FlowMon – Your Network Under Control!

B2B Workshop of ICT Companies, Tuesday, October 18, 2016

Hung Nguyen
Key Account Manager Benelux
Hung.Nguyen@Flowmon.com
Company Overview

• International vendor devoted to innovative network traffic & performance & security monitoring

• Company facts
  ▪ Founded in 2007, 50+ employees
  ▪ Headquarters Brno, Czech Republic
  ▪ Strong R&D background

• Achievements
  ▪ Gartner recognized since 2010
  ▪ Deloitte CE Technology Fast 50
  ▪ Partnerships: Cisco, Check Point
  ▪ 500+ customers worldwide
Flowmon Use Cases

2008
- Network visibility, reporting & troubleshooting
  - Flowmon Probe & Flowmon Collector

2009
- Network Behavior Analysis & Anomaly Detection
  - Flowmon ADS

2014
- Application Performance Monitoring
  - Flowmon APM

2014
- Full Packet Capture
  - Flowmon Traffic Recorder

2015
- DDoS Protection
  - Flowmon DDoS Defender
What is Flow Data?

- Modern method for network monitoring – flow measurement
- Cisco standard **NetFlow v5/v9**, IETF standard **IPFIX**
- Focused on **L3/L4** information and volumetric parameters
- Real network traffic to flow statistics reduction ratio **500:1**
Flowmon Components

- **Flowmon Probes**
  - Passive source of NetFlow/IPFIX data

- **Flowmon Collectors**
  - Flow collection, reporting, analysis

- **Flowmon modules (plugins)**
  - ADS, APM, FTR, DDoS, DR
Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time.

Recommendations

- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier.
Infected Corporate Networks

Prevention is not enough. You have to redefine your security strategy and incorporate tools to support post-breach phase by early detection and remediation.

CHECK POINT SECURITY REPORT 2014

73% of organizations had at least one bot detected, compared with 63% in 2012.

In 2013 88% of organizations experienced at least one potential data loss incident.
• Signature-less technology

  ▪ Advanced methods of artificial intelligence
    □ Bidirectional flows (client/server identification)
    □ Changes of network behavior in time
    □ Machine learning methods and heuristics
    □ Decision trees for monitoring of low & slow attacks
    □ Algorithms for finding clusters and outliers
Flowmon ADS Principles

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases
FlowMon Family Overview

FlowMon Solution

- Flow Monitoring
- Network Security Monitoring
- On Demand Packet Capture
- Network/Application Performance
- DDoS Protection

© INVEA-TECH 2015
User Interface
FlowMon Dashboard (FMD)

• Combines widgets from different modules (plug-ins)
Monitoring Center (FMC)

- Application for NetFlow data storage and visualization
- Graphs, tables and form for further data processing
- Top N statistics (users, sites, services)
- Predefined set of profiles (views) for standard protocols
- User defined profiles (based on IP address or ports)
- Alerts, thresholds
Monitoring Center (FMC)

- Intelligent reporting tool, exports to pdf, csv

- Monitoring of HTTP traffic – analysis & detection

<table>
<thead>
<tr>
<th>Počáteční čas</th>
<th>Protokol</th>
<th>Zdrojová IP adresa</th>
<th>Cílový port</th>
<th>HTTP hostname</th>
<th>HTTP URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-05-29 08:58:47.009</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>api.play.cz</td>
<td>/static/radio_logo/t90/cernahor</td>
</tr>
<tr>
<td>2013-05-29 08:58:52.164</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>0-act.channel.facebook.com</td>
<td>/pull?channel=p_100000382471604</td>
</tr>
<tr>
<td>2013-05-29 08:58:47.009</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>api.play.cz</td>
<td>/jsonp/getFeed/playcz?callback=</td>
</tr>
<tr>
<td>2013-05-29 08:59:02.483</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>tools.google.com</td>
<td>/service/update2?w=6;gEkzSS7Gjf</td>
</tr>
<tr>
<td>2013-05-29 08:58:54.258</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>ocsp.startssl.com</td>
<td>/sub/class2/server/ca</td>
</tr>
<tr>
<td>2013-05-29 08:59:02.488</td>
<td>TCP</td>
<td>192.168.3.179</td>
<td>http</td>
<td>tools.google.com</td>
<td>/service/update2?w=6;LLZJqhBNLr</td>
</tr>
</tbody>
</table>
• Application recognition
  NBAR2 support

• Geolocation
  - Automatically available in FMC and ADS
  - IP address location shown by flag
  - Integrated database – geolocation is available also offline

<table>
<thead>
<tr>
<th>Start Time - first seen</th>
<th>Duration</th>
<th>Protocol</th>
<th>Source IP address</th>
<th>Source Port</th>
<th>Destination IP address</th>
<th>Destination Port</th>
<th>TCP Flags</th>
<th>IOS</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-02-11 12:28:04.699</td>
<td>30.757</td>
<td>TCP</td>
<td>74.201.154.191</td>
<td>https</td>
<td>grevislon.customer.org</td>
<td>64702</td>
<td>.AR, SF</td>
<td>0</td>
<td>16</td>
<td>1582</td>
<td>1</td>
</tr>
<tr>
<td>2013-02-11 12:28:39.400</td>
<td>0.071</td>
<td>TCP</td>
<td>email.soznam.cz</td>
<td>https</td>
<td>hull.customer.org</td>
<td>11765</td>
<td>.AR, SF</td>
<td>0</td>
<td>20</td>
<td>11654</td>
<td>1</td>
</tr>
<tr>
<td>2013-02-11 12:28:12.734</td>
<td>30.123</td>
<td>TCP</td>
<td>knudsvig.customer.org</td>
<td>64939</td>
<td>173.194.35.83</td>
<td>https</td>
<td>.AR...</td>
<td>0</td>
<td>12</td>
<td>4412</td>
<td>1</td>
</tr>
<tr>
<td>2013-02-11 12:28:42.747</td>
<td>0.110</td>
<td>TCP</td>
<td>173.194.35.83</td>
<td>https</td>
<td>knudsvig.customer.org</td>
<td>64939</td>
<td>.AR...</td>
<td>0</td>
<td>6</td>
<td>642</td>
<td>1</td>
</tr>
<tr>
<td>2013-02-11 12:28:34.349</td>
<td>0.000</td>
<td>UDP</td>
<td>knudsvig.customer.org</td>
<td>11914</td>
<td>65.55.223.16</td>
<td>40025</td>
<td>......</td>
<td>0</td>
<td>2</td>
<td>332</td>
<td>1</td>
</tr>
</tbody>
</table>
Questions?

Hung Nguyen
Hung.Nguyen@Flowmon.com
+31624914056

Flowmon Networks a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com