Virtual Private Network (VPN)

Con il termine VPN si indica una risorsa di connettività, distribuita su una infrastruttura condivisa, che mantiene le stesse politiche e prestazioni di una rete privata, ma che, a differenza di quest'ultima, permette di ridurre i costi totali di gestione.

Sostanzialmente una VPN può essere distinta sia per la tecnologia:

- **Trusted**: sfrutta uno o più circuiti noleggiati da un fornitore di telecomunicazioni. Ogni circuito si comporta come il singolo cavo di una ipotetica rete controllata dall'utente. La riservatezza consiste nell'assicurazione, data dal fornitore, che il cliente è il solo ad utilizzare e ad avere accesso ai dispositivi di un determinato circuito. Le più diffuse tecnologie impiegate sono:
    - Circuiti ATM;
    - Circuiti Frame Relay;
    - Trasporto di frames di livello 2 su Multiprotocol Label Switching (MPLS);
    - MPLS con restrizioni nella distribuzione delle informazioni di routing attraverso l'uso del Border Gateway Protocol (BGP).
- **Secure**: utilizza mezzi di comunicazione pubblici e mantiene la riservatezza di quanto trasportato mediante l'uso di un protocollo di tunnel crittografato e specifiche procedure di sicurezza. Le principali tecnologie impiegate includono:
    - IPsec: principalmente in modalità Tunnel Mode, per connessioni site-to-site;
    - IPsec all'interno di L2TP;
    - SSL 3 o TLS;
    - PPTP.
- **Hybrid**: nasce dall'uso combinato di trusted VPN e secure VPN.

che per l'impiego che se ne fa:

- **Remote access**: quando ad accedere alle risorse dell'organizzazione è un utente remoto;
- **Site-to-site (o router-to-router)**: in generale è un'alternativa diretta all'infrastruttura WAN. In pratica permette la connessione di sedi distaccate, di dipartimenti interni o di società con le quali si ha un rapporto di collaborazione, ad una parte o alla totalità delle risorse di rete dell'organizzazione.

I sistemi operativi Microsoft permettono la realizzazione di una VPN senza l'impiego di hardware o software aggiuntivo, sia per quanto riguarda la parte server che client.

IPSec

IPSec fornisce un metodo robusto e facilmente espandibile a garanzia della sicurezza del protocollo IP, sia esso versione 4 che 6, e dei protocolli di livello superiore (come ad esempio UDP e TCP), proteggendo i pacchetti che viaggiano tra due sistemi host, tra due security gateway (ad esempio router o firewall) oppure tra un sistema host ed un security gateway.

L'architettura IPSec offre:

- Controllo degli accessi;
- Integrità dei datagrammi;
- Autenticazione dell'origine dei dati;
- Rifiuto dei pacchetti introdotti nuovamente in rete (una forma parziale di verifica dell'integrità di sequenza);
- Riservatezza (mediante l'uso della crittografia);
- Limitata riservatezza del flusso del traffico.

grazie all'utilizzo di:

- **una coppia di archivi per ogni interfaccia IPSec**: uno per la gestione delle politiche di sicurezza (Security Policy Database), l'altro per la raccolta dei parametri di ogni singola associazione di sicurezza attiva (Security Association Database);
- **due protocolli per la sicurezza del traffico:** AH (Authentication Header) ed ESP (Encapsulating Security Payload);
- **un protocollo per la gestione del materiale chiave:** IKE (Internet Key Exchange).

e diverse modalità di funzionamento:

- **Modalità Trasporto (Transport Mode)**: quando, tra due sistemi terminali di una connessione IPSec, viene ad essere garantita la sicurezza dei protocolli di livello superiore ad IP;
- **Modalità Tunnel (Tunnel Mode)**: quando gli attori vengono ad essere i security gateway e la sicurezza è data a tutto il pacchetto IP.

Vediamo adesso in modo più approfondito i singoli componenti dell'architettura per poi passare alle diverse modalità di funzionamento.

Security Policy Database (SPD)

SPD definisce i requisiti di sicurezza per IPSec. E' consultato ogni qualvolta sia necessario trattare del traffico, sia in ingresso che in uscita e basandosi su caratteristiche legate al protocollo IP oppure a quanto contenuto nei protocolli di livello superiore, permette l'applicazione di un semplice criterio:

- **Scarta**: impedirà al pacchetto di entrare/uscire;
- **Non applicare**: non applicherà i servizi di sicurezza al pacchetto in uscita e non si aspetterà di averne sul pacchetto in entrata;
- **Applica**: applicherà i servizi di sicurezza al pacchetto in uscita e si aspetterà di averne sul pacchetto in entrata.

Security Association (SA) e Security Association Database (SAD)

Una SA è un insieme di accordi circa i protocolli, gli algoritmi crittografici e le chiavi da utilizzare per la comunicazione IPSec.

Ogni SA, che sia creata manualmente o come vedremo dopo, mediante IKE, definisce, anche in base al protocollo utilizzato, che sia esso AH o ESP, un legame di tipo unidirezionale. Supponendo, ad esempio, di avere due sistemi, A e B, connessi mediante IPSec, si avrà per ognuno dei due una $SA_{ingresso}$ ed una SA_{uscita}, aventi però gli stessi parametri dal punto di vista crittografico.

SAD è l'archivio all'interno del quale, ogni singolo sistema conserverà un elenco delle SA attive, identificandole con un parametro a 32 bit, chiamato Security Parameter Index (SPI) ed una serie di dati come l'indirizzo IP di destinazione e l'identificativo del protocollo di sicurezza utilizzato (Security Protocol Identifier).

IKE (Internet Key Exchange)

IKE è un protocollo ibrido di tipo generico che agisce nelle fasi iniziali di una comunicazione, permettendo la creazione di SA e la gestione dell'archivio a queste dedicato (SAD). Prima di passare a vedere come questo viene raggiunto, vediamone i principali elementi costitutivi:

- **Internet Security And Key Management Protocol (ISAKMP)**: definisce le procedure ed i formati dei pacchetti per stabilire, negoziare, modificare e cancellare una SA. Fornisce inoltre un'architettura di riferimento per la gestione delle chiavi, indipendente dal protocollo usato per lo scambio delle stesse, dal metodo di autenticazione nonchè dagli algoritmi crittografici impiegati. L'implementazione attuale prevede l'uso combinato delle caratteristiche di due protocolli:
    - **OAKLEY**: un protocollo con il quale due parti autenticate possono giungere ad un accordo circa il materiale chiave da utilizzare e di cui IKE sfrutterà le caratteristiche per lo scambio chiave;
    - **SKEME**: un protocollo di scambio chiave simile a OAKLEY di cui però IKE utilizzerà caratteristiche diverse come il metodo crittografico a chiave pubblica e quello di rinnovo veloce della chiave.

E' di fondamentale importanza notare che, essendo IKE un protocollo generico, potrebbe essere utilizzato per la creazione di SA per differenti protocolli, vi è quindi la necessità di definire quello che è il suo ambito di utilizzo o Domain of Interpretation (DOI). Nel nostro caso, si parlerà quindi di IPSec DOI. Altri protocolli definiranno un proprio DOI.

