



# SWITCH

The Swiss Education & Research Network



## NfSen reloaded

21<sup>st</sup> TF-CSIRT

Peter Haag

May 4<sup>th</sup> 2007



## What's new? - Spot the 10 differences!

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



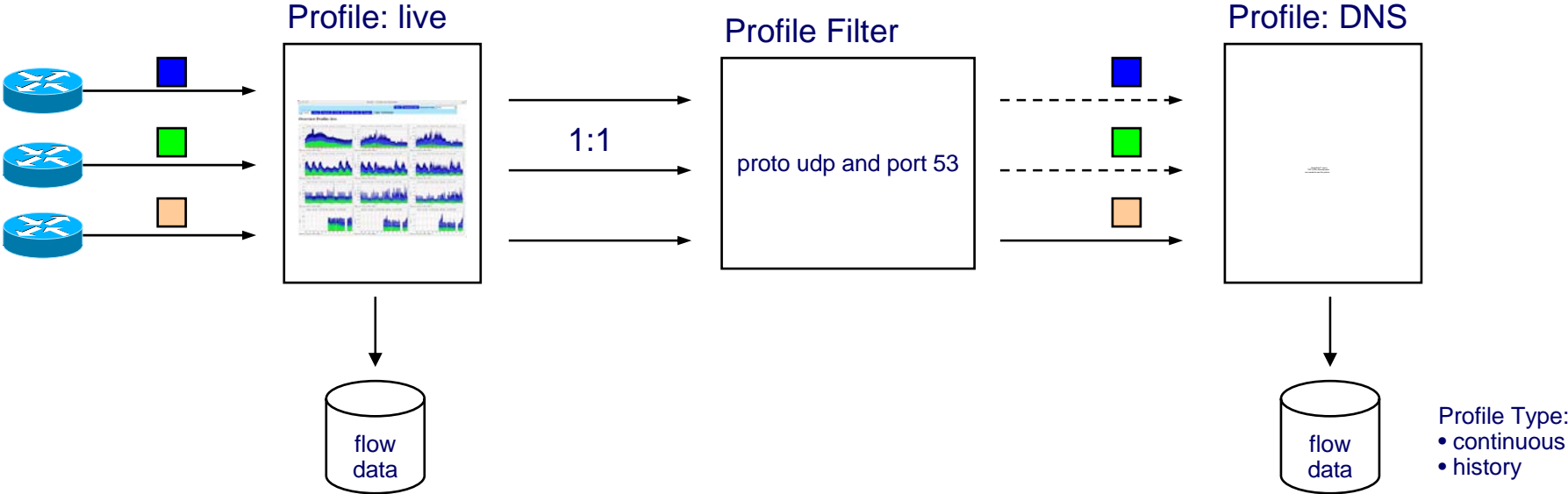
QuickTime™ and a  
TIFF (LZW) decompressor  
are needed to see this picture.

