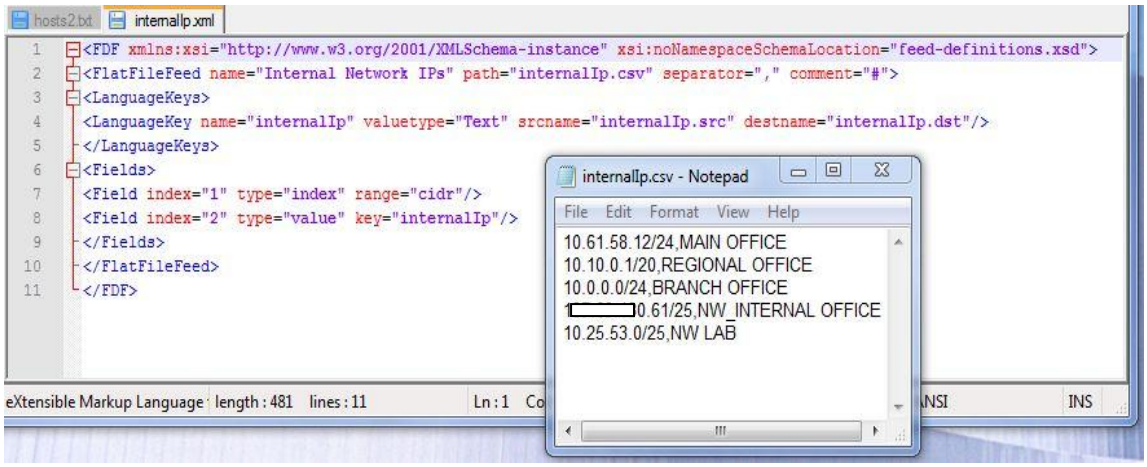
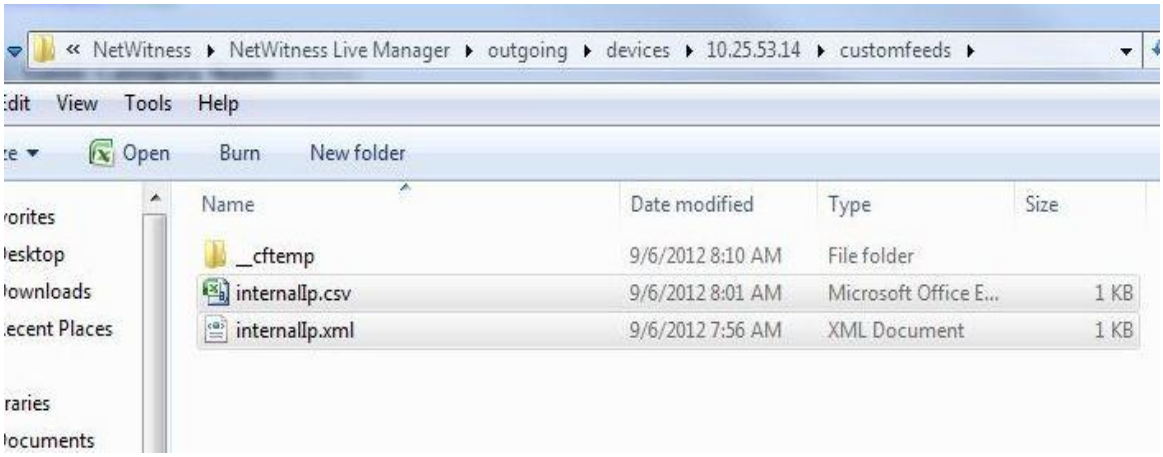
Creating and Deploying Custom Feeds Using Live Manager - Part II

In the following example we want to identify traffic entering our internal network from a external source and identify traffic leaving our internal network to an unknown destination.

First step we need to create an xml file that provides some structure for our decoders which we need and will be how the decoder labels and identifies our data. This requires both an xml file and a csv similar to what is shown below. The csv file is a essentially a feed that can easily updated and maintained as our network changes and grows overtime.

