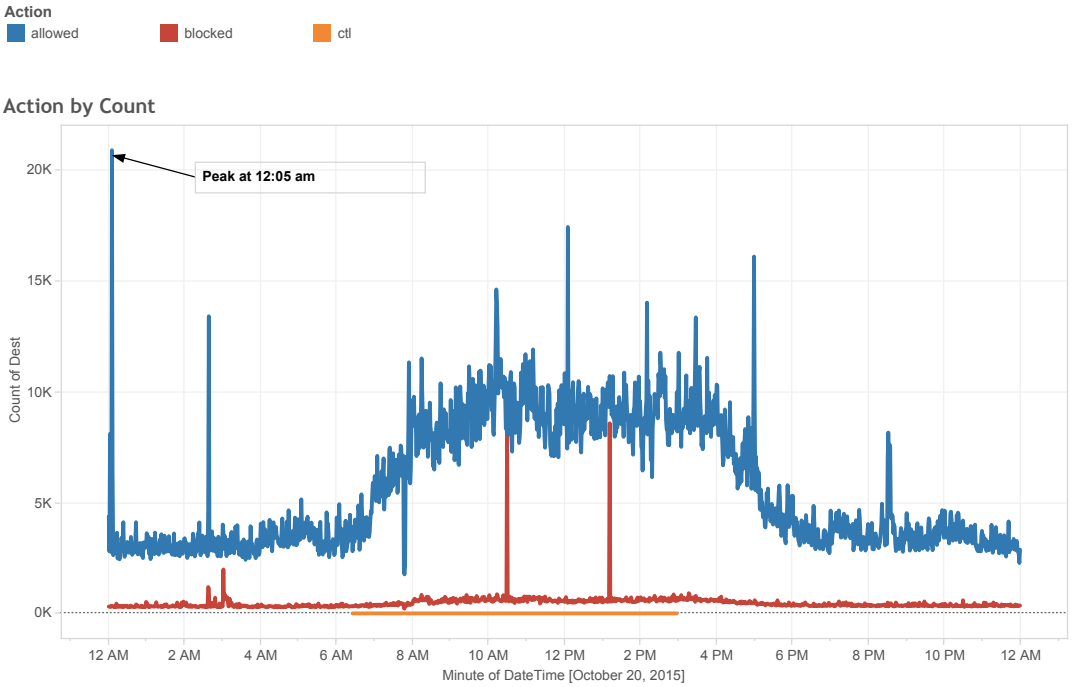
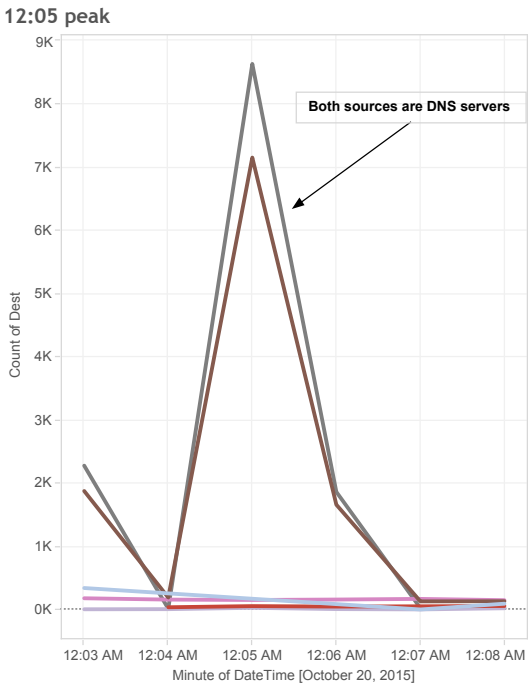
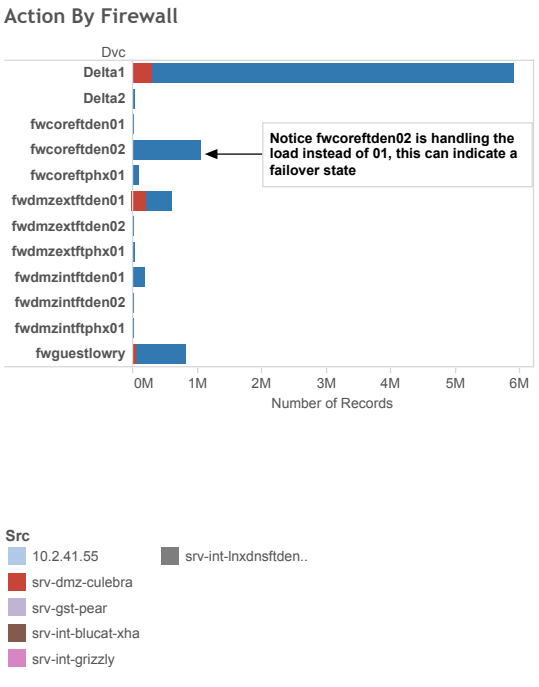
Firewall Activity 10/20/2015

Firewall activity for 10/20/2015 - 8,846,563 records. High number of allows around 12 am, otherwise follows buisiness hours. "Delta" firewall cluster sees the majority of the traffic.



