

# Smart and Secure Cyber Infrastructure.

**Cees de Laat**  
**System & Network Engineering**  
**University of Amsterdam**

COMMIT/

SE





# What Happens in an Internet Minute?

1,572,877 GB of global IP data transferred<sup>1</sup>

10 Million ads displayed<sup>2</sup>

347,222 Tweets<sup>3</sup>

3.3 Million pieces of content shared<sup>4</sup>

6.9 Million messages sent<sup>4</sup>

Netflix + Youtube = more than 1/2 of all traffic<sup>5</sup>

438,801 Wiki page views<sup>7</sup>

\$400 Million during Alibaba peak day sales<sup>6</sup>

10 Million WeChat messages at its peak<sup>9</sup>

34.7 Million instant messages (MIM) sent<sup>8</sup>

194,064 app downloads<sup>10</sup>

\$133,436 in sales<sup>11</sup>

31,773 hours of music played<sup>12</sup>

38,194 photos uploaded<sup>13</sup>

57,870 page views<sup>14</sup>

100 hours of video uploaded<sup>16</sup>

138,889 hours of video watched<sup>16</sup>

23,148 hours of video watched<sup>17</sup>

4.1 Million searches<sup>15</sup>

## And Future Growth is Staggering



By 2017, mobile traffic will have grown **13X** in just 5 years<sup>1</sup>



In 2017, there will be **3X** more connected devices than people on Earth<sup>1</sup>

All digital data created reached **4 zettabytes** in 2013<sup>18</sup>

**1,572,877 GByte/minute = (8\*1,572,877\*10^9/60 bit/s)/(10\*10^12 bit/s per fiber) = 21 fibers with each about 100 \* 100 Gb/s channels**



Amazon Uses Trucks to Drive Data Faster



PERSONAL TECHNOLOGY  
The Cable-Cutting Dream Is Kind ...



Altice Plans Fiber Upgrade That Could Leave Rivals in the Dust



Netflix Now Lets You Download, But Many Top Shows Are Off Limits

TECH

## Amazon Uses Trucks to Drive Data Faster

Cloud-computing unit, Amazon Web Services, unveils new offerings at annual conference in Las Vegas



Amazon unveiled the 'Snowmobile' service on Wednesday in Las Vegas. PHOTO: AMAZON WEB SERVICES

By **JAY GREENE** By **LAURA STEVENS**  
Updated Nov. 30, 2016 7:19 p.m. ET

4 COMMENTS

LAS VEGAS—In Amazon Web Services, [Amazon.com](http://Amazon.com) Inc. has built one of the most powerful computing networks in the world, on pace to post more than \$12 billion in revenue this year.

But the retail giant on Wednesday proposed a surprising way to move data from large corporate customers' data centers to its public cloud-computing operation: by truck.

Networks can move massive amounts of data only so fast. Trucks, it turns out, can move it faster.

The tractor-trailer hauls a massive storage device, dubbed Snowmobile, in the form of a 45-foot shipping container that holds 100 petabytes of data. A petabyte is about 1 million gigabytes.

The company, however, isn't promising lightning speed. Ten Snowmobiles would reduce the time it takes to move an exabyte from on-premises storage to Amazon's cloud to a little less than six months, from about 26 years using a high-speed internet connection, by the company's calculations.

**1 fiber does about 16 Tbit/s  
= 2 Tbyte/s  
⇒ 50000 s/ExaByte  
⇒ One week/ExaByte  
Or stick Joe and Harvey in a RV  
for 2 months.**

