UNIBOX

An Intelligent Network Controller

Knowledge Base:

Control Module

Publication Date
June 14, 2013

Applicable Products

The administration guide applies to the following products –

- Unibox U-50
- UniBox U-100
- UniBox U-200
- UniBox U-500
- UniBox U-1000

Disclaimer

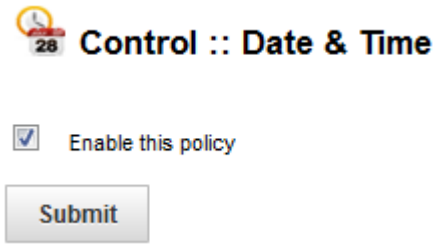
WIFI-SOFT SOLUTIONS PRIVATE LIMITED MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Wifi-soft shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

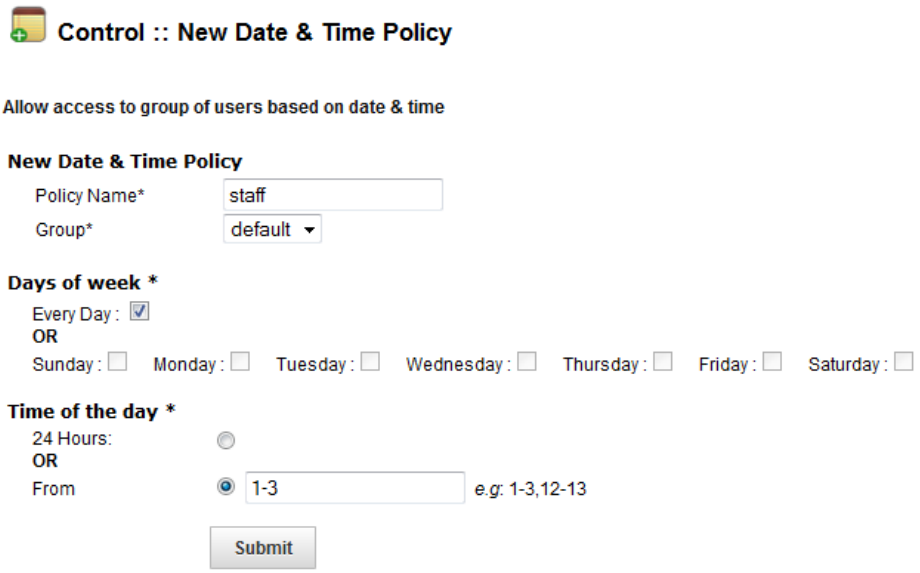
The only warranties for Wifi-soft products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Wifi-soft shall not be liable for technical or editorial errors or omissions contained herein.

Wifi-soft assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Wifi-soft.

1) How to set Date and time policy in Unibox?
   - ✓ Open unibox dashboard in web browser.
   - ✓ Navigate to policy section under control panel.
   - ✓ Click on Date and time policy option from left pane.
   - ✓ First we need to enable policy, click on enable policy checkbox and click on submit.



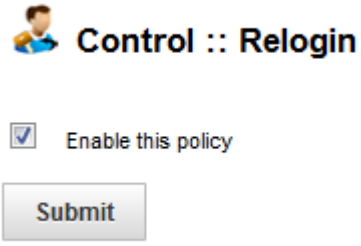
   - ✓ Once the policy is enabled, create new date and time policy by clicking on "New Date and Time policy" option from left pane.



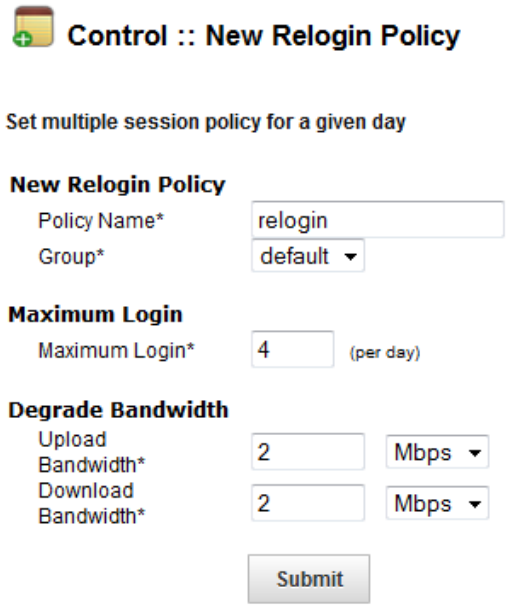
   - ✓ Give name for the policy.
   - ✓ Select group from drop down list on policy will be applied.
   - ✓ Select days of week, can select Everyday or specific days of week.
   - ✓ Mention time of the day, can select as 24 hours or specific time intervals at that time policy will get applied.
   - ✓ Click on submit to save policy configuration settings.

2) How to set Relogin policy in Unibox?
   - ✓ Open unibox dashboard in web browser.
   - ✓ Navigate to policy section under control panel.
   - ✓ Click on relogin option from left pane.

- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.



- ✓ Once the policy is enabled, create new relogin policy by clicking on "Relogin policy" option from left pane.