Lo scopo di IKE viene raggiunto attraverso una negoziazione in due fasi:

- **Fase 1**: stabilisce una SA per ISAKMP da utilizzare come canale sicuro per effettuare la successiva negoziazione IPSec, in particolare:

    - Negozia i parametri si sicurezza;
    - Genera un segreto condiviso;
    - Autentica le parti.

    vi sono due possibili tipi di Fase 1:

    - **Main mode**: consiste nello scambio di sei messaggi di cui tre inviati dall'originatore al destinatario e tre di risposta nel senso contrario;
    - **Aggressive mode**: utilizza solo tre messaggi. Due messaggi inviati dall'originatore ed uno di risposta.

    la differenza principale, oltre al numero di messaggi utilizzati risiede nel fatto che la prima modalità, anche se più lenta, garantisce una protezione dell'identità.

- **Fase 2 (definita anche "Quick mode")**: è simile ad una negoziazione "Aggressive mode" ma meno complessa visto che sfrutta la comunicazione già in atto. Serve principalmente a negoziare dei servizi IPSec di carattere generale ed a rigenerare il materiale chiave.

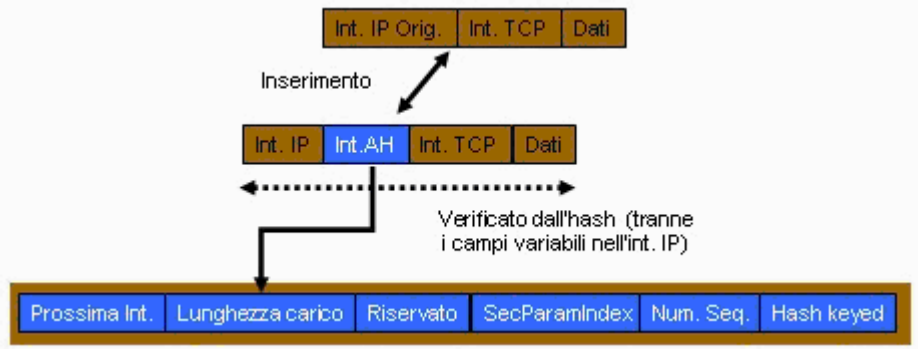
Dopo questa panoramica sui componenti, in cui ho volutamente tralasciato la struttura dei messaggi scambiati, passiamo a vedere le varie modalità di funzionamento.

Authentication Header (AH)

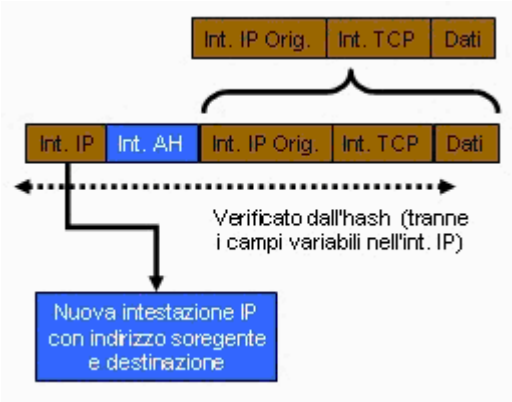
Il protocollo AH garantisce sia per l'intestazione IP che per i dati trasportati nel pacchetto, l'autenticazione, l'integrità e la protezione contro un eventuale riutilizzo ma non la riservatezza.

Per raggiungere il suo scopo utilizza una funzione crittografica di hash del pacchetto così che il destinatario possa verificarne l'integrità ed al tempo stesso l'identità del mittente.

AH può essere implementato nella modalità Transport Mode (utilizzando la porta IP 51):



o nella modalità Tunnel Mode, in cui l'intero pacchetto IP originario viene incapsulato in un nuovo pacchetto:



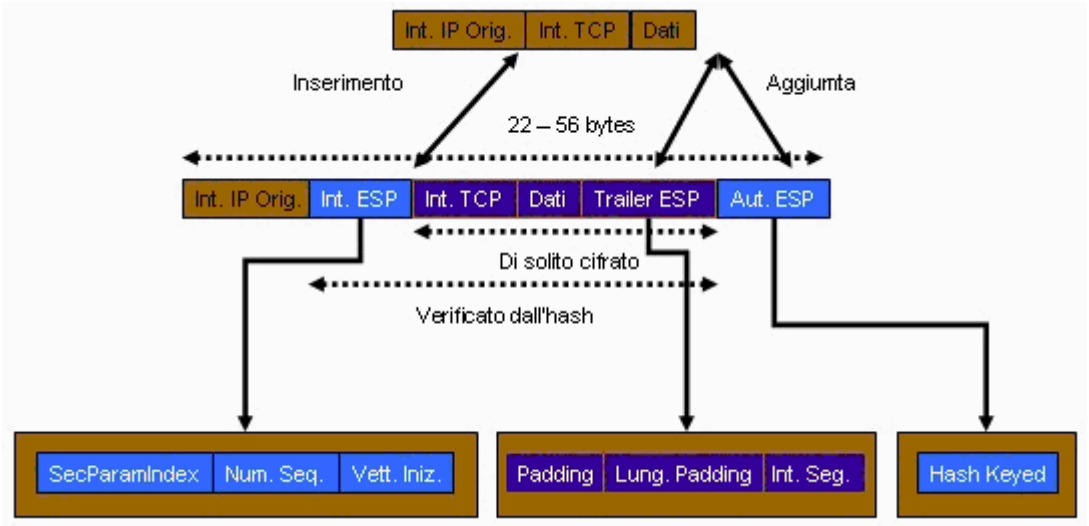
questa modalità è quella più utilizzata tra gateway o gateway e sistema host, per trasmettere in modo sicuro i dati attraverso un mezzo non sicuro, ad esempio Internet, creando una vera e propria rete privata virtuale (VPN).

Come ultima opzione, AH può essere combinato il protocollo ESP.

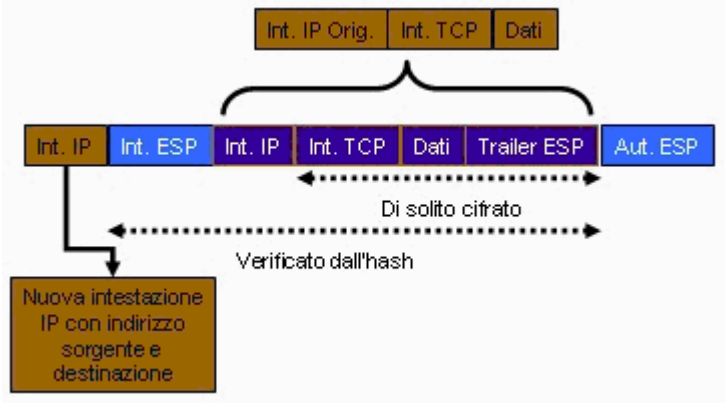
Encapsulating Security Payload (ESP)

Il protocollo ESP garantisce, oltre a quanto visto in precedenza per il protocollo AH, anche la riservatezza delle comunicazioni.

Anch'esso può essere implementato nella modalità Transport Mode (utilizza la porta IP 50):



che Tunnel Mode:



e in modalità combinata con AH.

Laboratorio

Obiettivo

Realizzare un collegamento IPSec tra due sistemi limitandone il criterio ai protocolli HTTP e SSL ed utilizzare l'autenticazione mediante certificati rilasciati da una CA autonoma.

