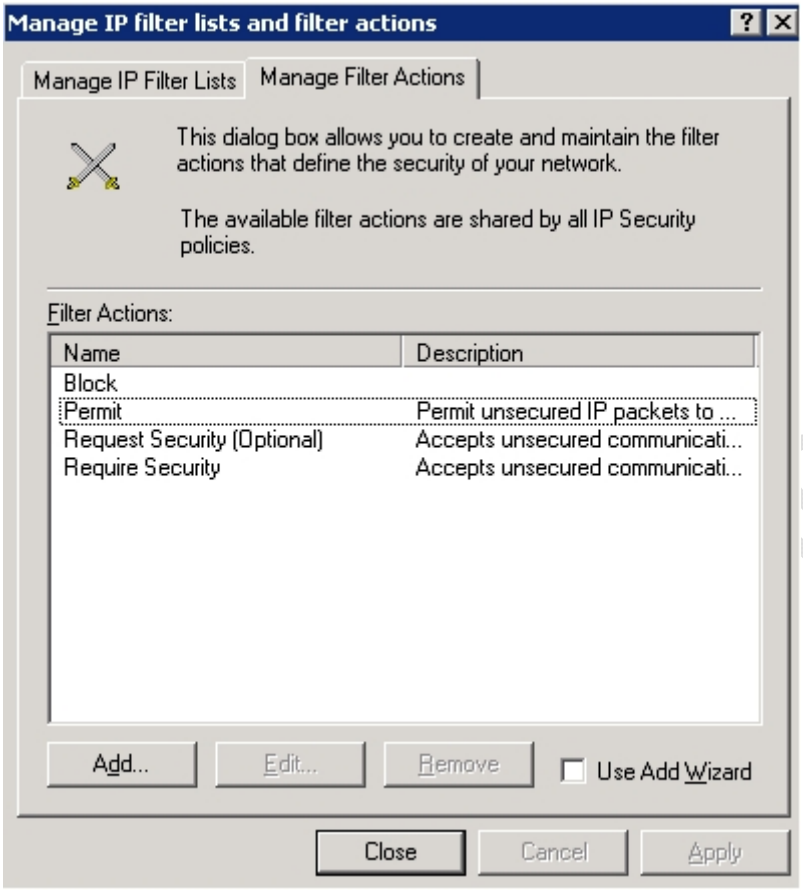

Fig.10

Adesso ritorniamo alla precedente schermata

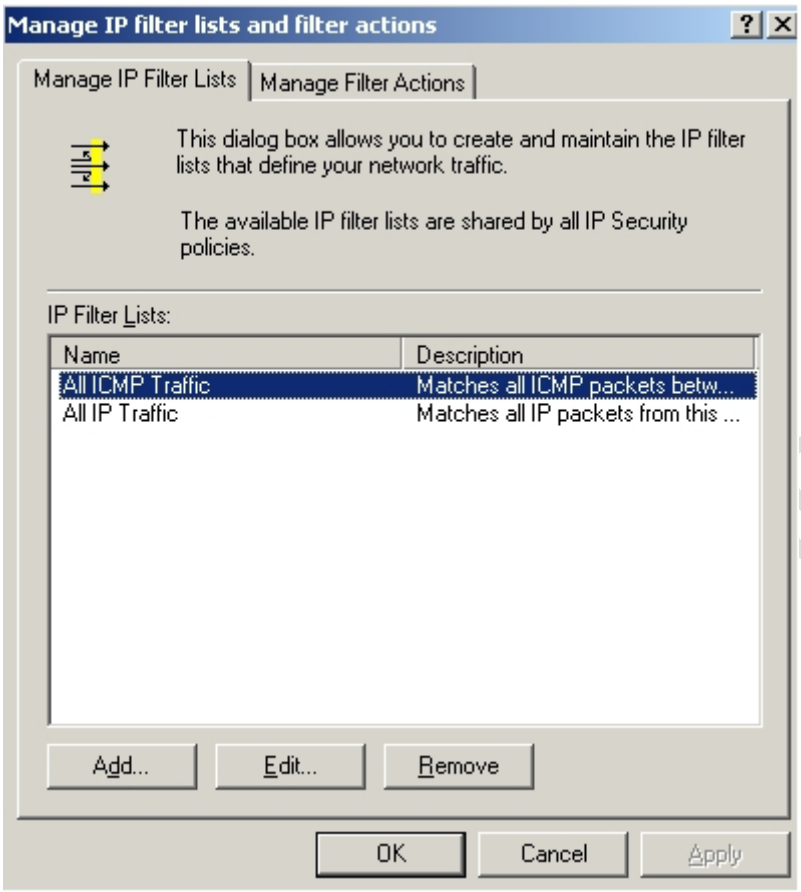

Fig.11

Adesso dalla schermata di Figura 11 aggiungiamo dei filtri IP.

Di default sono presenti All ICMP Traffic e All IP Traffic.

Quindi clicchiamo su **Add**

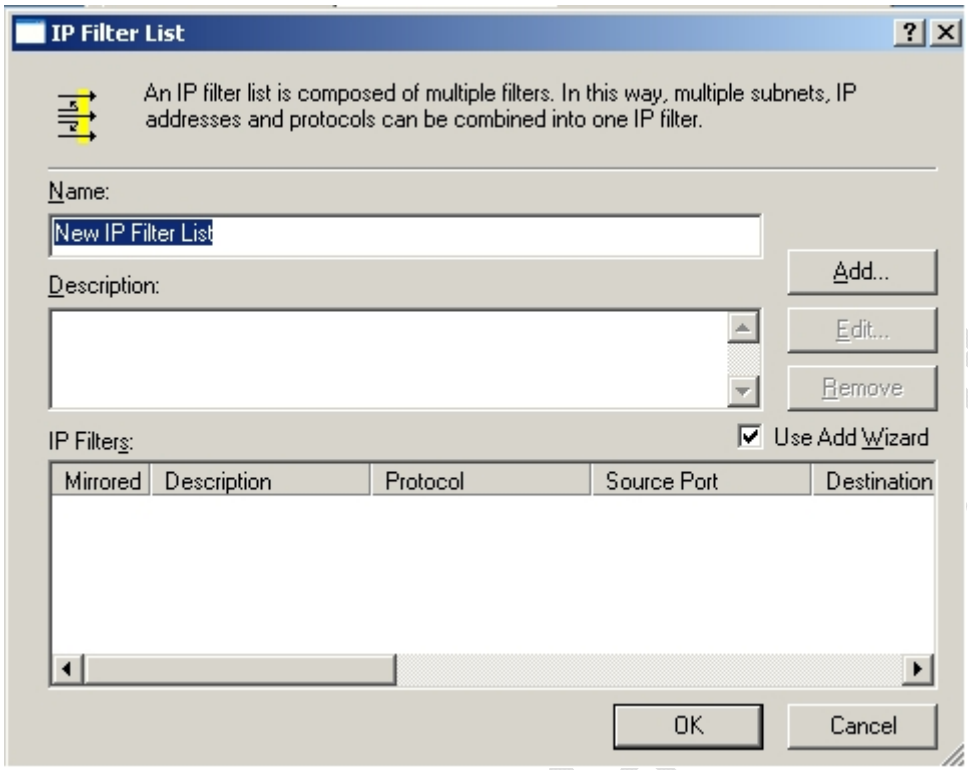

Fig.12

Adesso nel campo Name inseriamo il nome del filtro ES: DNS Traffic, il campo Description lo lasciamo in bianco e deselezioniamo l'opzione **Use Add Wizard** come in Figura 13.

