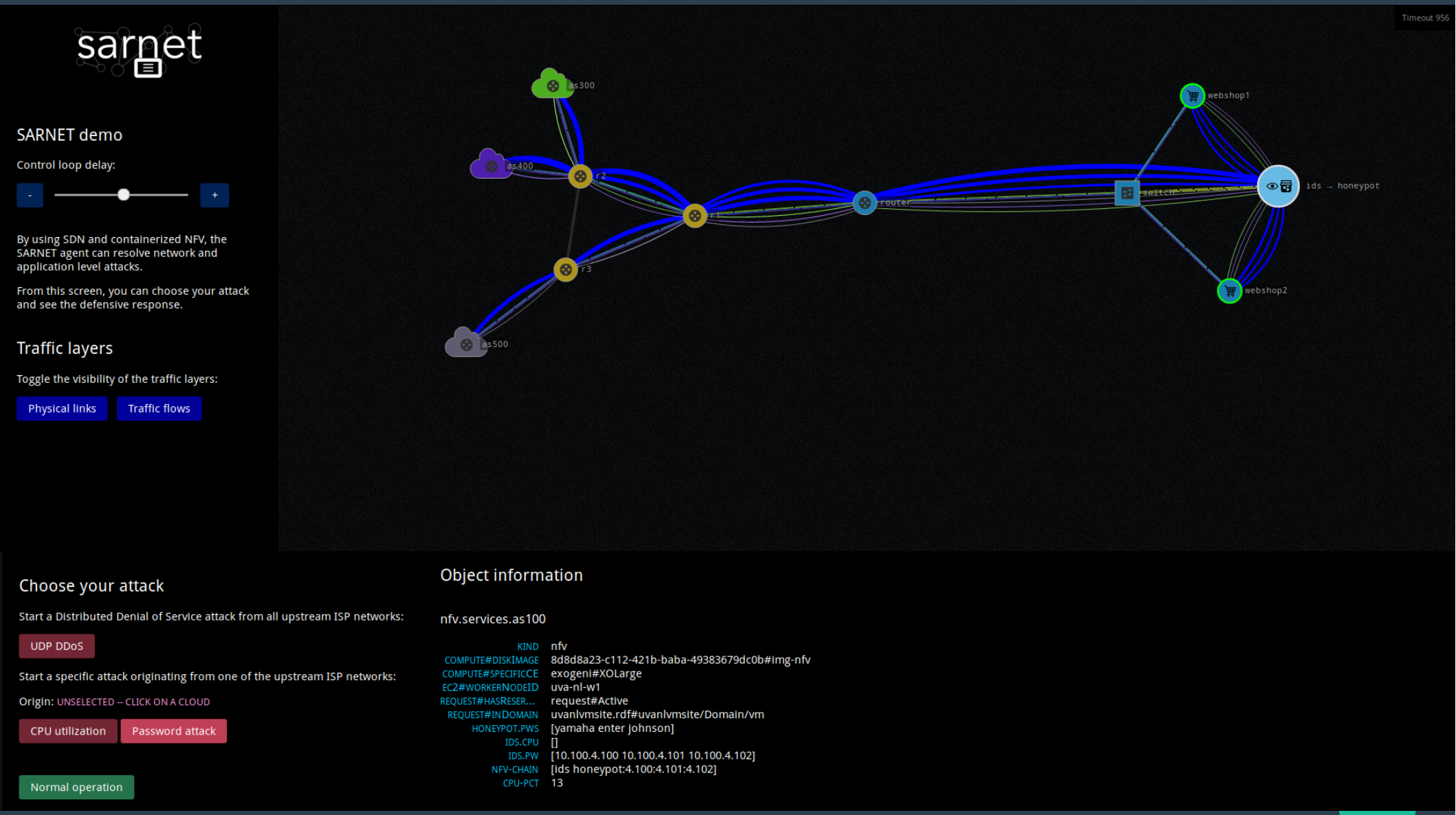
Research update; 3rd SARNET meeting

Ralph Koning

Scenario


sarnet
SARNET demo
Control loop delay:
-
+
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.
From this screen, you can choose your attack and see the defensive response.
Traffic layers
Toggle the visibility of the traffic layers:
Physical links
Traffic flows
Timeout 956
as300
as400
as500
r2
r3
webshop1
webshop2
ids → honeypot
router
switch
Choose your attack
Start a Distributed Denial of Service attack from all upstream ISP networks:
UDP DDoS
Start a specific attack originating from one of the upstream ISP networks:
Origin: UNSELECTED -- CLICK ON A CLOUD
CPU utilization
Password attack
Normal operation
Object information
nfv.services.as100
KIND nfv
COMPUTE#DISKIMAGE 8d8d8a23-c112-421b-baba-49383679dc0b#img-nfv
COMPUTE#SPECIFICCE exogeni#XOLarge
EC2#WORKERNODEID uva-nl-w1
REQUEST#HASRESER... request#Active
REQUEST#INDOMAIN uvanlvmsite.rdf#uvanlvmsite/Domain/vm
HONEYPOT.PWS [yamaha enter johnson]
IDS.CPU []
IDS.PW [10.100.4.100 10.100.4.101 10.100.4.102]
NFV-CHAIN [ids honeypot:4.100:4.101:4.102]
CPU-PCT 13

Sampling