Scenario

I sistemi utilizzati saranno i seguenti:

A. **Sistema MS Windows XP PRO ENG:**
   IP 192.168.0.1/192.168.0.11
   Servizio web (HTTP e SSL).
B. **Sistema MS Windows 2000 PRO ITA**:
   IP 192.168.0.5/192.168.0.15
   Accesso al servizio web.
C. **Sistema MS Windows 2000 ADV SRV ENG**:
   IP 192.168.0.7
   MS Certificates Services, completo di interfaccia Web.
   (Autorità di certificazione in grado di rilasciare certificati di tipo 2)

Configurazione sistemi

Vediamo adesso come configurare i due sistemi, tenendo presente che le operazioni da effettuare sul sistema B non verranno mostrate in quanto si rifanno alle procedure adottate per il sistema A con l'unica eccezione, nei filtri, data dall'inversione degli indirizzi delle parti.

Tutte le operazioni saranno effettuate utilizzando un utente con privilegi amministrativi.

Configurazione sistema A

Nel sistema, dove è stato già configurato il servizio web IIS ed il supporto per SSL, operemo su due fronti:

- installazione certificati;
- configurazione criteri IPSec

Installazione certificati

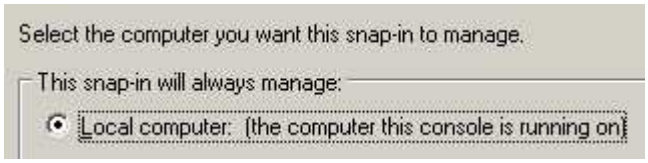
Vediamo come effettuare l'installazione del certificato della CA nell'archivio Autorità di certificazione fonti attendibili sia del programma di navigazione che del computer.

Nel primo caso ci collegheremo, mediante il programma di navigazione, alla URL della CA http://192.168.0.7/certsrv quindi sceglieremo la voce 'Retrieve the CA certificate or certificate revocation list'. Nella pagina che ci verrà visualizzata (http://192.168.0.7/certsrv/certcarc.asp) basterà scegliere il collegamento 'Install this CA certification path', in alto a sinistra. Dopo aver risposto 'Yes' ad eventuali messaggi di avviso di protezione, ci verrà visualizzato l'esito positivo dell'operazione.

Passiamo al computer. Prima di proseguire occorrerrà effettuare un'esportazione del certificato della CA. Per fare questo, ci collegheremo alla CA attraverso http://192.168.0.7/certsrv quindi sceglieremo la voce 'Retrieve the CA certificate or certificate revocation list'. Questa volta, nella pagina che ci verrà visualizzata (http://192.168.0.7/certsrv/certcarc.asp) attiviamo l'opzione per il formato di codifica Base64 quindi selezioniamo il collegamento 'Download CA certification path'. Ci verrà chiesto cosa vogliamo fare con il file certnew.p7b, selezioniamo 'Save' e lo salviamo da qualche parte.

Ora mandiamo in esecuzione la Microsoft Management Console (start > run > mmc.exe) ed aggiungiamo lo snap-in per la gestione dei certificati, avendo cura di selezionare il Computer account:

quindi scegliamo il computer locale:



una volta fatto questo, clic su 'Close' e quindi 'OK'.

Nella finestra di mmc, espandere il ramo 'Trusted Root Certification Authorities':

quindi fare clic con il tasto destro del mouse sulla voce 'Certificates'. Dal menu contestuale scegliere 'All tasks > Import...'

Verrà avviata la procedura guidata di importazione. Al messaggio di benvenuto, fare clic su 'Next' quindi digitare il percorso relativo al file salvato in precenza. Es. C:\certnew.p7b

Cliccare su 'Next' e nella finestra successiva scegliere quanto proposto:

proseguire con 'Next' e quindi 'Finish'. Dopo breve dovreste ottenere il risultato della procedura:

Passiamo ora a richiedere un certificato IPSec.

Colleghiamoci alla URL della CA http://192.168.0.7/certsrv e scegliamo la voce 'Request a certificate' quindi nella schermata successiva scegliamo 'Advanced request'.

Il sistema ci presenterà tre scelte, selezioniamo la prima 'Submit a certificate request to this CA using a form' e clicchiamo su 'Next >'.

Nel modulo che ci verrà visualizzato bisognerà inserire questi dati (quelli non specificati saranno lasciati nella loro configurazione predefinita):

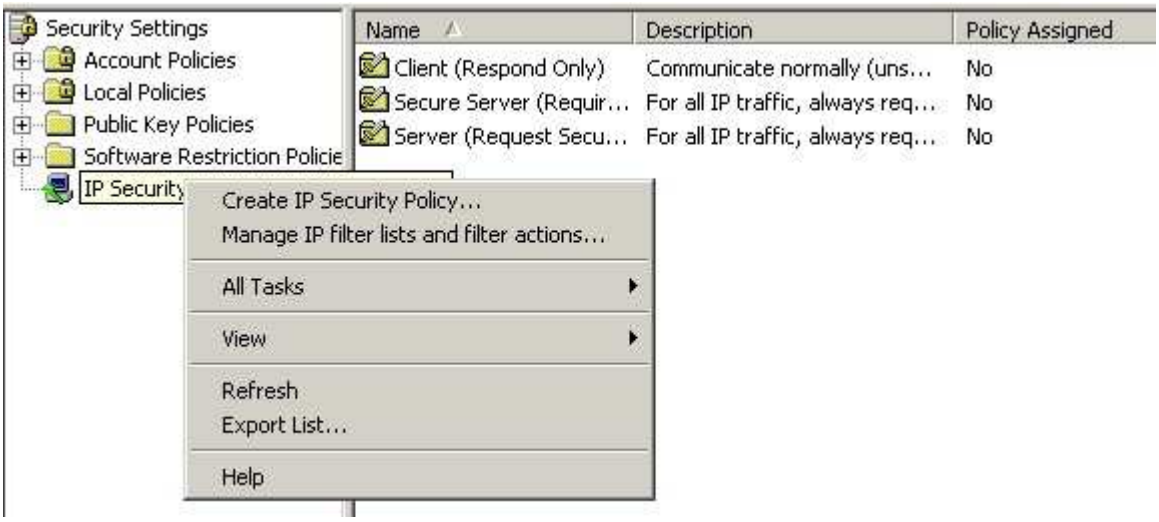
- **Name**: l'identità del richiedente;
- **Email**: l'indirizzo di posta elettronica del richiedente;
- **Intended purpose**: IPSec Certificate (oppure 'Client Authentication Certificate');
- **CSP**: Microsoft Base Cryptographic Provider v1.0;
- **Key Size**: 1024;
- **Mark keys as exportable**: attivare l'opzione solo se si intende effettuare un backup del certificato e del materiale chiave;
- **Use local machine store**: attivare l'opzione.

cliccare su 'Submit'. Dopo alcuni eventuali avvisi di protezione, a cui risponderemo sempre 'Yes', ci verrà data la possibilità di installare il certificato appena generato. Facciamolo, cliccando sull'apposita voce 'Install this certificate'.

