How to configure Application Mapping

created by: Rainer Bemsel – **Version** 1.0 – **Dated:** Dec/25/2010

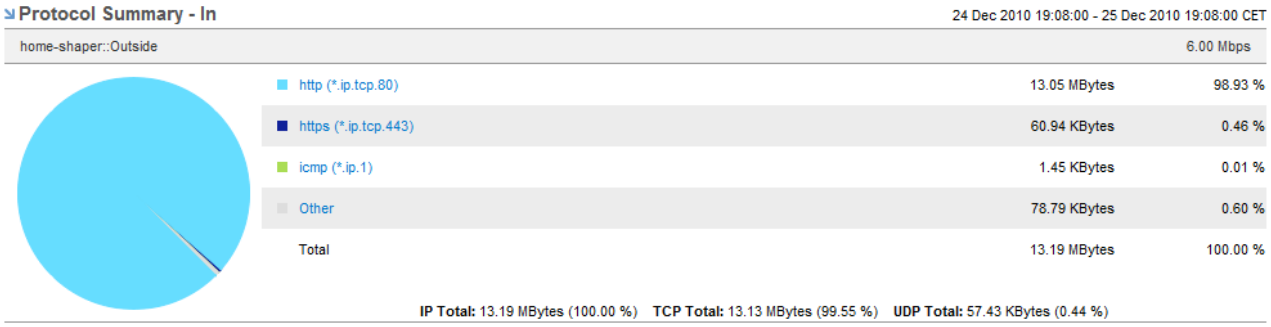
Wouldn't it be nice to have the option to differentiate between regular HTTP Traffic and HTTP Traffic going to a specific website, such as SAP Portal or an intranet server? Reporter Analyzer from NetQoS, acquired by CA Technologies does have a feature, called Application Mapping to configure exactly that purpose.

For this technical tip, I did use CA NetQoS Reporter Analyzer Version 9.0

I do have a portal with following IP address, which is being accessed using HTTP

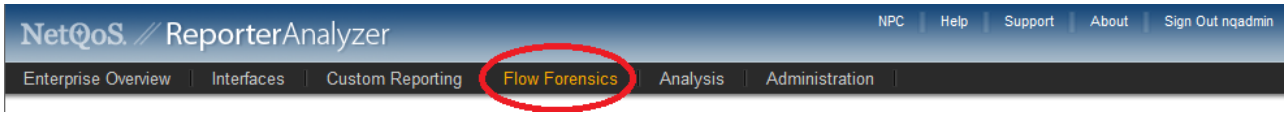
Destination IP Address	82.165.91.63
TCP Port	80

Seeing over 98% HTTP traffic, how much did go to the web server of choice (www.bemsel.com). To differentiate those HTTP traffic, application mapping could help.

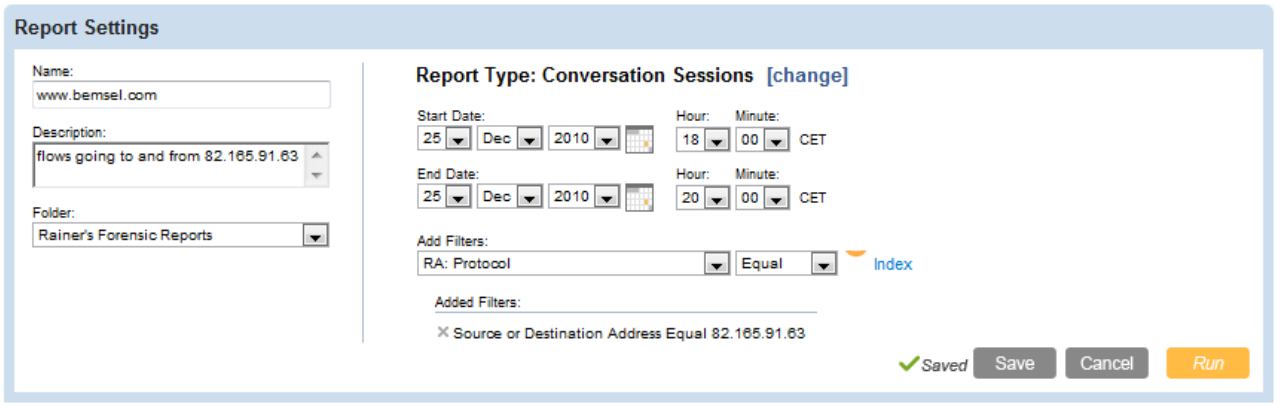


To make sure you get required flows, run a flow forensic report against all flows with a filter set to the portals IP address

To create a new Flow Forensic Report, proceed with following short steps.