Out

2. What Are Clothes

3. Opinion The Rev

Most Popular

1. U.S. to Po Least \$10 Student Coming

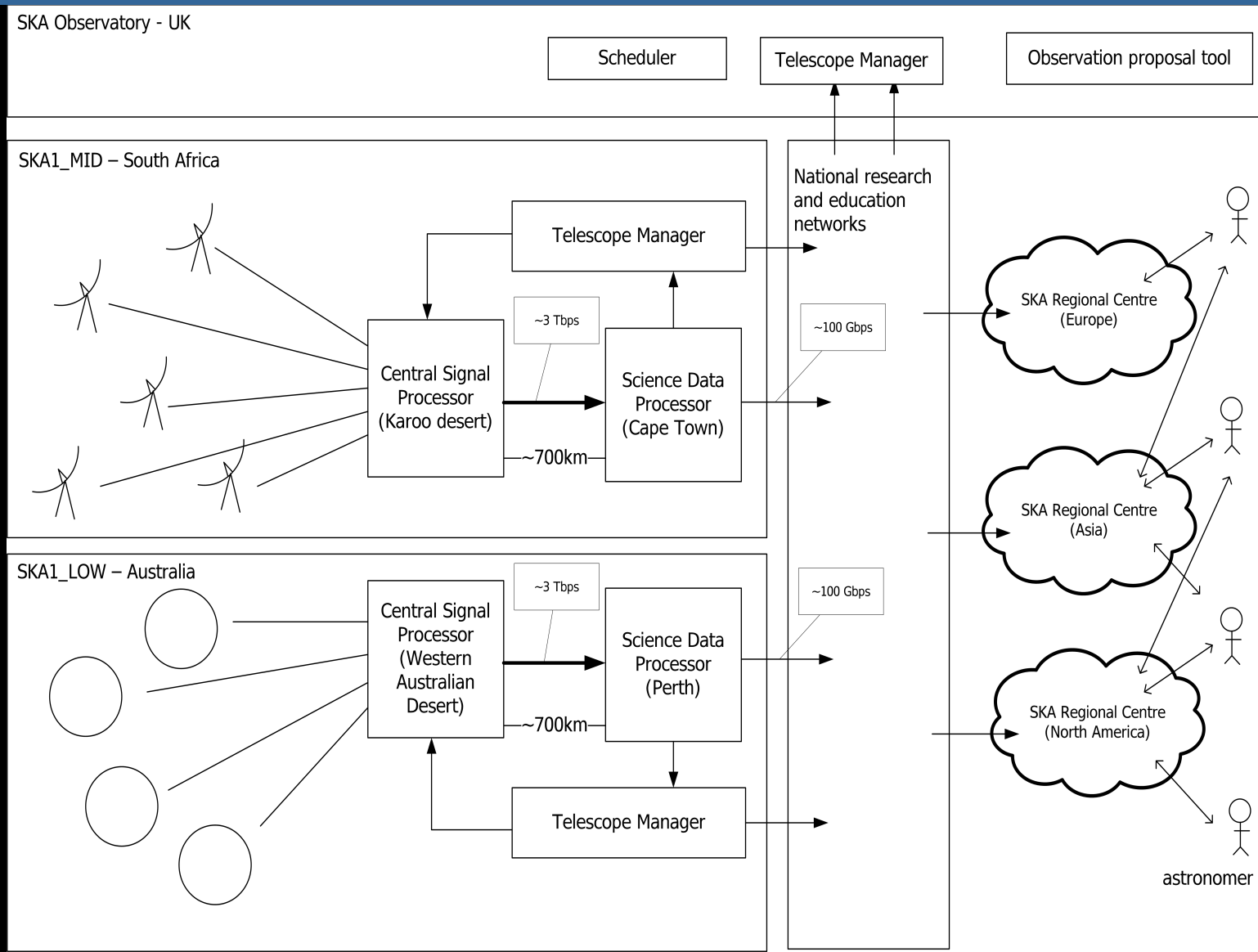
2. Opinion: Trump's Pick Scar

3. Trump's His Busi Draws Q

4. Creator of Mac Dies

5. Trump's Choice S Absolute

# SKA: Depending on analysis load & physics mode they want to investigate to use SDN in real time to direct bursts of data to different compute resources and do load balancing.



