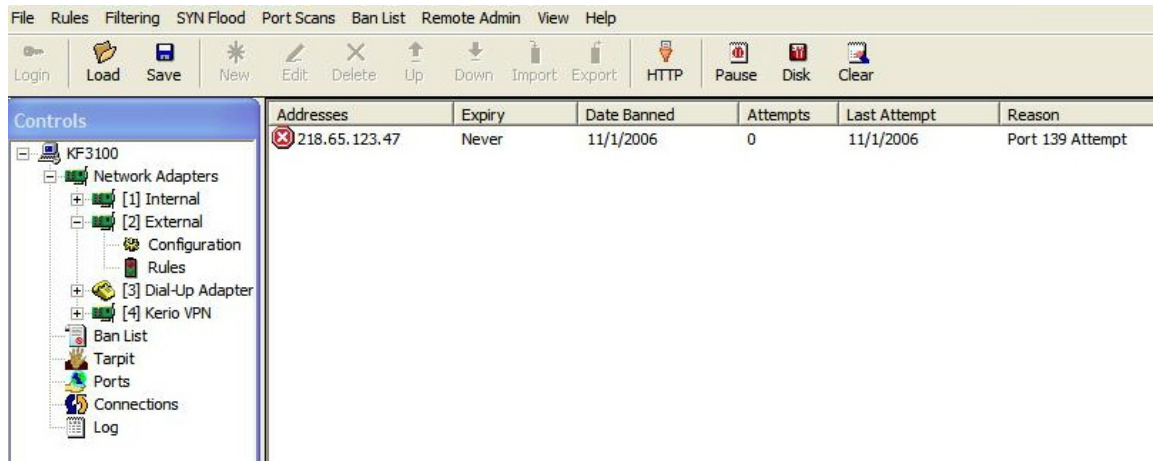
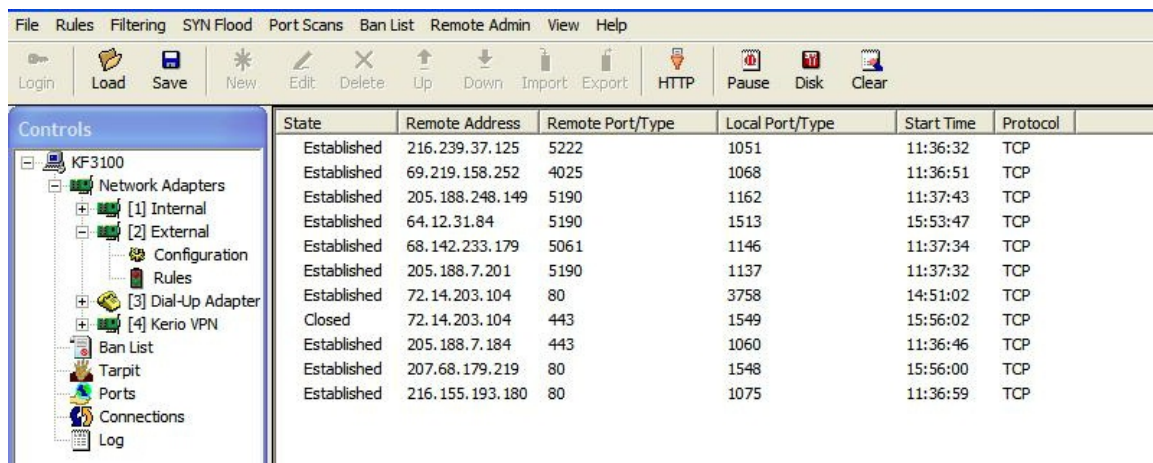