- Sampling
  - Ringbuffer with n values (Default: n=10)
  - New samples arrive asynchronously at about every 0.8 seconds (per metric)
  - Samples for sales from two services are added together, worst case this takes about 1.6 seconds.

- Detect: 30 percent of the samples in the window are below or above treshold.

- Recover: if 70 percent of the samples in the window are above or below treshold.

Scenario 2

Secure Autonomous Response Network SARNET agent metrics

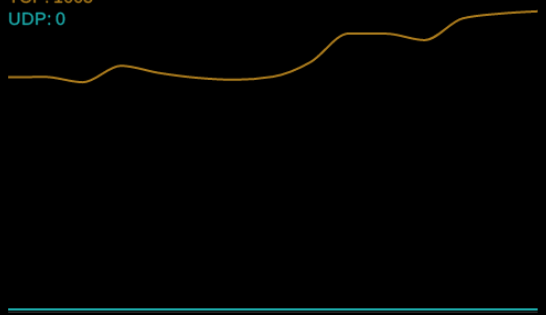
Network metrics

Bandwidth:

Utilized: 492Mbit/s

Flows:

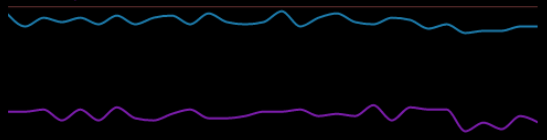
TCP: 1663
UDP: 0



Application metrics

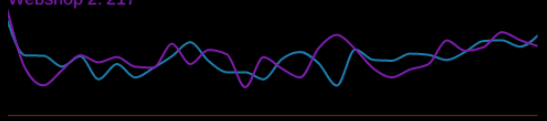
CPU:

Webshop 1: 76%
Webshop 2: 32%



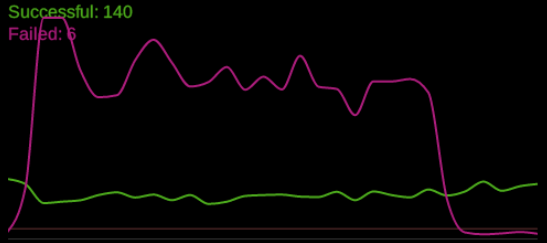
Successful transactions:

Webshop 1: 233
Webshop 2: 217

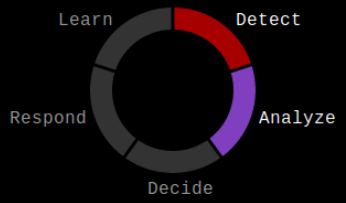


Login attempts:

Successful: 140
Failed: 6



Control loop



DETECT

ANALYZE

Known crackers: 10.100.4.100, 10.100.4.101, 10.100.4.102

Latest password attempts:
* star
* little
* chevy

DECIDE

Deploy IDS to gather additional data
Deploy honeypot to divert and capture attack