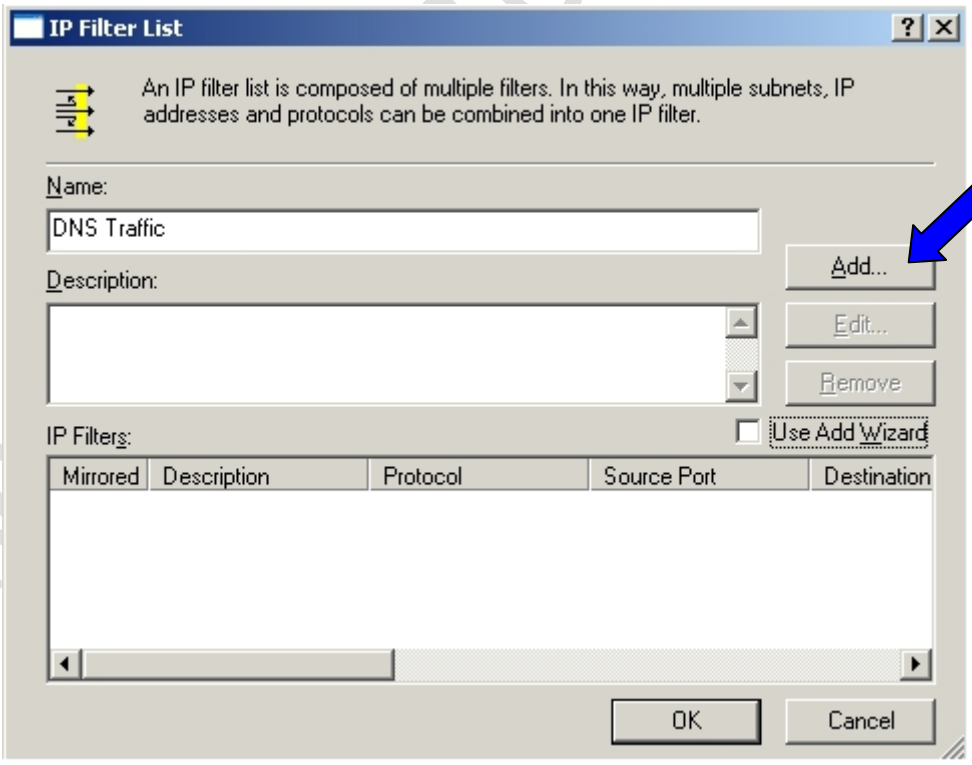

Fig.13

Adesso clicchiamo su **Add** come indicato dalla freccia di Figura 13.

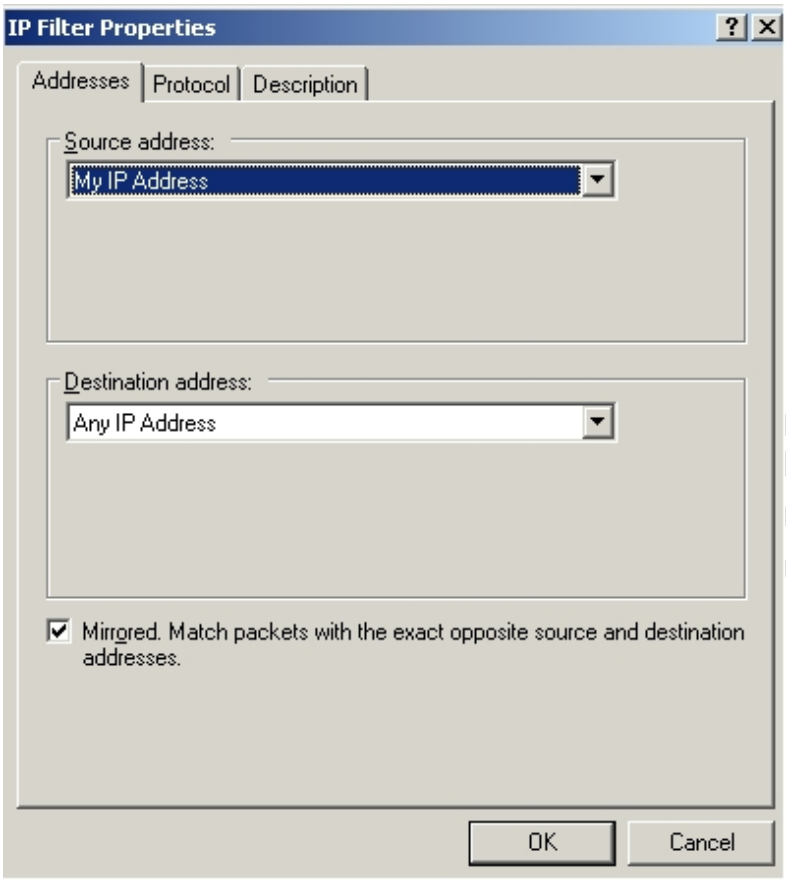

Fig.14

All'interno di questa schermata possiamo configurare il **Source Address** e il **Destination Address**.

Andando all'interno del menù a tendina possiamo selezionare una tra le nove opzioni presenti. Vedi Figura 15.

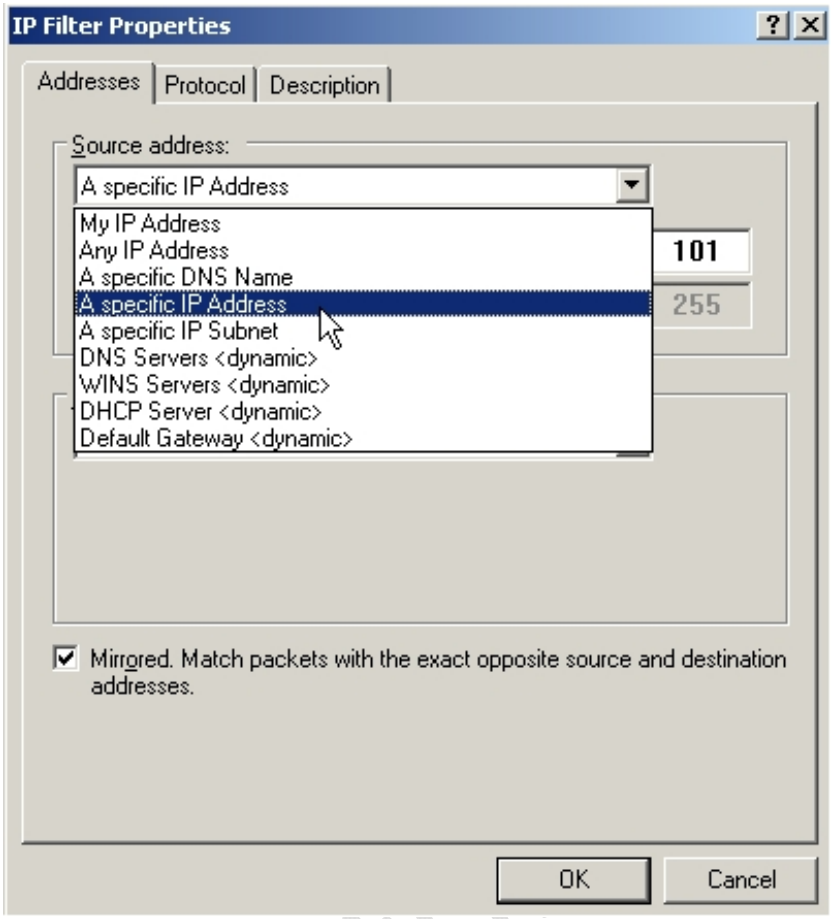

Fig.15

Quelle da noi più utilizzate sono:

- Any IP Address : Da qualunque indirizzo IP
- A specific IP Address : Specifichiamo solo l'indirizzo IP sorgente
- A specific IP Subnet : Specifichiamo l'indirizzo IP e la Subnet Mask

Una volta selezionata la sorgente e la destinazione (vedi Figura 16), scegliamo se fare il **Mirrored**. Infatti in basso a destra della schermata come segnalato in Figura 16 c'è una casellina che noi possiamo spuntare o deselezionare.
Se scegliamo di selezionare questa opzione non facciamo nient'altro che permettere ai pacchetti con opposta destinazione e sorgente di arrivare fino a noi.
In pratica tutti i pacchetti di ritorno dalla destinazione arriverebbero alla sorgente.

