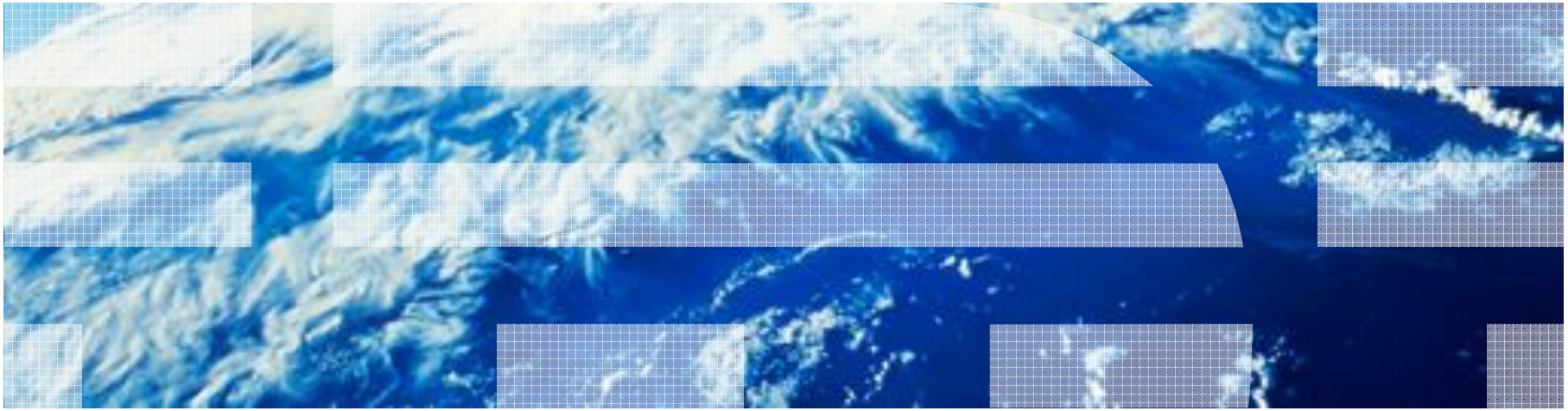
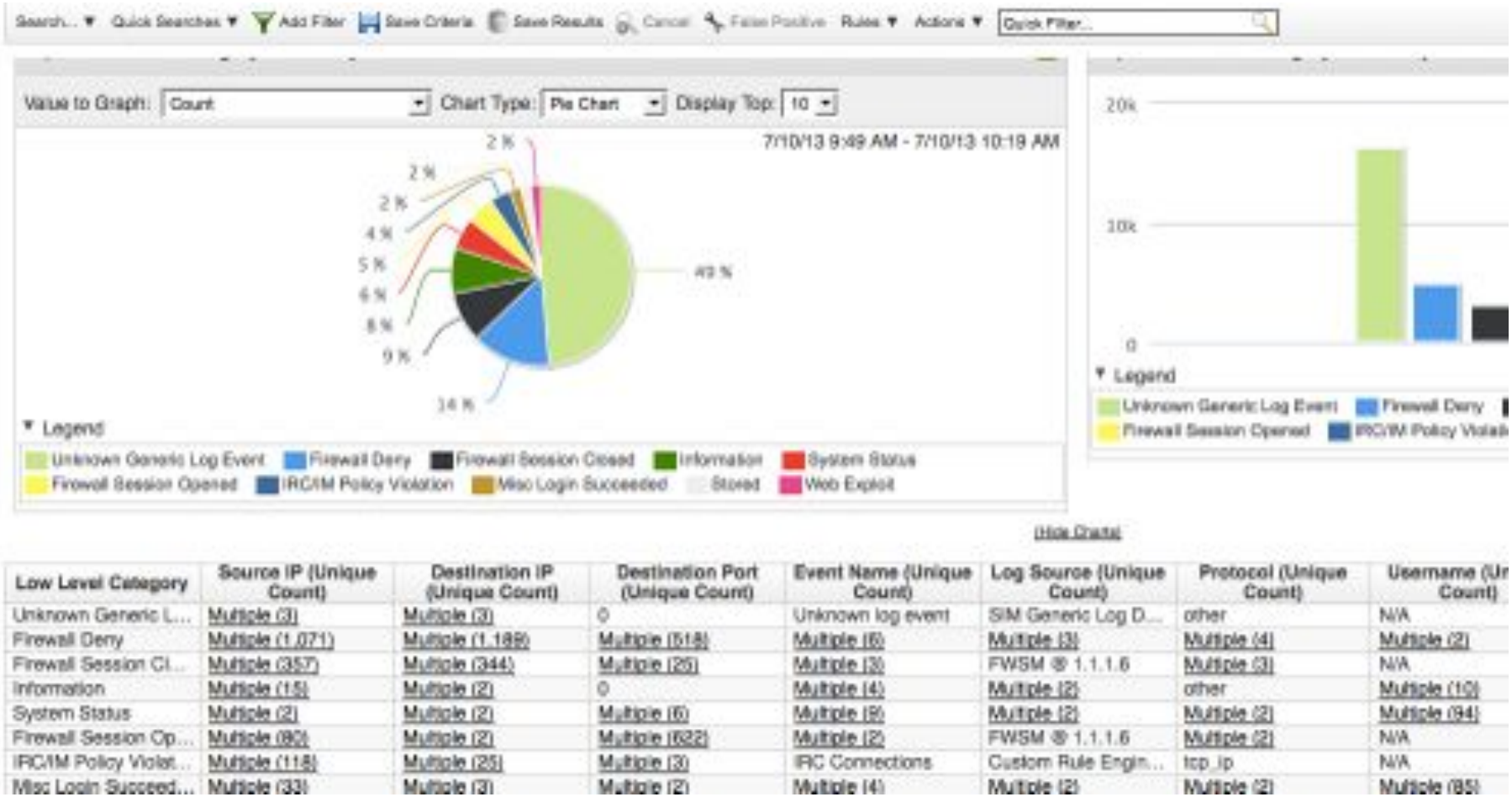
Ray Menard
2013-07-09

