Content Filter Troubleshooting

Testing and Troubleshooting

After creating the content filtering policy open your web browser and try to access a website within the selected categories.

If the site opens:

- Check the web URL to see if the site is being accessed using the SSL protocol. The Content Filter engine can only filter out HTTP traffic. The Content Filter engine looks at the “get packet” to check against the category server, https packets encrypt the get packet making it difficult for the categories server to categorize the URL domain.

- Configure the SSL-Inspection feature. (on supported routers)

- Delete browser cache.

- Make sure the computer is pointing to the router for DNS queries.

- Verify that content filtering is licensed (if using category based services).

![](Content Filter Category Service License Status)

- Flush DNS cache on your computer and router. To flush the DNS cache on the router you will need to access the device via CLI using the console connection or SSH. Once you have a CLI
session established issue the following command(s) to clear the DNS cache:

Router> configure terminal

Router(config)# ip dns server cache-flush

• The content filter engine may not know what ports it needs to check against. This is not always the case but there are some instances, especially when configuration file has been carried over through multiple firmware upgrades, where the content filter engine may not be checking port traffic. To specify what ports the content filter needs to check against please do the following. Access the ZyXEL router via SSH and issue the following commands.

To display a list of ports being used by the Content Filter engine use the following command:

Router# show utm-manager content-filter defaultport

To add ports to the service checklist use the following command(s):

Router#configure terminal
Router(Config)# (enter the commands below)
utm-manager content-filter defaultport 80
utm-manager content-filter defaultport 8080
utm-manager content-filter defaultport 443
utm-manager content-filter defaultport 3128
exit
write

Add any additional port(s) you wish the content filter engine to check.

• If you are experiencing issues with SSL Inspection not filtering
encrypted sites with content filter please use the following commands to specify what ports SSL Inspection needs to check.

To display a list of ports being used by SSL Inspection use the following command:

Router# show utm-manager ssl-inspection defaultport

To add ports to the service checklist use the following command(s):

Router# configure terminal
Router(Config)# (enter the commands below)
utm-manager ssl-inspection defaultport 443
utm-manager ssl-inspection defaultport 465
utm-manager ssl-inspection defaultport 995
utm-manager ssl-inspection defaultport 993
utm-manager ssl-inspection defaultport 990
exit
write

Add any additional port(s) you wish the content filter engine to check.

• Contact Tech Support for further assistance.