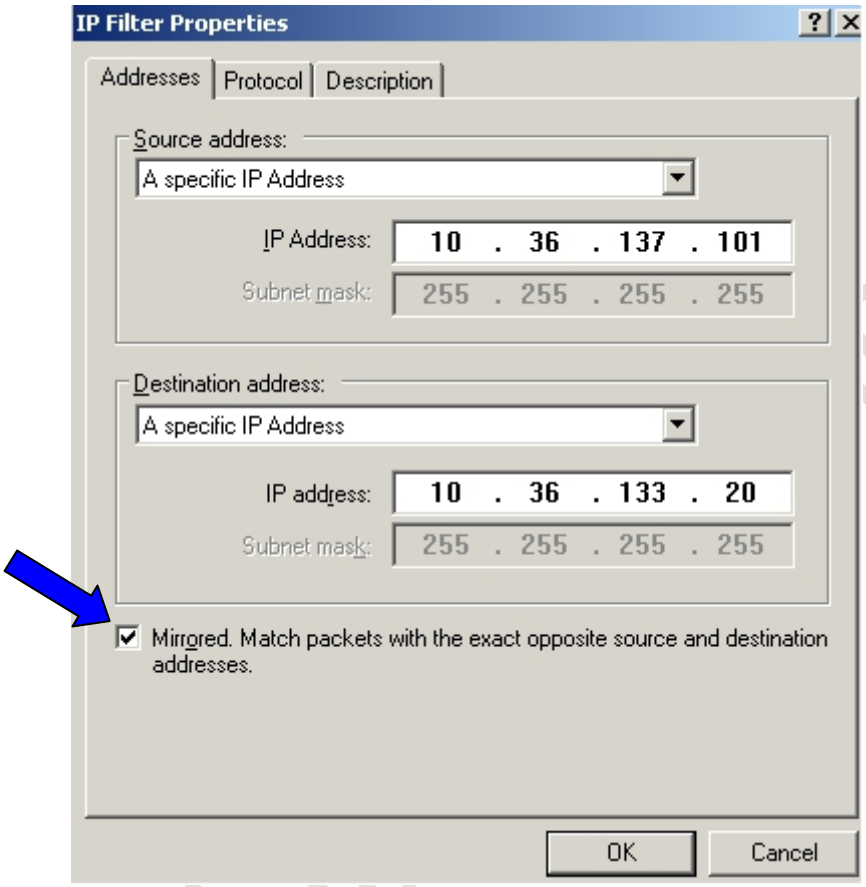

Fig.16

Fatto questo passiamo alla scelta del protocollo cliccando sulla linguetta **Protocol** come raffigurato in Figura 17

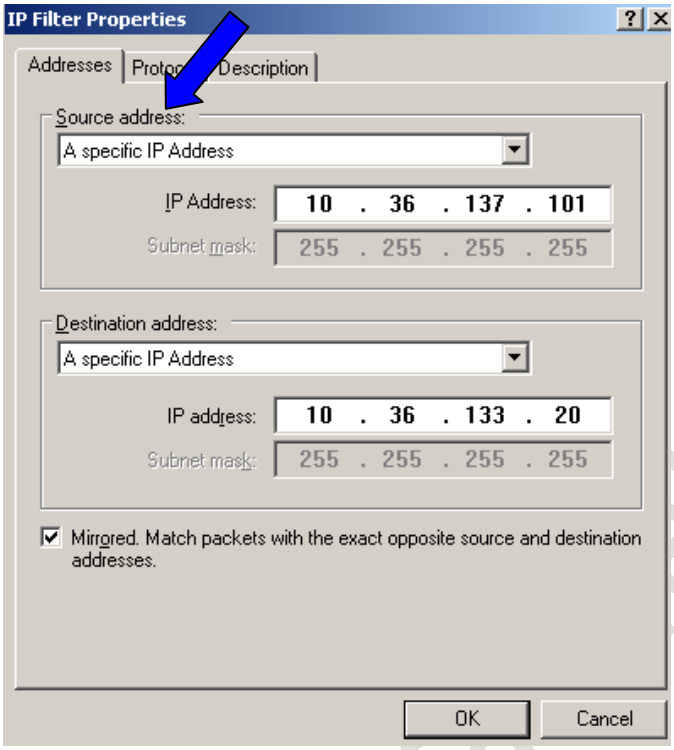

Fig.17

Arriviamo quindi alla seguente schermata Figura 18

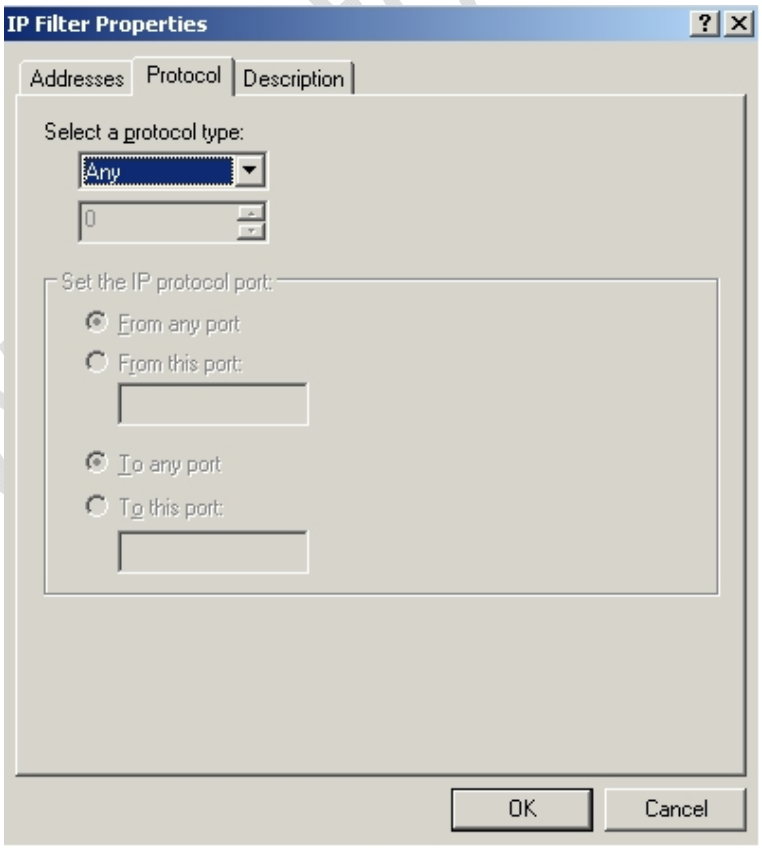

Fig.18

Qui possiamo scegliere il tipo di protocollo che vogliamo utilizzare, basta selezionare il menu a tendina e ci compariranno tutti quelli presenti (Figura 19)

