Flow-Based Network Intelligence you can depend on.
Network Auditing Forensics and Security

Saving you time and money

• **Mitigation**
  – Total visibility of network traffic.
  – Forensics
  – Containment
  – Damage Assessment

• **Detection**
  – Alert when changes occur outside of learnt baselines and how new patterns can be recognized
Network Forensic analysis methods

• Packet Size Distribution Analysis
  – Analyze traffic patterns by standard deviation to identify what aspects have changed the most in a specific period. Can lead to early detection of issues. Identify Worms, increasing flows or data floods.

• Count Analysis
  – Count records as part of a result to quickly identify excessive flows or change. Enables quick identification of Port Scanners, P2P users, DDoS attacks or other multi threaded conversations. Identify long lasting flows or conversations
Network Forensic analysis methods

• Standard Deviation Analysis
  – Analyze traffic patterns by standard deviation to identify what aspects have changed the most in a specific period, Can lead to early detection of issues. Identify Worms, increasing flows or data floods.

• Bi-directional Analysis
  – Show forward and reverse conversations and In versus Out conversations to quickly identify which side of the conversation is responsible for traffic usage/flows.
Network Forensic analysis methods

• Cross-Section Analysis
  - Stacked graphs enable comparison of any two network traffic parameters. As an example, a stacked bar QoS analysis can graphically show the details of each application running within every class of service.

• Custom Group analysis
  - IP addresses can be categorized in logical groups for reporting, billing and capacity planning. Enhanced Application grouping coming soon.
Network Forensic analysis methods

• Percentile Analysis
  – Most commonly known for its benefit in Billing also has a large benefit for security and alerting. For example a burst may occur once or may occur in ever increasing frequency. A percentile analysis of a threshold event will provide an indication of change.

• QoS Analysis
  – QoS policies can help to reduce the effects of Dos and DDoS traffic floods and keep key applications available during attacks.
Network Forensic analysis methods

- **Drilldown Analysis**
  - Once an area of concern is identified drilldown into it for as much detail as required.

- **Baseline Analysis**
  - Perform Baselines over long term or real time for any element. Knowledge of baselines provides the intelligence to create alerts.
NetFlow Auditor freeform drilldown

Who needs short-term Network Analytics?
- Security Specialists
- Performance Managers
- VoIP Engineers

Who needs long-term Network Trending?
- Capacity Planners Architects
- Data Centre Managers
- Service Billing

Device/Interface, Business Group, Customer/User, AS, QoS

Applications

Conversations

Real-time

Time

Long Term

Last Minute, Last 15 Minutes, Last Hour, Last Day/Week/Month ....
Quickly find Servers such as P2P Servers
Or track conversations
Quickly find Servers such as P2P Servers
Or track conversations
Packet Size Distribution

The graph shows the distribution of packet sizes over time, specifically from August 03, 2009, 08:25 to 08:39. The x-axis represents the time periods, while the y-axis represents the number of packets. The data is categorized into different size ranges and shows variations in packet distribution over the selected time frame.
### IP Conversations Stacked. See Anomalies, Servers, P2P?

#### Title: Washington DC Secured Servers (MB Sum)

<table>
<thead>
<tr>
<th>No.</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>MB Sum</th>
<th>MB %</th>
<th>mbps Ave</th>
<th>K.Packets Sum</th>
<th>K.Flows Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>144.135.8.199</td>
<td>61.88.67.70</td>
<td>17.552</td>
<td>9.44%</td>
<td>0.164</td>
<td>12.342</td>
<td>1.222</td>
</tr>
<tr>
<td>2</td>
<td>84.95.240.228</td>
<td>61.88.67.70</td>
<td>11.984</td>
<td>6.45%</td>
<td>0.112</td>
<td>9.960</td>
<td>4.885</td>
</tr>
<tr>
<td>3</td>
<td>195.56.146.179</td>
<td>61.88.67.70</td>
<td>7.175</td>
<td>3.86%</td>
<td>0.067</td>
<td>5.031</td>
<td>1.540</td>
</tr>
<tr>
<td>4</td>
<td>6.7.232.214</td>
<td>61.88.67.70</td>
<td>6.642</td>
<td>3.57%</td>
<td>0.062</td>
<td>4.897</td>
<td>0.785</td>
</tr>
<tr>
<td>5</td>
<td>209.10.40.109</td>
<td>61.88.67.91</td>
<td>5.930</td>
<td>3.19%</td>
<td>0.055</td>
<td>4.157</td>
<td>0.872</td>
</tr>
<tr>
<td>6</td>
<td>209.9.146.17</td>
<td>61.88.67.70</td>
<td>5.800</td>
<td>3.12%</td>
<td>0.054</td>
<td>4.381</td>
<td>0.452</td>
</tr>
<tr>
<td>7</td>
<td>64.34.147.105</td>
<td>61.88.67.91</td>
<td>4.791</td>
<td>2.58%</td>
<td>0.045</td>
<td>4.899</td>
<td>0.904</td>
</tr>
<tr>
<td>8</td>
<td>64.74.221.203</td>
<td>61.88.67.91</td>
<td>4.624</td>
<td>2.49%</td>
<td>0.043</td>
<td>3.242</td>
<td>2.686</td>
</tr>
<tr>
<td>9</td>
<td>203.36.65.3</td>
<td>61.88.67.70</td>
<td>4.425</td>
<td>2.38%</td>
<td>0.041</td>
<td>3.317</td>
<td>0.499</td>
</tr>
<tr>
<td>10</td>
<td>64.74.221.233</td>
<td>61.88.67.70</td>
<td>4.271</td>
<td>2.30%</td>
<td>0.040</td>
<td>3.083</td>
<td>0.390</td>
</tr>
<tr>
<td>11</td>
<td>56.151.148.233</td>
<td>61.88.67.70</td>
<td>3.663</td>
<td>1.97%</td>
<td>0.034</td>
<td>2.564</td>
<td>0.267</td>
</tr>
<tr>
<td>12</td>
<td>209.10.146.45</td>
<td>61.88.67.70</td>
<td>3.542</td>
<td>1.90%</td>
<td>0.033</td>
<td>2.699</td>
<td>0.503</td>
</tr>
<tr>
<td>13</td>
<td>66.151.148.200</td>
<td>61.88.67.91</td>
<td>3.389</td>
<td>1.82%</td>
<td>0.032</td>
<td>2.374</td>
<td>0.871</td>
</tr>
</tbody>
</table>
For specific Servers see all talkers and applications.