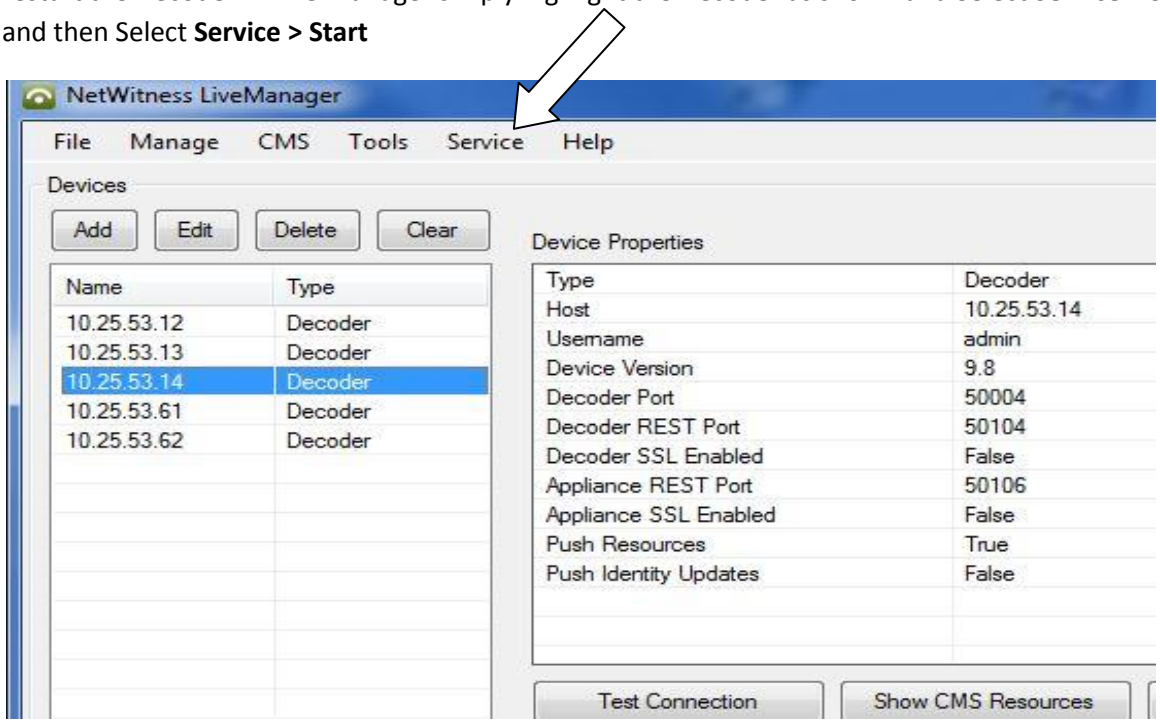


Copy both files to the customfeeds directory in Live Manager on the Analyists workstation located in C:\Program Files (86)\NetWitness\Netwitness Live Manager\outgoing\devices\<decoder's ip>\ customfeeds.



Restart the Decoder Service in Live Manager.

We need to restart the Decoder to generate the _feed file associated with our csv and xml files. To restart the Decoder in Live Manager simply highlight the Decoder as shown and Select **Service > Stop** and then Select **Service > Start**



Add the required lines in the index-concentrator.xml file on the Cencentrator. In this example we need to add two lines one for 'Internal IP Source' and another for 'Internal IP Destination'.

```
<key description="Internal IP Source" level="IndexValues" name="internalIp.src" format="Text" valueMax="10000" />
<key description="Internal IP Destination" level="IndexValues" name="internalIp.dst" format="Text" valueMax="10000" />
```

Restart the Concentrator Service

SSH to the Concentrator and restart the nwconcentrator service as shown below.