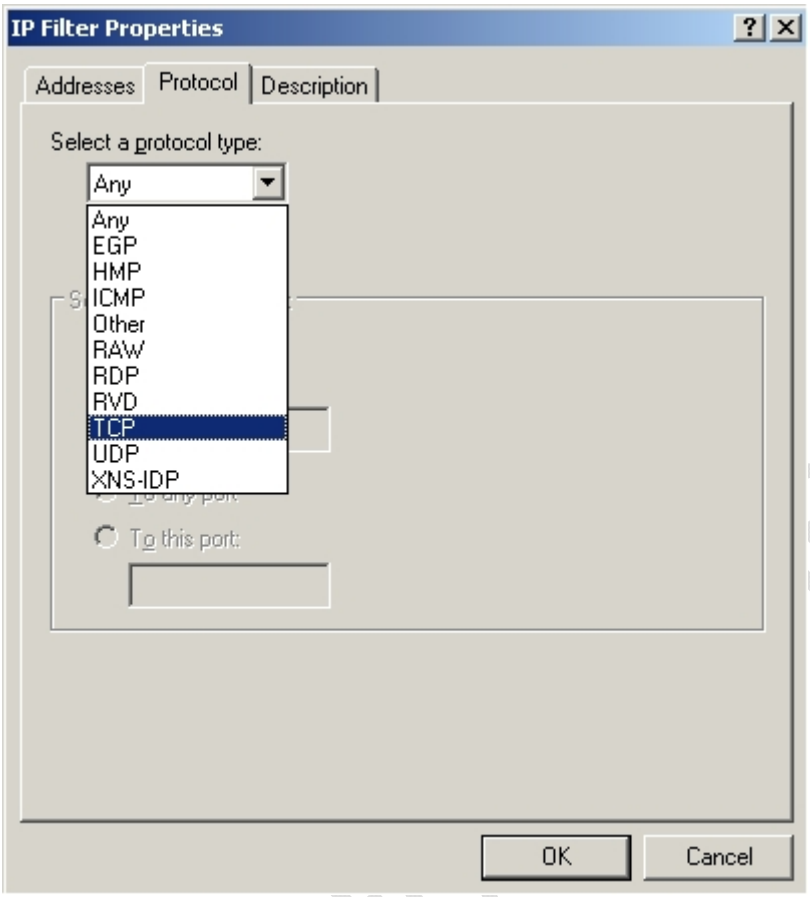

Fig.19

Una volta selezionato il tipo di protocollo possiamo settare le Porte

- From any port To any port : da qualunque porta (Figura 20)
- From this port To any port : ci permette di impostare un IP Filter da una specifica porta sorgente verso tutte le porte (Figura 21)
- From any port To this port : ci permette di impostare un IP Filter da tutte le porte sorgenti ad una specifica porta di destinazione (Figura 22)
- From this port To this port : ci permette di impostare un IP Filter da una specifica porta sorgente verso una specifica porta di destinazione (Figura 23)

Una volta configurato il tutto clicchiamo su **OK**.

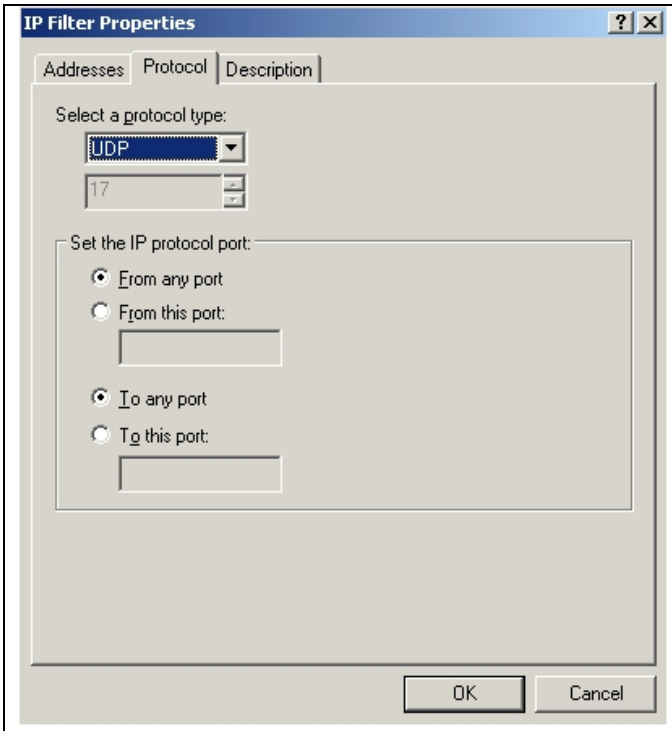

Fig.20

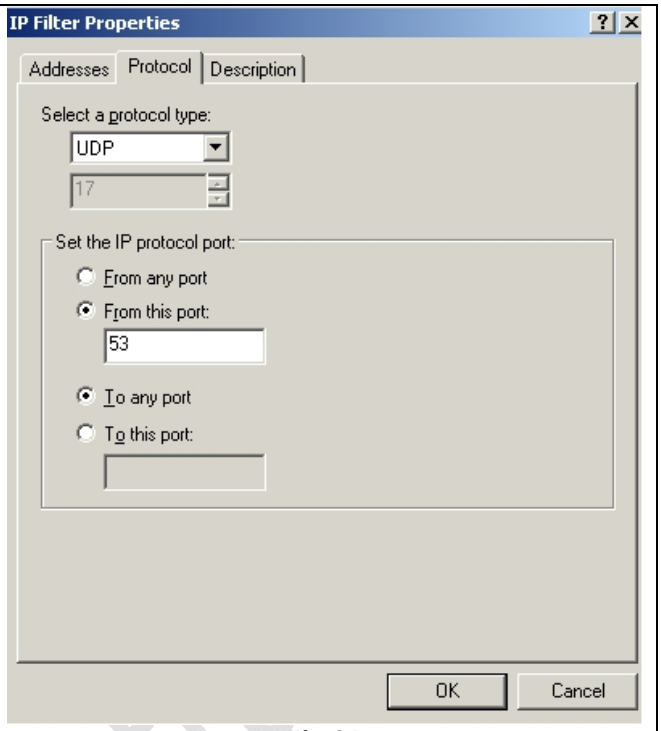

Fig.21

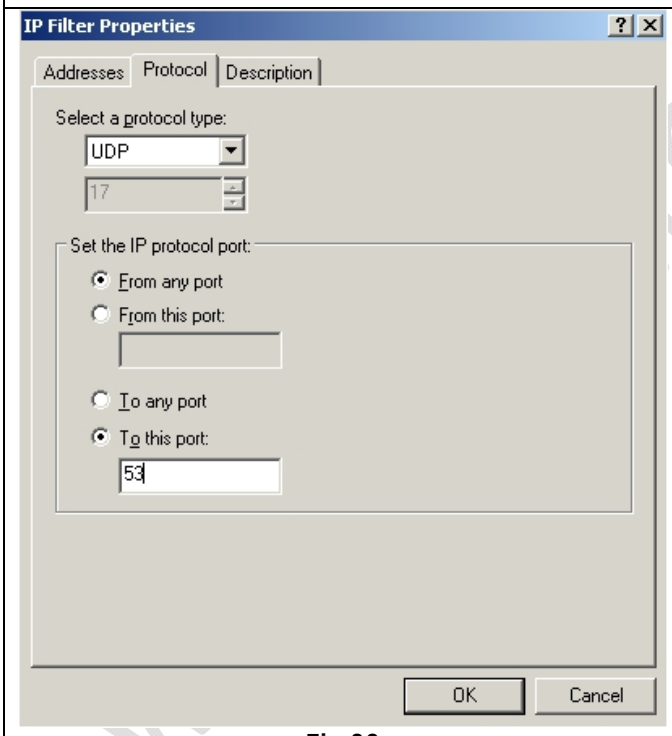

Fig.22

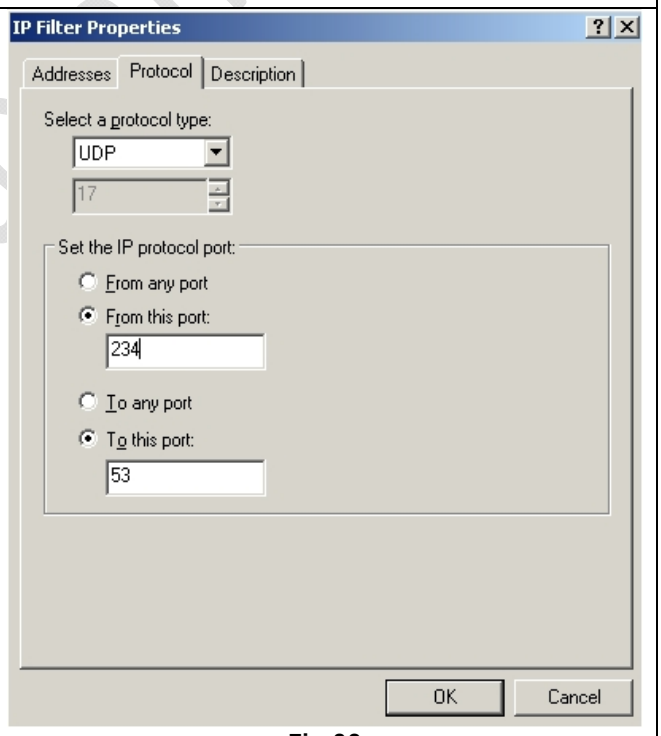

Fig.23

Vedremo che all'interno della schermata IP Filter List (Figura 24) troviamo il riassunto di tutto quello che abbiamo creato.