NetFlow Auditor

Title: (MB Sum)

MB_Sum

Properties...

- Templates
- Devices
- Business Groups
- IP and Subnet
- Applications

QoS
- Baseline
- Measurement

Applications

<table>
<thead>
<tr>
<th>No.</th>
<th>Source Port</th>
<th>Source IP</th>
<th>MB Sum</th>
<th>Bits Sum</th>
<th>K.Flows Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>144.135.8.199</td>
<td>17.667</td>
<td>12.434</td>
<td>1.257</td>
</tr>
<tr>
<td>2</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>84.95.240.228</td>
<td>11.984</td>
<td>9.960</td>
<td>4.885</td>
</tr>
<tr>
<td>3</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>195.56.146.179</td>
<td>7.175</td>
<td>5.031</td>
<td>1.548</td>
</tr>
<tr>
<td>4</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>8.7.232.214</td>
<td>6.642</td>
<td>4.897</td>
<td>0.785</td>
</tr>
<tr>
<td>5</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>209.10.40.109</td>
<td>5.930</td>
<td>4.157</td>
<td>0.872</td>
</tr>
<tr>
<td>6</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>209.0.146.17</td>
<td>5.800</td>
<td>4.381</td>
<td>0.452</td>
</tr>
<tr>
<td>7</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>64.34.147.105</td>
<td>4.791</td>
<td>4.699</td>
<td>0.904</td>
</tr>
<tr>
<td>8</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>64.74.221.203</td>
<td>4.634</td>
<td>3.253</td>
<td>2.691</td>
</tr>
<tr>
<td>9</td>
<td>(80) <a href="http://www/http">http://www/http</a></td>
<td>203.36.59.3</td>
<td>4.427</td>
<td>3.329</td>
<td>0.503</td>
</tr>
</tbody>
</table>
Flow-Based Network Intelligence you can depend on
## NetFlow Auditor Smart Investment

Grows as your needs grow

<table>
<thead>
<tr>
<th>Performance</th>
<th>Professional</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anomaly Detection</strong></td>
<td><strong>Add-on</strong></td>
<td><strong>Scalable Flow Capture</strong></td>
</tr>
<tr>
<td>For very high-flow capture</td>
<td>• Learns Baseline and Alerts when traffic deviates on link, servers, services P2P profiling, DDoS, ICMP, DNS, QoS, Nefarious Traffic.</td>
<td>• Coupled with Professional 100% Full Flows for full compliance and billing • Coupled with Performance Supports very high-flow environment for real-time root cause analysis</td>
</tr>
<tr>
<td><strong>Security / Compliance</strong></td>
<td><strong>Forensics</strong></td>
<td><strong>Comparative Baselining</strong></td>
</tr>
<tr>
<td>QoS</td>
<td>95(^{th}) Percentile Billing</td>
<td>• 100% Full Flow forensics, Supports Detailed Anomaly Detection and 95(^{th}) Percentile or usage based Billing. • Comprehensive Network Behavior Anomaly Detection from intelligently learnt baselines.</td>
</tr>
<tr>
<td><strong>Root Cause Analysis</strong></td>
<td><strong>QoS Billing</strong></td>
<td><strong>Troubleshooting</strong></td>
</tr>
<tr>
<td>QoS Billing</td>
<td>• Top Traffic. • Supports Anomaly Detection on top traffic. • Couple with Enterprise for high-flow eg ISPs</td>
<td><strong>QoS</strong></td>
</tr>
<tr>
<td><strong>Bandwidth Utilization</strong></td>
<td><strong>Add-on</strong></td>
<td><strong>Lite</strong></td>
</tr>
<tr>
<td>• Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright 2009 IdeaData Pty Ltd
NetFlow Auditor Unique Capabilities

- Comparative Baselining
- Real-Time Forensic Analysis
- Network Behavior Anomaly Detection option
- Long-Term trending
- Event alerting by Time of day and thresholds
- Highly flexible exceed and degrade threshold capability
- Learn traffic baselines
- Collection Tuning

- Unattended Alerting and Reporting
- Flexible Filters
  - Root Cause Analysis
  - Security Forensics
  - Performance Analysis
  - Data Center Analysis
- Multi-device Correlation and De-duplication
- 95th Percentile
- Scalability in collection
- Self Healing

Scalability, Granularity, Flexibility