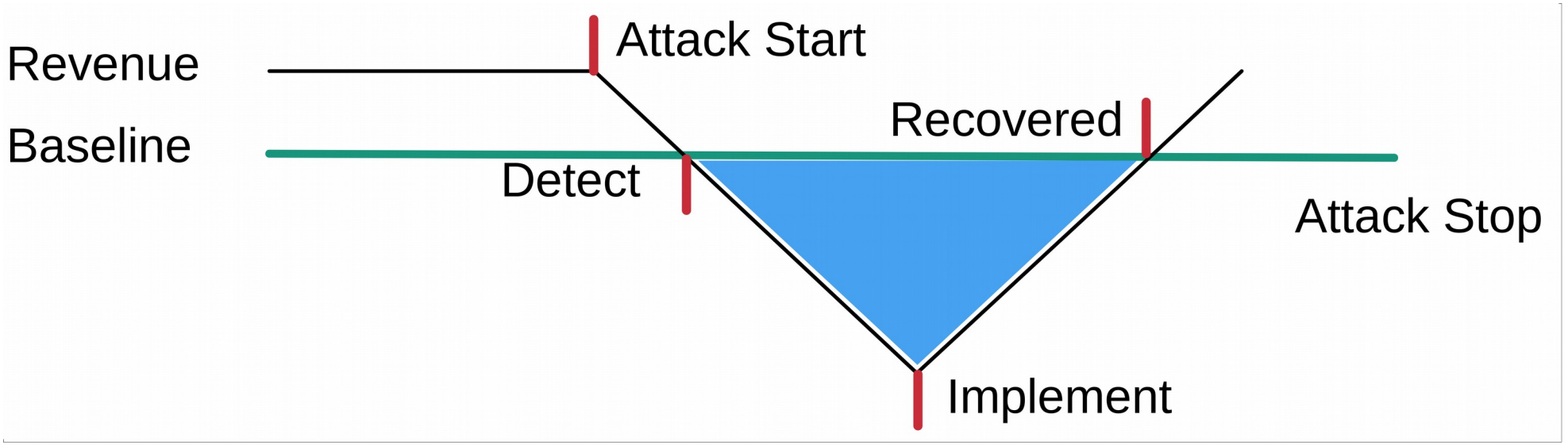
RESPOND

Deployed NFV chain:
* ids
* honeypot:4.100:4.101:4.102

Observables

- DDoS attack
  - Detected if: Abnormal UDP, Sales < thresh(200)
  - Recover if: Sales > thresh
- CPU attack
  - Detected if: CPU > thresh(85)
  - Recovered if: CPU < thresh, Sales > thresh
- PWD attack
  - Detected if: failed > ok OR failed > thresh(20)
  - Recovered if: failed < thresh
- How to determine the right thresholds and observables?
  - ML might help though has its caveats
  - Determining what observables are needed and which ones are important cannot really be automated, unless we have all the data.

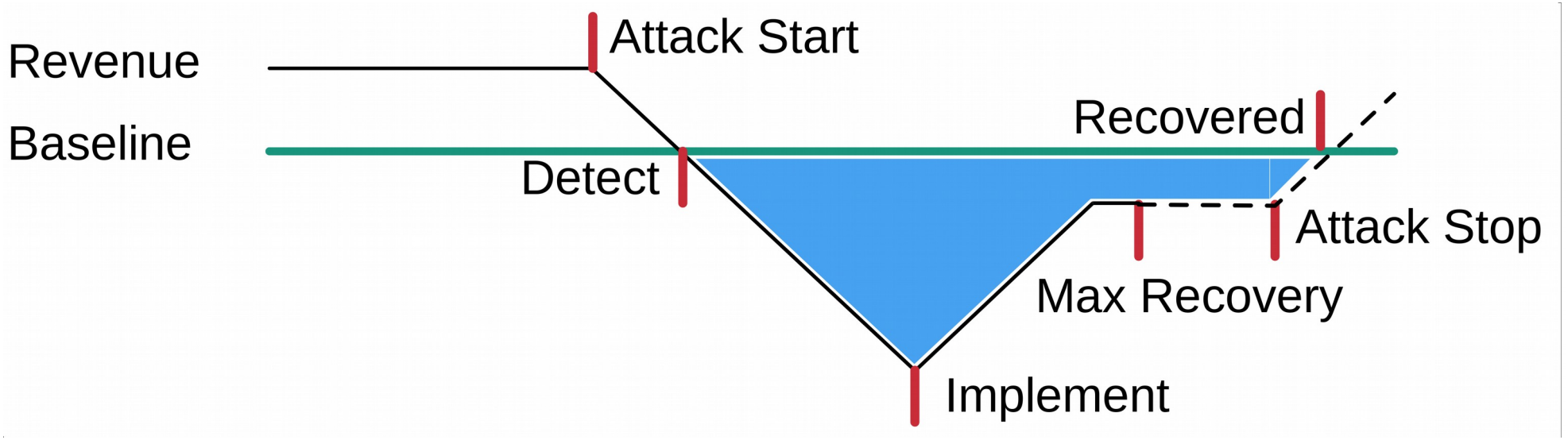
Effectiveness



Determining effectiveness

- Take the samples for a observable
- Subtract the threshold for that observable
- Invert the samples when needed (for sales)
- Set all negative values to 0
- Use trapezoidial rule to determine integral
- Maybe normalize by dividing by baseline?