Quindi clicchiamo su **OK**.

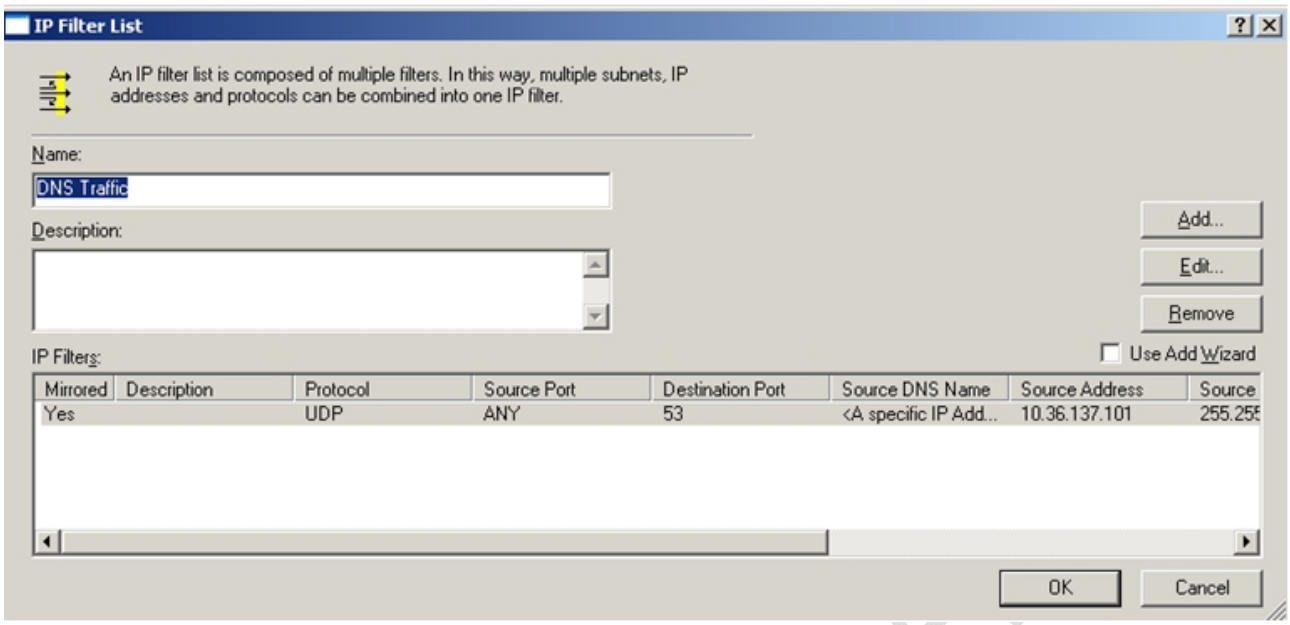

Fig.24

Ritorniamo alla schermata delle **Local Security Setting** (vedi Figura 3) e cliccando di destro su **IP Security Policies on Local Computer** selezioniamo **Create IP Security Policy**.... come in Figura 25