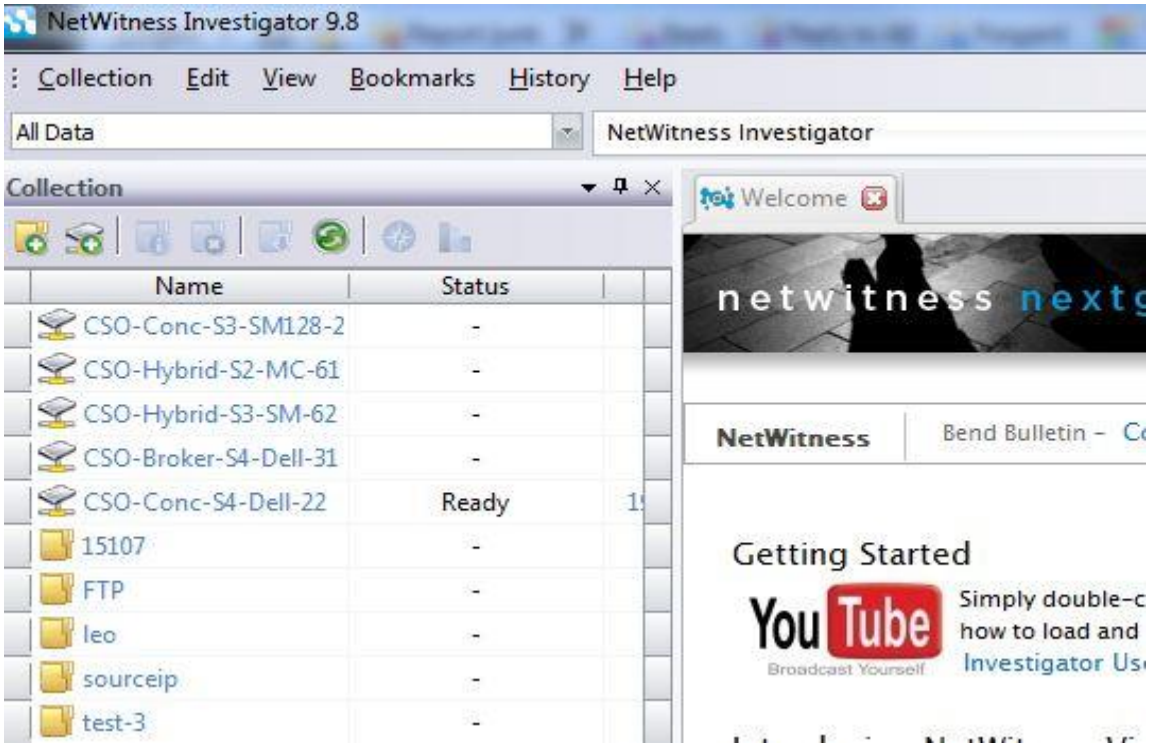
```
# monit restart nwconcentrator
```

Confirm it has restarted using the summary command.

```
# monit summary
        Process 'nwcrashreporter'       running
        Process 'nwconcentrator'        running
        Process 'nwappliance'           running
        System 'system_CSO-Conc-S4-Dell-22' running
```

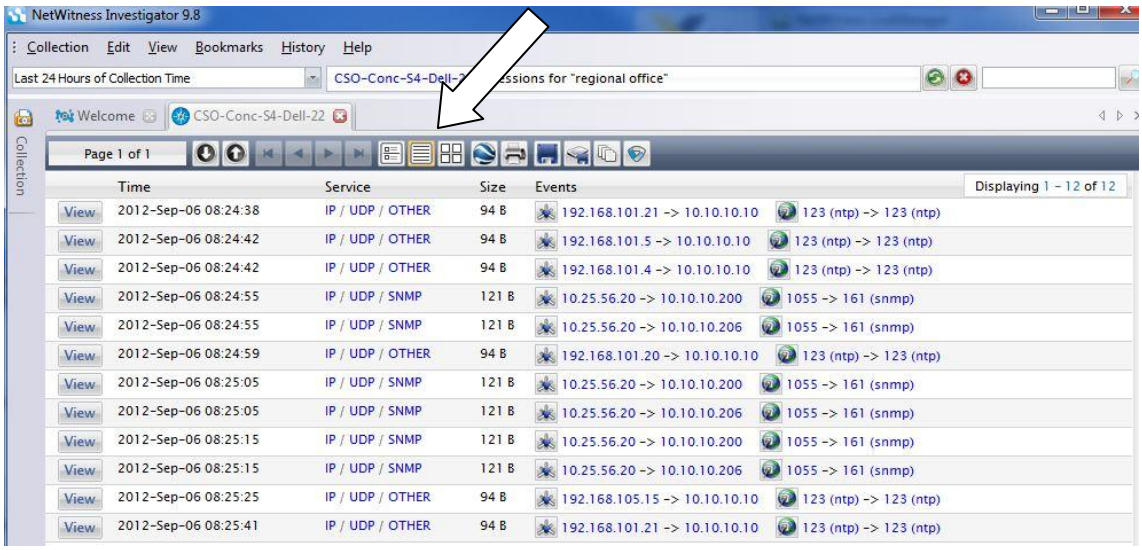
Viewing Results in Investigator

Open the Concentrator Collection in NW Investigator



Launch the collection by double clicking on it and view results listed in 'Internal IP Source' and Internal IP Destination'

Select Meta and view results. In this example we selected 'regional office (12)'. **Select Event View** to see the inbound IP connections listing the IP address on both sides of the connection.