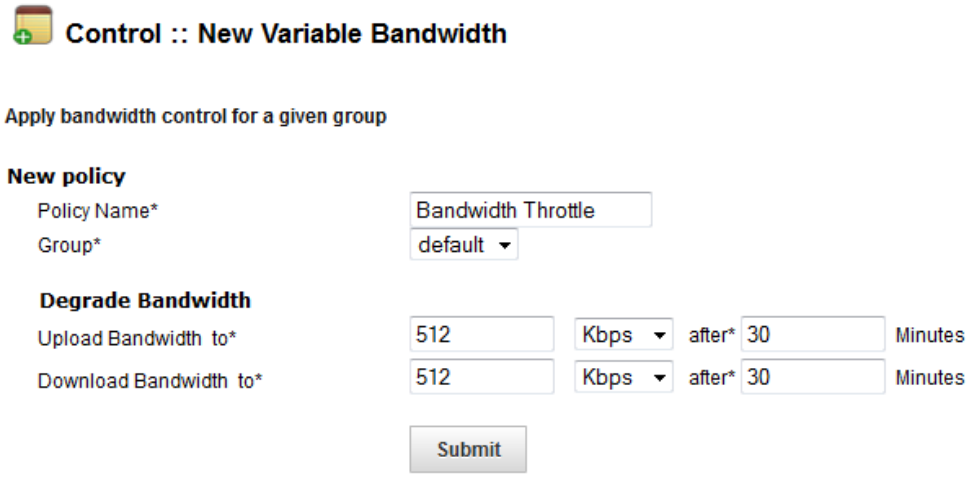


- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Give maximum number limit.
- ✓ Mention degrade bandwidth options such as upload and download bandwidth.
- ✓ Click on submit to save policy configuration settings.

3) How to set Variable Bandwidth policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on variable bandwidth option from left pane.
- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.

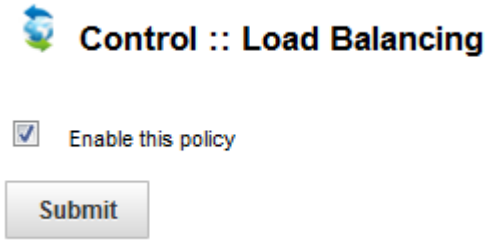
- ✓ Once the policy is enabled, create new variable bandwidth policy by clicking on “New variable bandwidth policy” option from left pane.



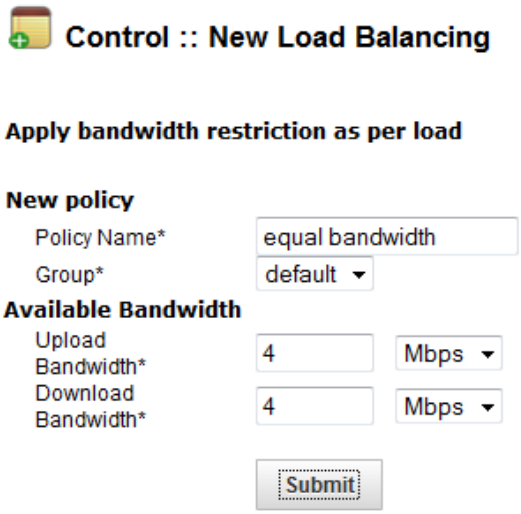
- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Give bandwidth degrade restrictions.
- ✓ Click on submit to save policy configuration settings.

4) How to set Load balancing policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on variable balancing option from left pane.



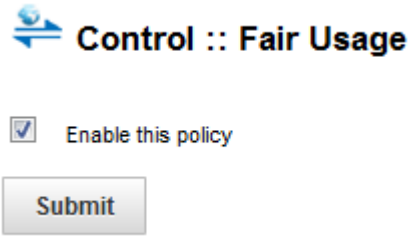
- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.
- ✓ Once the policy is enabled, create new load balancing policy by clicking on “New load balancing policy” option from left pane.



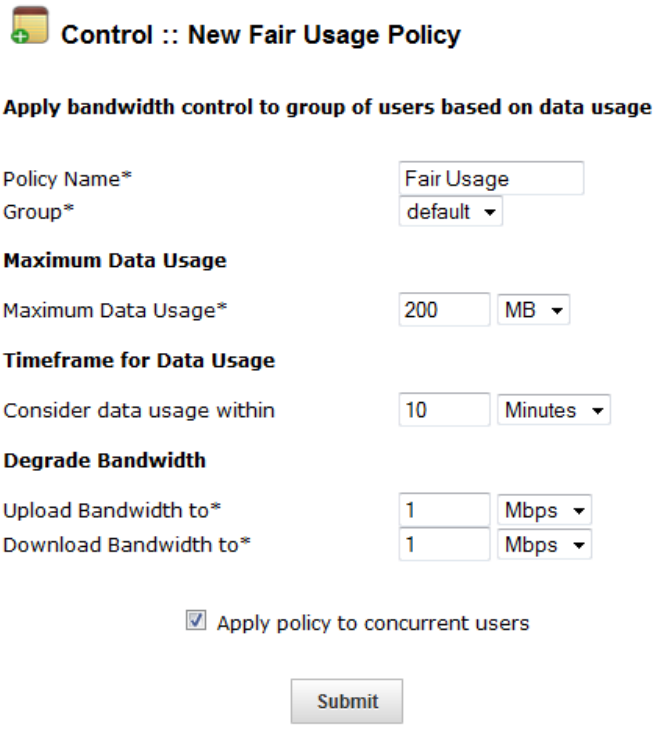
- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Mention available bandwidth for upload and download.
- ✓ Click on submit to save policy configuration settings.