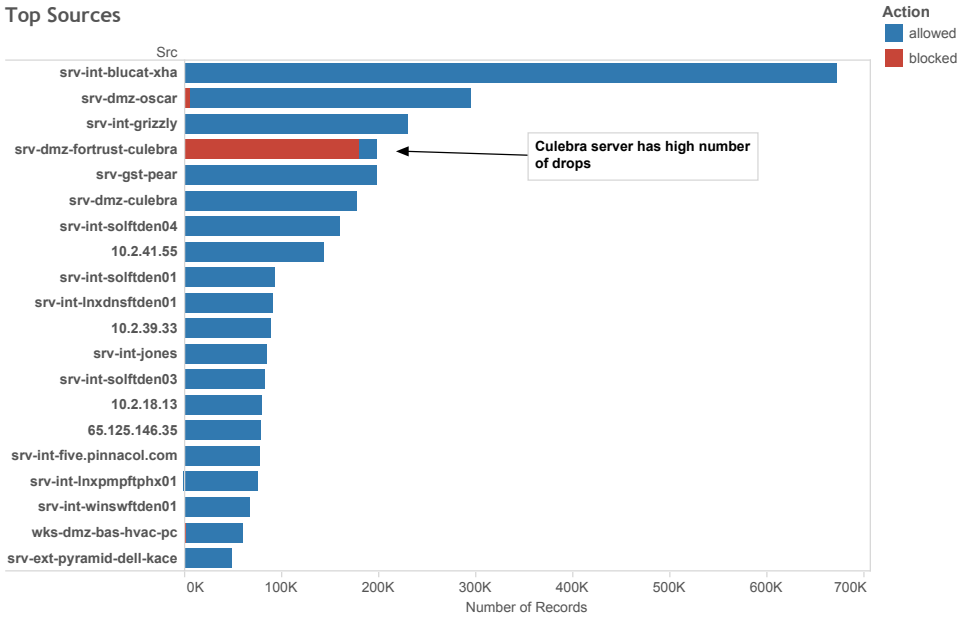




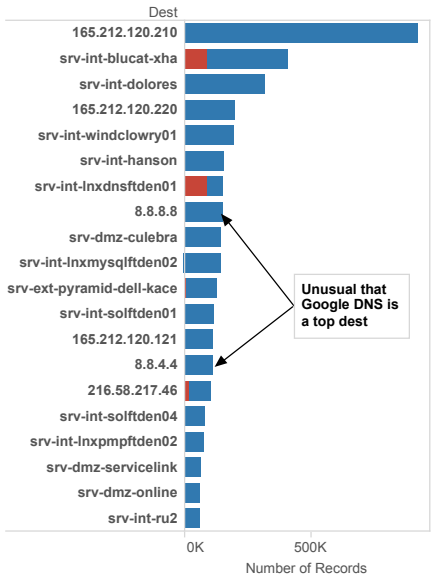
Firewall Activity 10/20/2015

Top sources are unsurprisingly servers with external web functions, top is a DNS server. However there is unusal activity going to Google DNS servers when we look at top destinations.

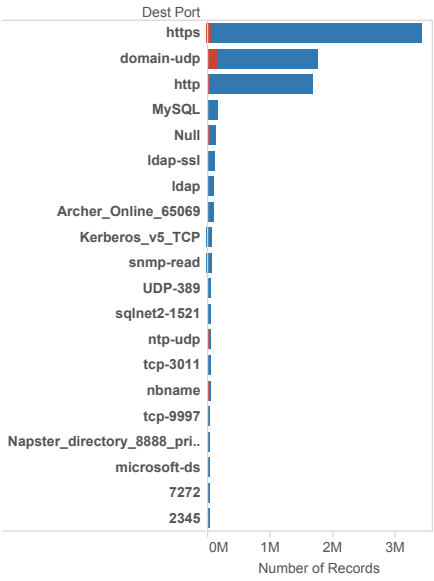
Top Sources



Top Destinations



Top Destination Ports

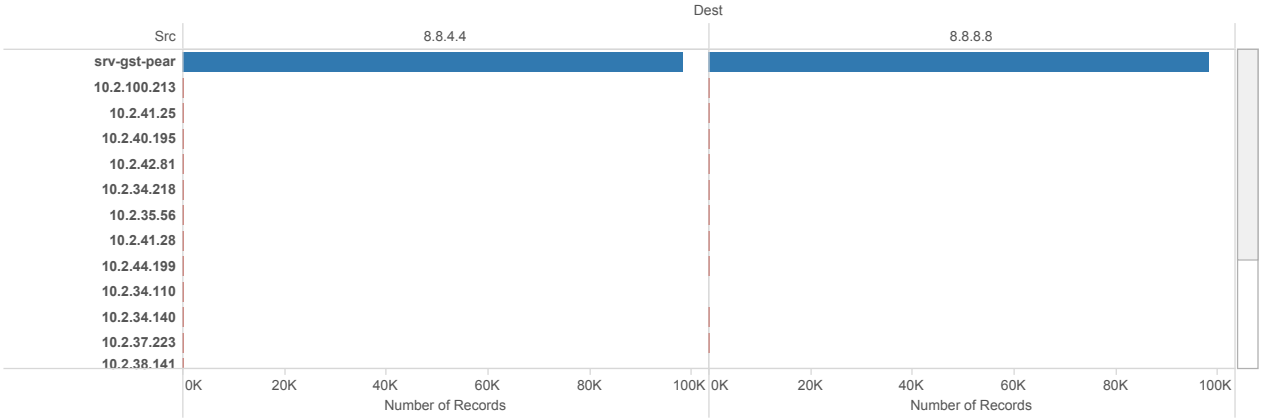


Firewall Activity 10/20/2015

Investigating Google DNS by first filtering out guest network connections show one server with the majority of the connections--srv-gst-pear--that is expected behaviour. Once that is filtered out we see a handful of suspect internal machines.

Action
allowed blocked

Google DNS No Guest Network



Google DNS No srv-gst-pear