# All Things NBAD

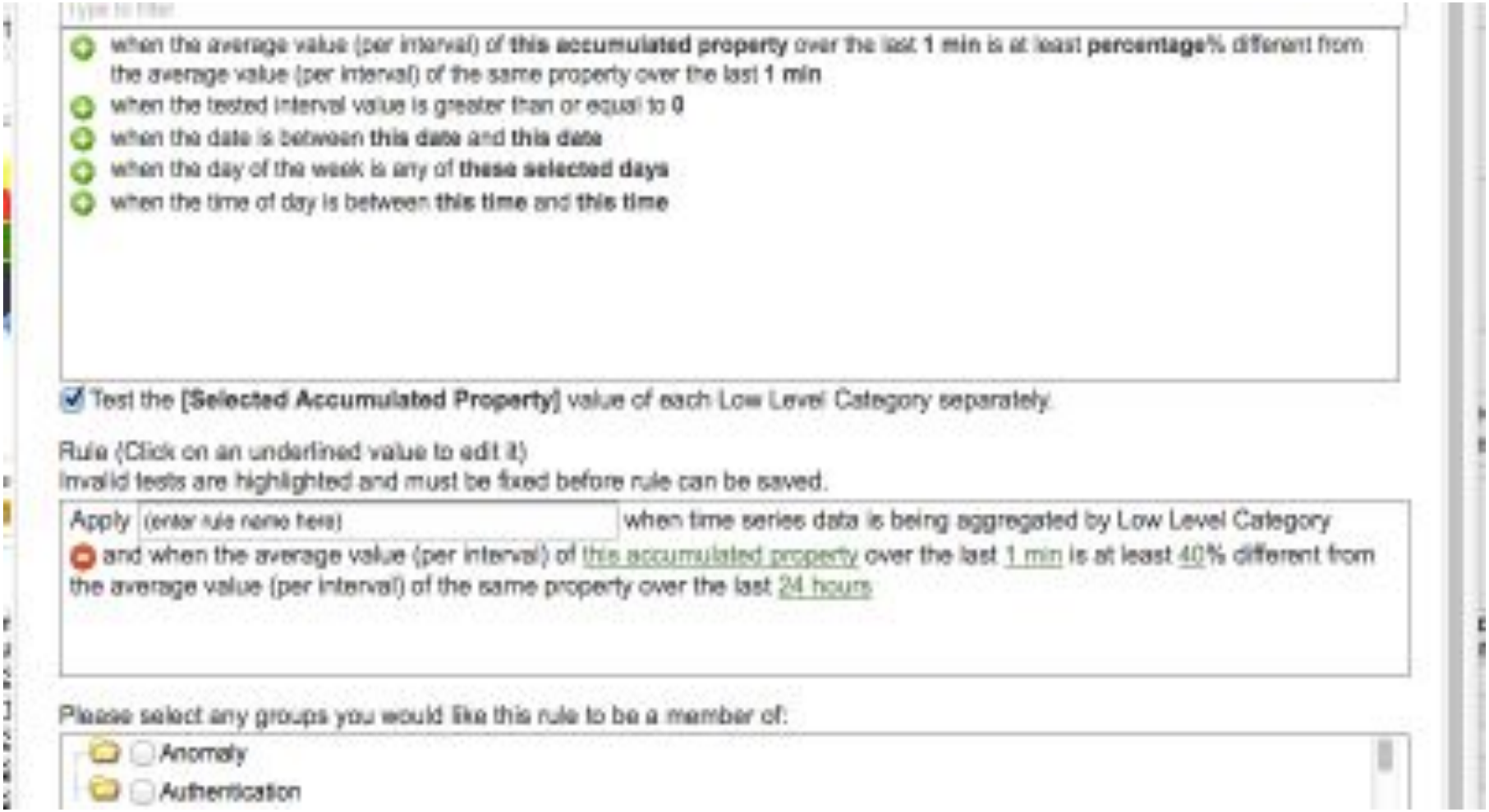


# Today

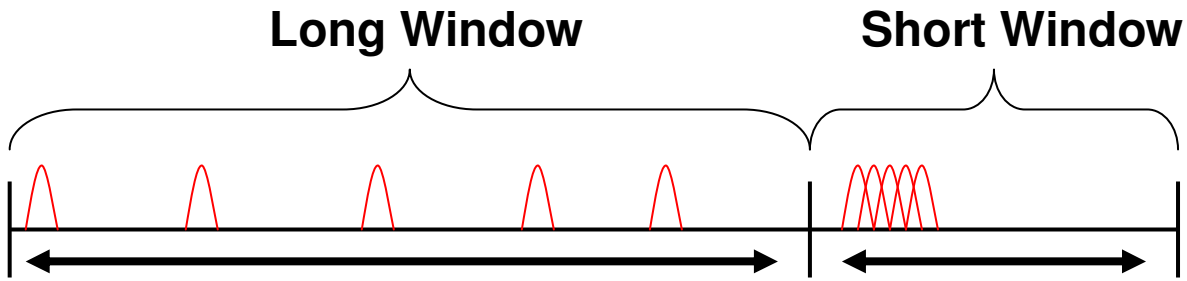



| Low Level Category | Source IP (Unique Count) | Destination IP (Unique Count) | Destination Port (Unique Count) | Event Name (Unique Count) | Log Source (Unique Count) | Protocol (Unique Count) | Username (Unique Count) |
|---|---|---|---|---|---|---|---|
| Unknown Generic L... | Multiple (3) | Multiple (3) | 0 | Unknown log event | SIM Generic Log D... | other | N/A |
| Firewall Deny | Multiple (1,071) | Multiple (1,186) | Multiple (518) | Multiple (6) | Multiple (3) | Multiple (4) | Multiple (2) |
| Firewall Session Cl... | Multiple (357) | Multiple (344) | Multiple (25) | Multiple (3) | FWSM @ 1.1.1.6 | Multiple (3) | N/A |
| Information | Multiple (15) | Multiple (2) | 0 | Multiple (4) | Multiple (2) | other | Multiple (10) |
| System Status | Multiple (2) | Multiple (2) | Multiple (6) | Multiple (8) | Multiple (2) | Multiple (2) | Multiple (94) |
| Firewall Session Op... | Multiple (80) | Multiple (2) | Multiple (622) | Multiple (2) | FWSM @ 1.1.1.6 | Multiple (2) | N/A |
| IRC/IM Policy Violat... | Multiple (118) | Multiple (25) | Multiple (3) | IRC Connections | Custom Rule Engin... | tcp_ip | N/A |
| Misc Login Succeed... | Multiple (33) | Multiple (3) | Multiple (2) | Multiple (4) | Multiple (2) | Multiple (2) | Multiple (85) |