# Learned from Scinet & INDIS

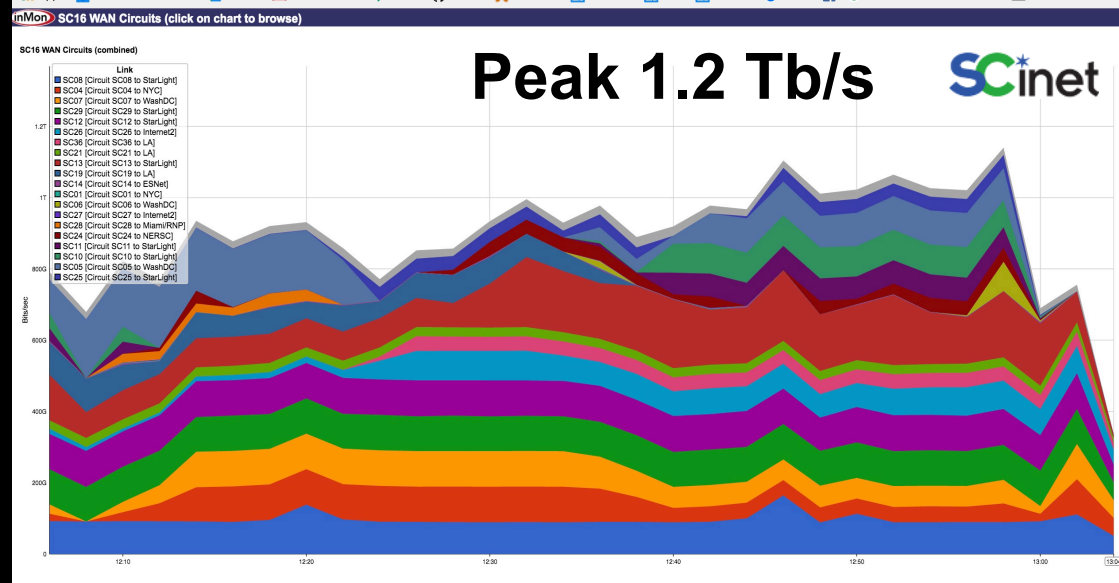
- 2013 - 2016

- SDN

- Security

- Traffic management, policing, control

- Hybrid – optical ring - approach to reach Tb/s



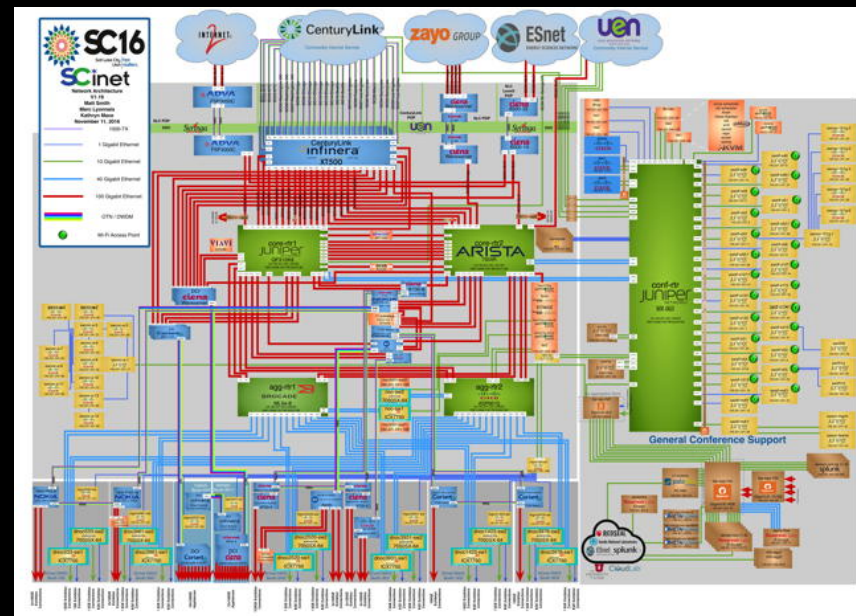
- 2017 - 2020

- NFV

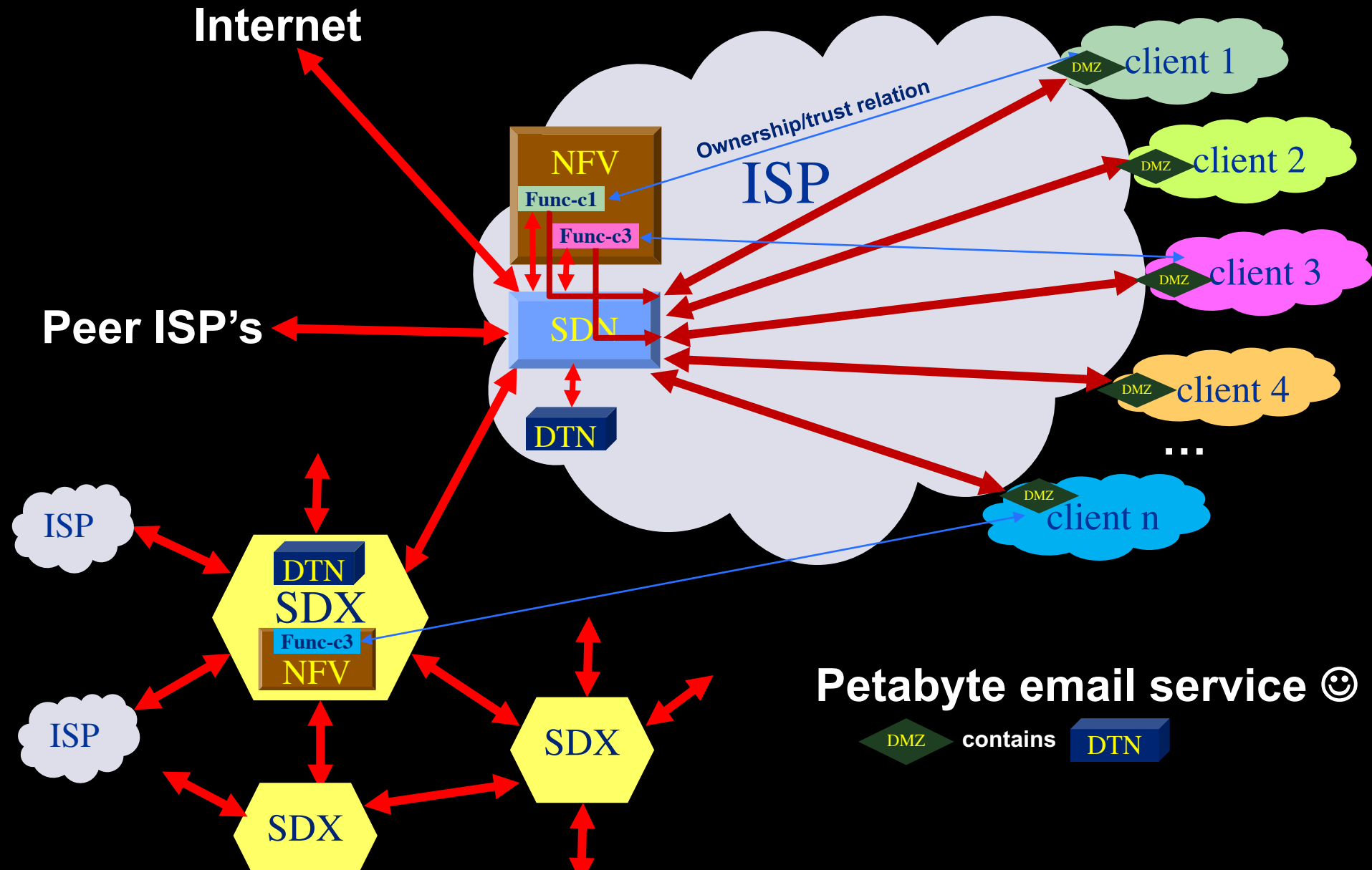
- SDX

- DTN @ core → petabyte email network

- Data abstractions (e.g. NDN)