5) How to set fair usage policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on fair usage option from left pane.



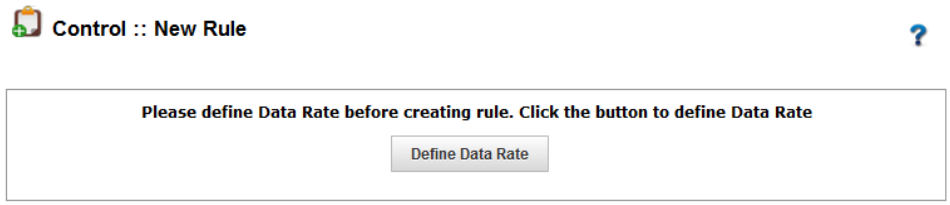
- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.
- ✓ Once the policy is enabled, create new fair usage policy by clicking on “New fair usage policy” option from left pane.



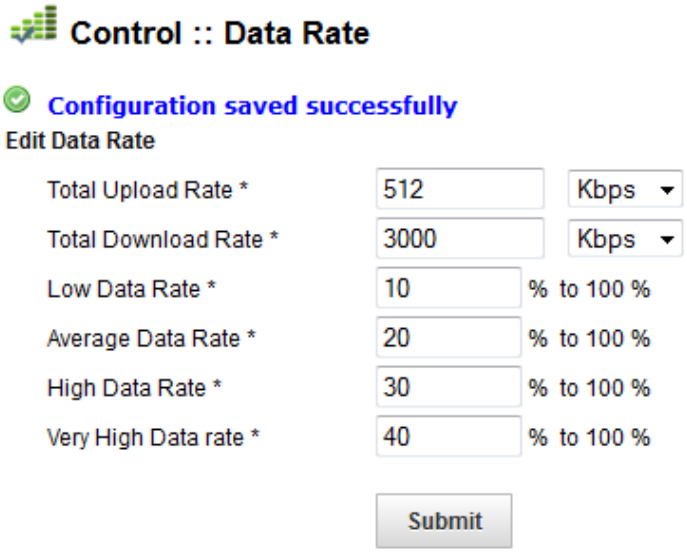
- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Mention maximum data usage. Select data size from drop down list.
- ✓ Mention timeframe for data usage, select data size from drop down list.
- ✓ Mention degrades bandwidth for upload and download.
- ✓ If you want to apply this policy for the concurrent users then tick check box for the same.
- ✓ Click on submit to save policy configuration settings.

6) How to set data rate in bandwidth control?

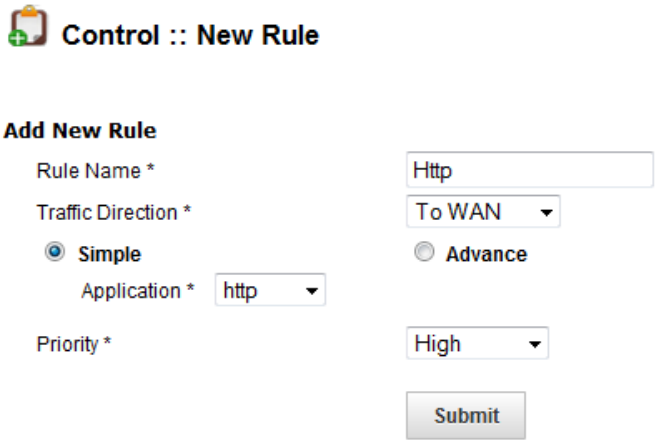
- ✓ Open unibox dashboard in web browser
- ✓ Navigate to bandwidth control section under control TAB.
- ✓ First create new data rule. Click on New rule from left pane.



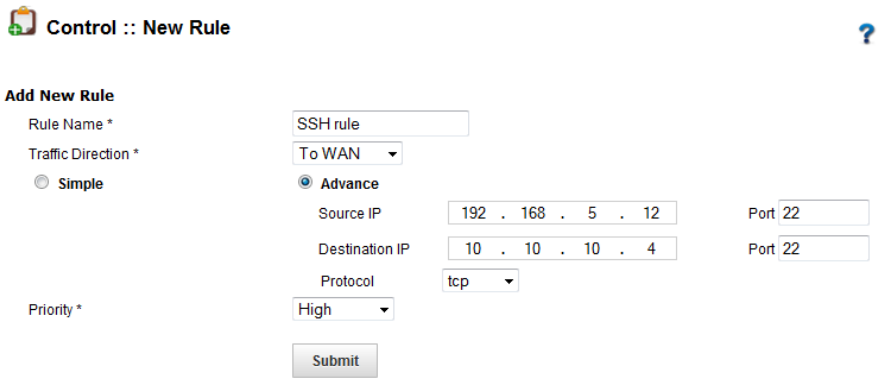
- ✓ Mention total upload rate.



- ✓ Mention Download rate.
- ✓ Mention low, average, high and very high rate in terms of percentage but the sum of all rate should be equal to 100.
- ✓ Click on submit to save data rate.
- ✓ Click on New rule.
- ✓ Give name for the rule.
- ✓ Select traffic direction option from drop down list.
- ✓ There are two types of Rules
    - Simple: It is applied on the selected application from drop down list.