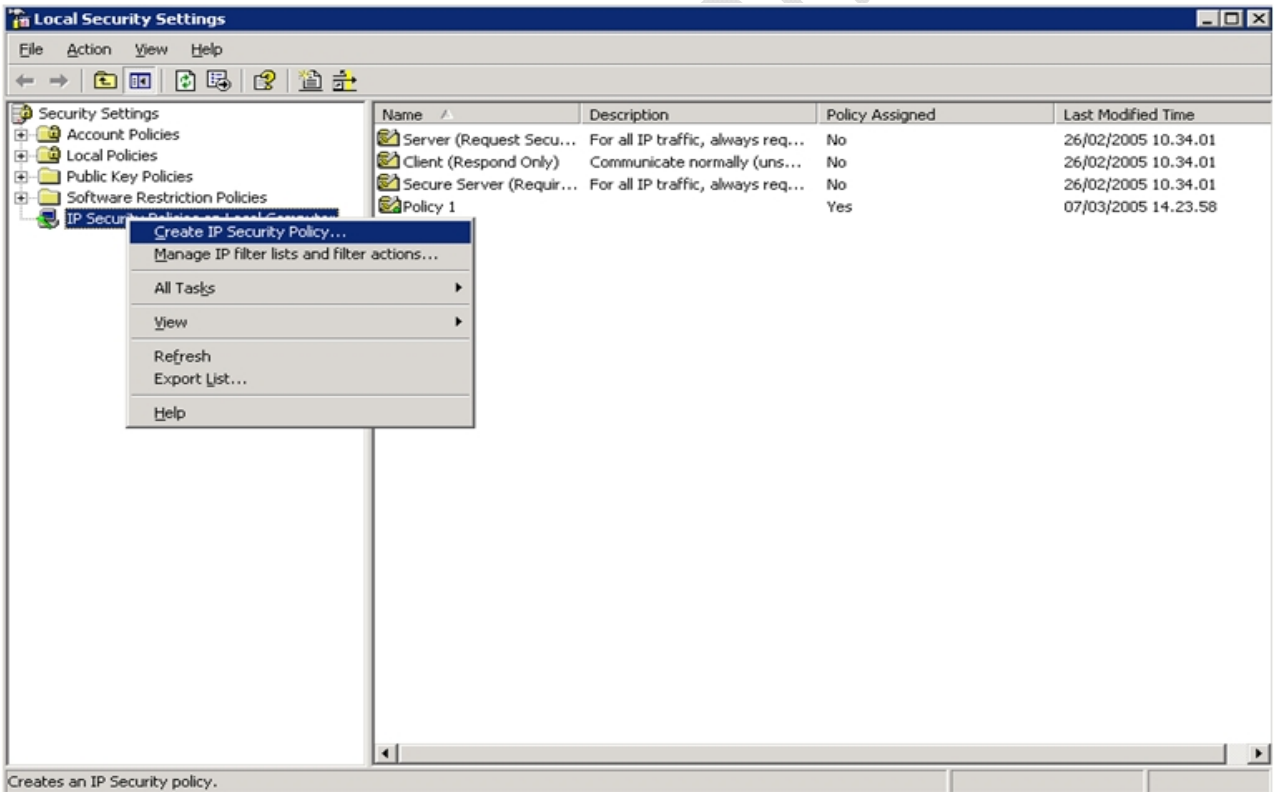

Fig.25

Quindi

Fig.26

Clicchiamo su **Next**

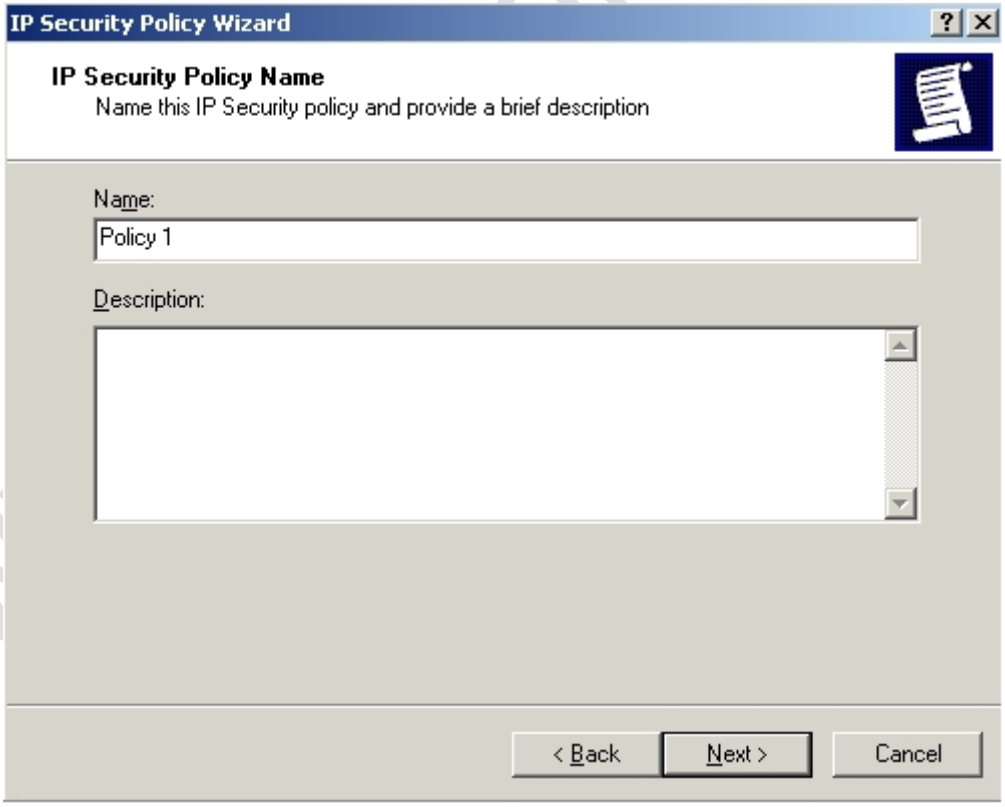

Fig.27

A questo punto inseriamo il nome della Policy cioè : Policy 1 come in Figura 27

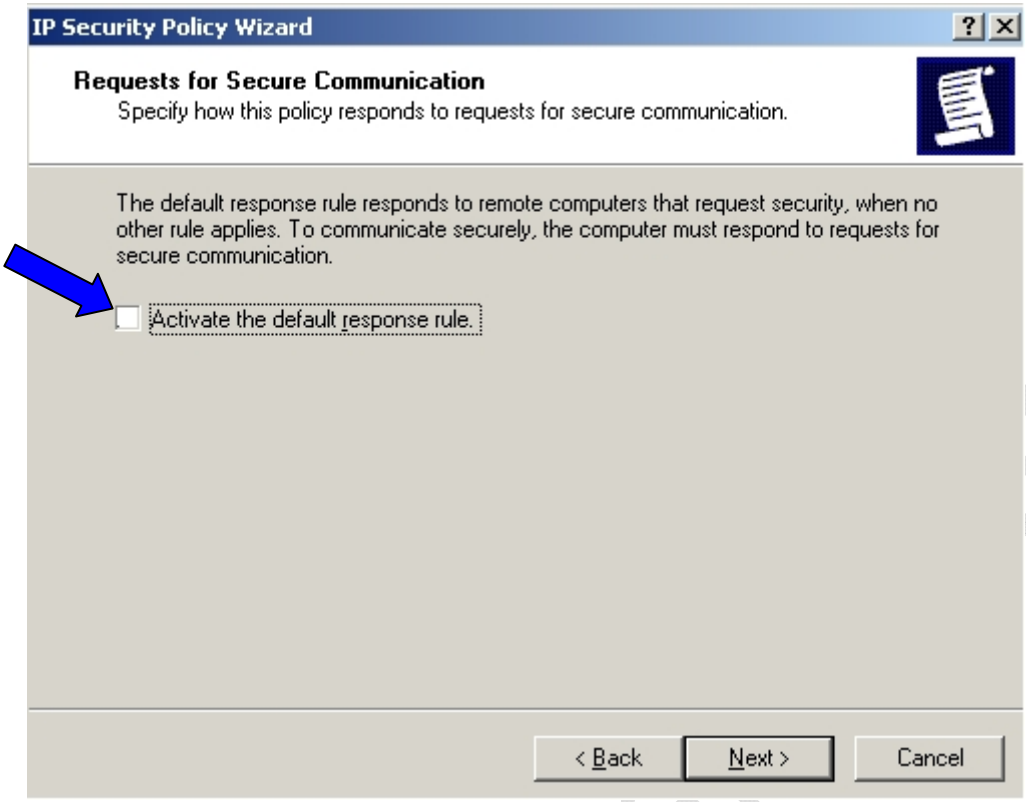

Fig.28

Qui deselezioniamo **Activate the default response rule** (vedi Figura 28).

Fig.29

In questa schermata lasciamo tutto invariato così al termine possiamo editare le proprietà della Policy e clicchiamo su **Finish**. (vedi Figura 29)

Ci apparirà alla fine la seguente schermata, la prima cosa che dobbiamo fare è deselezionare **Use Add Wizard** come in Figura 30

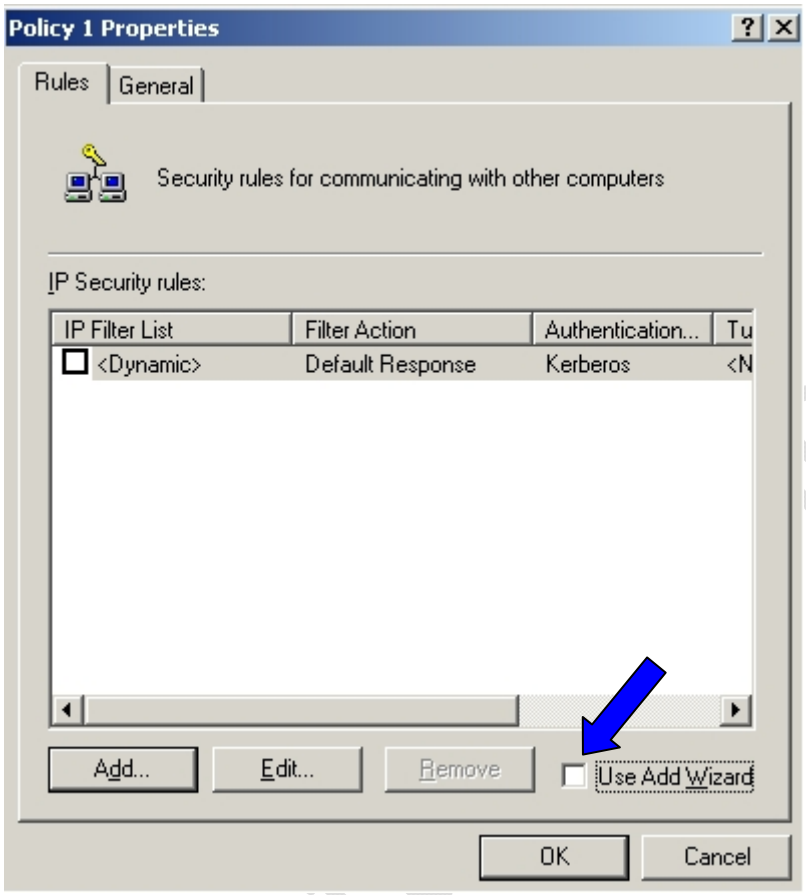

Fig.30

Aggiungiamo la prima regola.
Clicchiamo su **Add** ottenendo la seguente schermata (Figura 31)

