Flow Forensics for Problem Identification

Flow Based Analytics

Know Your Network, Run Your Business
Introducing NetFlow Technology

<table>
<thead>
<tr>
<th>Item</th>
<th>Day</th>
<th>Date</th>
<th>Time</th>
<th>Number</th>
<th>Called</th>
<th>Call To</th>
<th>Min Code</th>
<th>Rate Pd</th>
<th>Feature</th>
<th>Airtime Charge</th>
<th>LD/Addl Charge</th>
<th>Total Charge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WED</td>
<td>02/17/2010</td>
<td>9:09AM</td>
<td>770-368</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>2 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>2</td>
<td>WED</td>
<td>02/17/2010</td>
<td>1:48PM</td>
<td>678-777</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>5 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>3</td>
<td>THU</td>
<td>02/18/2010</td>
<td>11:01AM</td>
<td>213-447</td>
<td>40000</td>
<td>LOSANGELE CA</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>4</td>
<td>THU</td>
<td>02/18/2010</td>
<td>3:45PM</td>
<td>404-519</td>
<td>40000</td>
<td>ATLANTA GA</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>5</td>
<td>THU</td>
<td>02/18/2010</td>
<td>6:39PM</td>
<td>678-777</td>
<td>40000</td>
<td>ATLANTA GA</td>
<td>2 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>6</td>
<td>THU</td>
<td>02/18/2010</td>
<td>6:53PM</td>
<td>678-777</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>4 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>7</td>
<td>THU</td>
<td>02/18/2010</td>
<td>8:39PM</td>
<td>678-777</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>6 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>8</td>
<td>FRI</td>
<td>02/19/2010</td>
<td>10:55AM</td>
<td>404-936</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>3 RM70</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>9</td>
<td>FRI</td>
<td>02/19/2010</td>
<td>11:37AM</td>
<td>678-777</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>10</td>
<td>FRI</td>
<td>02/19/2010</td>
<td>11:59AM</td>
<td>404-797</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>11</td>
<td>FRI</td>
<td>02/19/2010</td>
<td>3:01PM</td>
<td>678-777</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>2 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>12</td>
<td>TUE</td>
<td>02/23/2010</td>
<td>9:39PM</td>
<td>404-519</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>13</td>
<td>TUE</td>
<td>02/23/2010</td>
<td>9:50PM</td>
<td>404-519</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>1 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>14</td>
<td>WED</td>
<td>02/24/2010</td>
<td>9:04AM</td>
<td>770-368</td>
<td>40000</td>
<td>INCOMING CL</td>
<td>2 TESM</td>
<td>DT</td>
<td>M2MC</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

**Flow Table** - 880 records

- Client Host: 10.201.3.96
- Client Zone: Sales and Marketing
- Server Host: 72.21.202.71
- Server Zone: United States
- Service Summary: http (80/tcp)
- Average Rate: 4.64M

NetFlow Technology

Telephone Bill

Lancope Performance Monitoring and Security Solutions
## Flow-based Anomaly Detection

<table>
<thead>
<tr>
<th>Client Host</th>
<th>Server Host</th>
<th>Service Summary</th>
<th>Server Total Bytes</th>
<th>Client Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.214</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.212</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.216</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.208</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.213</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.209</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.206</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.211</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.185</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.113</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
<tr>
<td>222.36.40.139</td>
<td>209.182.176.112</td>
<td>vnc (5900/tcp)</td>
<td>0</td>
<td>96</td>
</tr>
</tbody>
</table>

**Anomalous Traffic Counts and Statistics**
Flow Data is about the footprint

It extends into areas of the network that we don’t generally deploy probes
Internal Visibility Through NetFlow
Deploy Flow Collection at a central location and enable NetFlow at each remote site...
“10G Ethernet is so fast few probe technologies can keep up and those that can are extremely expensive”
Questions and Contact

Chris Smithee
Network Security Manager
csmithee@lancope.com