Click on "Flow Forensics" tab
On the right pane, click on NEW to create a new report
Choose a time frame for max. 2hours
Add "Source or Destination Address" as Filter and add the required IP Address as parameter
Click on Save



When clicking on **RUN**, it will take a few moments to complete the report. Just be patient and you should get a result, similar to this

Report Results

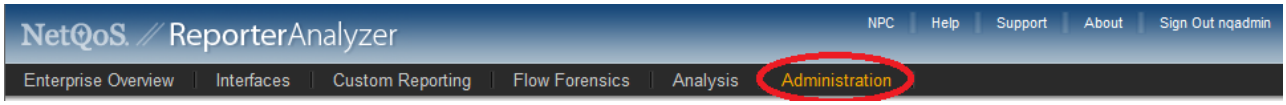
Router Addr	Interface In	IP Protocol	Src Addr	Src Port	Dest Addr	Dest Port	ToS	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Flow Duration	Pkts	Rate (Pkts)	% Total (Pkts)
192.168.10.152	1	icmp (*.ip.1)	192.168.10.234	0	82.165.91.63	0	Default Traffic (0)	240 Bytes	8.85 Kbps	< 1.00 %	4	217 ms	4	18.43 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50284	82.165.91.63	80	Default Traffic (0)	10.02 KBytes	5.11 Kbps	< 1.00 %	1	15 secs 698 ms	61	3.89 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50285	82.165.91.63	80	Default Traffic (0)	2.65 KBytes	2.73 Kbps	< 1.00 %	1	7 secs 762 ms	22	2.83 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50291	82.165.91.63	80	Default Traffic (0)	7.19 KBytes	4.84 Kbps	< 1.00 %	1	11 secs 865 ms	41	3.46 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50292	82.165.91.63	80	Default Traffic (0)	1.26 KBytes	1.81 Kbps	< 1.00 %	1	5 secs 591 ms	10	1.79 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50294	82.165.91.63	80	Default Traffic (0)	5.95 KBytes	4.11 Kbps	< 1.00 %	1	11 secs 575 ms	40	3.46 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50297	82.165.91.63	80	Default Traffic (0)	4.55 KBytes	3.68 Kbps	< 1.00 %	1	9 secs 899 ms	29	2.93 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50298	82.165.91.63	80	Default Traffic (0)	3.42 KBytes	2.76 Kbps	< 1.00 %	1	9 secs 901 ms	25	2.53 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50299	82.165.91.63	80	Default Traffic (0)	4.53 KBytes	3.66 Kbps	< 1.00 %	1	9 secs 906 ms	28	2.83 pkts/s	< 1.00 %
192.168.10.152	1	tcp (*.ip.6)	192.168.10.234	50306	82.165.91.63	80	Default Traffic (0)	1.04 KBytes	765 bps	< 1.00 %	1	10 secs 867 ms	7	0.64 pkts/s	< 1.00 %

1 of 6 Size: 10 Page: 1 Go

After seeing destination and source address with 82.165.91.63 you are fine with the next step.

Change Application Mapping Default Settings

1. In Reporter Analyzer click on Administration

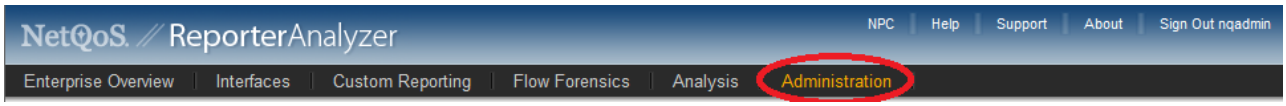


2. In the left pane, select "**Application Settings**"

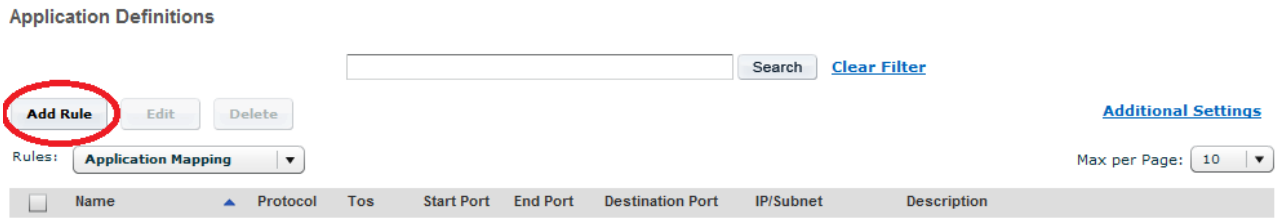
3. Set the TCP und UDP Rebase Ports to 63000