## 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**

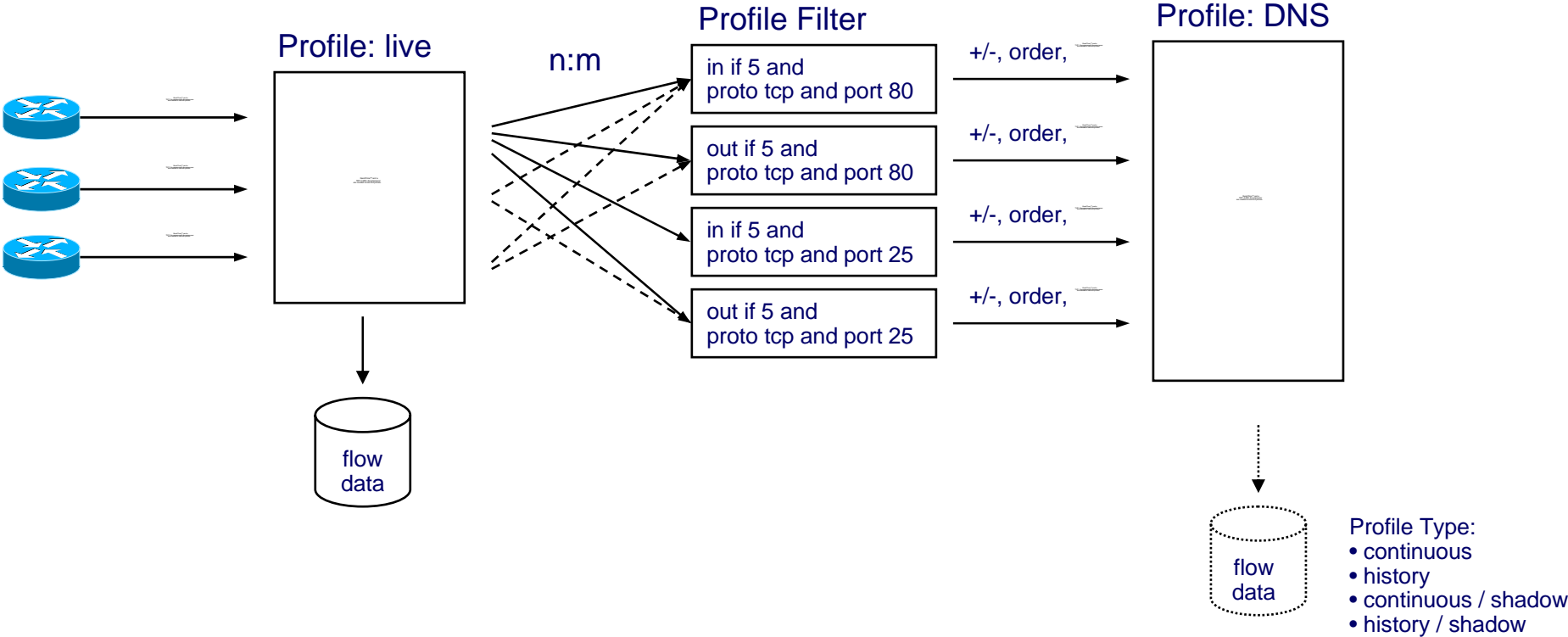


## NfSen 1.2.x:



**Once defined,  
no longer changeable**

## NfSen 1.3.x:



Any time changeable

## Channel Properties:

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

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