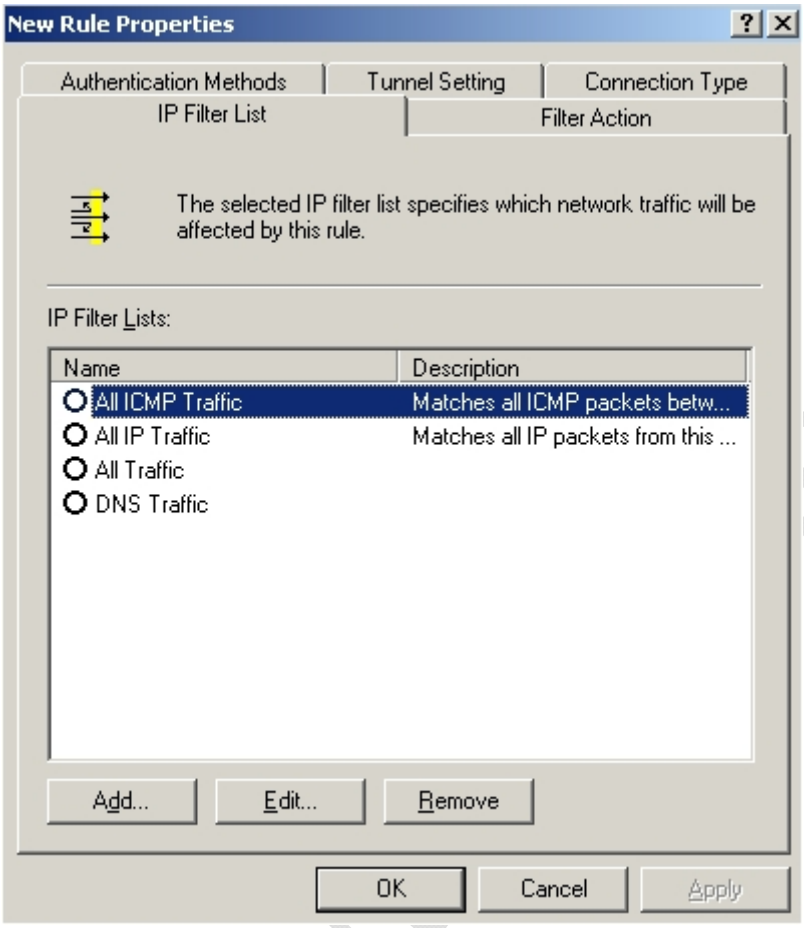

Fig.31

Adesso all'interno della schermata selezioniamo il Filtro creato in precedenza vedi Figura 32.

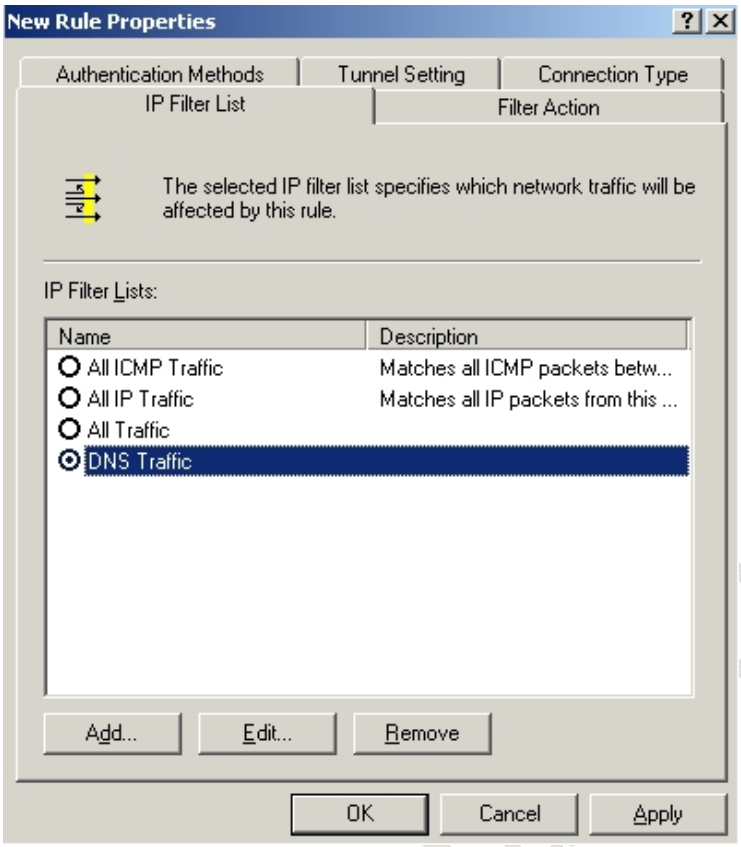

Fig.32

Poi ci spostiamo nella sezione **Filter Action** e selezioniamo l'azione da attribuire al filtro come in Figura 33.

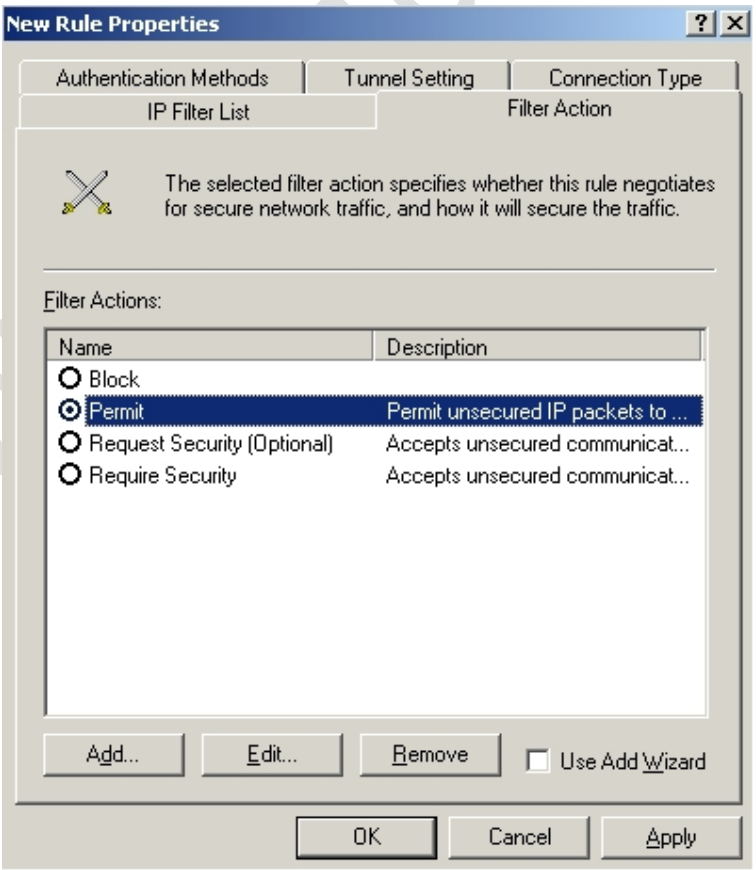

Fig.33

Quindi clicchiamo su **Apply**, successivamente su **OK**.

A questo punto ci troveremo di fronte alla seguente schermata Figura 34.

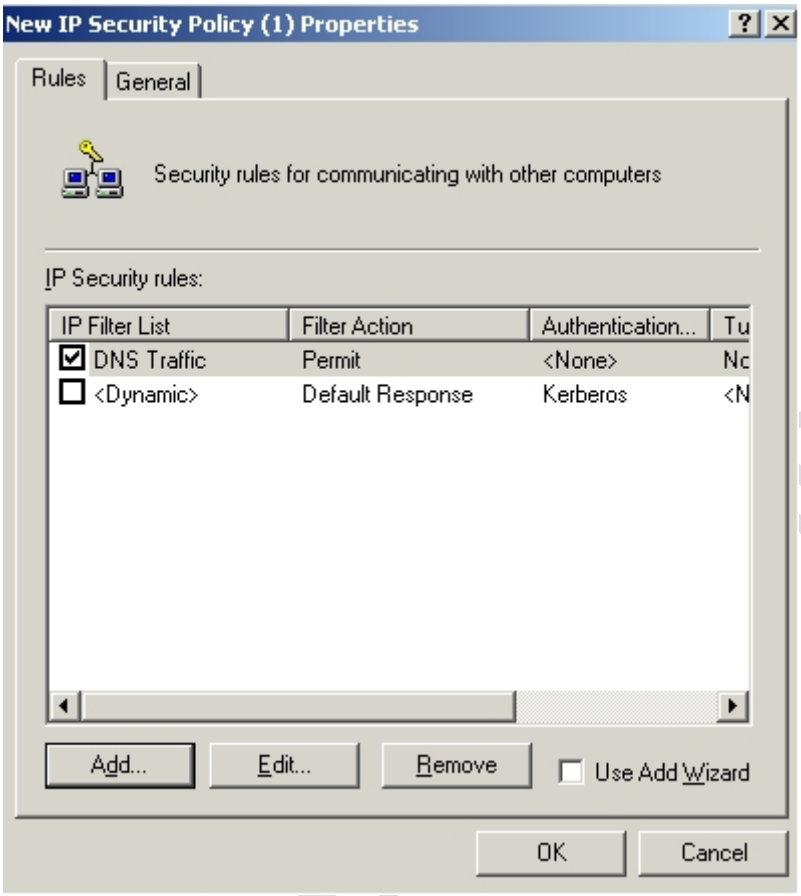

Fig.34

Notiamo la riga aggiunta con il riassunto dei filtri selezionati e dei permessi attribuiti a questi ultimi.