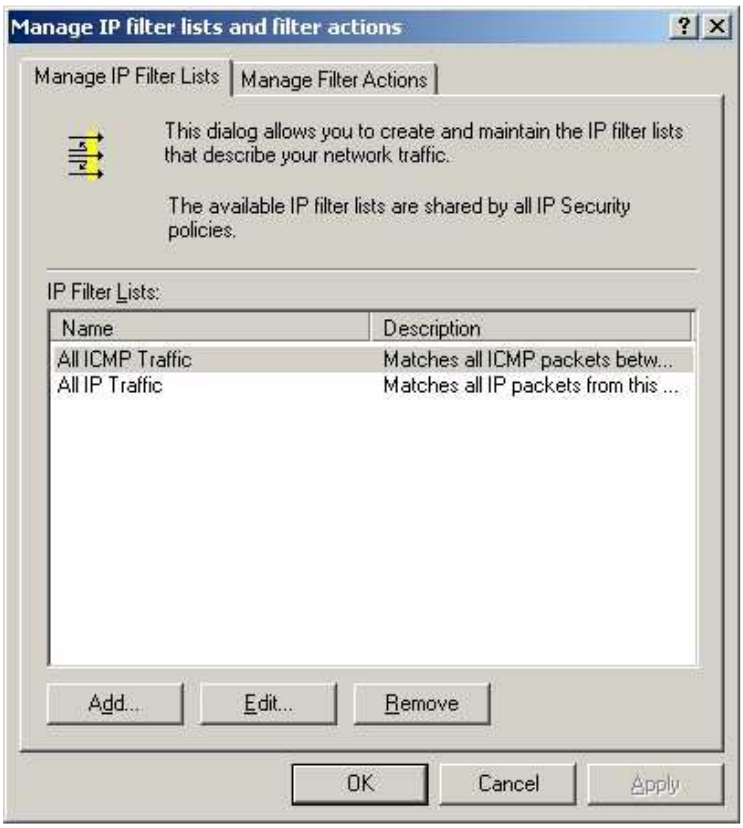
Un'ultima schermata ci comunicherà l'avvenuta esecuzione della procedura.

Configurazione criteri IPSec

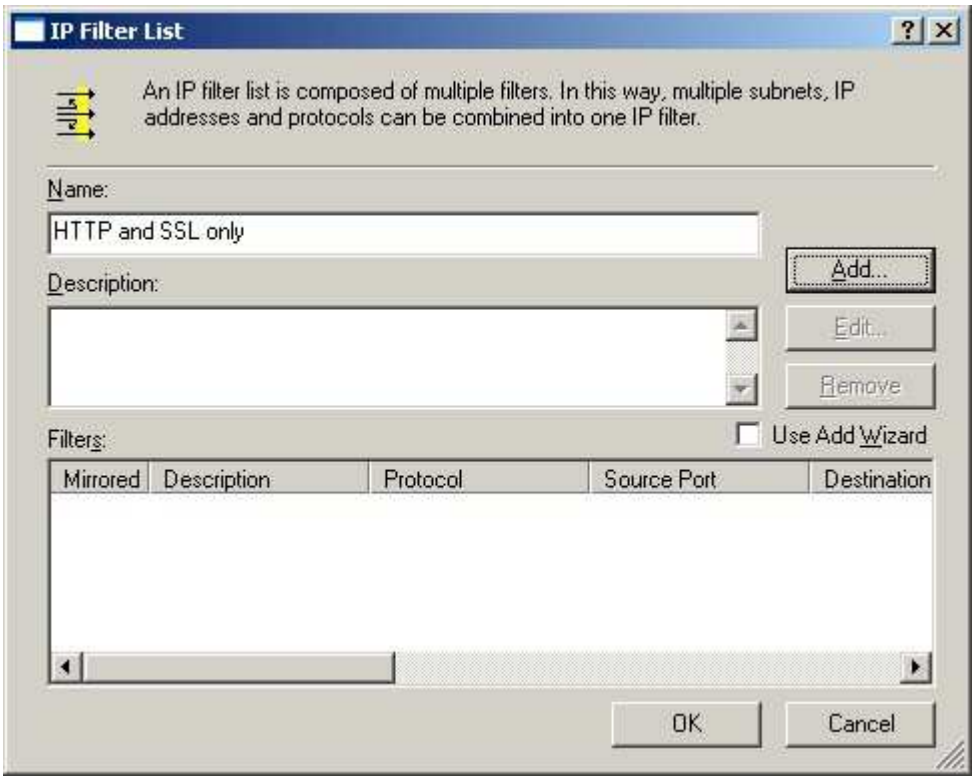
Mandiamo in esecuzione lo snap-in 'Local Security Settings' e ci spostiamo sulla voce 'IP Security Policies on Local Computer', quindi premiamo il tasto destro. Ci comparirà il seguente menu contestuale:



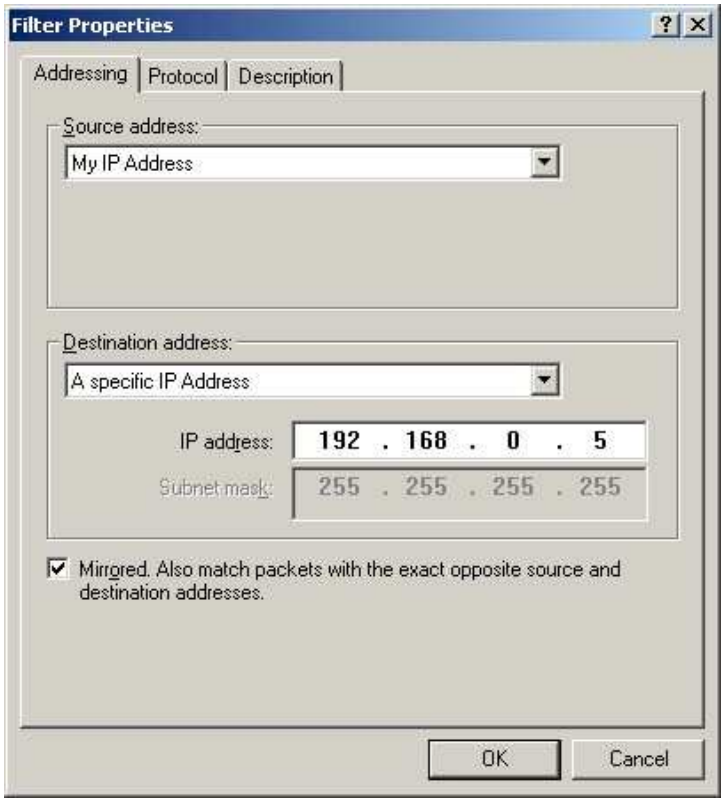
Selezionamo quindi la voce 'Manage IP filter lists and filter actions ...'. Verrà visualizzata la relativa finestra:



Selezioniamo 'Add...'. Nella finestra che verrà visualizzata inseriamo un nome per la lista di filtri che andremo a creare e deselezioniamo la voce 'Use add Wizard':

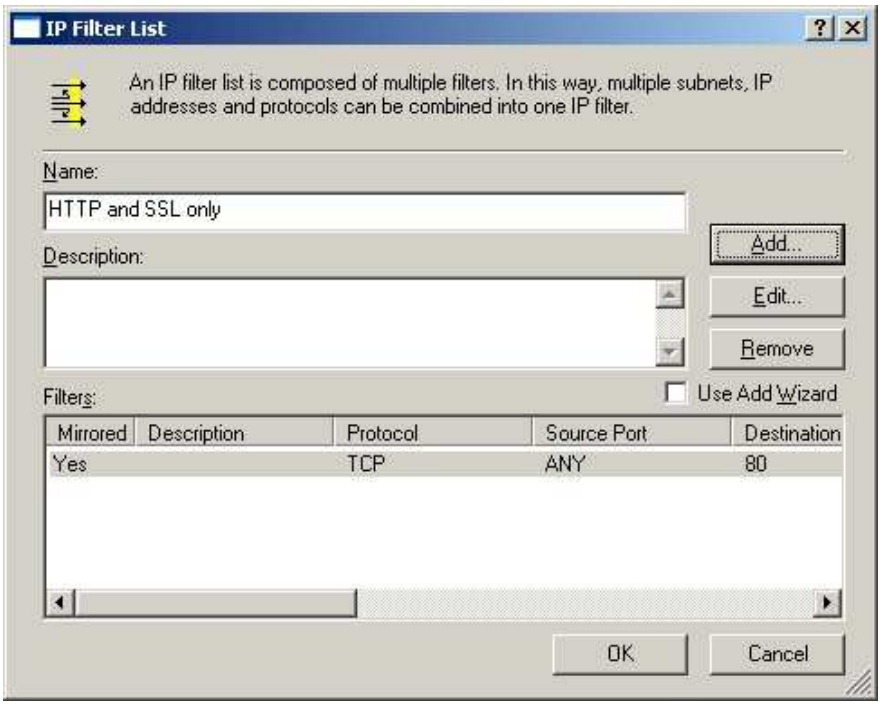


Dopo di che clicchiamo su 'Add...'. Configuriamo le proprietà del filtro secondo quanto richiesto:



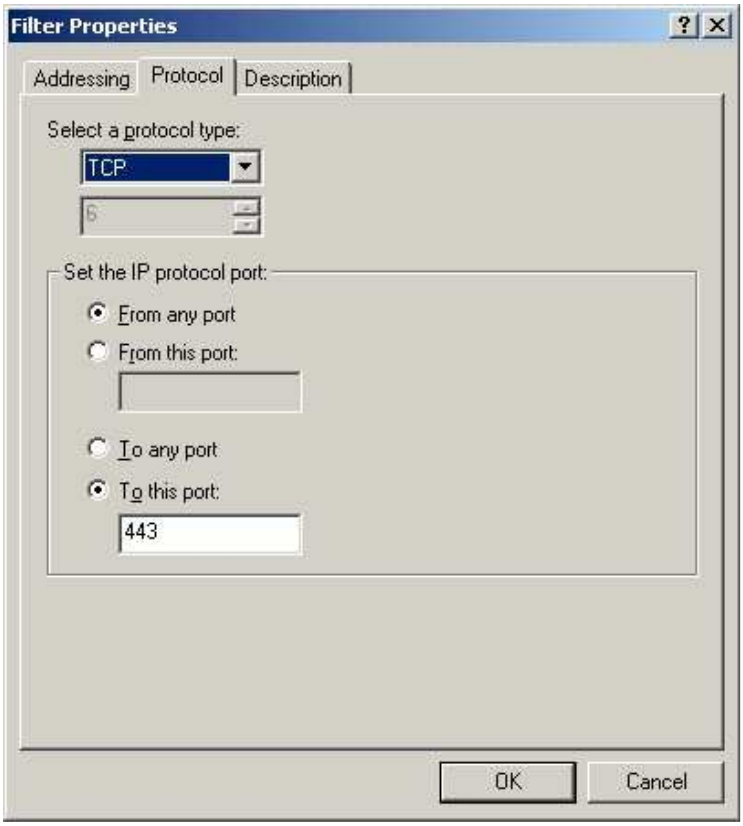
facciamo lo stesso per quel che riguarda il protocollo:

e clicchiamo su 'OK'. La lista dei filtri visualizzerà il filtro appena inserito:



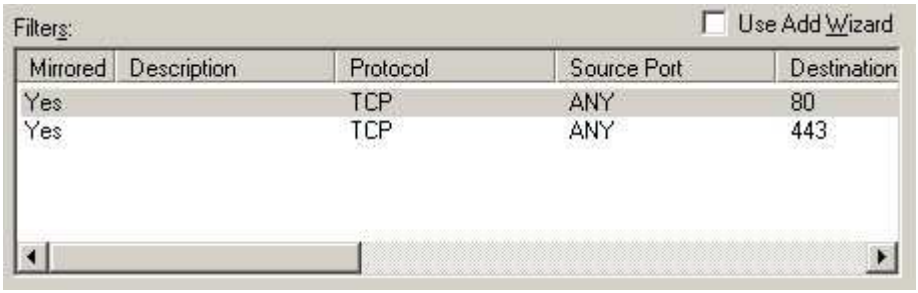
selezioniamo nuovamente 'Add...' per inserire il filtro relativo ad SSL.

Apparirà una nuova finestra per l'inserimento delle proprietà del filtro. In questo caso, mantenendo quelli che sono gli indirizzi (Addressing) inseriti in precedenza per il filtro creato per il protocollo HTTP, bisognerà semplicemente variare i dati del protocollo:



Dopo di che selezioniamo 'OK'.

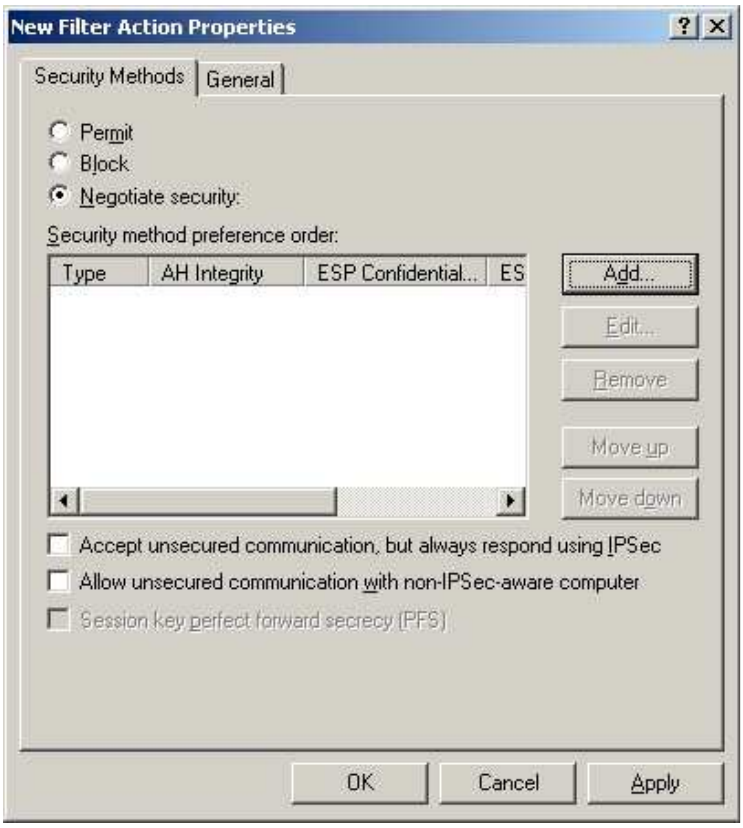
Quindi, al termine dell'operazione, i filtri inseriti dovranno essere due:



Selezioniamo 'OK' e quindi 'Close'. Ritorneremo al punto di partenza:

Ora bisognerà scegliere che azione intraprendere per il filtro appena creato. Selezioniamo quindi l'etichetta 'Manage Filter Actions'' e nella relativa finestra di proprietà, dopo aver deselezionato 'Use Add Wizard', clicchiamo su 'Add...'