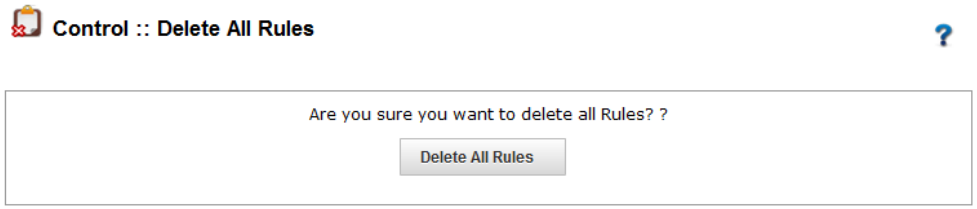
    - Advanced: Here you can mention source and destination IP addresses with port number to control flow of data, Select type of transmission protocol.



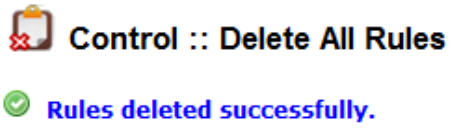
- ✓ Select priority from drop down list.
- ✓ Click on submit to save the configuration changes.

7) How to delete all data rules in unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to bandwidth control section under control TAB.



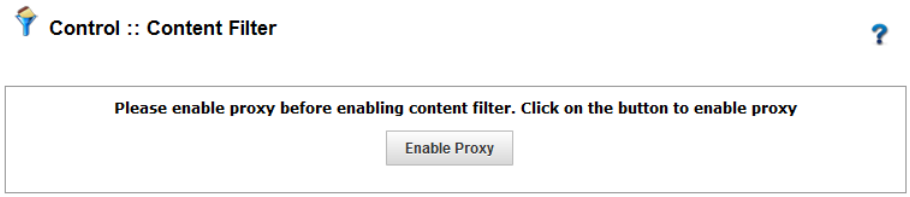
- ✓ Click on delete all data rules from left pane.

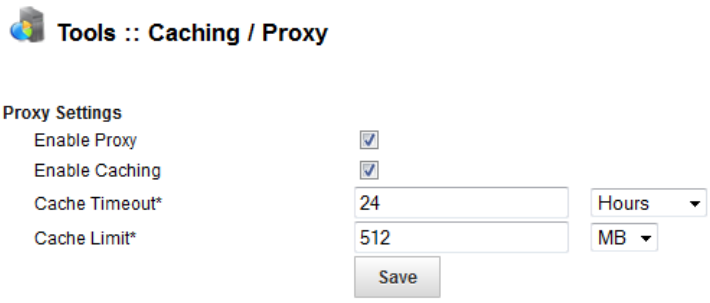


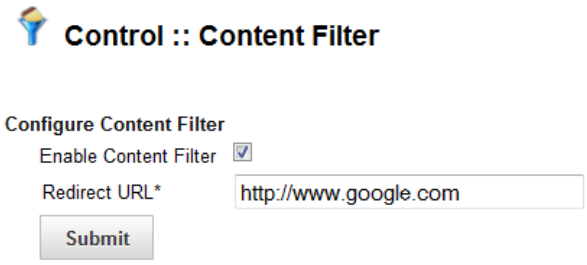
- ✓ All rules will be deleted.

8) How to apply URL blocking or content filter feature in Unibox?

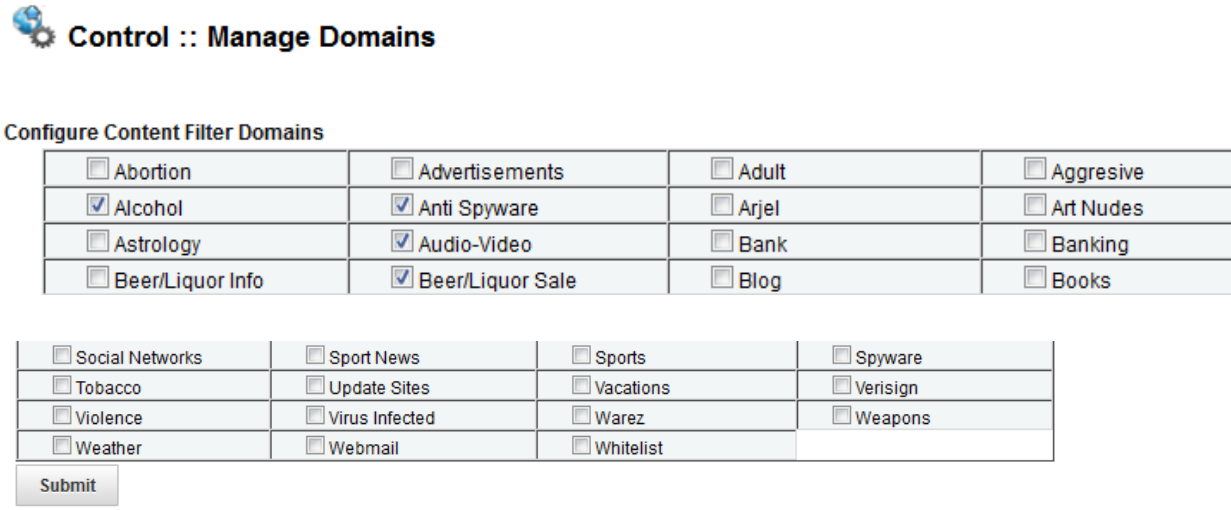
- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to content filter section under control TAB.
- ✓ To enable content filter make sure that you should enable proxy settings.
- ✓ Go in tools, caching proxy and enable proxy.