# Anomaly Rule

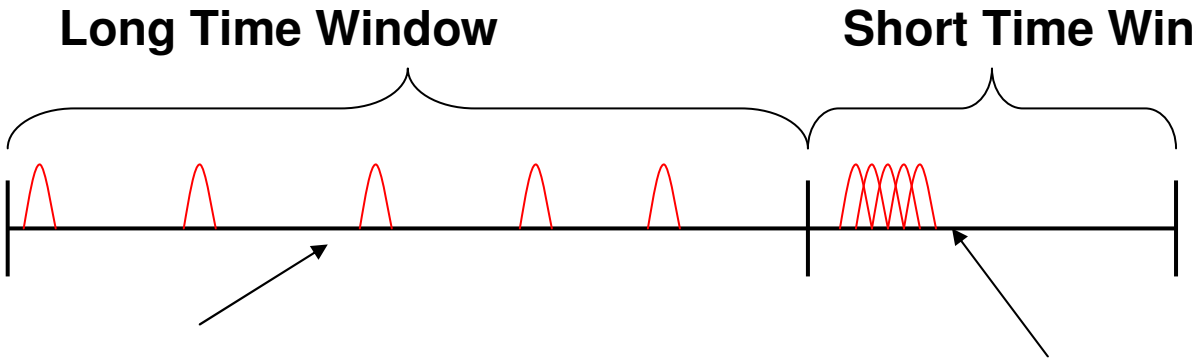


- Looks for obvious changes in traffic patters, very good at catching
  - Sudden increase in traffic/event rates
  - Sudden decreases in traffic
  - New Traffic that has never been seen
- Large Window (Long Window):
- Short Window:
- % of Change required to alert




100% increase in activity

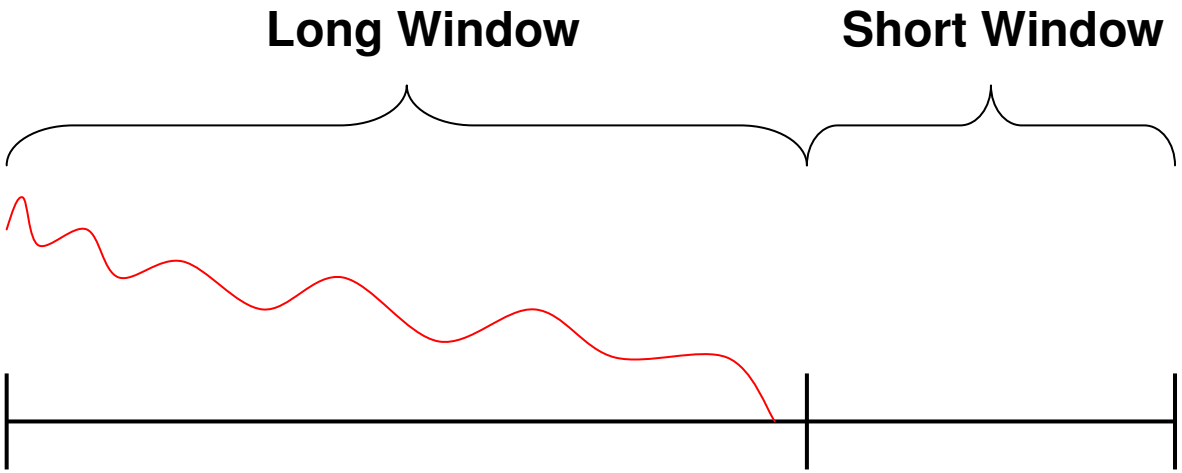
# Sudden Increase in Traffic Patterns




**Long Window: Defines Normal Behavior: Example: Over long window the cumulative average time SSH traffic is active is 2% of the time**

**Short Window: Comparison window average is compared against the long window average. In this case the short window shows 4% activity of SSH traffic. This 100% increase in volume triggers an event**