Don't forget to click **SAVE** at the end of that configuration page !!!

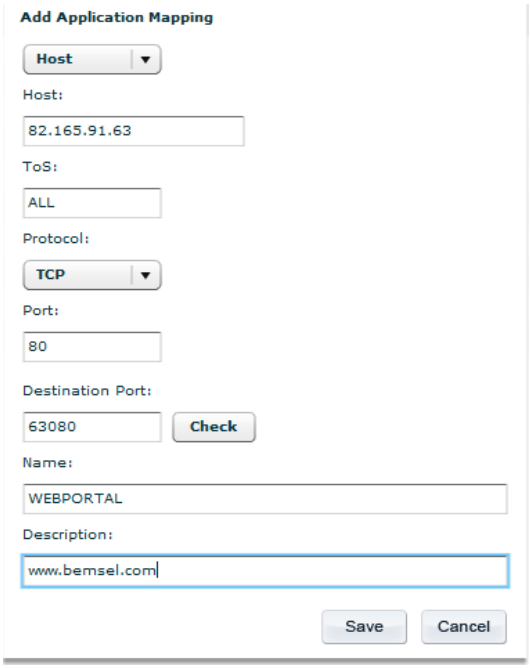
You are still in Administration Page.

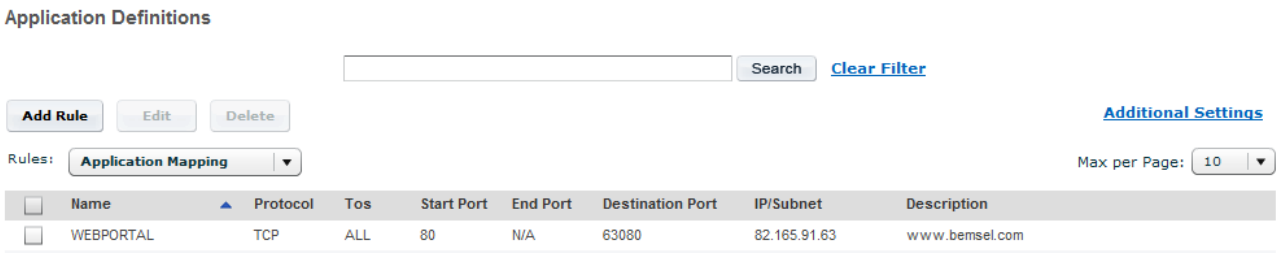


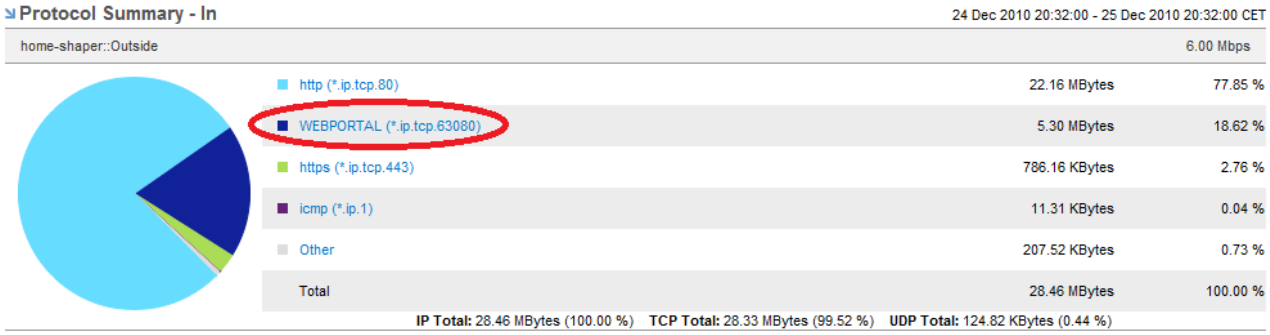
Click on Application Definitions on the left Pane under "Define an Application"



