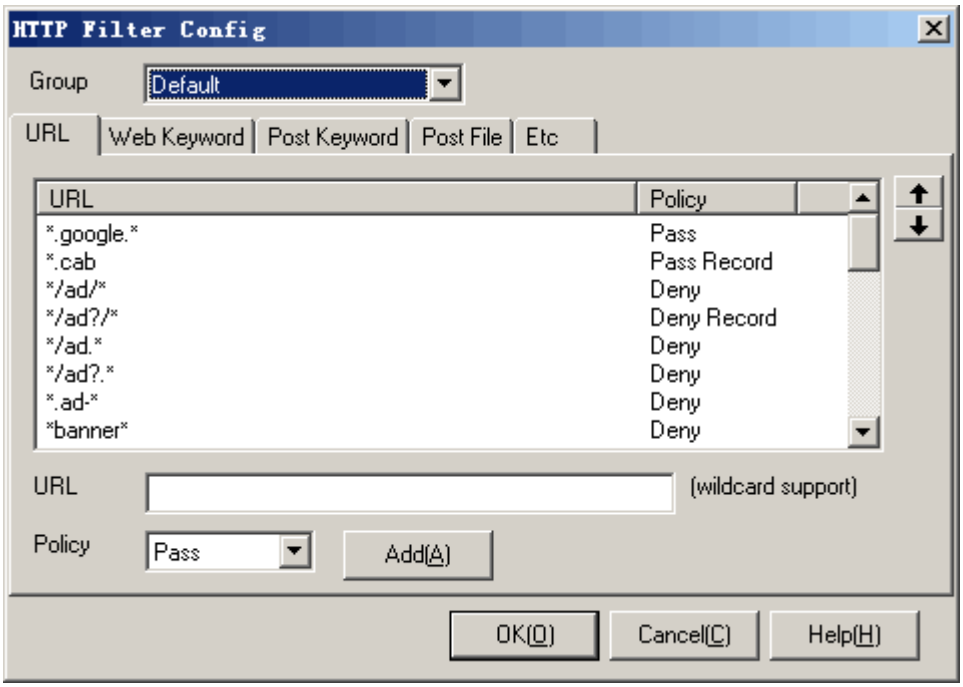
5.9. HTTP Filter

HTTP filter module is used for filtering HTTP, including URL, web page contents, post contents, post files and so on. Following shows a [HTTP 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. [URL]: Input an URL into the [URL] blank. The URL does not include a prefix "http://". Select a policy in the [Policy] list, and then press <Add>. When the computers in this group request an URL which matches this item, the policy will be applied. [URL] filter applies wildcard match.
6. [Web Keyword]: Input a keyword into the [Keyword] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group visit a web page including the keyword which matches this item, the policy will be applied.
7. [Post Keyword]: Input a keyword into the [Keyword] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group post some content including the keyword which matches this item, the policy will be applied.
8. [Post File]: Input a file name into the [File] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group post a file through web browser which matches this item, the policy will be applied. [Post file] filter applies wildcard match.
9. [Deny http proxy tunnel]: When selecting this option, it will ban the users from using http proxy or http tunnel. Only the standard HTTP GET and POST method can pass through.
10. [Deny IP host]: When selecting this option, it will ban the users from visiting web server through IP address (for example, http://64.233.189.22), and it will only pass the URL request with domain name (for example, http://www.google.com).
11. [Output size limit]: When selecting this option, you should fill the edit blank in the same line. When it works, the exceeding bytes will be denied to post.
12. [Download size limit]: When selecting this option, you should fill the edit blank in the same line. When it works, the exceeding bytes will be denied to download.

13. Press <OK> or <Cancel>.

Additional instruction:

1. [URL] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (URL is "admin.*", policy is "Pass"), in the second policy (URL is "ad*", policy is "deny"), it means that all the web sites including "admin.*" will be passed, but all the other web sites including "ad" will be denied.
2. [Web Keyword] filters are running in the order of top-down. For example, in the first policy (keyword is "medical", policy is "Pass"), in the second policy (keyword is "sex", policy is "Deny"), it means that all the web pages including "medical" will be passed, but all the other web pages including "sex" will be denied.
3. [Post Keyword] filters are running in the order of top-down. For example, in the first policy (keyword is "contract", policy is "Deny"), in the second policy (keyword is "=", policy is "Pass Record"), it means that all the post requests including "contract" will be denied, and the other requests will be passed and record.
4. [Post File] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (file name is "*.doc", policy is "Deny"), in the second policy (file name is "*", policy is "Pass Record"), it means all the posted files with postfix "*.doc" will be denied, and the other files will be passed and recorded.
5. Post keyword filters only works in the "HTTP-POST" method. For "HTTP-GET" method, please use URL filters.
6. When a post filter or a URL filter works, the <Active Wall> will identify ANSI and UTF8 formats automatically.
7. When a HTTP request is transferred in one time, it may go through several filters. If one of the filters is "Deny" or "Deny Record", the connection will be terminated at once.

 Tip: Since HTTP protocol is the most common place, many software go through HTTP tunneling to contact with outside in order to transpierce a fire wall. Therefore start the option [Deny HTTP proxy tunnel] and it will work.