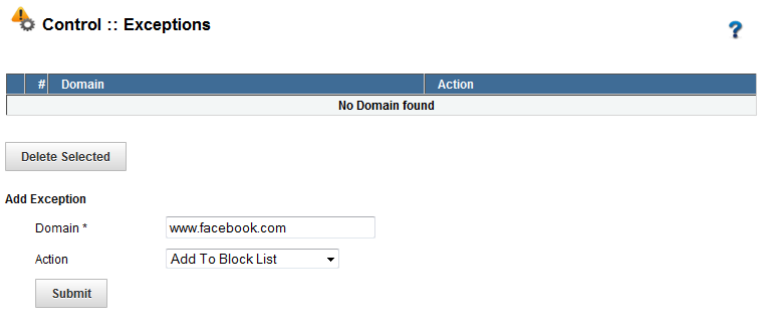
- ✓ Tick check box to enable content filter.
- ✓ Mention redirection URL.
- ✓ Click on submit to enable.
- ✓ Click on manage domain option from left pane to block URL's by selecting categorized groups.



- ✓ Click on submit to save configuration.

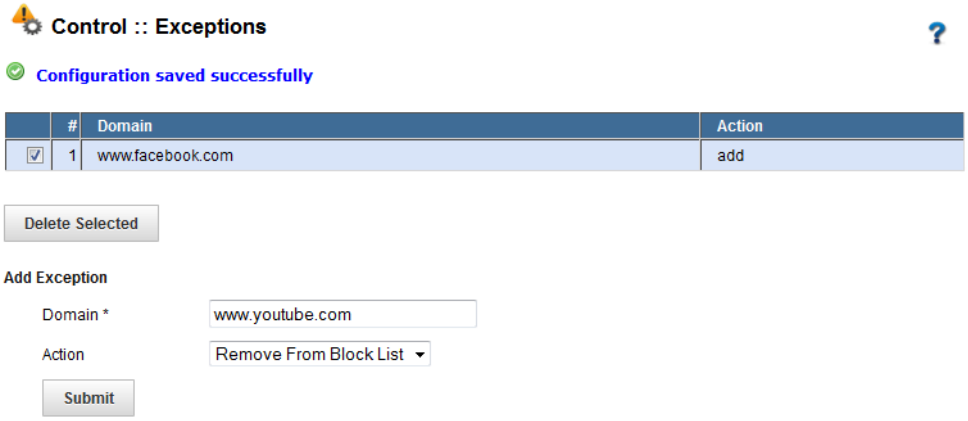
9) How to add or remove URL's to block list?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to content filter section under control TAB.
- ✓ Click on Exceptions option from left pane.
- ✓ To block URL:



  - Mention URL in Domain textbox and take action selecting "Add to block list" from drop down list.

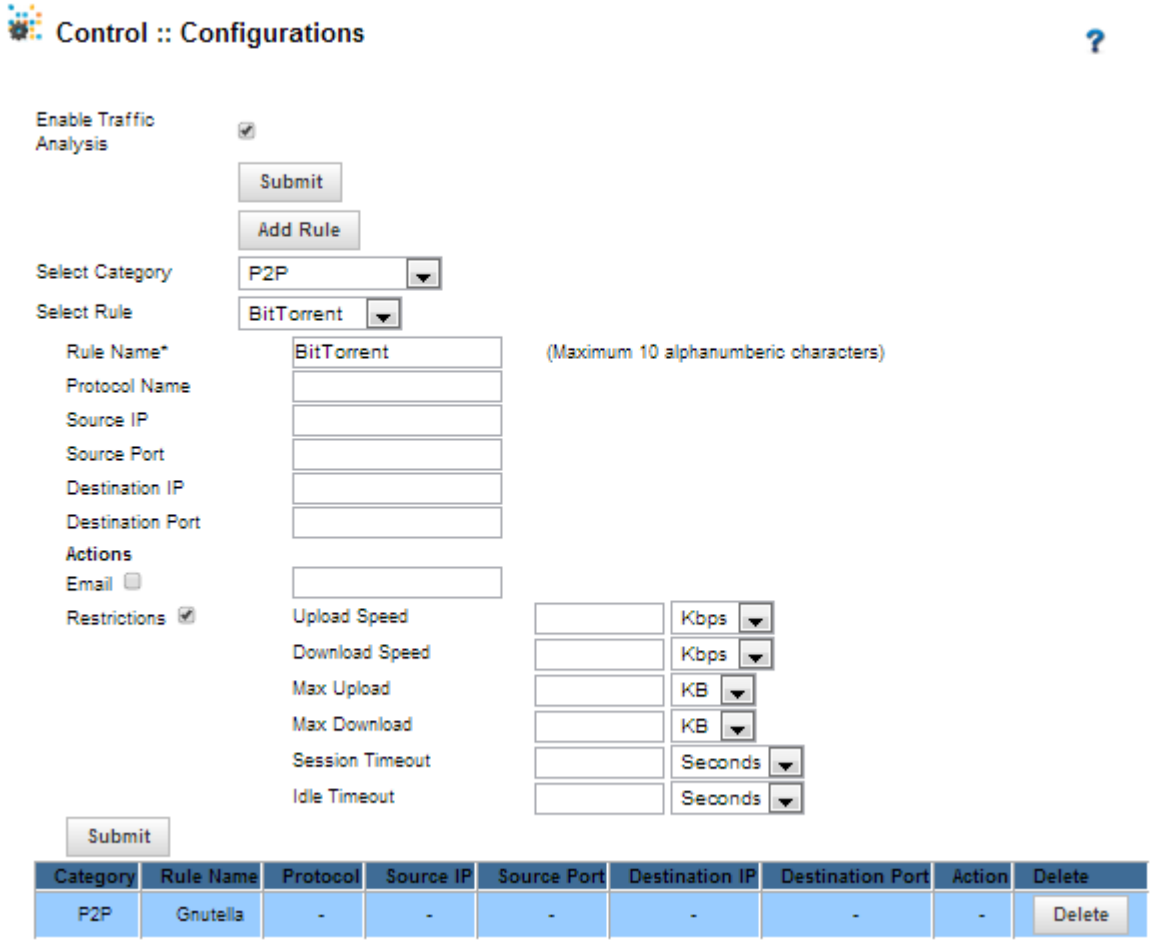
- ✓ To Remove URL from blocked list:



- ✓ Mention URL in domain textbox and take action selecting "Remove from blocked list" from drop down list.
- ✓ Click on submit to save changes made.

10) How to block torrents in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to traffic analysis section under control panel.
- ✓ Enable Traffic analysis by ticking check box, click on submit.
- ✓ Once traffic analysis is enabled, click on add rule to set rules.
- ✓ Select the type of traffic you want to block from drop down list.
- ✓ Once the type is selected, select rule from drop down list.
- ✓ Give name for rule.



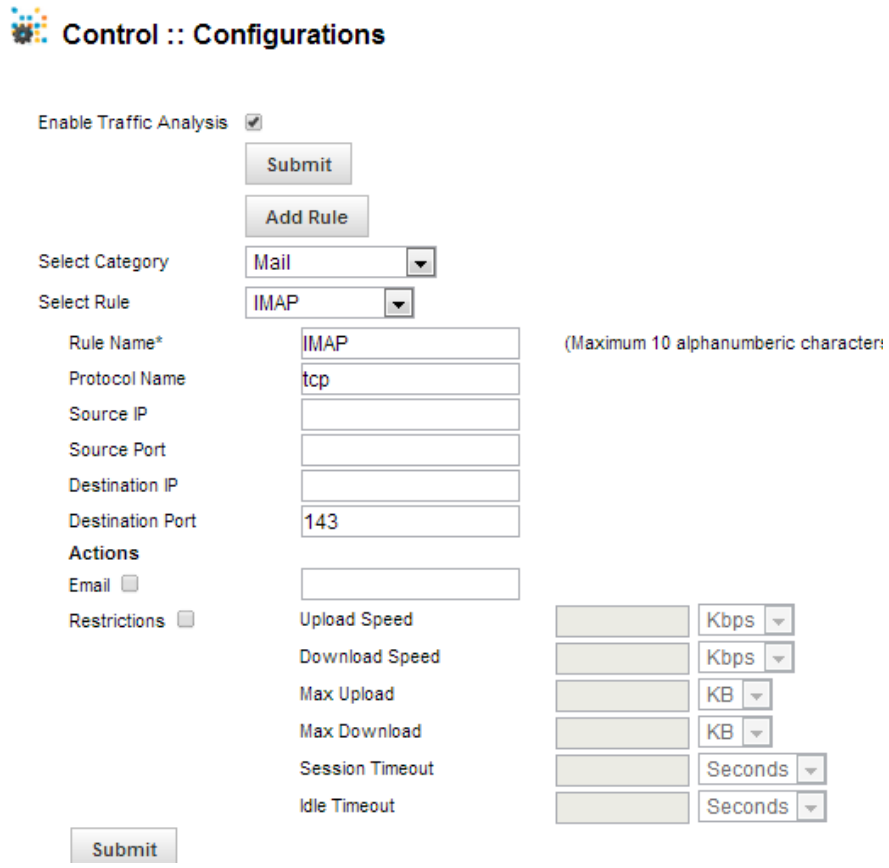
- ✓ Give protocol name, mention source port, source IP, Destination port, destination IP.
- ✓ Select the actions, if you want notification of traffic analysis then mention mail ID.
- ✓ If you want to restrict traffic, then mention upload speed, download speed, max upload & download Session timeout and idle timeout.
- ✓ Click on submit to save rule.

11) How to block specific traffic in unibox?

