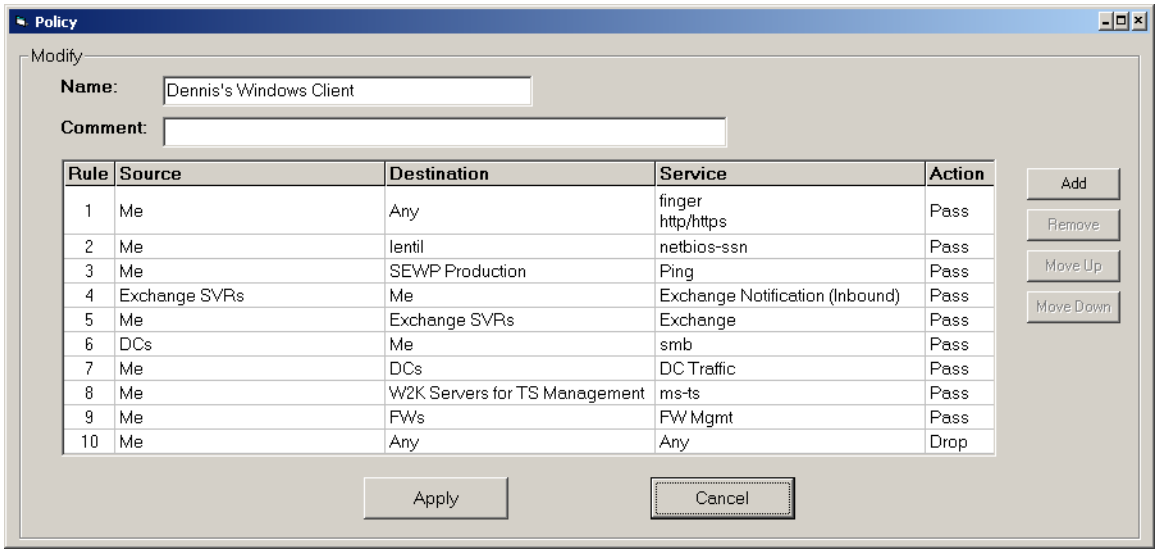
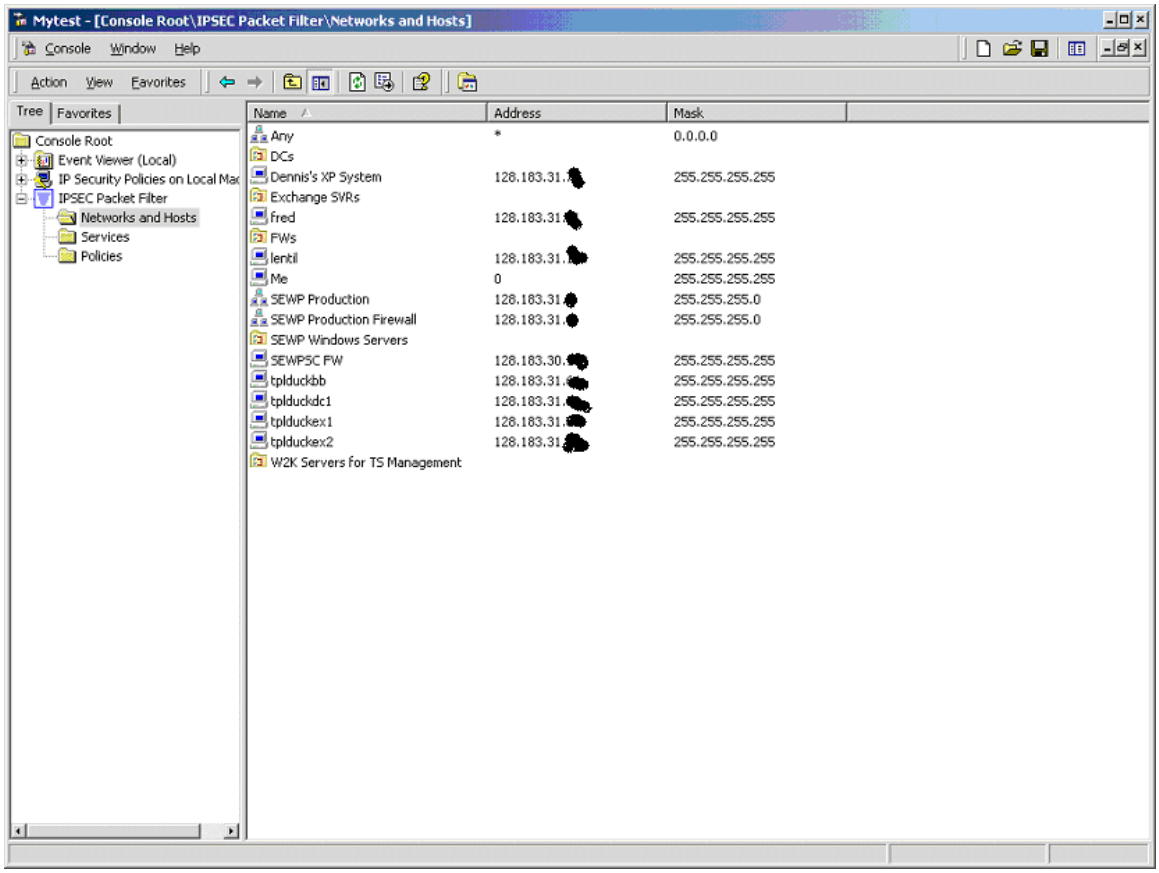
Notes on IPSECPF