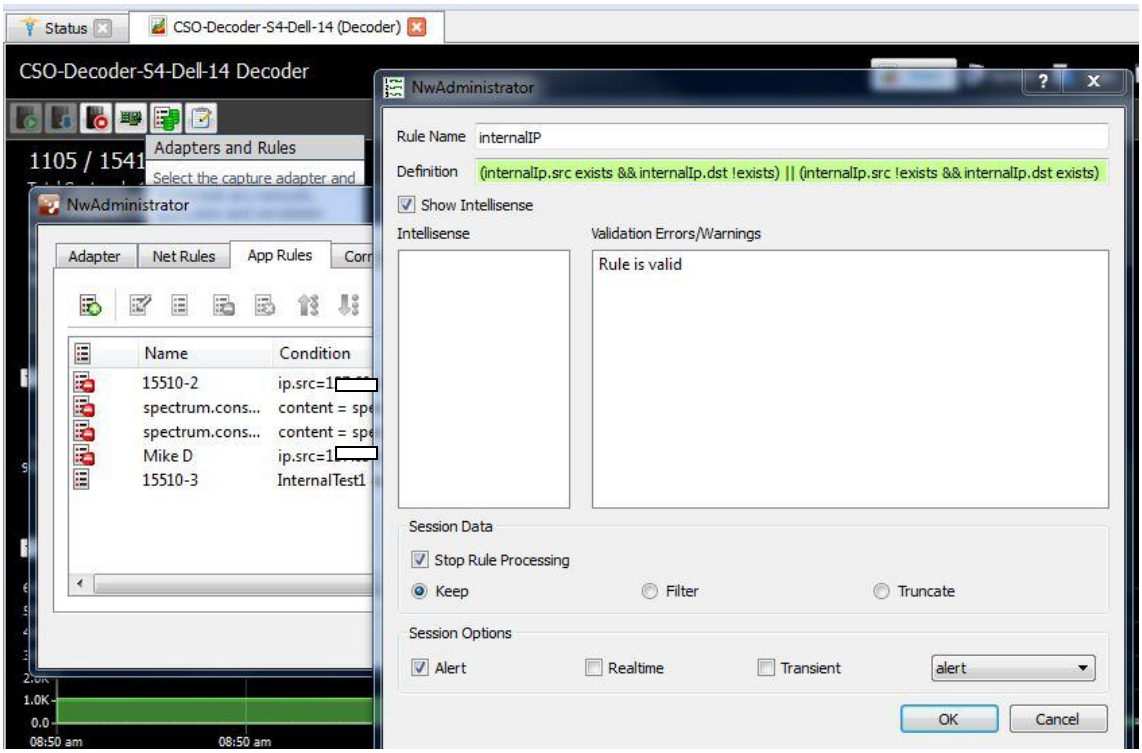
Create an Alert that filters the results

We want to view all traffic from or to any external IP address and see any communication attempts with an external IP. This can be accomplished in a filter or App Rule on the decoder.

