Flow-Based Network Intelligence you can depend on.

Network Behavior Anomaly Detection

The longer it learns, the smarter it becomes
NetFlow Auditor is Part of a Threat Detection Mitigation Plan

- Forensics coupled with add-on Anomaly Detection
- Identify Nefarious Traffic, DDoS, SlowDoS
- It leverages existing infrastructure
- Rapid Deployment
- Flexible, Scalable and Granular
- Enterprise, Telco and Defense Sensitivity
Anomaly Detection – Preset Detection Rules

### NetFlow Auditor

#### Long Term

#### Real Time

#### My Analytics

- Customised Reports
- Templates
- Schedule Status
- Report Administration
- Alert Administration
- Anomaly Detection
- Anomaly Alert
- Baseline Build
- Custom Filter

#### My Alerts

<table>
<thead>
<tr>
<th>Duration</th>
<th>ID 1</th>
<th>ID 2</th>
<th>ID 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 min</td>
<td>38</td>
<td>53</td>
<td>196</td>
</tr>
<tr>
<td>1 hrs</td>
<td>209</td>
<td>247</td>
<td>960</td>
</tr>
<tr>
<td>6 hrs</td>
<td>1053</td>
<td>1899</td>
<td>5544</td>
</tr>
<tr>
<td>24 hrs</td>
<td>1893</td>
<td>3523</td>
<td>9116</td>
</tr>
</tbody>
</table>

#### Configuration

- Management Devices
- Business Groups
- Applications
- QoS
- Administrator

#### Table Data

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Protocol</th>
<th>IP Address/Domain</th>
<th>Port</th>
<th>Search</th>
<th>Protocol</th>
<th>IP Address/Domain</th>
<th>Port</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>3003</td>
<td>Dissemination - Destination</td>
<td>Standard Alert</td>
<td>Spamming</td>
<td>Administrator</td>
<td>Active</td>
<td>10</td>
<td>62</td>
<td>294</td>
</tr>
<tr>
<td>3600</td>
<td>P2P Monitoring</td>
<td>Anomaly Detection</td>
<td>Nefarious</td>
<td>Administrator</td>
<td>Active</td>
<td>-</td>
<td>3</td>
<td>106</td>
</tr>
<tr>
<td>3640</td>
<td>IP Talkers Variations</td>
<td>Anomaly Detection</td>
<td>IPGroup</td>
<td>Administrator</td>
<td>Active</td>
<td>-</td>
<td>-</td>
<td>323</td>
</tr>
<tr>
<td>3660</td>
<td>UDP Monitoring</td>
<td>Anomaly Detection</td>
<td>Application</td>
<td>Administrator</td>
<td>Active</td>
<td>-</td>
<td>-</td>
<td>120</td>
</tr>
<tr>
<td>3560</td>
<td>ICMP Ports Unreachable</td>
<td>Anomaly Detection</td>
<td>ICMP</td>
<td>Administrator</td>
<td>Active</td>
<td>55</td>
<td>224</td>
<td>1241</td>
</tr>
</tbody>
</table>

### Graph

- bps vs Time (04-11-20 22:00 to 04-11-20 22:30)
### Anomaly Detection

#### Alert Detection

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Category</th>
<th>Measure</th>
<th>Owner</th>
<th>Status</th>
<th>15 min</th>
<th>1 hrs</th>
<th>6 hrs</th>
<th>24 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Baseline and Alert</td>
<td>Anomaly Alert</td>
<td>Device</td>
<td>Flows</td>
<td>Administrator</td>
<td>Active</td>
<td>94</td>
<td>134</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port - Lower</td>
<td>Anomaly Alert</td>
<td>Device</td>
<td>Flows</td>
<td>Administrator</td>
<td>Active</td>
<td></td>
<td></td>
<td>21</td>
<td>79</td>
</tr>
</tbody>
</table>

Criteria:
- Device: `Border2.com`
- Display by: `Count`
- Bidirectional: checked
- Reverse Criteria: unchecked
- Flow De-duplication: unchecked
- Based on: Ingress

### My Alerts

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>Count</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 min</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1 hrs</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>6 hrs</td>
<td>121</td>
<td>407</td>
</tr>
<tr>
<td>24 hrs</td>
<td>364</td>
<td>1711</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Category</th>
<th>Measure</th>
<th>Owner</th>
<th>Status</th>
<th>15 min</th>
<th>1 hrs</th>
<th>6 hrs</th>
<th>24 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Flows baseline Alert</td>
<td>Anomaly Alert</td>
<td>Device</td>
<td>Flows</td>
<td>Administrator</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anomaly Detection – P2P