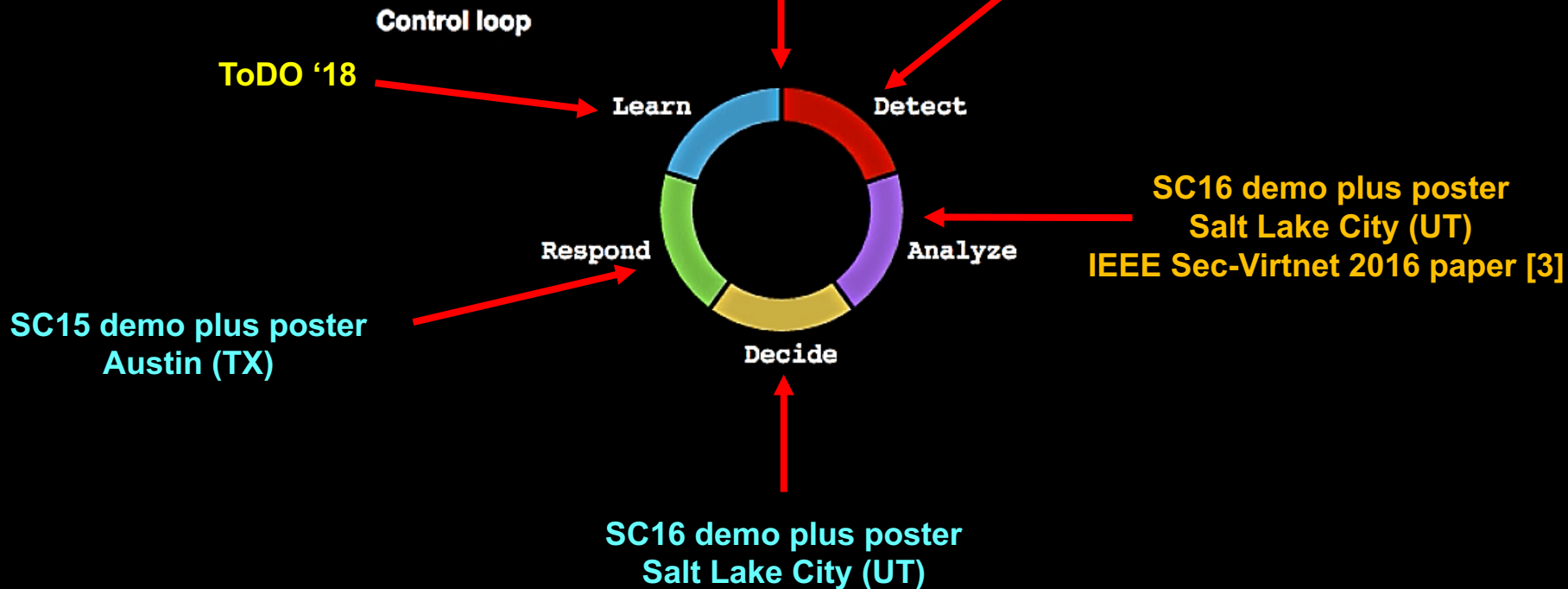
# Networks of ScienceDMZ's & SDX's



# Status SARNET Operational Level

Laboratory: ExoGeni & PRP  
Fieldlab with KLM & CIENA  
OSA-Optical Forum Conference paper [1]

CoreFlow  
Berkeley Internship 2016  
SC16 INDIS workshop paper [2]



1. Paper: R. Koning, A. Deljoo, S. Trajanovski, B. de Graaff, P. Grosso, L. Gommans, T. van Engers, F. Fransen, R. Meijer, R. Wilson, and C. de Laat, "Enabling E-Science Applications with Dynamic Optical Networks: Secure Autonomous Response Networks ", OSA Optical Fiber Communication Conference and Exposition, 19-23 March 2017, Los Angeles, California.
2. Paper: Ralph Koning, Nick Buraglio, Cees de Laat, Paola Grosso, "CoreFlow: Enriching Bro security events using network traffic monitoring data", SC16 Salt Lake City, INDIS workshop, Nov 13, 2016.
3. Paper: Ralph Koning, Ben de Graaff, Cees de Laat, Robert Meijer, Paola Grosso, "Analysis of Software Defined Networking defences against Distributed Denial of Service attacks", The IEEE International Workshop on Security in Virtualized Networks (Sec-VirtNet 2016) at the 2nd IEEE International Conference on Network Softwarization (NetSoft 2016), Seoul Korea, June 10, 2016.

# Basic operating system loop

Chrome File Edit View History Bookmarks Window Help

localhost:4567/vi/7

- netapps (provider, zone)
- connections

Mode:  
 info  
 info edge  
 draw  
 delete node  
 delete edge  
 Last result:  
 getting links  
 new netapp

Zone:  
 eu-west-1a:  eu-west-1b:  eu-west-1c:  gbl-1-a:  gbl-1-b:  us-east-1a:  us-east-1b:  us-east-1c:  us-east-1d:  us-west-2a:  us-west-2b:  us-west-2c:  us-west-1a:  us-west-1c:  sa-east-1a:  sa-east-1b:  ap-northeast-1a:  ap-northeast-1b:  ap-southeast-1a:  ap-southeast-1b:

Use canvas to change configuration

Create generator

- number of vms
- preferential attachment algorithm (take into account geoiip)

```

Bicomponents[#, #] :=
  [[edge, c, i, x, v = VertexDegree[#, vl = VertexList[#], If[Length[#] <= 1, Return[{}];
  length[#] > 1,
  take[#, 2];
  intersection@@c;
  length[#] > 0, # = Delete[c, Position[#, i[[1]]], r = c]];
  = Map[First, Map[Sort[#, v[[Position[v1, #][[1]]] < v[[Position[v1, #2][[1]]] & #,
  ]];
  geQ[#, UndirectedEdge[edge[[1]], edge[[2]]],
  = Map[Last, Map[Sort[#, v[[Position[v1, #][[1]]] < v[[Position[v1, #2][[1]]] & #,
  ]]]];

Bicomponents[#, #] := Module[{v = VertexDegree[#, vl = VertexList[#],
  Bicomponents[#,
  {Function[{x}, Total[v[[Position[v1, #][[1]]] & /@x][[#1]] <
  Total[v[[Position[v1, #][[1]]] & /@x][[#2]] & #, #]}]}];

ArticulationVertices[#, #] := Module[{v = VertexDegree[#, vl = VertexList[#],
  {Function[{x}, Total[v[[Position[v1, #][[1]]] & /@x][[#1]] <
  Total[v[[Position[v1, #][[1]]] & /@x][[#2]] & #, #]}]}];

ArticulationVertices[#, #] := CreateLinkReal[ConnectTwoComponents@@MyBicomponents[#, #],
  #] := GraphPlot[#, VertexLabeling -> True, DirectedEdges -> False] & /@hist
  
```

Start the dynamics, such that an updated graph will trigger the function call and display the graph when the network changes.

```

In[166]:= Dynamic[ResolveArticulationVertices[network]]
Dynamic[MyPlot[network]]

Out[166]= Null

Out[167]= {
  {1-2-3-4-5, 1-2-3-4-5},
  {1-2-3-4-5, 1-2-3-4-5},
  {1-2-3-4-5, 1-2-3-4-5}
}

network = Graph[{1 <-> 2, 2 <-> 3, 3 <-> 1, 3 <-> 4, 4 <-> 5, 5 <-> 6}];
GraphPlot[network, VertexLabeling -> True, DirectedEdges -> False];
  
```

Find all positions at

```

In[2]:= Position[{{a, #}, #}]
Out[2]:= {{1, 3}, {2, 1}, {3, 2}}
  
```

Find only those down

```

In[1]:= Position[{1 + x, #}]
Out[1]:= {{1, 2}, {3}, {4}}
  
```

Test directed edges:

```

In[2]:= {EdgeQ[#, 1 -> 2], EdgeQ[#, 2 -> 1], EdgeQ[#, 1 -> 1]}
Out[2]:= {True, True, False}
  
```

creating: {13125, 13127}  
 creating: {13128, 13127}  
 creating: {13125, 13124}

100%



# SC16 DEMO SARNET Operational Level

sarnet

Connected

## SARNET demo

Control loop delay:



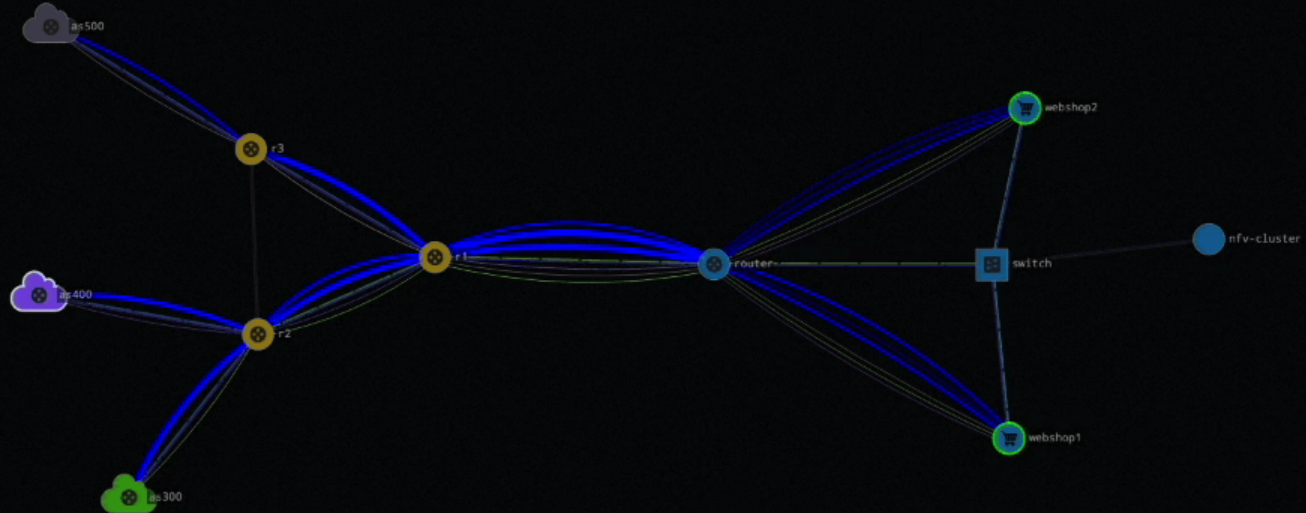
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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



## 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: e2.edge2.as400

CPU utilization Password attack

Normal operation

## Object information

e2.edge2.as400

```
KIND router
COMPUTE#DISKIMAGE 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#lmg-router
COMPUTE#SPECIFICCE exogeni#XOSmall
IC2#WORKERNodeID uva-nl-w1
REQUEST#HASRESERVAT... request#Active
REQUEST#INDOMAIN uvanlmsite.rdf#uvanlmsite/Domain/vm
CPU-PCT 22
```