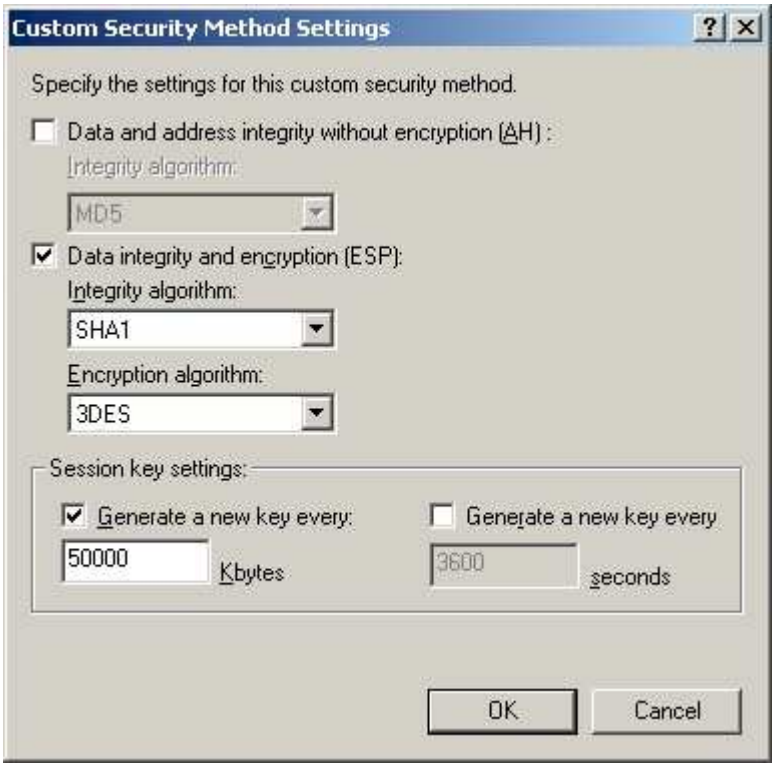
Scegliamo 'Negotiate security' e deselezioniamo 'Accept unsecured communication, but always respond using IPSec':



quindi clicchiamo su 'Add...'.

Nella finestra che ci chiede il metodo di sicurezza da utilizzare selezioniamo 'Custom', dopo di che clic sul pulsante 'Settings...'

Impostiamo le proprietà in questo modo:



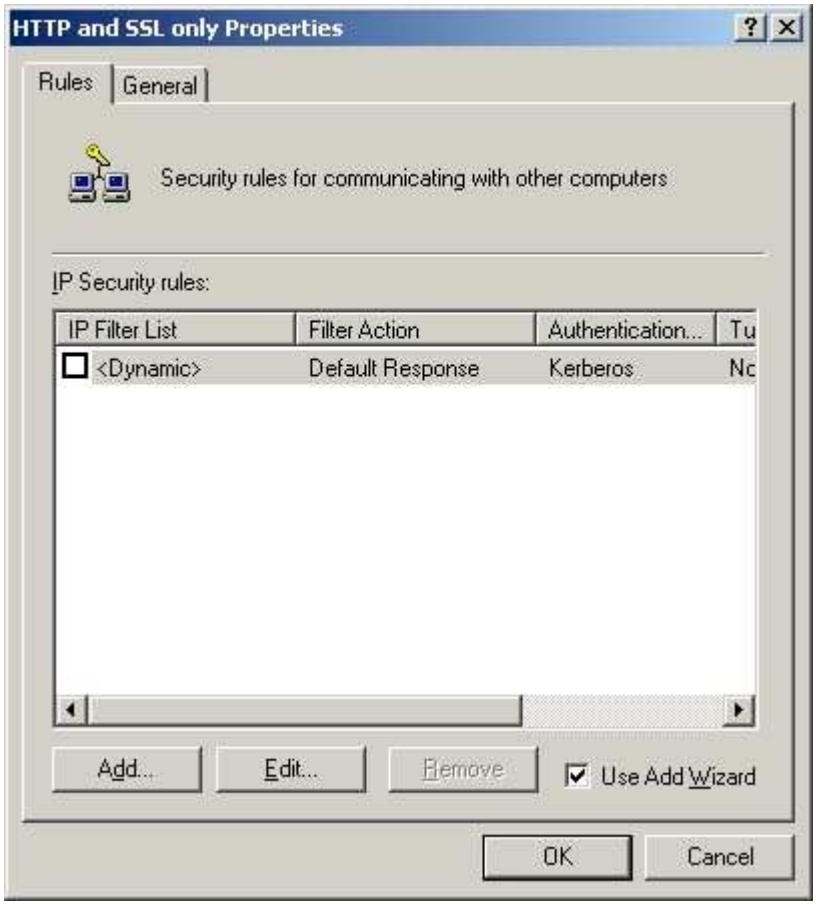
quindi clicchiamo su 'OK' per chiudere la finestra delle proprietà e nuovamente su 'OK' per chiudere la finestra di scelta del metodo di sicurezza.

Ritornati nella finestra relativa alle azioni, selezioniamo l'etichetta 'General' ed inseriamo un nome, quindi clicchiamo su 'OK' e su 'Close'.

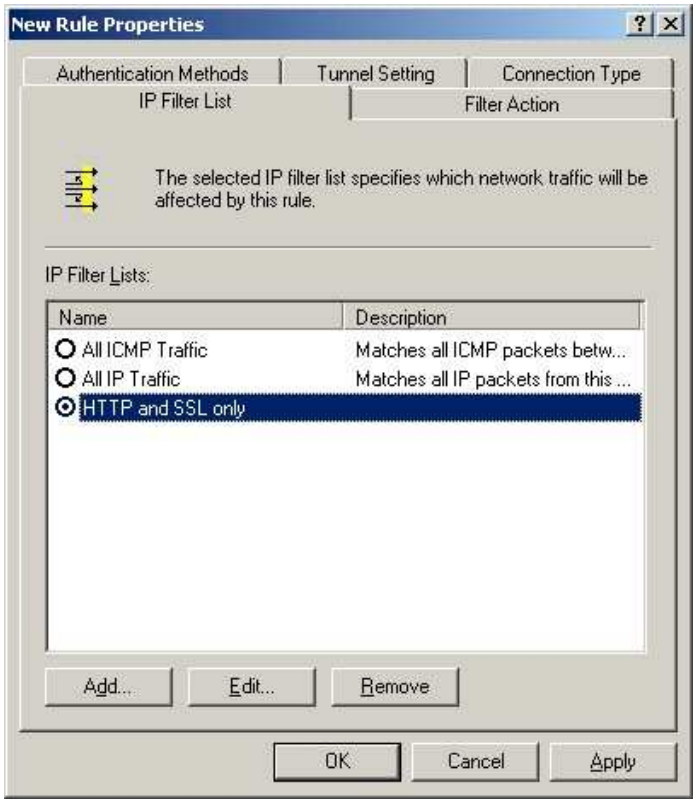
Definiamo adesso una nuova politica IPSec. Per farlo clicchiamo con il tasto destro del mouse sulla voce 'IP Security Policies on Local Computer' e dal menu contestuale selezioniamo 'IP Security Policy...', verrà avviata la procedura guidata di creazione.

Clic su 'Next' quindi inseriamo un nome per la politica IPSec che andiamo a creare dopo di che clicchiamo su 'Next'. Disattiviamo la voce che ci chiede di attivare la regola predefinita 'e selezioniamo 'Next', quindi 'Finish', assicurandoci che l'opzione di modifica delle proprietà sia attiva.