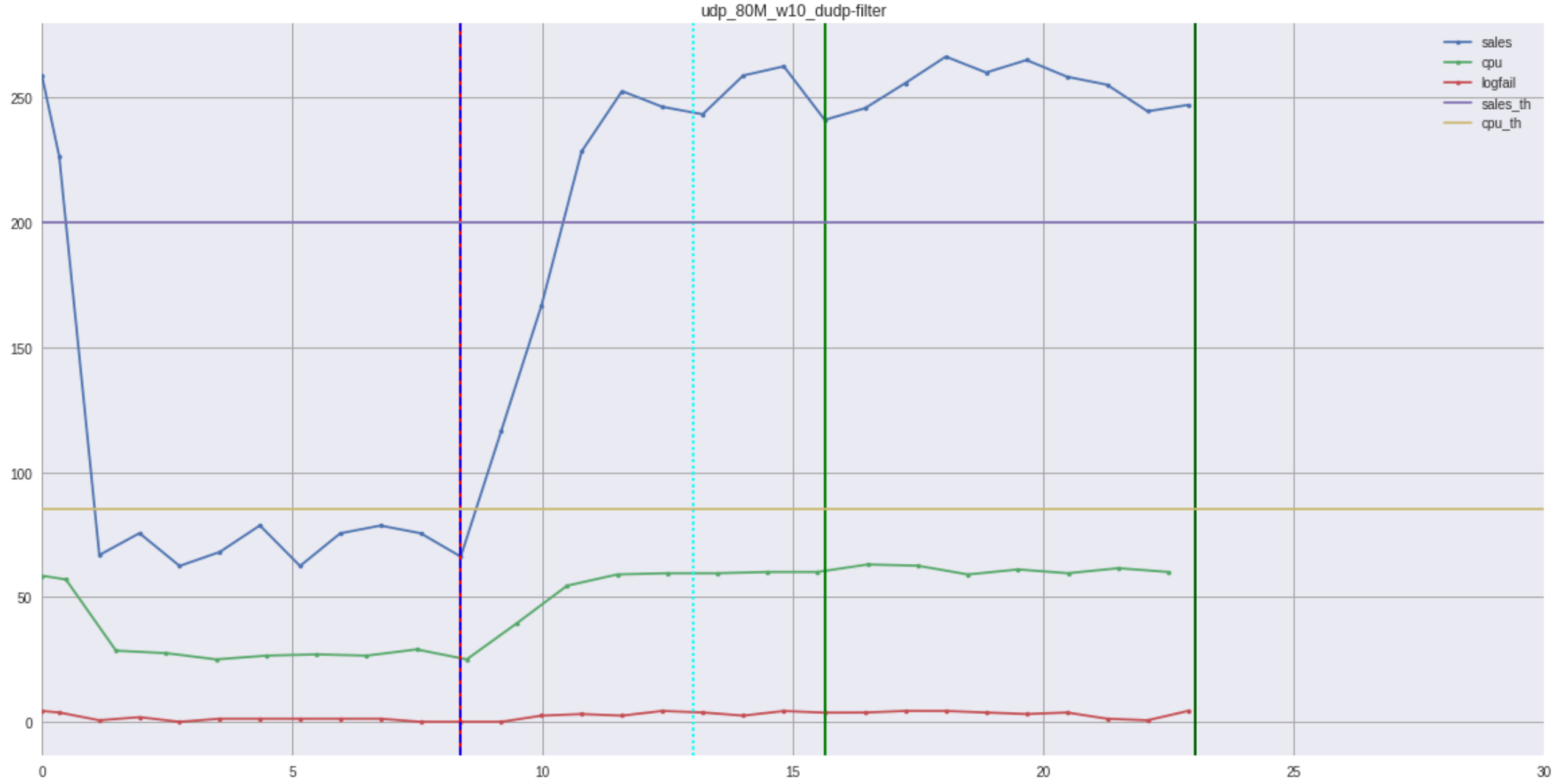
Partial recovery



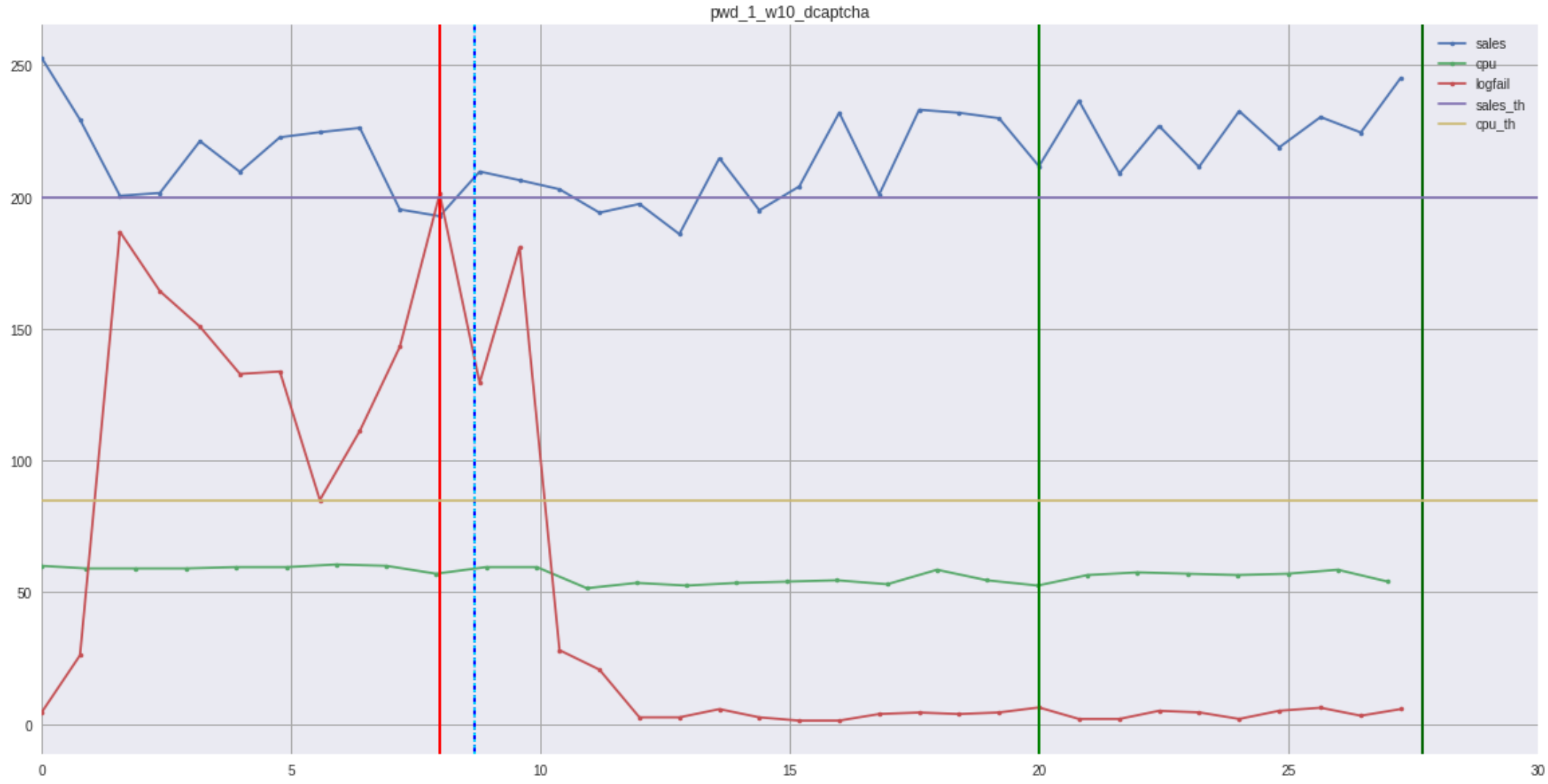
Partial recovery

- Current method: when variability does not exceed <insert arbritrary value> from the mean.
- Better? Regression line in sample window and look at the slope..
- How long should we wait to call partial recovery.
  - It can still fully recover… eventually?

