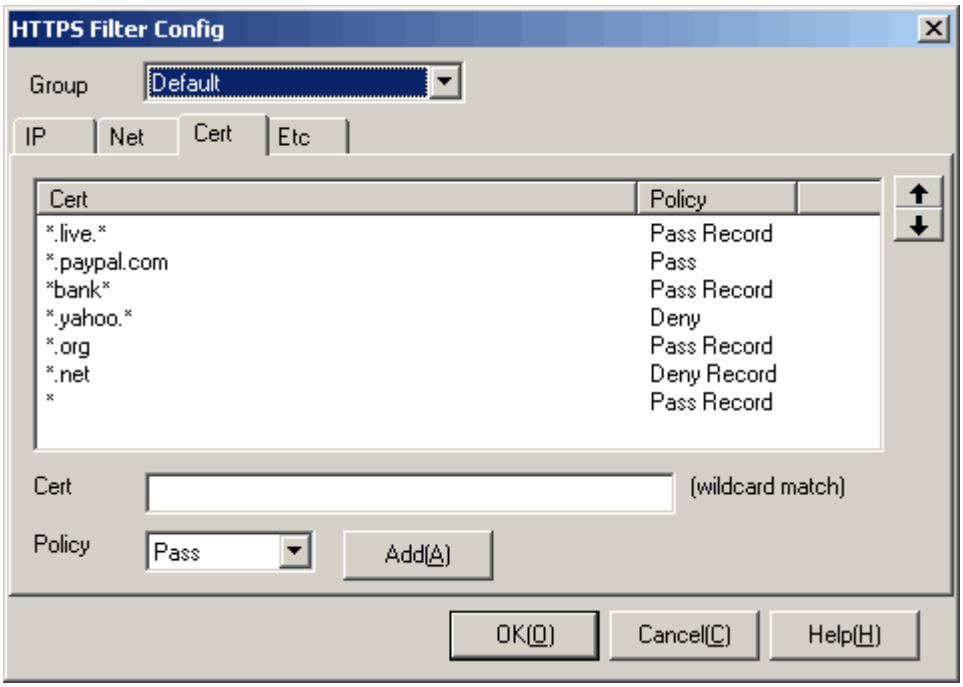
5.14. HTTPS Filter

The HTTPS filter module is used for filtering HTTP over SSL, including IP address, net address, server side certificate, SSL version and so on. Following shows a [HTTPS Filter Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Fill the edit blanks, select a policy, and then press <Add>.
3. Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
4. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
5. Add IP filtering: select [IP] tab, input IP address, select a policy and then press <Add>.
6. Add subnet filtering: select [Net] tab, input a network number and a length of mask, select a policy, and then press <Add>.
7. [Cert]: in the [Cert] tab, input a certificate into [Cert] blank, select a policy, and then press <Add>. When the computers in this group visit a server which certificate matches this item, the policy will be applied. [Cert] filter applies wildcard match.
8. [Deny https proxy tunnel]: When selecting this option, it will ban the users from using https tunnel. Only the standard HTTPS protocol can pass through.
9. [Deny server without certificate]: When selecting this option, it will ban the users from visiting a server which use the standard SSL protocol but has no certificate.
10. [Disable SSL 2.0]: When selecting this option, it will ban the users from using SSL version 2.0 protocol.
11. [Disable SSL 3.0]: When selecting this option, it will ban the users from using SSL version 3.0 protocol.
12. [Disable TLS 1.0]: When selecting this option, it will ban the users from using TLS version 1.0 protocol.
13. Press <OK> or <Cancel>.

Additional instruction:

1. [Subnet]: CIDR network prefix presentation (RFC 1878) is used for recording IP address. For example, a network address 210.31.233.0, with its mask 255.255.255.0, can be recorded as

210.31.233.0/24; a network address 166.133.0.0, with its mask 255.255.0.0, can be recorded as 166.133.0.0/16; a network address 192.168.0.0, with its mask 255.255.255.240, can be recorded as 192.168.0.0/28, etc.

2. The order of IP/Net filtering is from narrow to wide range. For example, IP "61.141.238.1" policy is "Pass", and subnet "61.141.238.0/24" policy is "Deny", which means that the only IP "61.141.238.1" can be passed in the subnet "61.141.238.0/24", all the other IP addresses are denied.
3. [Cert] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (certificate is "*.paypal.*", policy is "Deny"), in the second policy (certificate is "*", policy is "Pass Record"), it means all the servers which certificate match "*.paypal.*" will be denied, and the other servers will be passed and recorded.

 Tip: Since HTTPS is the most common protocol on the Internet, many software go through HTTPS tunneling to contact with outside in order to transpierce a firewall. Please enable the option [Deny https proxy tunnel] and [Deny server without certificate] to deny https tunnel.