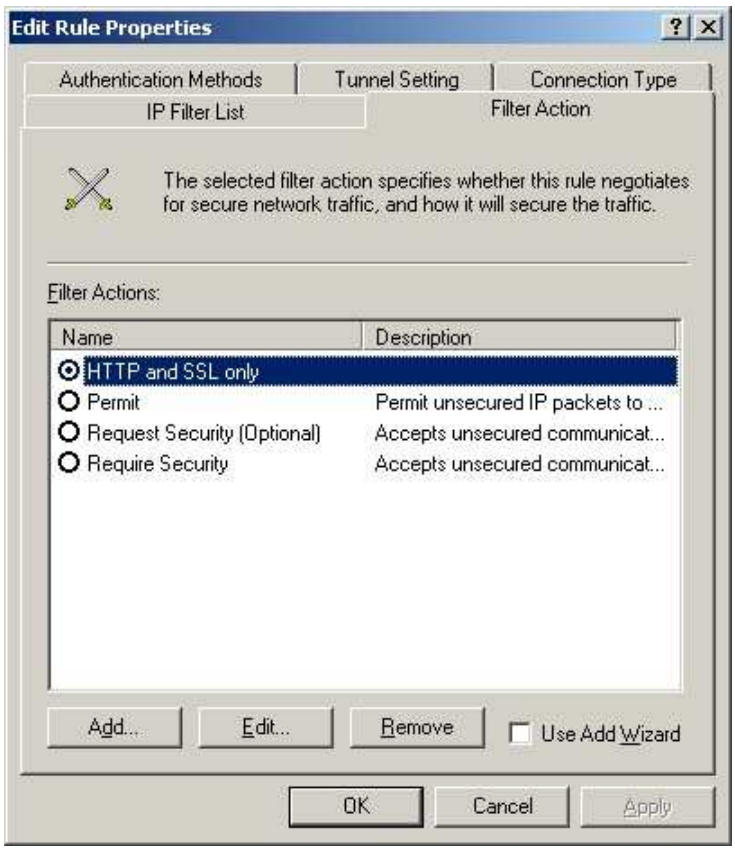
Dopo poco verrà visualizzata la finestra relativa alle proprietà da modificare:



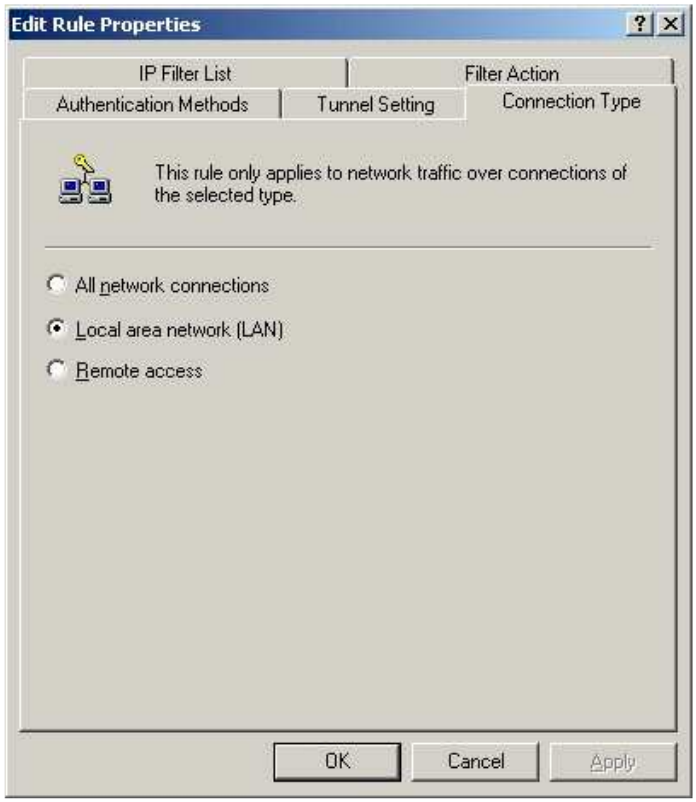
deselezioniamo l'opzione 'Use Add Wizard' dopo di che clic su 'Add...'. Ci verrà la lista filtri contentente anche quello creato in precedenza:



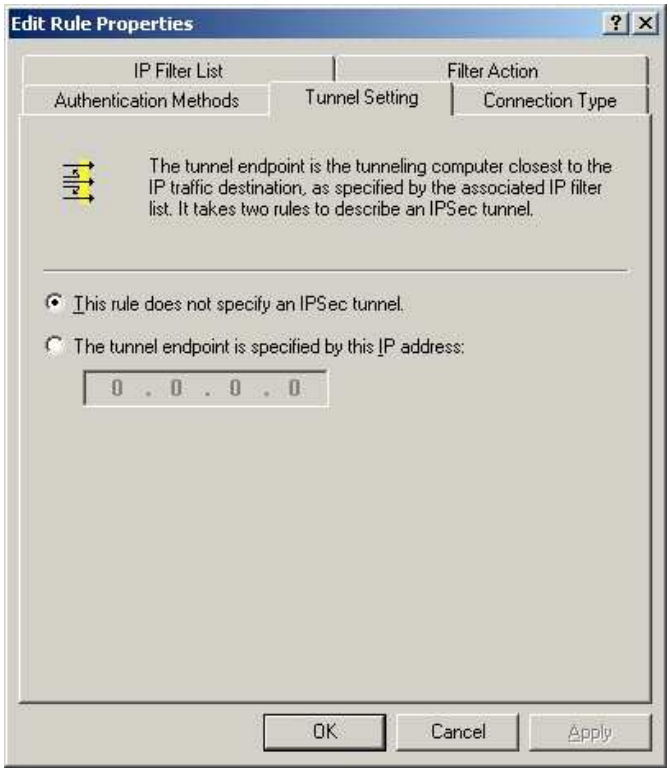
attiviamolo, dopo di che spostiamoci nelle proprietà 'Filter Action' cliccando sulla relativa etichetta. Anche in questo caso, ritroveremo l'azione creata in precedenza:



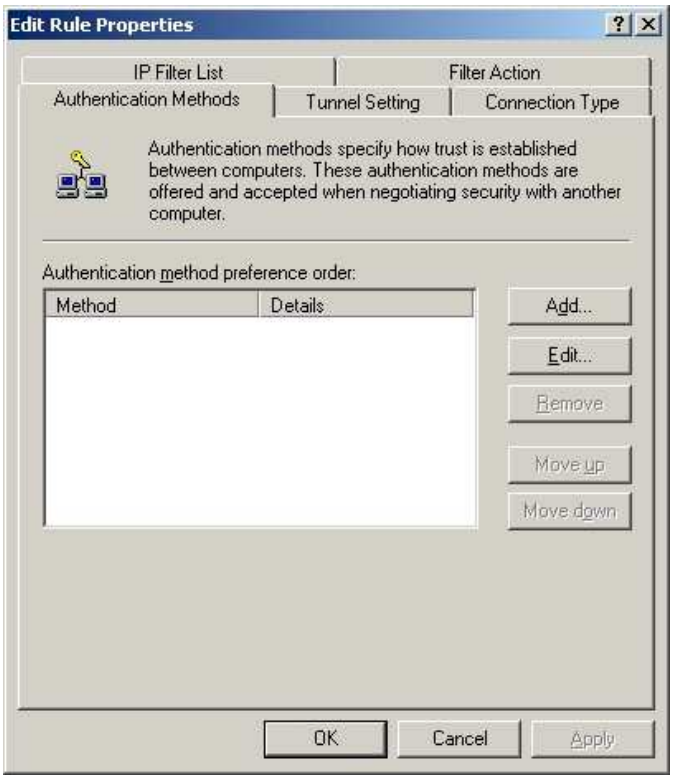
selezioniamola e passiamo all'etichetta 'Connection Type':



la voce da selezionare sarà naturalmente quella relativa alla LAN. Fatto questo, ci spostiamo alle proprietà 'Tunnel Setting':