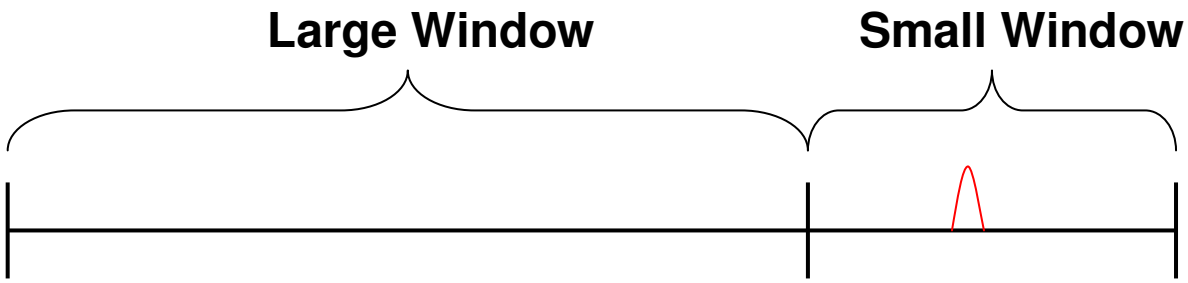
# Sudden Decrease in Traffic Patterns




**Type of Issues this could capture:**

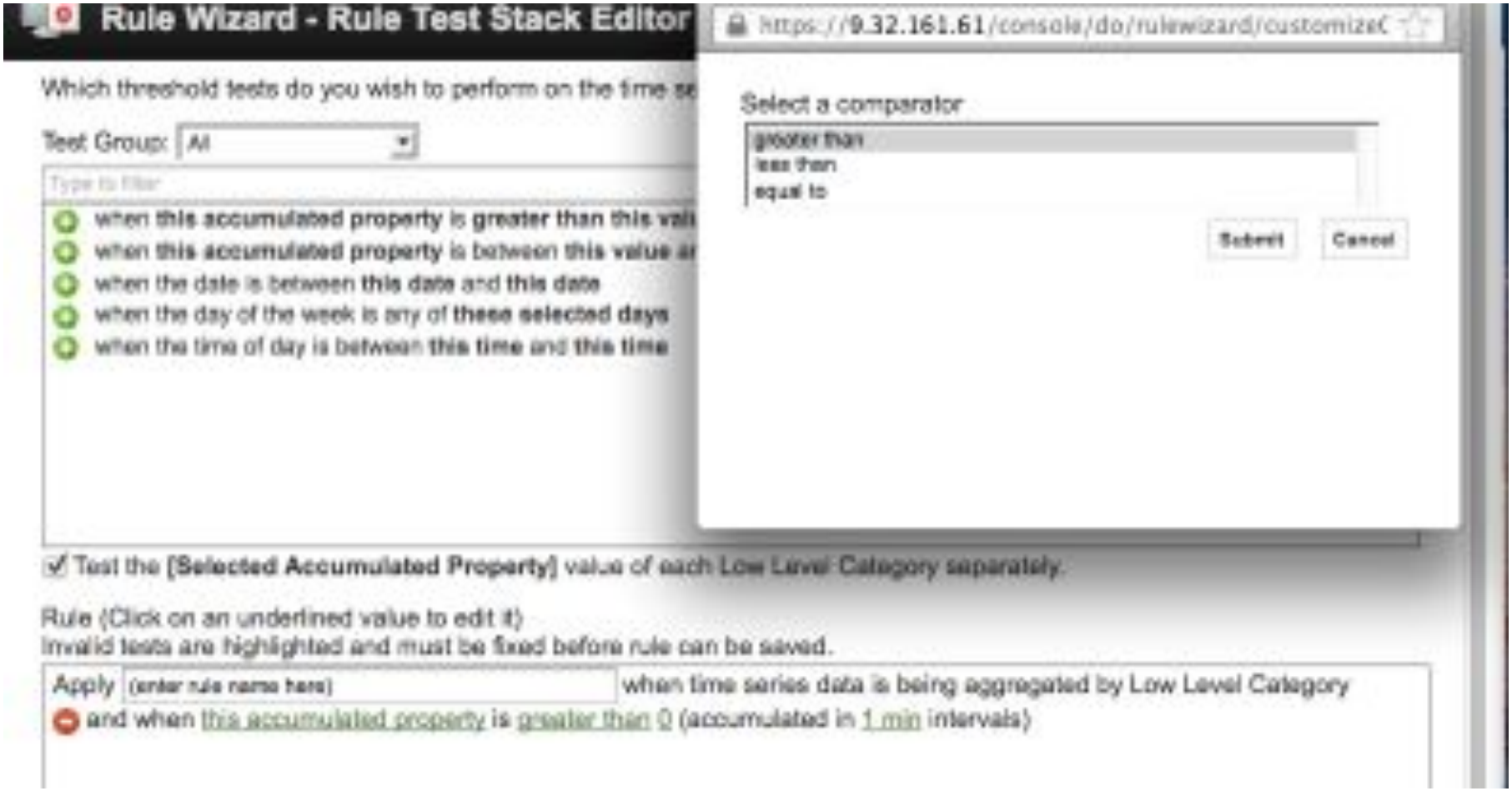
- **Service DoS (i.e. business application stops responding to requests)**
- **Hardware Failure on critical asset:  Web Server Died**

# New Traffic on the scene




**Type of Issues this could capture:**
- **New Service Installed on a server**
- **Rogue Server Deployed**

# Threshold



# Behavior

Exponential smoothing schemes weight past observations using exponentially decreasing weights This is a very popular scheme to produce a smoothed Time Series. Whereas in Single Moving Averages the past observations are weighted equally, Exponential Smoothing assigns exponentially decreasing weights as the observation get older.

In other words, recent observations are given relatively more weight in forecasting than the older observations.