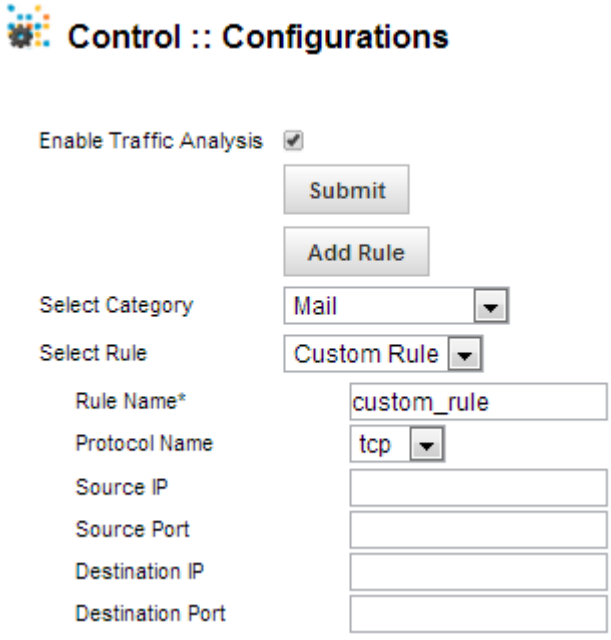
- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to traffic analysis section under control TAB.
- ✓ Enable Traffic analysis by ticking check box, click on submit.
- ✓ Once traffic analysis is enabled, click on add rule to set rules.

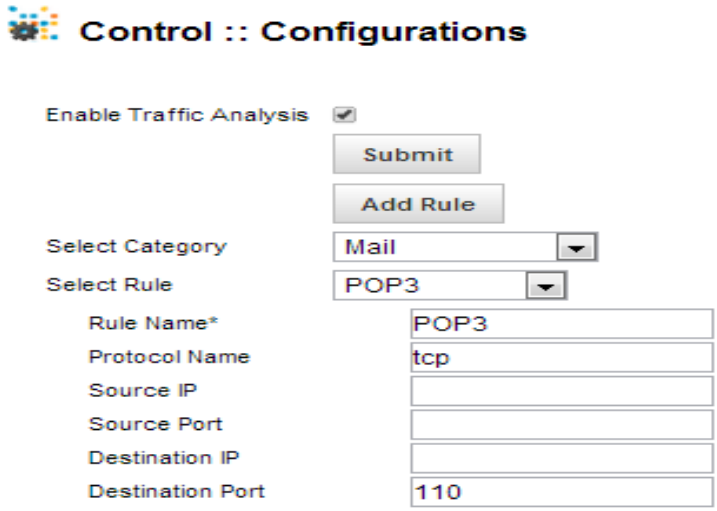
There are various types of traffic that can be blocked under unibox:

- ✓ To block MAIL traffic:
- ✓ Select category as Mail from drop down list.
- ✓ Select the type of mailing protocol you want to block (Ex. POP3 or IMAP).



✓ These rules are predefined, if you want to add new rule then select option as custom rule. Select protocol name and configure rest of the settings.

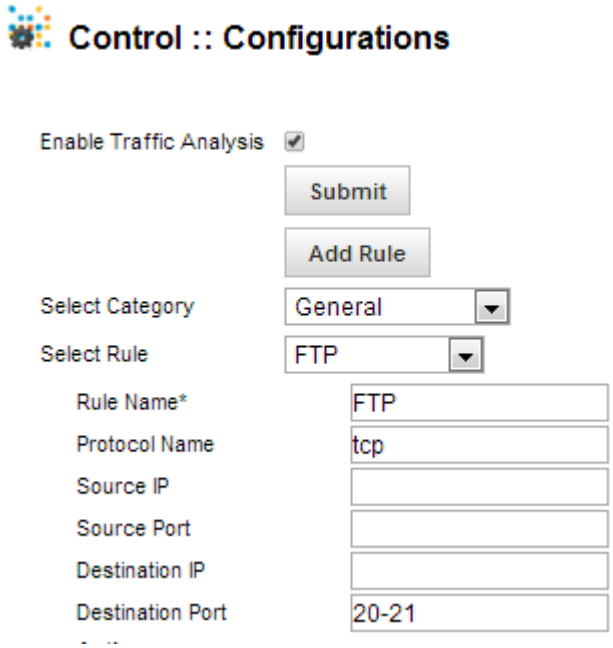




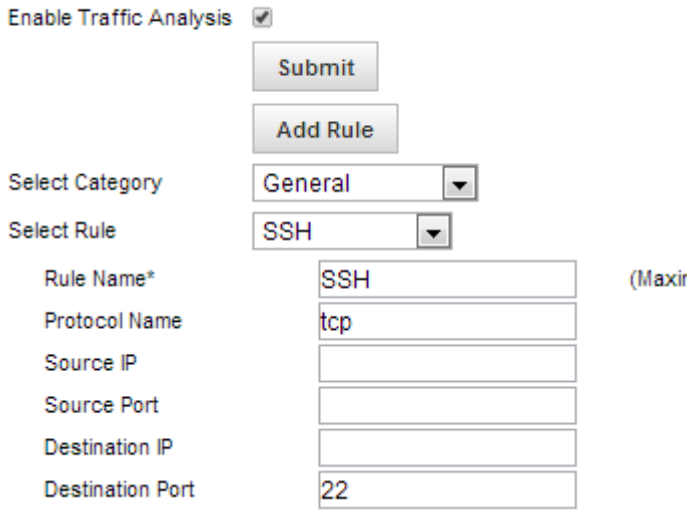
- ✓ Click on submit to save rule.

✓ To block General Traffic:

- ✓ General rule is categorized in to four types naming FTP, SSH, HTTP and custom rule.
- ✓ To block FTP traffic:



- Select FTP from drop down list.
- Give rule name and protocol name, destination port is predefined.
- Configure rest settings and click on submit to save FTP rule.
- To block SSH traffic:
  - This is predefined rule with rule name, protocol and destination port.