Many months ago I started whittling away on a program that would allow me to define packet filters on a windows box using a standard looking firewall ruleset definition interface. I have created an MMC snapin program, IPSECPF. Using the program I can create a policy that looks like this:

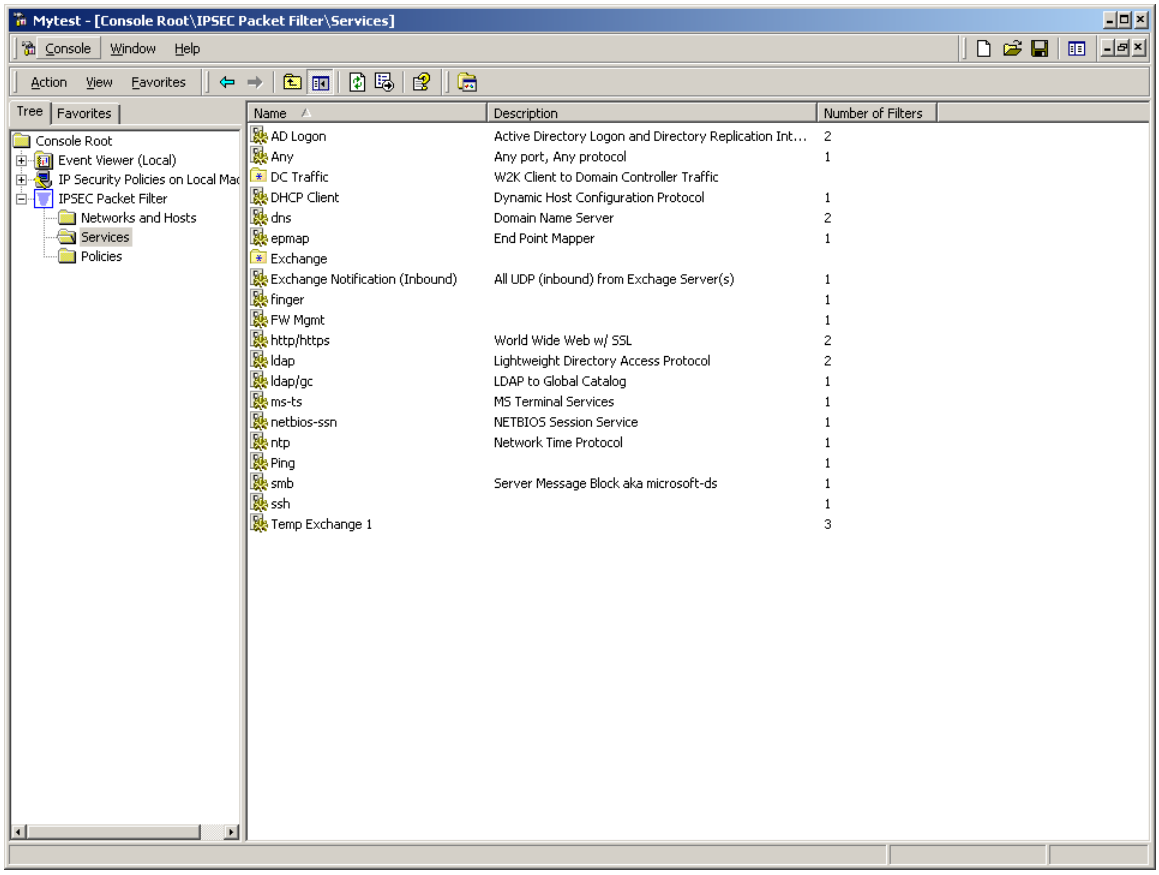


Notice the traditional drop all default at the bottom—by default the rules are mirrored so that inbound is also dropped. There are two other inbounds, one for Exchange (new mail notification on UDP any), and SMB from domain controllers (used to make MMC Computer Management work from DCs to clients).

