NFSEN: How is My Network Being Used (Apps)?

AfNOG 2009 - Cairo

Mark Tinka
Sunday Folayan
I Use it to Look at BGP Peers!
Here is the Profile for BGP

<table>
<thead>
<tr>
<th>Profile:</th>
<th>BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group:</td>
<td>(nogroup)</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
<tr>
<td>Type:</td>
<td>Continuous</td>
</tr>
<tr>
<td>End:</td>
<td>2007-04-25-13:40</td>
</tr>
<tr>
<td>Last Update:</td>
<td>2007-04-25-13:40</td>
</tr>
<tr>
<td>Size:</td>
<td>39.1 MB</td>
</tr>
<tr>
<td>Max. Size:</td>
<td>unlimited</td>
</tr>
<tr>
<td>Expire:</td>
<td>7 Days</td>
</tr>
<tr>
<td>Status:</td>
<td>OK</td>
</tr>
</tbody>
</table>

Channel List:
Entries for Two Peers
Application Ports

Profile: Ports

TCP

UDP

ICMP

other

Profileinfo:
Type: continuous
Max: unlimited
Exp: 7 days 0 hours
Start: Apr 18 2007 - 13:40 UTC
End: Apr 25 2007 - 13:35 UTC

Wed Apr 25 01:35:00 2007 Bits/s any protocol

Select Single Timeslot

Display 1 day

Packets

Flows

Lin Scale  Stacked Graph

Log Scale  Line Graph
Focusing on Applications

<table>
<thead>
<tr>
<th>Colour</th>
<th>Sign</th>
<th>Order</th>
<th>Filter</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>#18FF77</td>
<td>+</td>
<td>2</td>
<td>proto tcp and (port 80 or port 443)</td>
<td>psg0, psg1</td>
</tr>
<tr>
<td>#FFFF18</td>
<td>+</td>
<td>1</td>
<td>proto tcp and (port 25 or port 995 or port 110 or port 143 or port 465 or port 993)</td>
<td>psg0, psg1</td>
</tr>
</tbody>
</table>
Making a New Channel

Profile: mail
Group: (nogroup)
Description: Mail Deaggregated
Type: Continuous
Start: 2007-04-27 12:45
Last Update: 2007-04-27 12:55
Size: 60.0 KB
Max. Size: 100.0 MB
Expire: never
Status: OK

Channel List: +
New Channel Form

[Image of a channel form with fields for Channel name, Colour, Sign, Order, Filter, Sources, Available Sources, and Selected Sources, along with buttons for Cancel and Add Channel]
SMTP Channel

- Name for Legend
- Pick Contrasting Colors
- Get Secure and Insecure
- Which Interfaces
Good Habit to Show What We Missed
Unclassified?
Select only Unclassified
What we Want to See

Options:
- List Flows
- Stat TopN

Top:
- 20

Stat:
- Flow Records
- order by: bytes

Aggregate:
- proto
- srcPort
- dstPort

Limit:
- Packets > 0

Output:
- line
- / IPv6 long

Clear Form process
And we Get Stats!

Aggregated flows 269938
Top 20 flows ordered by bytes:

<table>
<thead>
<tr>
<th>Date flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-04-26 15:19:53.943</td>
<td>4155.149</td>
<td>TCP</td>
<td>196.3.64.137:18710 →</td>
<td>196.200.216.242:14962</td>
<td>141847</td>
<td>15.3 M</td>
<td>77</td>
</tr>
</tbody>
</table>

Summary: total flows: 314900, total bytes: 333.7 M, total packets: 1.2 M, avg bps: 287782, avg pps: 131, avg bpp: 274
Total flows processed: 314900, skipped: 0, Bytes read: 16375196
Sys: 0.396s flows/second: 794351.5 Wall: 1.278s flows/second: 246269.0
Who Was It?

At your site, you would use better names 😊
To Whom Were They Talking?

Broken in-addr.arpa 😞
Yep, in-addr.arpa 😞

% host 192.103.19.37
;; connection timed out; no servers could be reached
Try Whois

% whois -h whois.arin.net 192.103.19.37

OrgName:    Nokia Data Communications Corporation
OrgID:      NDCC-2
Address:    2300 Tall Pines Drive, Suite 100
City:       Largo
StateProv:  FL
PostalCode: 34641
Country:    US

Hi Joel 😊