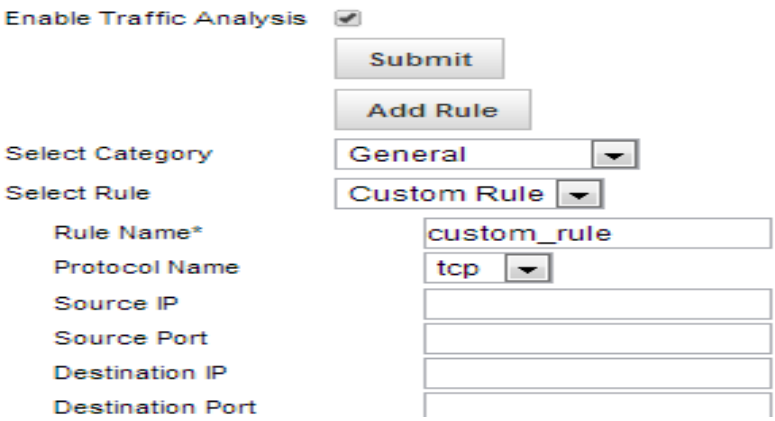


- Configure rest settings and click on submit to save SSH rule.

- To block HTTP traffic:

  - This is predefined rule with rule name, protocol and destination port.
  - Configure rest settings and click on submit to save HTTP rule.

- Block general traffic configuring custom rule:

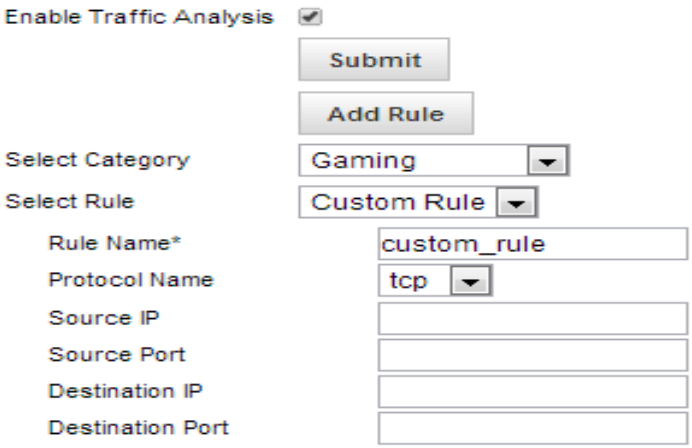


- This is not predefined rule, select protocol for rule, port number.
- Configure rest settings and click on submit to save custom rule.

✓ To block gaming traffic:

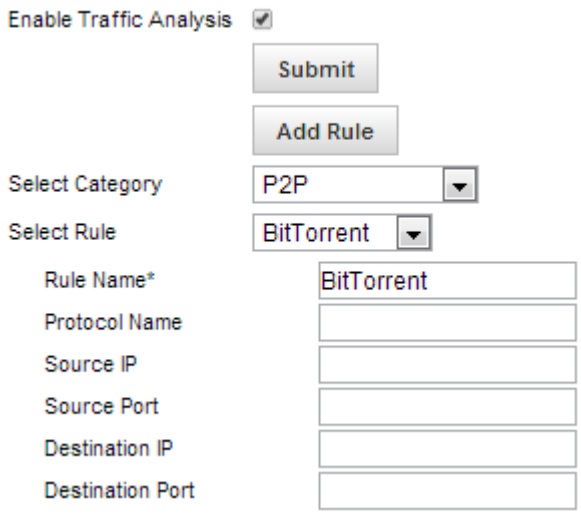
- This is predefined rule with rule name, protocol and destination port.
- Configure rest settings and click on submit to save CS rule.

▪ To block gaming traffic by setting rule:



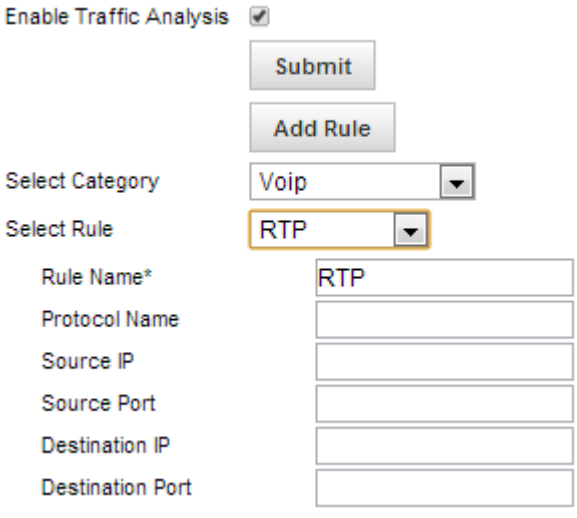
- This is not predefined rule, select protocol for rule, port number.
- Configure rest settings and click on submit to save custom rule.

✓ To block P2P traffic:



- All the rules are predefined with rule name, protocol and destination port.
- Configure rest settings and click on submit to save rule.

✓ To block VOIP traffic:



- This is predefined rule with rule name, protocol and destination port.
- Configure rest settings and click on submit to save RTP (Real time transport protocol) rule.

12) How to check traffic analysis reports?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on the reports option from left pane.
- ✓ Click on the name of rule to view the traffic analysis details.