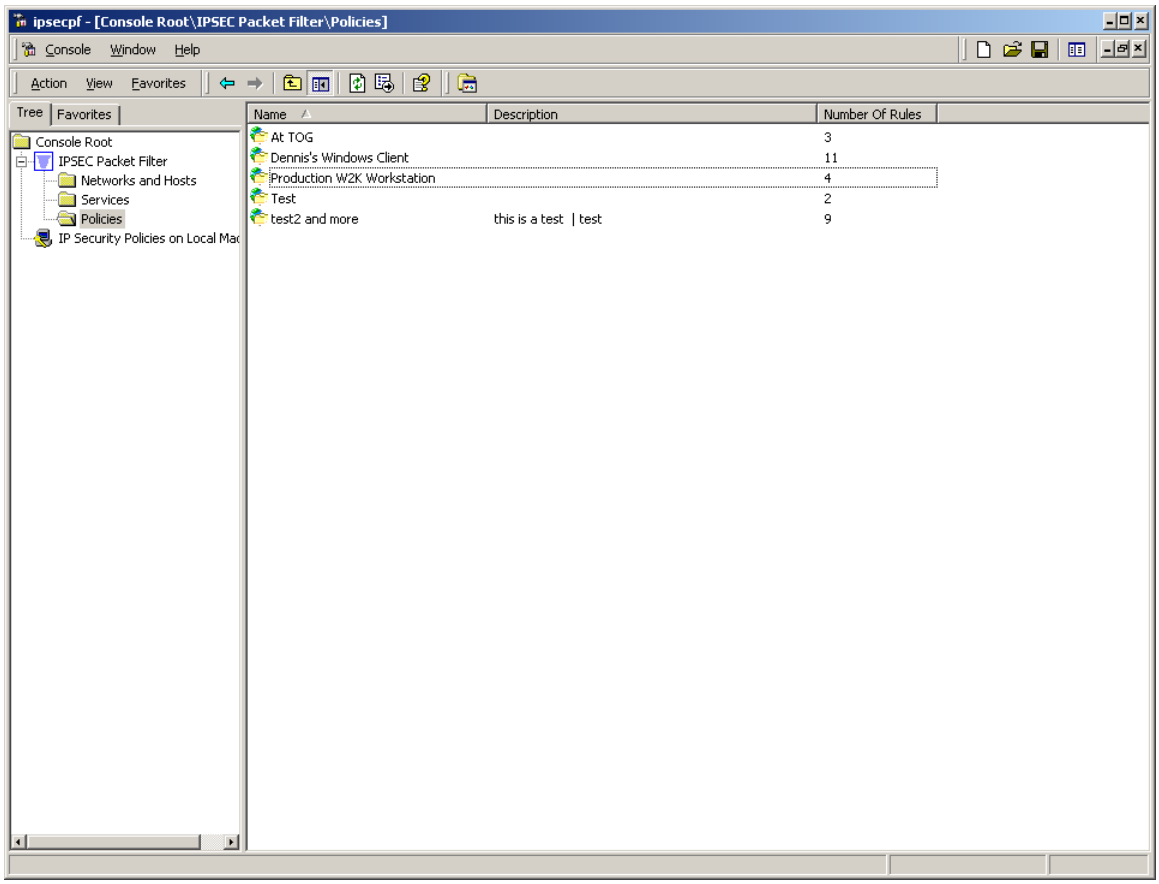
The screen above is from the policy portion of the IPSECPF MMC. The overall MMC looks like this…



Networks/hosts definitions are shown above. One of the most important features of IPSECPF is the ability to group resources (e.g. Exchange SVRs) above.



Service definitions, most of the ones above are built-in. I hope to keep expanding the number of built-in service definitions. But new definitions are pretty easy to define and edit. Notice, again, that you can group them (e.g. DC Traffic, client to domain controller traffic, which comprises 8 services)



Policy definitions. They can be edited, or installed. If installed they must be activated using the Microsoft "IP Security Policies" snapin. This other snapin can be activated in the same MMC instance with IPSECPF.

Restrictions/Limitations

- Requires the program IPSECPOL from the Windows Resource kit…IPSECPOL must be at version 1.22 or greater (earlier versions will just fail). IPSECPF contains a link to download the current version. IPSECPOL must be used to manipulate IPSEC policies—Microsoft does not provide an API.
- No export/import for local definitions (future objective).
- No definition for ESP/AH/IKE, just simple packet filtering (future objective).
- The underlying MS ISPEC implementation does not allow for definition of port ranges or of an ephemeral port. IPSEPCPF allows definition by port number of the common TCP/UDP services. It only allows all or nothing ICMP (no type/code definition).
- There can be only one instance of the IPSPECPF snapin running on a computer, but there is no mutex/singleton to prevent running more than one.
- The filters generated by IPSECPF are fed to IPSECPOL on installation. The filter names must be unique so the filter names are arbitrarily generated and hence somewhat ugly.
- Does not support Windows XP (yet). Windows XP replaces ISPECPOL with IPSECMD.