Show hide Count to see the multiple often compounding causes of Anomaly Detection
Anomaly Detection – Make your own rules
3 Easy steps to monitor anything - Steps 1 & 2

(1) Click the element you want NetFlow Auditor to learn a Baseline

(2) Click Anomaly Detection
Anomaly Detection – Make your own rules
3 Easy steps to watch anything - Steps 3

(3) Simply save default definition or fine tune using filter and configure.
Anomaly Detection
Intelligent Baseline Learning
## Standard Alerting

### My Analytics
- **Customised Reports**
  - Templates
  - Schedule Status
  - Report Administration
- **Alert Administration**
  - Standard Alert
  - Category
  - Trap
- **Anomaly Detection**
  - Anomaly Alert
  - Baseline Build
  - Custom Filter

### My Alerts
- **15 min**: 0, 1, 9
- **1 hr**: 1, 10, 78
- **6 hrs**: 121, 151, 607
- **24 hrs**: 364, 417, 1711

### Table
<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Category</th>
<th>Measure</th>
<th>Owner</th>
<th>Status</th>
<th>15 min</th>
<th>1 hr</th>
<th>6 hrs</th>
<th>24 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP - Source Heavy Traffic</td>
<td>Standard Alert</td>
<td>Device</td>
<td>Utilization</td>
<td>Administrator</td>
<td>Active</td>
<td>-</td>
<td>-</td>
<td>11</td>
<td>52</td>
</tr>
<tr>
<td>Interface Inbound Traffic</td>
<td>Standard Alert</td>
<td>Device</td>
<td>Utilization</td>
<td>Administrator</td>
<td>Active</td>
<td>2</td>
<td>3</td>
<td>38</td>
<td>285</td>
</tr>
<tr>
<td>Protocol</td>
<td>Standard Alert</td>
<td>Device</td>
<td>Utilization</td>
<td>Administrator</td>
<td>Active</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>90</td>
</tr>
</tbody>
</table>

### Criteria
- **Device**: Border2.broadriver.com
- **Source Interface**: 
- **Flow De-duplication**: Based on Ingress

### Standard Alert Criteria
- **bps**:
  - > 2,000,000 Information: 2134, 2009-10-08 07:31
  - > 4,000,000 Warning: 610, 2009-10-08 04:19
  - > 6,000,000 Critical: 231, 2009-10-08 03:12
- **bps_Utilization**:
  - > 1% Information: 164, 2009-10-07 20:08
  - > 2% Warning: 29, 2009-10-07 17:15
  - > 5% Critical: 0, 2009-10-07 16:00
Standard Alerting – Heavy Traffic Analysis
Denial of Service Attack (D/DoS) Tactics

- Most attacks involve packet flooding
- Saturate the system with external requests
- Force a reset/reboot
- Consume so many resources the system is unable to respond
What is a Denial of Service Attack?

- An attempt to deny legitimate right to a computing resource
- Typical targets: Web services, Email, Network Infrastructure
- Intent: Overload the recipient system so it can no longer correctly function or respond to normal traffic
- Attacks range from simple e-vandalism to attempted felony theft and cyber-terrorism
- From a single source or widely distributed (DDoS)
- Slow Dos
Flow-Based Network Intelligence you can depend on
NetFlow Auditor Smart Investment
Grows as your needs grow

- **Anomaly Detection Add-on**
  - Learns Baseline and Alerts when traffic deviates on link, servers, services P2P profiling, DDoS, ICMP, DNS, QoS, Nefarious Traffic.

- **Scalable Flow Capture**
  - For very high-flow capture
  - 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

- **Security / Compliance**
  - Forensics
  - Comparative Baselining
  - QoS
  - 95th Percentile Billing
  - 100% Full Flow forensics, Supports Detailed Anomaly Detection and 95th Percentile or usage based Billing.
  - Comprehensive Network Behavior Anomaly Detection from intelligently learnt baselines.

- **Root Cause Analysis**
  - QoS Billing
  - Top Traffic.
  - Supports Anomaly Detection on top traffic.
  - Couple with Enterprise for high-flow eg ISPs

- **Troubleshooting**
  - QoS Billing
  - Hot Top Traffic.

- **Bandwidth Utilization**
  - Interface

---

Copyright 2009 IdeaData Pty Ltd

NetFlow Auditor
Powered by Digitoll®
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