## 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.**

## Same data - displayed differently!

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



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

## 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.

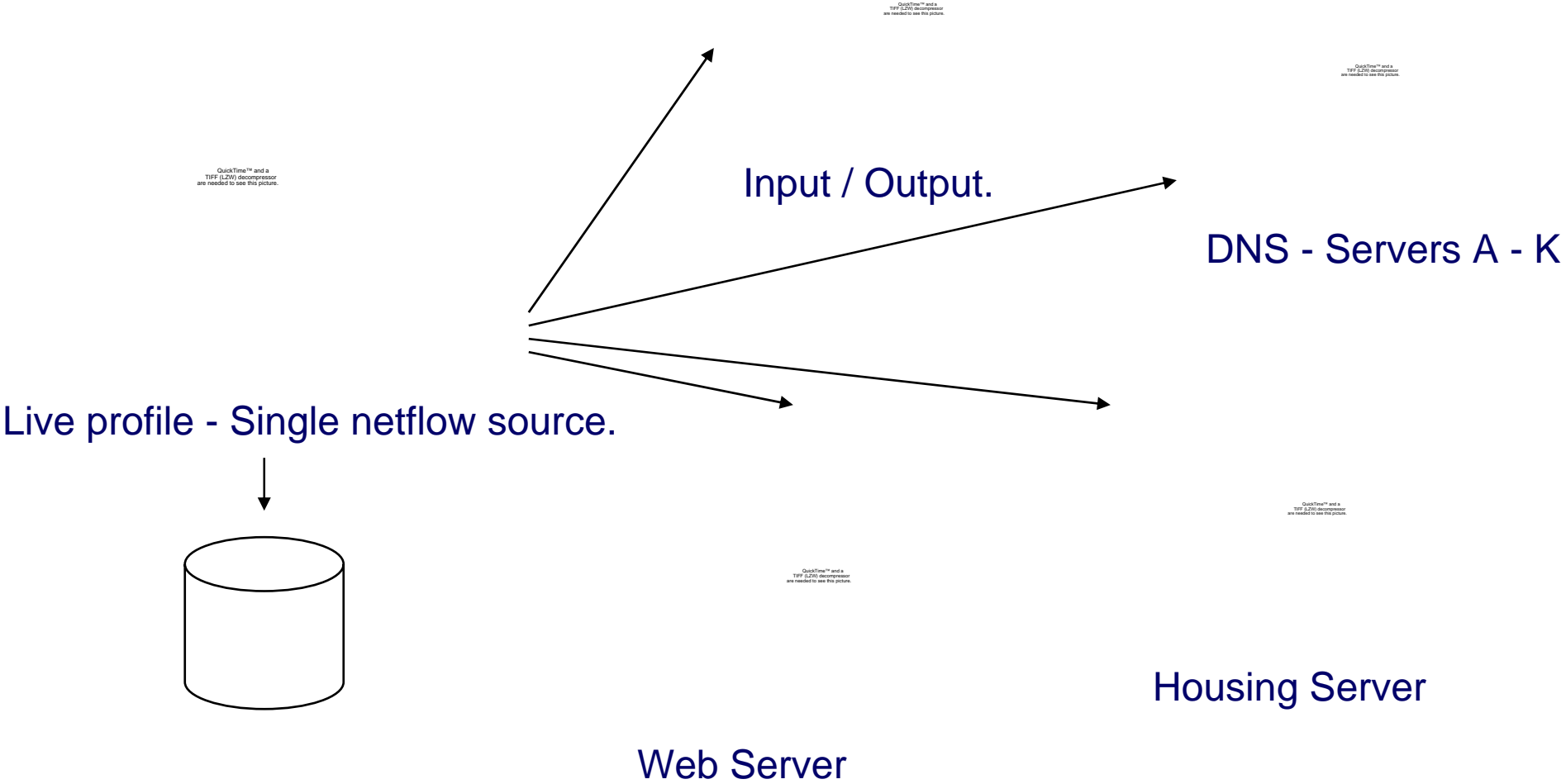
## Pros:

- Consumes only little disk space.
- Lots of different profiles possible.

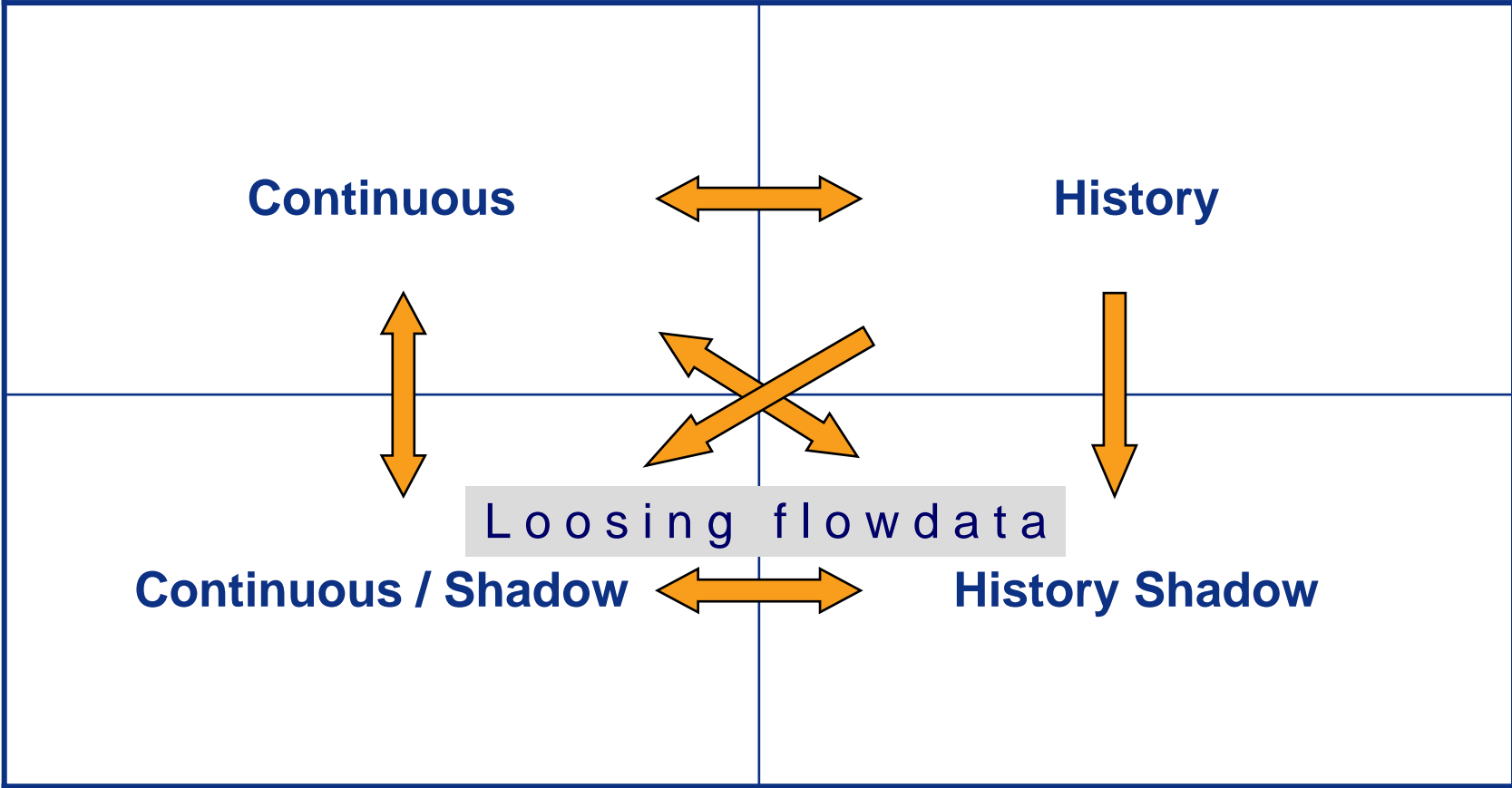
## Cons:

- No dedicated expire parameters.
- Longer processing time, needs to filter more data.

## Examples:



## Type conversion:



## IP Lookup:

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



## IP Lookup:

- Looks up IPv4 IP address in [cyberabuse.org](http://cyberabuse.org)

## Customize Lookup:

Copy `Lookup.pm`  $\Rightarrow$  `Lookup_site.pm`

Implement you own lookup function.

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

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

## Alerting:

- No alerting at all so far for NfSen  $\leq$  1.2.x
- Many user requests for implementing.

*but ... what is an alert??*

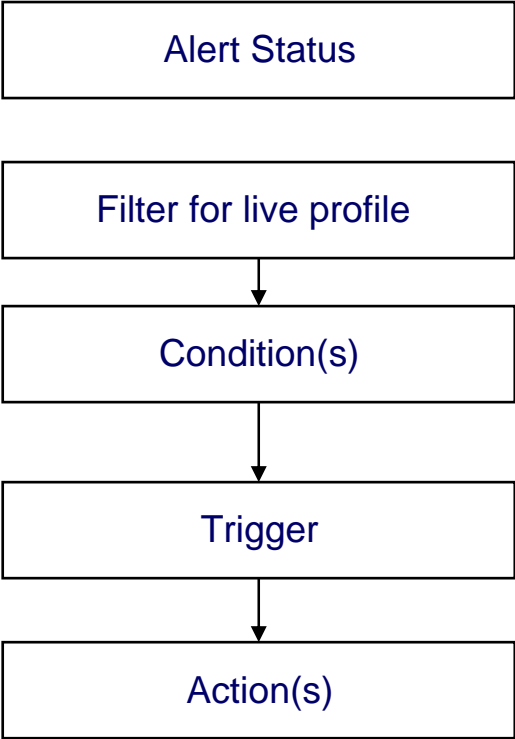
As simple as ...