# SC16 DEMO SARNET Operational Level

sarnet

Connected

## SARNET demo

Control loop delay:



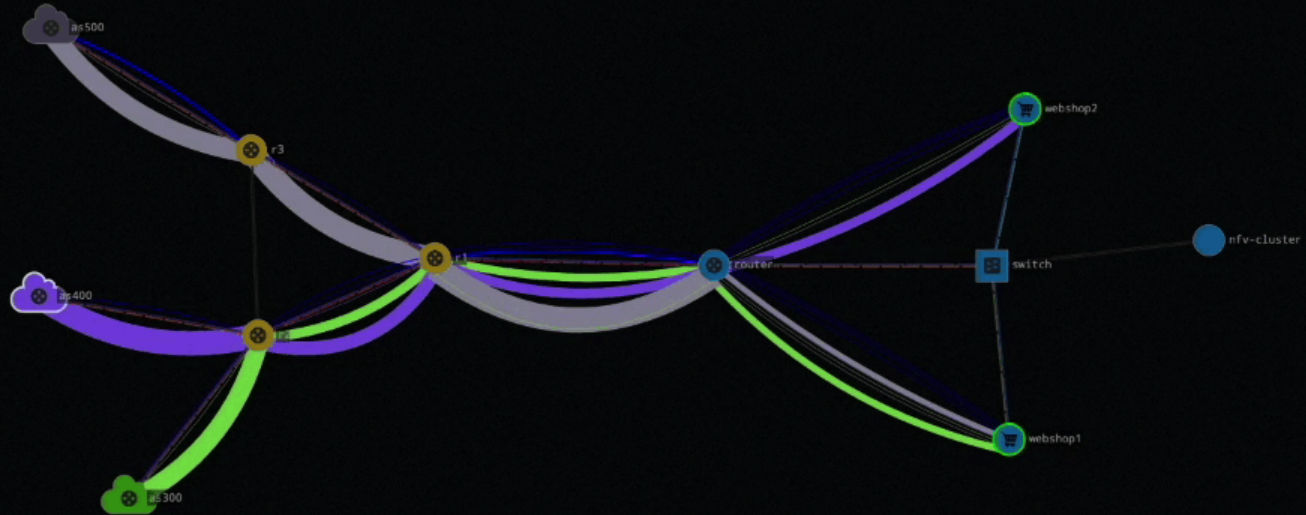
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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



## 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: e2.edge2.as400

CPU utilization Password attack

Normal operation

## Object information

e2.edge2.as400

```
KIND: router
COMPUTE#DISKIMAGE: 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#img-router
COMPUTE#SPECIFIC: exogeni#XOSmall
EC2#WORKERNODEID: uva-nl-w1
REQUEST#HASRESERVATION: request#Active
REQUEST#INDOMAIN: uvanlvm/site.rdf#uvanlvm/site/Domain/vm
CPU#PCT: 17
```

Edge domains flood the network with UDP traffic



# SC16 DEMO SARNET Operational Level

Secure Autonomous Response Network SARNET agent metrics

## Network metrics

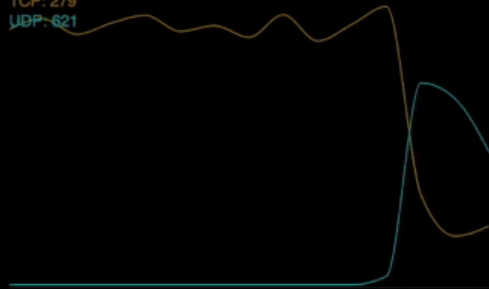
### Bandwidth:

Utilized: 867Mbit/s



### Flows:

TCP: 279  
UDP: 621



## Application metrics

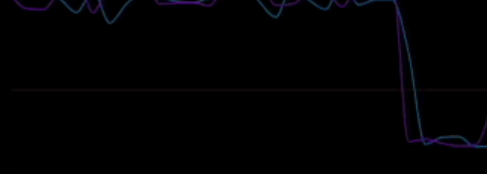
### CPU:

Webshop 1: 38%  
Webshop 2: 60%



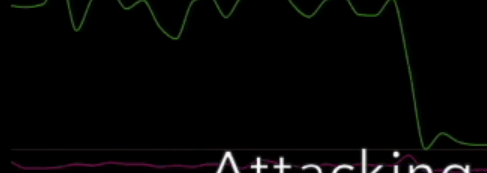
### Successful transactions:

Webshop 1: 39  
Webshop 2: 99

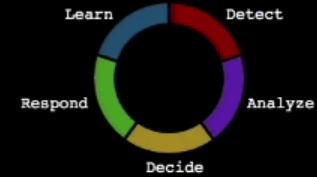


### Login attempts:

Successful: 24  
Failed: 2



## Control loop



### DETECT

Revenue below threshold  
Abnormal UDP flows detected

### ANALYZE

DDoS domains: AS300, AS400, AS500

### DECIDE

Filter UDP traffic at edge domains

### RESPOND

Attacking domains are identified

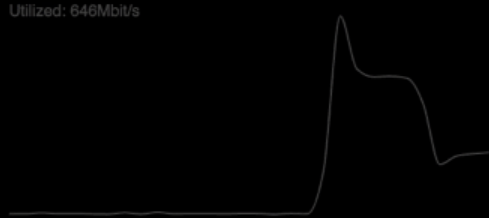
# SC16 DEMO SARNET Operational Level

Secure Autonomous Response Network SARNET agent metrics

## Network metrics

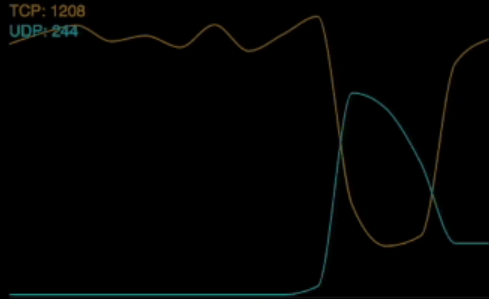
### Bandwidth:

Utilized: 646Mbit/s



### Flows:

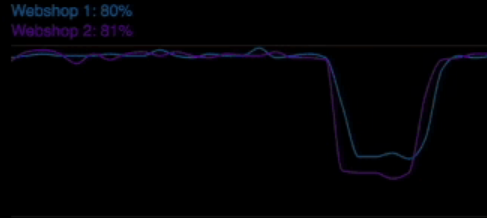
TCP: 1208  
UDP: 244



## Application metrics

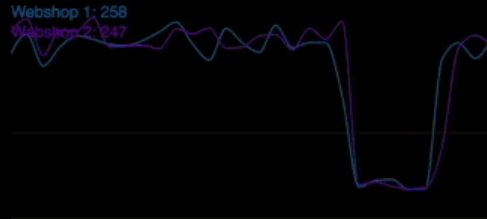
### CPU:

Webshop 1: 80%  
Webshop 2: 81%



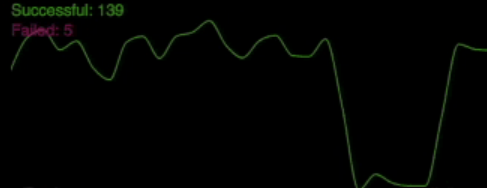
### Successful transactions:

Webshop 1: 258  
Webshop 2: 247

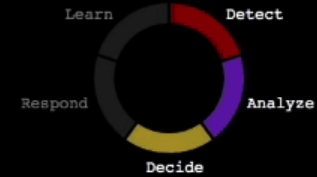


### Login attempts:

Successful: 139  
Failed: 5



## Control loop



### DETECT

Abnormal UDP flows detected

### ANALYZE

DDoS domains: AS300, AS400, AS500

### DECIDE

Filter UDP traffic at edge domains

### RESPOND

Flow filters are installed at the network edge

# SC16 DEMO SARNET Operational Level

sarnet

Connected

## SARNET demo

Control loop delay:



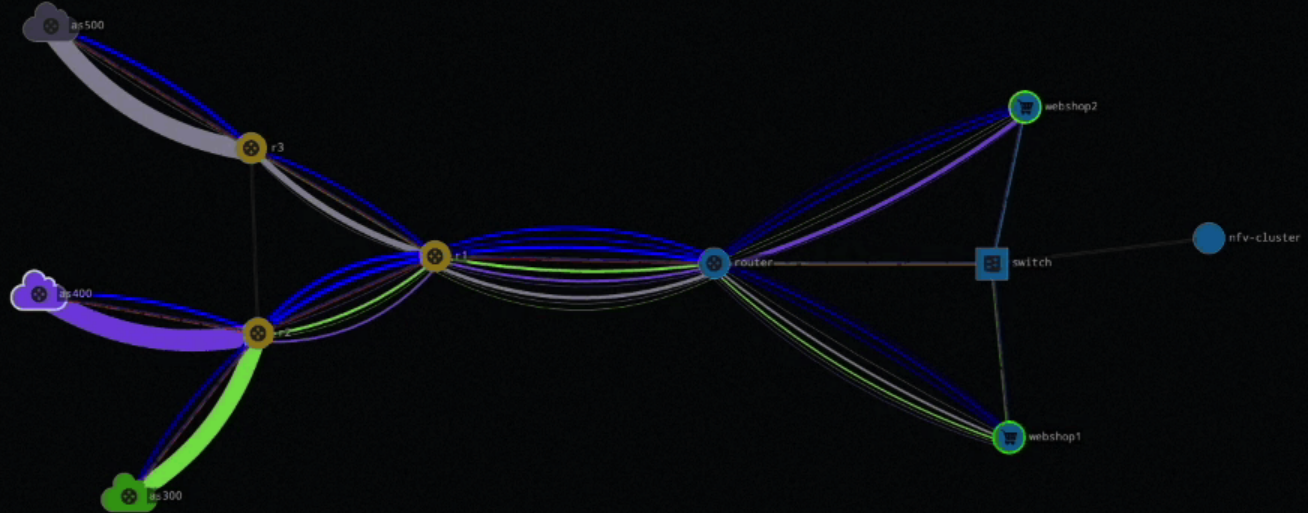
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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



