NfSen reloaded

21st TF-CSIRT
Peter Haag
May 4th 2007
NfSen reloaded

What’s new? - Spot the 10 differences!
So - what’s really new?

• Channel based architecture.
• Most flexible - more configurable.
  – New Profile groups.
  – Individual display parameters per channel.
  – Converting profiles.
• GUI improvements
  – Sliding cursor
  – Lots of tables can expand/collaps
• Shadow profiles.
• IP Lookup.
• Alerting module.
• Lots of internal changes, to make it extensible:
  – nfsend daemon.
  – Allow other applications to talk to NfSen.
• Simulator mode for student training
NfSen 1.2.x:

Profile: live

Profile Filter

proto udp and port 53

Profile: DNS

Profile Type:
- continuous
- history

Once defined, no longer changeable
NfSen reloaded - All about channels

NfSen 1.3.x:

Profile: live

Profile Filter

- in if 5 and proto tcp and port 80
- out if 5 and proto tcp and port 80
- in if 5 and proto tcp and port 25
- out if 5 and proto tcp and port 25

Profile: DNS

Profile Type:
- continuous
- history
- continuous / shadow
- history / shadow

Any time changeable
Channel Properties:
NfSen reloaded - All about channels

Advantages:

• Much more flexibility to display flows.
• Much more options to create a profile. ( for example AS related profiles )
• High flexibility to add / delete channels any time.
• Change profile / channel parameters any time.
NfSen reloaded

Same data - displayed differently!
Shadow Profiles:
• Standard continuous or history profiles.
• Only graphical (rrd) data but no netflow data stored.
• Processing flows is based on live profile data with profile filters applied.

Pros:
• Consumes only little disk space.
• Lots of different profiles possible.

Cons:
• No dedicated expire parameters.
• Longer processing time, needs to filter more data.
NfSen reloaded - Shadow Profiles

Examples:

Live profile - Single netflow source.

Input / Output.

DNS - Servers A - K

Web Server

Housing Server
NfSen reloaded - Shadow Profiles

Type conversion:

Continuous / Shadow  History Shadow

Loosing flow data
NfSen reloaded - Shadow Profiles

IP Lookup:

QuickTime™ and a TIFF (LZW) decompressor are needed to see this picture.
NfSen reloaded - Shadow Profiles

IP Lookup:
- Looks up IPv4 IP address in cyberabuse.org

Customize Lookup:
Copy Lookup.pm ⇒ Lookup_site.pm
Implement you own lookup function.

```perl
sub Lookup {
    my $socket = shift;
    my $opts = shift;

    if ( !exists $$opts{'lookup'} ) {
        print $socket "<h3>Missing lookup parameter</h3>
        return;
    }
    my $lookup = $$opts{'lookup'};
    print $socket "<h3>$ip: $hostname</h3>
    ...}
}
```

# End of Lookup
Alerting:  
• No alerting at all so far for NfSen <= 1.2.x  
• Many user requests for implementing.

but … what is an alert??

As simple as …
“send me an alert if the number of flows is > x”

or more complex …
“Execute this plugin once only, as long as the number of bytes for tcp port 80 from that netflow source is > than the 6h average of bytes or ....”
Alert details:

Alert Status

Filter for live profile

Condition(s)

Trigger

Action(s)
NfSen reloaded - Alerting

Conditions:

New alert
Name: UDPdos
Status: enabled

Filter applied to 'live' profile:
upstream
flows
proto udp and bpp < 1000

Conditions based on total flow summary:

Total flows
Total packets
Total bytes
Flows/s
Packages/s
bits/s

Absolute value
0
0
-
M
T
%

Condition:
Each time after
condition = true, and block next trigger for cycles

Action:
No action
Send alert email
Call plugin:

Cancel Create Alert
## Conditions:

**New alert**

<table>
<thead>
<tr>
<th>Name</th>
<th>UDPdos</th>
</tr>
</thead>
</table>

**Status**

<table>
<thead>
<tr>
<th>enabled</th>
</tr>
</thead>
</table>

**Filter applied to 'live' profile:**

- **upstream flows**
  - protocol udp and bps < 1000

**Conditions based on total flow summary:**

**Conditions based on individual Top 1 statistics:**

<table>
<thead>
<tr>
<th>Flows</th>
<th>SRC IP Address</th>
<th>&gt;</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any IP Address</td>
<td>&gt;</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Trigger:**