*“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:



Alerts details: smal-packets

Trigger	Status	Last Triggered
armed	<input checked="" type="checkbox"/> enabled	2007-04-16-13:20

Filter applied to 'live' profile:

upstream	bpp < 100
flows	

Conditions based on total flow summary:

0	Total flows	>	30 min average value	+	20	%	+
---	-------------	---	----------------------	---	----	---	---

Conditions based on individual Top 1 statistics:

Conditions based on plugin:

Trigger:

Each time after 2 x condition = true, and block next trigger for 3 cycles

Action:

No action

Send alert email To: haag@switch.ch

Subject: Alert triggered

Call plugin: demoplugin

Cancel Commit Changes

## Conditions:

### New alert

**Name**

**Status**  enabled

---

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

upstream flows

---

**Conditions based on total flow summary:**

<input type="checkbox"/>	0	Total flows	>	Absolute value	0	-	+
<input type="checkbox"/>		Total packets	<	10 min average value		k	
<input type="checkbox"/>		Total bytes	>	30 min average value		M	
<input type="checkbox"/>		Flows/s	>	1 hour average value		G	
<input type="checkbox"/>		Packages/s	>	6 hour average value		T	
<input type="checkbox"/>		bits/s	>	12 hour average value		%	
<input type="checkbox"/>			>	24 hour average value			

**Trigger:** Each time after 1 x condition = true, and block next trigger for 0 cycles

---

**Action:**

No action

Send alert email To:

Subject:

Call plugin:

## Conditions:

**New alert**

Name:

Status:  enabled

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

upstream flows:

Conditions based on total flow summary:

Conditions based on individual Top 1 statistics:

6 Flows of Top 1 SRC IP Address > 0

**Condition based on plugin:**

- Flows
- Packets
- Bytes
- Packages/s
- Bits/s
- Bytes/Packet

**Trigger:** Each time

**Action:**

No action

Send alert email To:  Subject:

Call plugin:

## Trigger:

**New alert**

Name:

Status:  enabled

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

upstream flows:

**Conditions based on total flow summary:**

Total flows > 1 hour average value +

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

**Conditions based on plugin:**

**Trigger:**

after  x condition = true, and block next trigger for  cycles

(dropdown menu open with options: Each time, Once only, Once only, while condition = true)

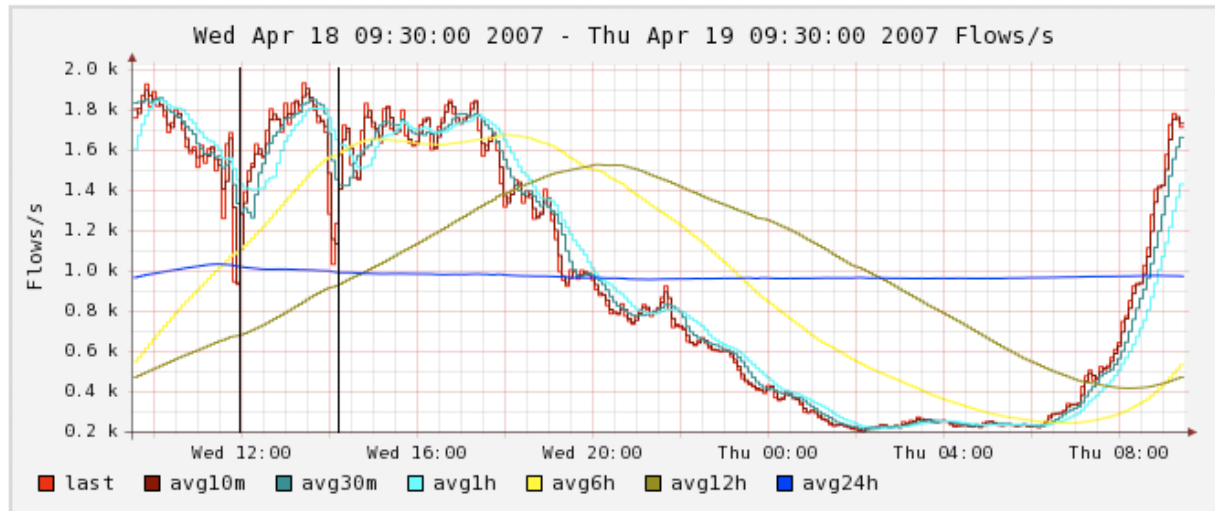
Send alert email To:  Subject:

Call plugin:

## Alert Info:

### Alert Infos:

Last cycle: 2007-04-19-09:30



	Last	Avg 10m	Avg 30m	Avg 1h	Avg 6h	Avg 12h	Avg 24h
Flows	493.6 k	504.1 k	510.3 k	447.2 k	165.8 k	143.8 k	292.5 k
	1.6 k/s	1.7 k/s	1.7 k/s	1.5 k/s	552.6 /s	479.2 /s	974.9 /s
Packets	7.3 M	7.6 M	7.2 M	6.7 M	3.4 M	3.7 M	5.8 M
	24.3 k/s	25.2 k/s	24.0 k/s	22.3 k/s	11.3 k/s	12.2 k/s	19.5 k/s
Bytes	6.6 GB	6.8 GB	6.5 GB	6.1 GB	3.1 GB	3.4 GB	5.4 GB
	176.8 Mb/s	181.9 Mb/s	172.2 Mb/s	161.4 Mb/s	83.6 Mb/s	91.7 Mb/s	144.2 Mb/s

Conditions:	0	1	Final:
State:	True	False	False

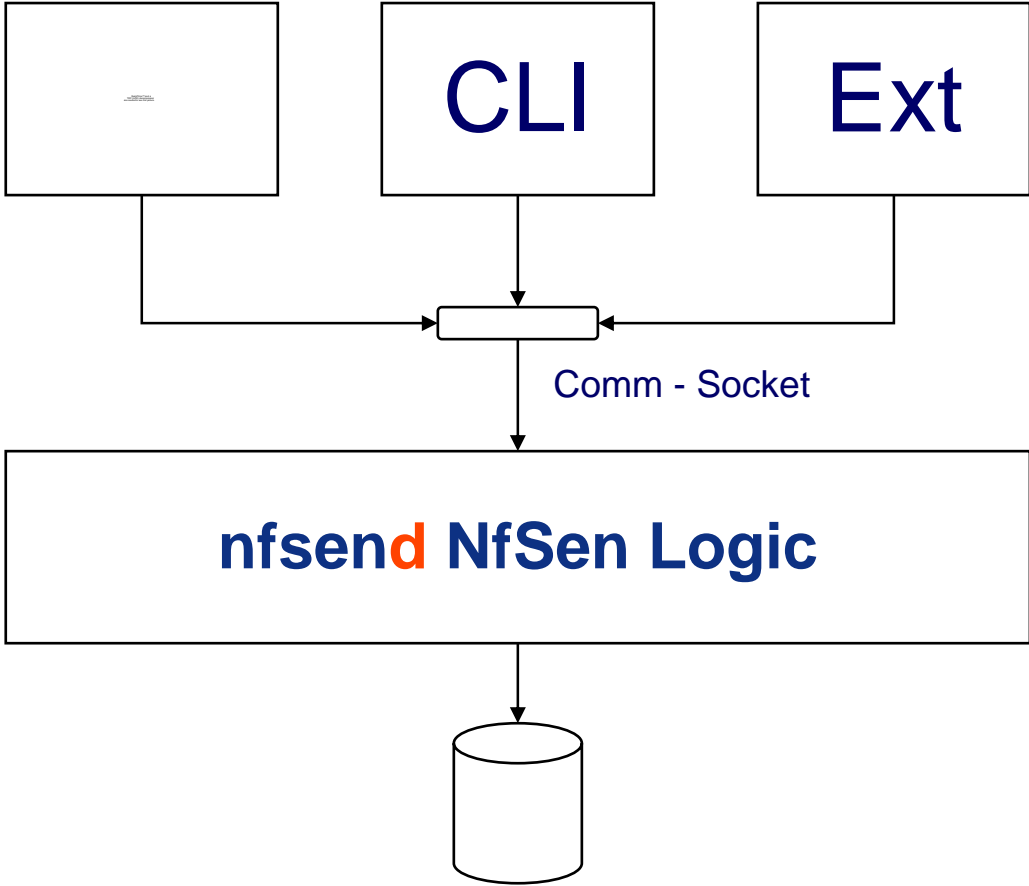
## Alert Info:

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

## Summary:

- **Alerting is a new feature  $\Rightarrow$  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 simulator:

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

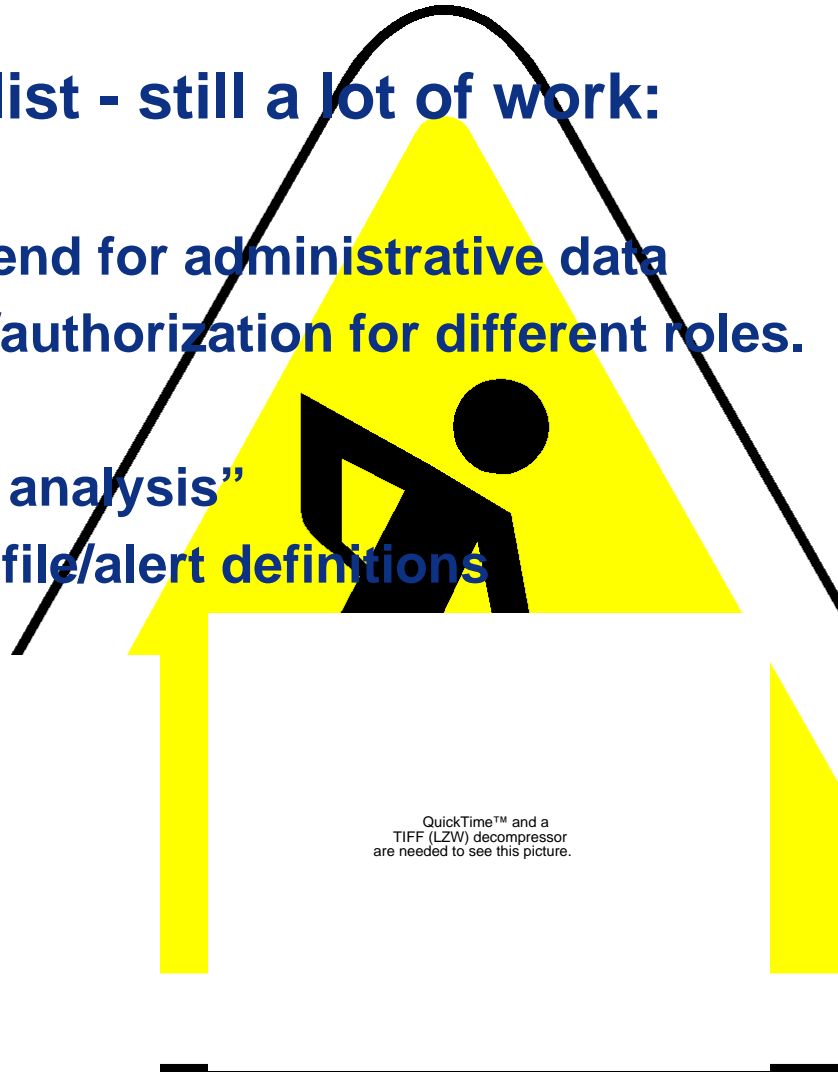
## **A very simply yet effective Simulator mode:**

- **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:

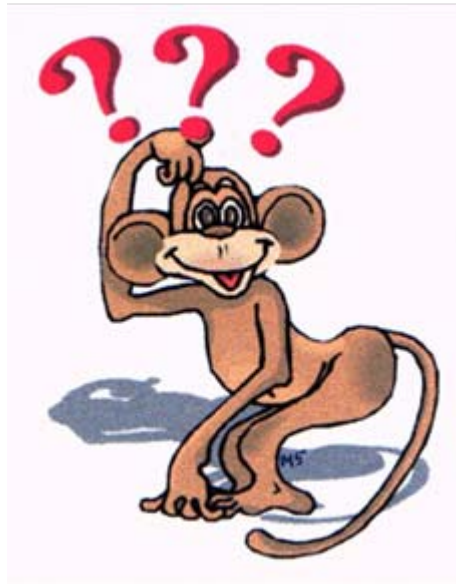
- Add SQLite as backend for administrative data
- User authentication/authorization for different roles.
- Views
- “Network behaviour analysis”
- Import/Export of profile/alert definitions
- ...



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

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

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



Thank you for your  
attention.  
Any Questions?