Benefits of using VisNetic Firewall over Windows Firewall

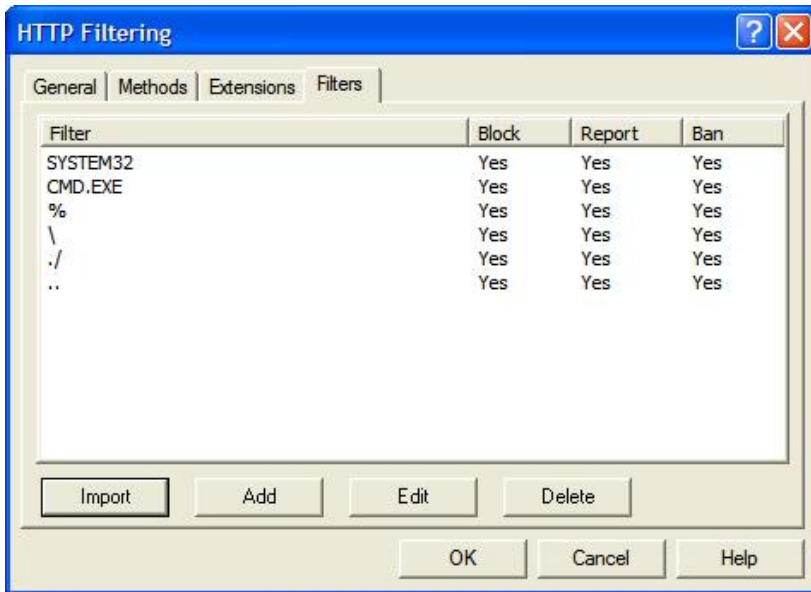
1) **Ban List** - Instead of just blocking the connection you can Ban the IP address of who is making the connection. This can be particularly effective in stopping repeated requests from a hacker who is trying a large number of hacks, looking for one that works. Entries to the Ban List can be made manually, or automatically using the "Ban IP" action on a Block rule, the Port Scan feature or the by using HTTP Filtering option.



2) **Active Connections** - This allows the user / admin the ability to see what connections are currently established on the local machine, this is useful if the Admin believes the server may have been compromised. Instead of trying to find specific programs, the Admin can look at the connections and block them via the firewall using the information given.



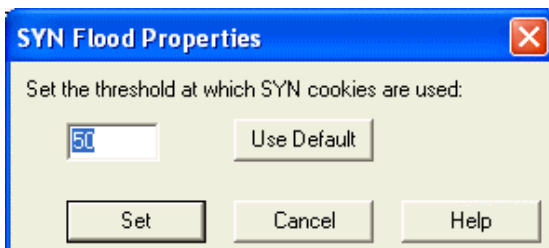
3) **HTTP Filtering** - When installed onto the same machine as a web server, VisNetic Firewall can monitor HTTP traffic and can filter out the bad requests that could potentially bring the web server down. This is quite useful if a specific method is mentioned online and it can be filtered directly at the firewall instead of waiting for a patch to fix the flaw.



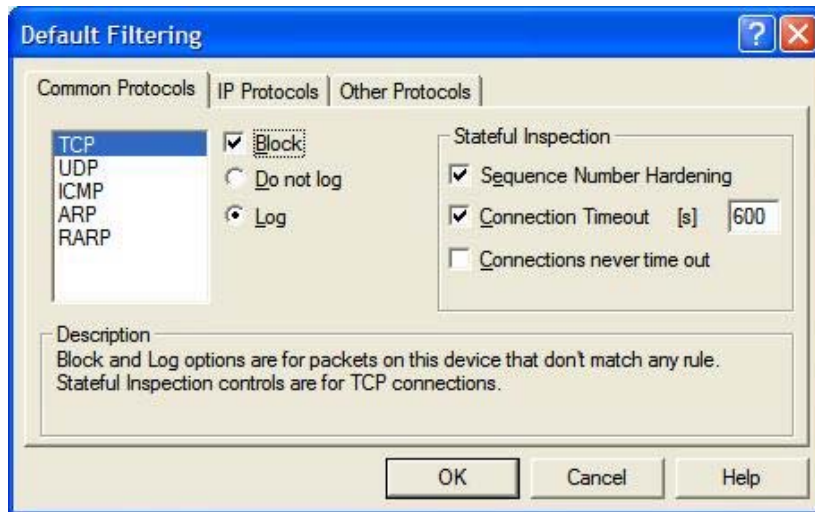
4) **Remote Admin** - This allows the Administrator the ability to connect to multiple computers running VisNetic Firewall directly from within the Firewall console, rather than using a 3rd party remote control program.

Using the remote administration component of the Server version of VisNetic Firewall, you can remotely administer any VisNetic Firewall using an encrypted communications link. You can also reboot or shut down the remote system using the remote admin controls. In addition to remotely administering other Server or Workstation firewalls, you can use the stand-alone Remote Administration Tool to remotely connect to your own Server firewall.

5) **Syn Flood Protection** - A SYN Flood is a common type of denial of service (DoS) attack used against servers. When launching a SYN Flood, an attacker bombards you with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. VisNetic Firewall employs SYN cookies to protect you from SYN Flood attacks.



6) **Control of all Protocols** - VisNetic Firewall is also more robust in the protocols that it has the ability to block / allow. Windows Firewall can block general traffic however it does not offer any ability (that I am aware of) to block ARP, NETBEUI, and IPX requests like VisNetic Firewall.



7) **Logging** - With VisNetic Firewall the logs are quite detailed and show exactly what's happening, what ports are being accessed, and are very informative.