- **Flow:**
  - Packets/s

- **Bytes:**
  - Each time

- **Bytes/Package:**

**Action:**

- **No action**
- **Send alert email**
  - To: [blank]
  - Subject: Alert trigger

- **Call plugin:**
  - [No alert plugins available]
### NfSen reloaded - Alerting

**Trigger:**

- **New alert**
  - **Name:** UDPdos
  - **Status:** Enabled

**Filter applied to 'live' profile:**
- **upstream**
  - proto udp and bpp < 1000

**Conditions based on total flow summary:**
- Total flows > 1 hour average value + 0 - +

**Conditions based on individual Top 1 statistics:**

**Conditions based on plugin:**

- **Trigger:**
  - Each time after 1 cycle
  - Once only
  - Once only, while condition = true

- **Send alert email**
  - **To:**
  - **Subject:** Alert triggered

- **Call plugin:**
  - No alert plugins available

- **Cancel** | **Create Alert**
NfSen reloaded - Alerting

Alert Info:

<table>
<thead>
<tr>
<th>Flows</th>
<th>Last</th>
<th>Avg 10m</th>
<th>Avg 30m</th>
<th>Avg 1h</th>
<th>Avg 6h</th>
<th>Avg 12h</th>
<th>Avg 24h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>493.6 k</td>
<td>504.1 k</td>
<td>510.3 k</td>
<td>447.2 k</td>
<td>165.8 k</td>
<td>143.8 k</td>
<td>292.5 k</td>
</tr>
<tr>
<td></td>
<td>1.6 k/s</td>
<td>1.7 k/s</td>
<td>1.7 k/s</td>
<td>1.5 k/s</td>
<td>552.6 /s</td>
<td>475.2 /s</td>
<td>974.9 /s</td>
</tr>
<tr>
<td>Packets</td>
<td>7.3 M</td>
<td>7.6 M</td>
<td>7.2 M</td>
<td>6.7 M</td>
<td>3.4 M</td>
<td>3.7 M</td>
<td>5.8 M</td>
</tr>
<tr>
<td></td>
<td>24.3 k/s</td>
<td>25.2 k/s</td>
<td>24.0 k/s</td>
<td>22.3 k/s</td>
<td>11.3 k/s</td>
<td>12.2 k/s</td>
<td>19.5 k/s</td>
</tr>
<tr>
<td>Bytes</td>
<td>6.6 GB</td>
<td>6.9 GB</td>
<td>6.5 GB</td>
<td>6.1 GB</td>
<td>3.1 GB</td>
<td>3.4 GB</td>
<td>5.4 GB</td>
</tr>
<tr>
<td></td>
<td>176.8 MB/s</td>
<td>181.9 MB/s</td>
<td>172.2 MB/s</td>
<td>161.4 MB/s</td>
<td>83.5 MB/s</td>
<td>91.7 MB/s</td>
<td>144.2 MB/s</td>
</tr>
</tbody>
</table>

Conditions: 0 1 Final: 1
State: True False False
NfSen reloaded - Alerting

Alert Info:

QuickTime™ and a TIFF (LZW) decompressor are needed to see this picture.
Summary:

• Alerting is a new feature ⇒ feedback

• Flexible conditions:
  What? flows, packets, bytes (total or Top N)
  Compare? >, <, outside
  Value? abs, avg value, %
  Plugin based.

• Flexible Triggers:
  Always condition == true
  Needs n time condition == true
  Once only as long condition == true
  Block for n cycles when fired

• Flexible Actions:
  Do nothing
  Send e-mail
  Run plugin
  Run system command
nfsend - NfSen daemon:
nfsend - NfSen daemon:
An external application may talk directly to NfSen and
• Create profiles, channels
• Start/stop collecting data (profile type change)
• Edit channel filters, or other channel/profile parameters
• ...
based on other external events.
NfSen reloaded - NfSim

NfSen simulator:
Goal: Train students using NfSen.
    ( Other NRENs in GN2 project )

A very simply yet effective Simulator mode:
• Process pre-collected netflow data
• Time slice user definable.
    ( A real 5 min time slice may be processed each 30s )
• Start/stop simulation at any time.
• Reset Simulation and start over again.
• Profiles, alerts can be tested with different parameters.
Next Steps - Todo list - still a lot of work:

NfSen 1.4:
- Add SQLite as backend for administrative data
- User authentication/authorization for different roles.
- Views
- “Network behaviour analysis”
- Import/Export of profile/alert definitions
- …
NfSen reloaded

Thank you for your attention.
Any Questions?