Launch NwAdministrator and open **Stats View** on the Decoder

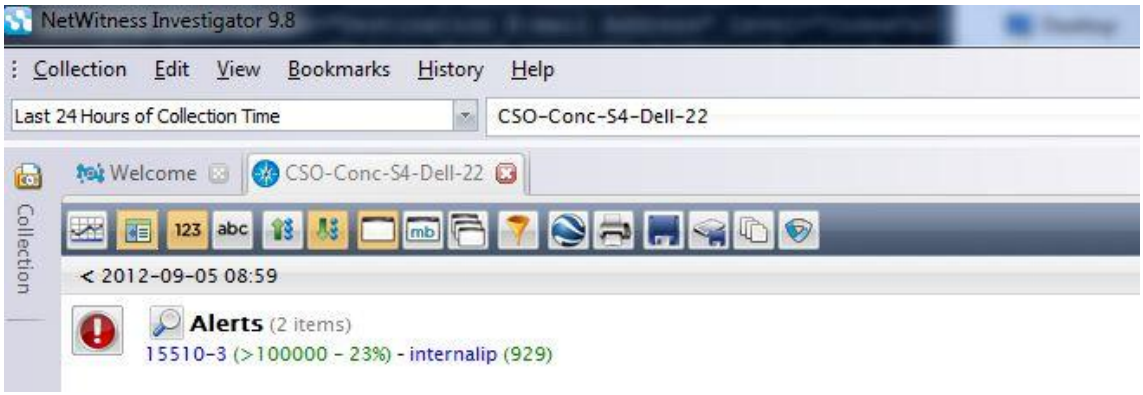
Select **Adapters and Rules** > App Rules Tab > Enter a Rule Name and Definition. In this example we used the following:

Rule Name: InternalIP
Definition: (internalIp.src exists && internalIp.dst !exists) || (internalIp.src !exists && internalIp.dst exists)
Session Options check the box 'Alert'
Select OK

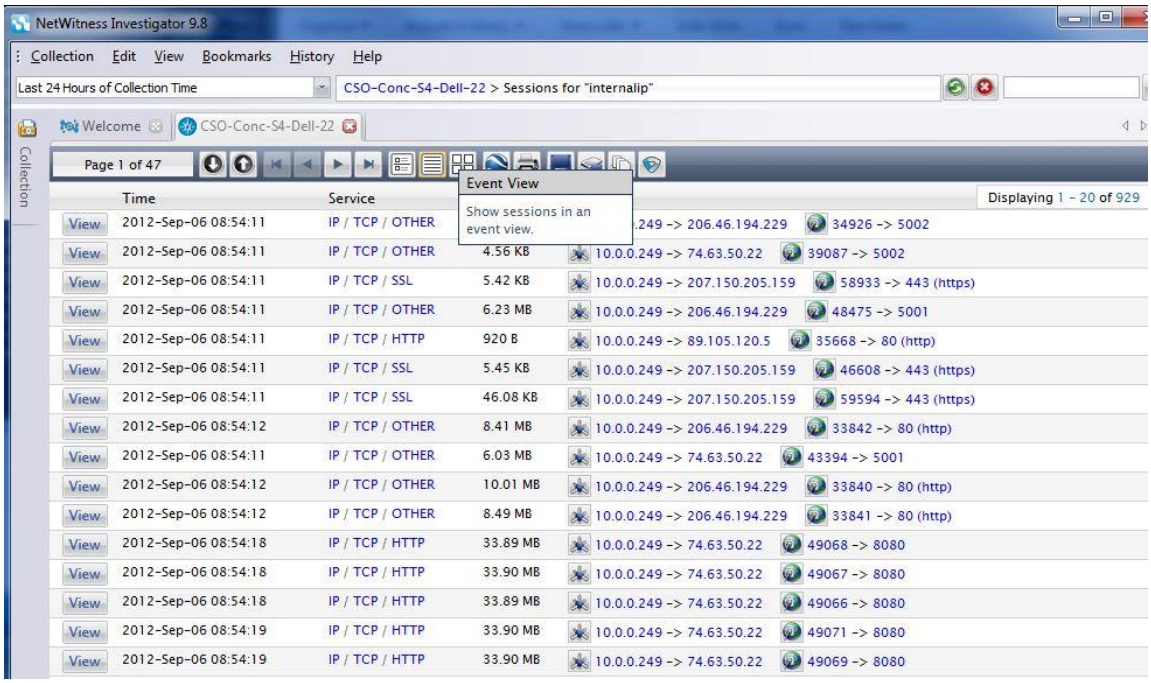


View the Filtered Results

Repeat the steps above in 'Viewing Results in Investigator' to view the results from the new rule. This time the results appear under the 'Alerts' section at the top of the collection titled 'Internalip' this time we see meta that applies to the rule listed in the Definition above.



Select 'InternalIp (929)' to view the meta generated by this rule.



The resulting Meta above are the connection attempts where one of the sides of the connection is not within the internal network as our filer was described. e.g. (internalIp.src exists && internalIp.dst !exists) || (internalIp.src !exists && internalIp.dst exists)