Add a rule to map all tcp_80 traffic for 82.165.91.63 to port 63080. Keep ToS to ALL





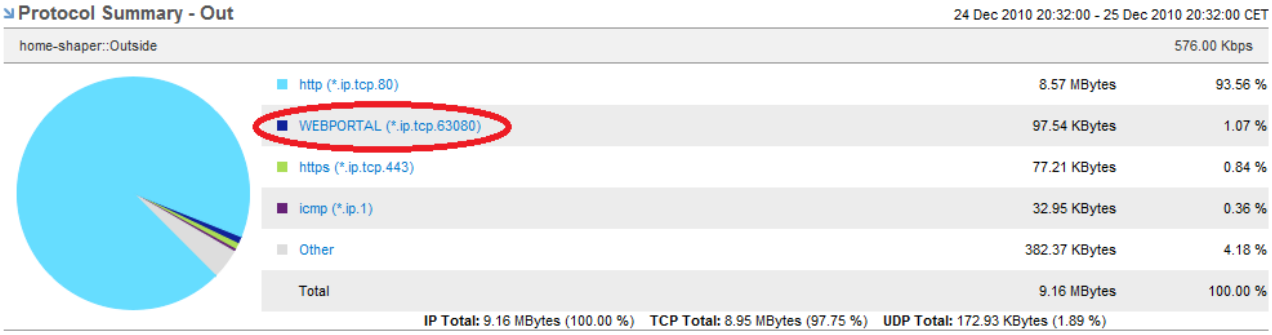


Protocol Summary - In 24 Dec 2010 20:32:00 - 25 Dec 2010 20:32:00 CET

home-shaper::Outside 6.00 Mbps

http (*.ip.tcp.80)	22.16 MBytes	77.85 %
WEBPORTAL (*.ip.tcp.63080)	5.30 MBytes	18.62 %
https (*.ip.tcp.443)	786.16 KBytes	2.76 %
icmp (*.ip.1)	11.31 KBytes	0.04 %
Other	207.52 KBytes	0.73 %
Total	28.46 MBytes	100.00 %

IP Total: 28.46 MBytes (100.00 %) **TCP Total:** 28.33 MBytes (99.52 %) **UDP Total:** 124.82 KBytes (0.44 %)



Protocol Summary - Out 24 Dec 2010 20:32:00 - 25 Dec 2010 20:32:00 CET

home-shaper::Outside 576.00 Kbps

http (*.ip.tcp.80)	8.57 MBytes	93.56 %
WEBPORTAL (*.ip.tcp.63080)	97.54 KBytes	1.07 %
https (*.ip.tcp.443)	77.21 KBytes	0.84 %
icmp (*.ip.1)	32.95 KBytes	0.36 %
Other	382.37 KBytes	4.18 %
Total	9.16 MBytes	100.00 %

IP Total: 9.16 MBytes (100.00 %) **TCP Total:** 8.95 MBytes (97.75 %) **UDP Total:** 172.93 KBytes (1.89 %)

With this simple application mapping, there was a separation of standard HTTP Traffic going to www.bemsel.com, shown as WEBPORTAL. All other HTTP Traffic is still visible in the protocol summary.

Application Mapping does have even more options

You can combine traffic from an application that uses several ports and consolidate it into one port for reporting the total traffic identified with that application

You might want to map traffic to one target port for situations like the following:

- To differentiate common protocols, like HTTP, based on type of application, such as CRM, Web portals, and Internet traffic. (as shown in this example)
- To aggregate VoIP traffic that uses several different ports into one port. You can aggregate all VoIP traffic with an appropriate ToS bit and map it to a single port to identify it in ReporterAnalyzer reports.
- To aggregate all mail traffic in an environment with two different mail systems using different protocols, such as IMAP and POP. All traffic using these two mail protocols from a core group of servers can be reported as a single application in one port. For example, IMAP uses TCP port 443 and POP mail uses TCP 109 and 100; these can be mapped to port 31000 and labeled as Mail.
- To identify all Microsoft Exchange Server traffic that uses a broad range of port numbers. You can map the traffic to a single port and label it as MS Exchange.