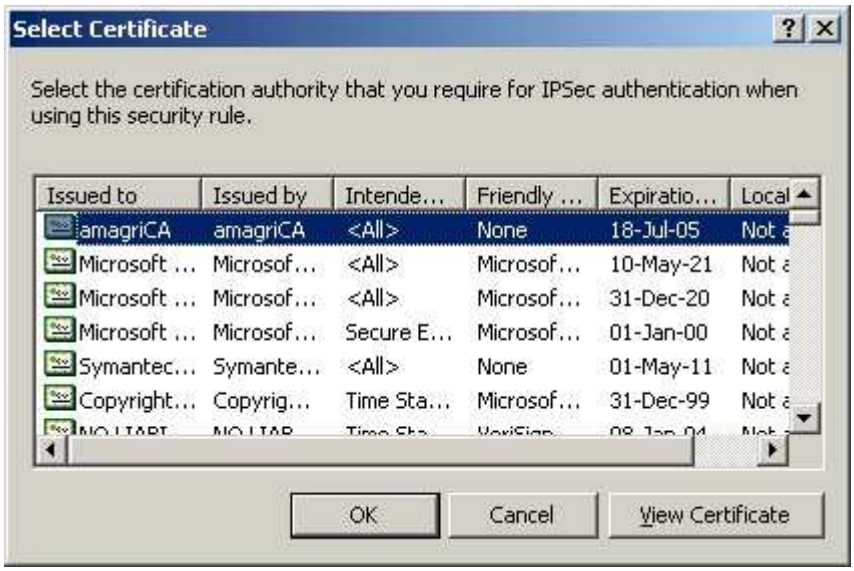


naturalmente non stiamo realizzando un tunnel quindi la prima voce corrisponde ampiamente alle nostre necessità. Clicchiamo all'allora sull'ultima etichetta, quella relativa ai metodi di autenticazione:



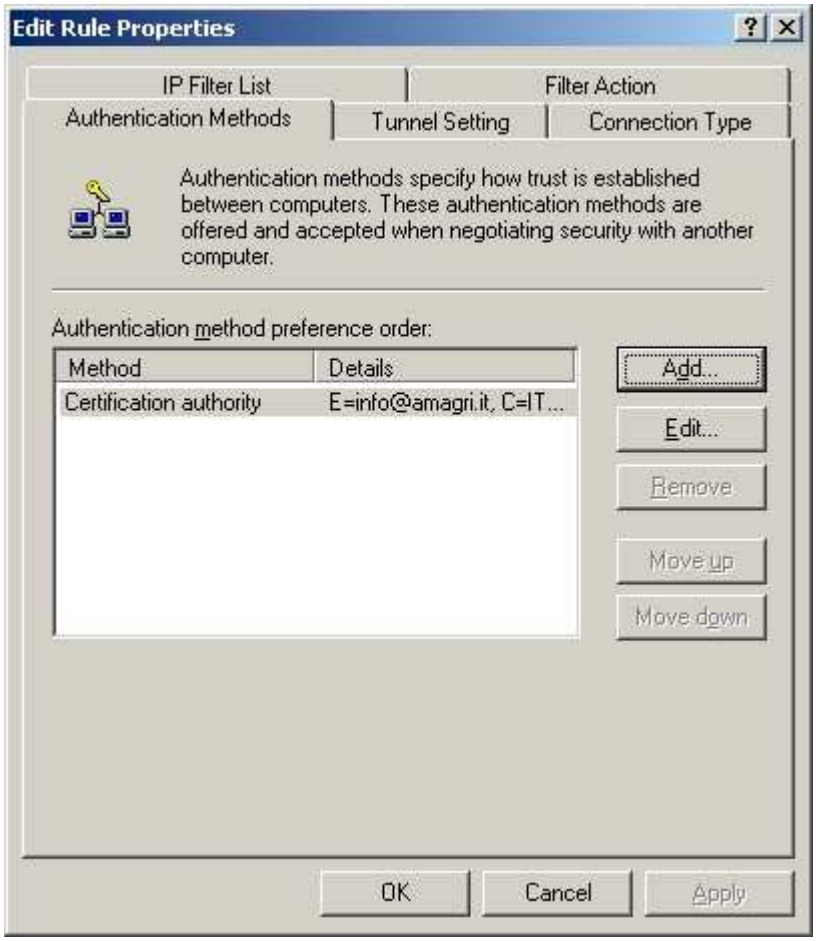
eliminiamo quelli eventualmente presenti e selezioniamo 'Add...':

quindi scegliamo 'Use a certificate from this certification authority (CA)' e clicchiamo su 'Browse...':



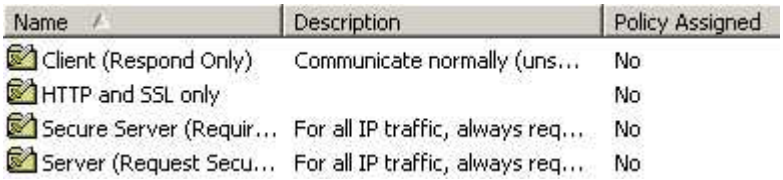
quindi selezioniamo il certificato di CA importato in precedenza e clicchiamo su 'OK'.

Ritorneremo alla finestra vista in precedenza, ma in questo caso sarà visualizzata la scelta appena effettuata:



Clic su 'OK', quindi 'Close'.

L'elenco dei criteri presenterà quello appena creato (HTTP and SSL only):



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
HTTP and SSL only		No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No

facciamo clic con il tasto destro del mouse sul criterio e selezioniamo 'Assign' per attivarlo.

Verifica

La verifica può essere effettuata in diversi modi:

- **MS Windows XP PRO**:
  - **Snap-in IP Security Monitor**: visualizzazione dettagliata di diverse tipologie di statistiche;
  - **Comando IPSecCMD**: permette di configurare le politiche, i filtri e le relative azioni da riga di comando;
  - **Eventi**:
    - IPSec Policy Agent;
    - IPSec driver: bisogna attivare la registrazione impostando la chiave di registro; HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\IPSEC\DiagnosticMode ad 1. La registrazione avviene una volta ogni ora;
    - IKE più dettagli SA: solo se impostato un criterio (success o failure) per politica 'Audit Logon Events' a livello locale o di dominio;
    - IPSec policy change: solo se impostato un criterio (success o failure) per politica 'Audit Policy Change' a livello locale o di dominio;
  - **Oakley Log**: si può attivare la regitrazione creando ed impostando la chiave di registro HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\PolicyAgent\Oakley\EnableLogging ad 1. Il file di log (Oakley.log) viene creato nella cartella systemroot\Debug. Per avviare la registrazione:
    net stop policyagent
    net start policyagent
  - **Network monitor**: effettua la cattura e l'analisi dettagliata dei diversi protocollo IPSec;
- **MS Windows 2000**:
  - **Comando IPSecMon:** visualizzazione dettagliata di diverse tipologie di statistiche;
  - **Comando IPSecPol**: permette di configurare le politiche, i filtri e le relative azioni da riga di comando;
  - **Oakley Log**: si può attivare la regitrazione creando ed impostando la chiave di registro HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\PolicyAgent\Oakley\EnableLogging ad 1. Il file di log (Oakley.log) viene creato nella cartella systemroot\Debug. Per avviare la registrazione:
    net stop policyagent
    net start policyagent
  - **Network monitor**: effettua la cattura e l'analisi dettagliata dei diversi protocollo IPSec;