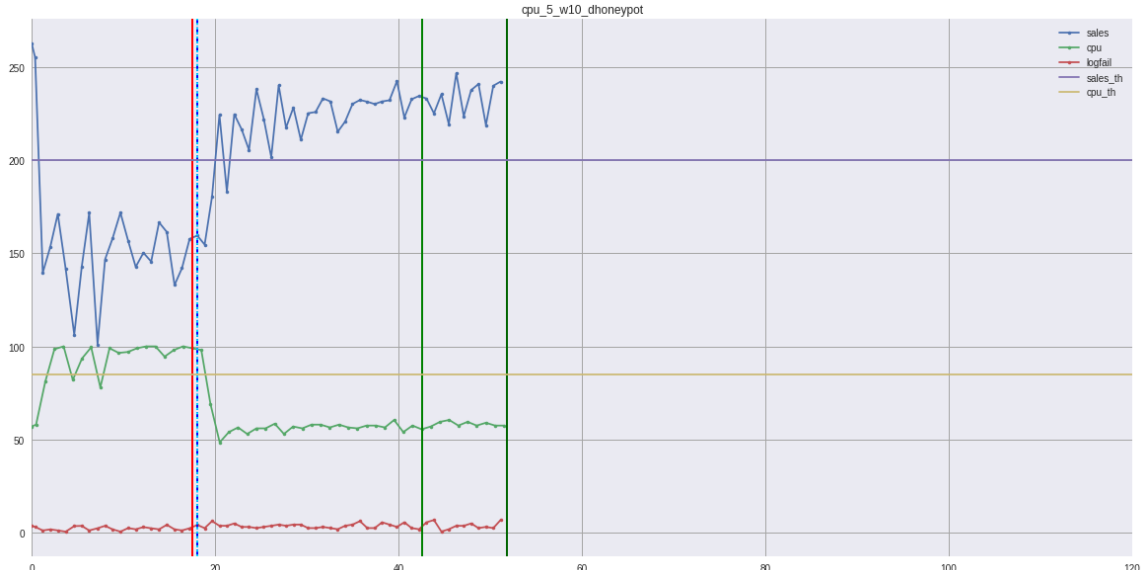
UDP filter

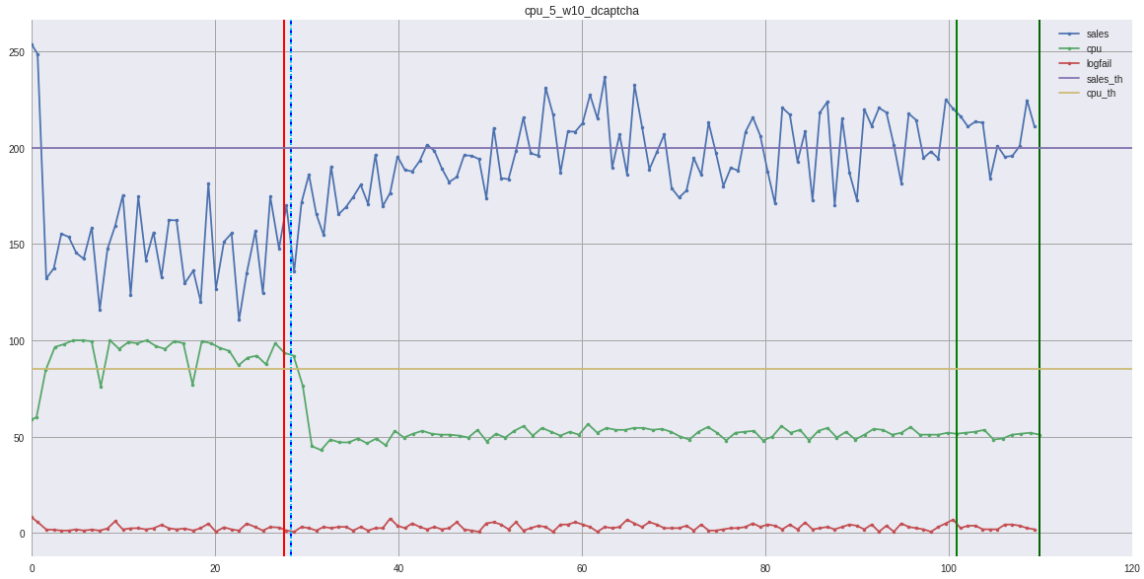

udp_80M_w10_dudp-filter
sales
cpu
logfail
sales_th
cpu_th
250
200
150
100
50
0
0
5
10
15
20
25
30

Password attack



Captcha recovery



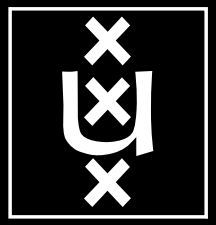


← Faster recovery

Timeout and scalability

- Timeout: After 120 seconds the chosen countermeasure fails.

- Scalability issue?
  - If it takes 2 minutes to try a single solution iterating over 30 solutions takes about an hour (worst case).
  - How about combined solutions.



University of Amsterdam

https://sarnet.uvalight.net/

mailto: r.koning at uva.nl

TNO innovation for life

NWO
Netherlands Organisation for Scientific Research

COMMIT/

AIRFRANCE KLM

ciena