Quindi se abbiamo altri filtri da aggiungere e assegnare il permesso eseguiamo la stessa procedura.

Una volta che abbiamo finito di inserire i filtri clicchiamo su **OK**.

Adesso dobbiamo soltanto avviare la Policy.

Per fare ciò andiamo alla schermata seguente Figura 35.

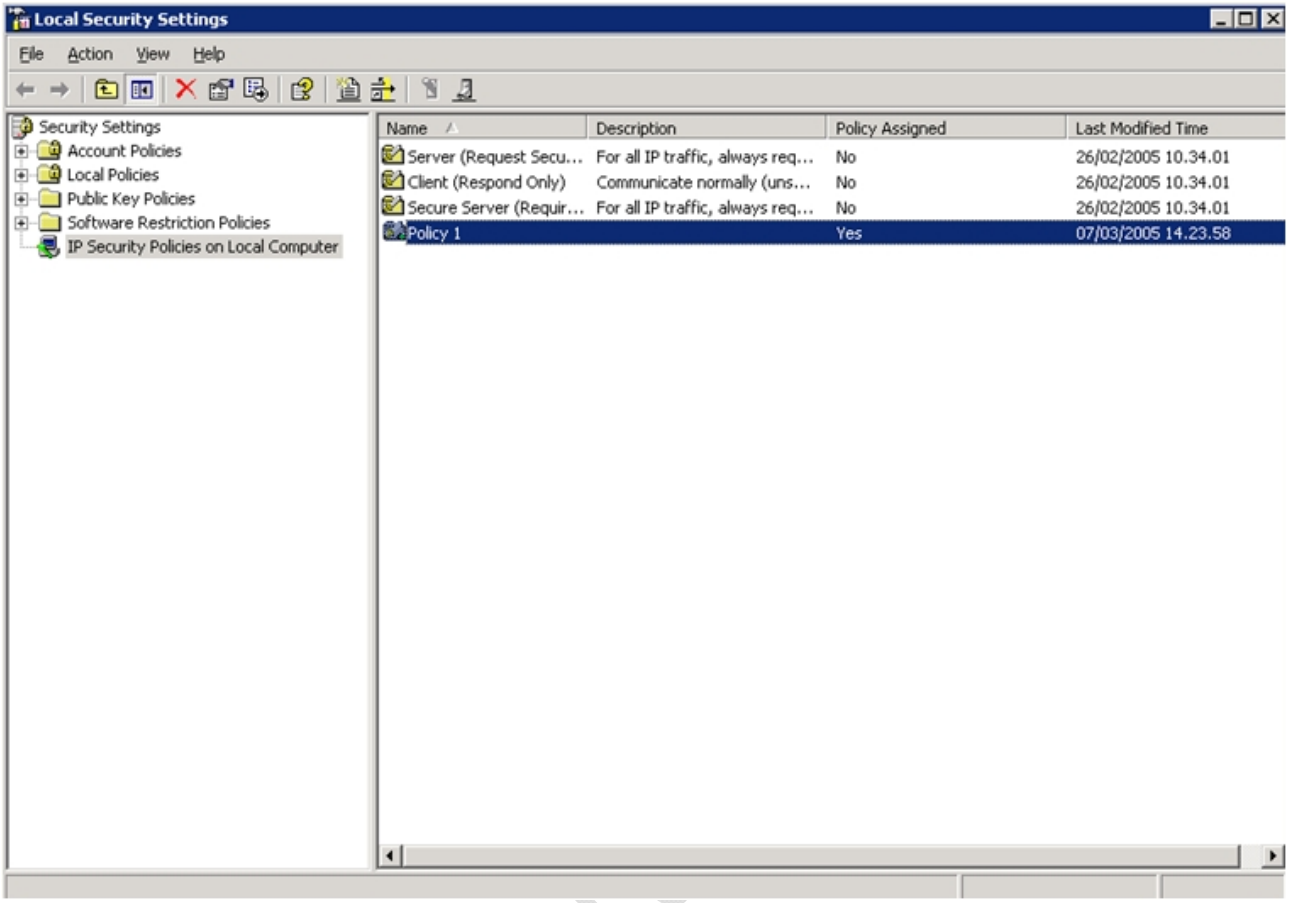

Fig.35

Clicchiamo di destro sulla Policy creata in precedenza e selezioniamo **Assign**.

Adesso la Policy sta funzionando.

!!!ATTENZIONE!!! D'ora in avanti quando modifichiamo la Policy facciamo attenzione a non sbagliare, perchè sarebbe un casino tornare allo stato precedente senza bloccare tutto e quindi lasciando vulnerabile la macchina.

!!!ATTENZIONE!!!

In ultimo volevo ricordarvi che prima di aggiungere un qualsiasi IP Filter sarebbe cosa buona creare un filtro chiamato All Traffic con le seguenti caratteristiche:

- Name: All Traffic
- Source Address : Any IP Address
- Destination Address : Any IP Address
- Protocol : Any

Poi all'interno delle proprietà della Policy creata selezionare nella sezione **IP Filter List** il filtro **All Traffic** e poi spostarsi nella sezione **Filter Action** e selezionare **Block**, quindi Apply e **OK**.

Dovremmo ottenere alla fine una schermata come quella in Figura 36.

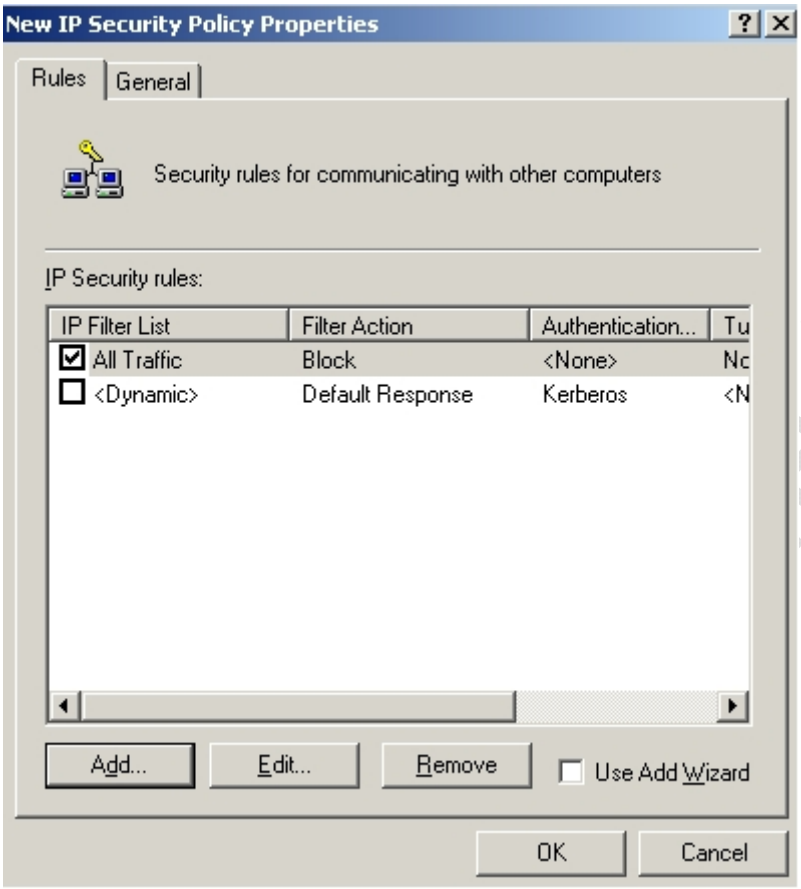

Fig.36