## 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: e2.edge2.as400

CPU utilization Password attack

Normal operation

## Object information

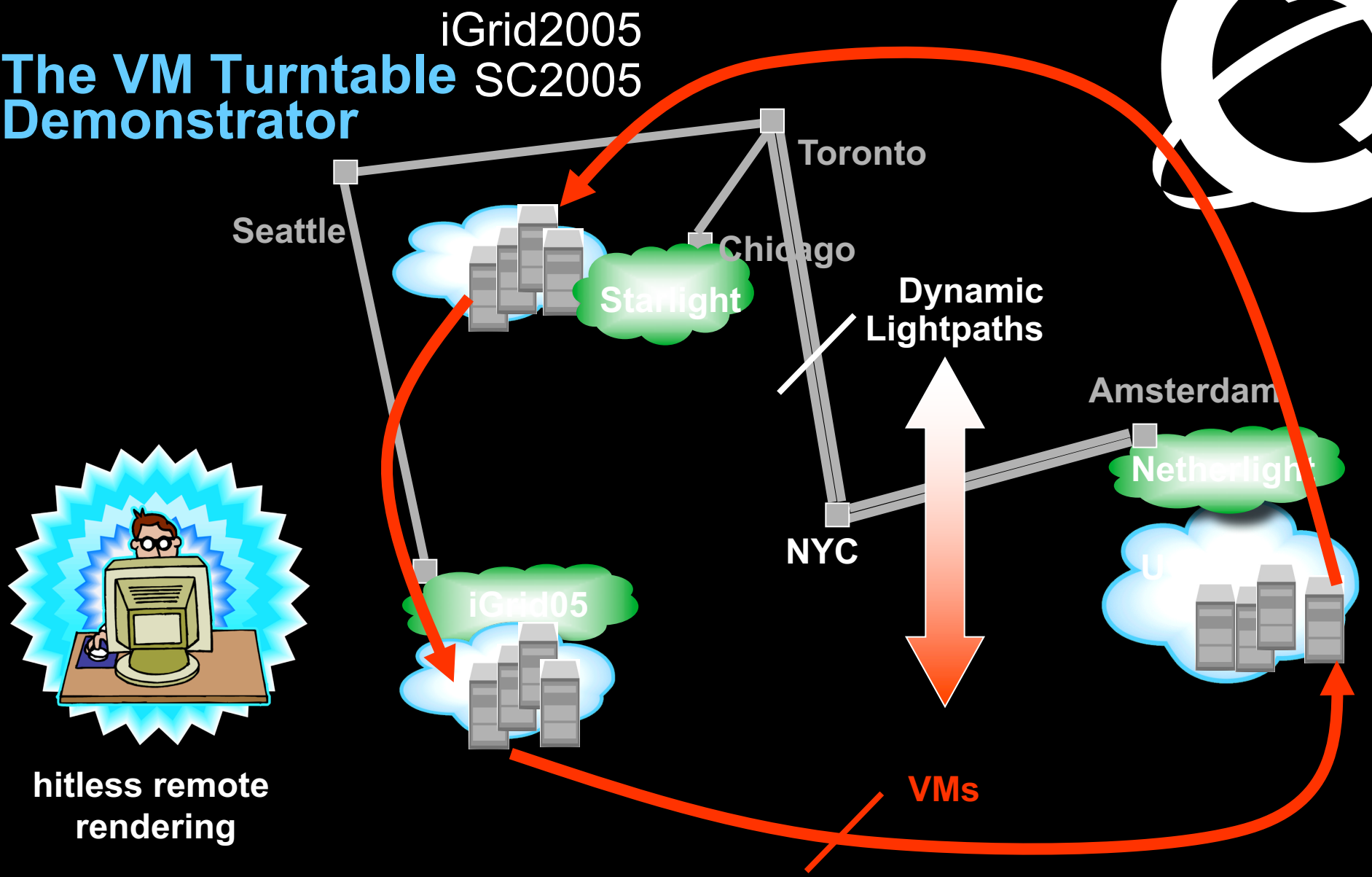
e2.edge2.as400

```
KIND: router
COMPUTE#DISKIMAGE: 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#img-router
COMPUTE#SPECIFIC:CE: exogeni#XOSmall
IC2#WORKERNODEID: uva-nl-w1
REQUEST#HASRESERVAT...: request#Active
REQUEST#INDOMAIN: uvanlvm/site.rdf#uvanlvm/site/Domain/vm
CPU#PCT: 27
```

Service is restored



# The VM Turntable Demonstrator



The VMs that are live-migrated run an iterative search-refine-search workflow against data stored in different databases at the various locations. A user in San Diego gets hitless rendering of search progress as VMs spin around

# Experiment outcomes

## Note, this was in 2005!



We have demonstrated seamless, live migration of VMs over WAN

For this, we have realized a network service that

- Exhibits predictable behavior; tracks endpoints

- Flex bandwidth upon request by credited applications

- Doesn't require peak provisioning of network resources

Pipelining bounds the downtime in spite of high RTTs

- San Diego – Amsterdam, 1GE, RTT = 200 msec, downtime  $\leq$  1 sec

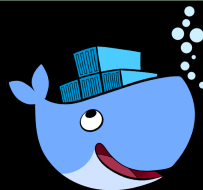
- Back to back, 1GE, RTT = 0.2-0.5 msec, downtime =  $\sim$ 0.2 sec\*

*\*Clark et al. NSDI 05 paper. Different workloads*

VM + Lightpaths across MAN/WAN are deemed a powerful and general alternative to RPC, GRAM approaches

We believe it's a representative instance of active cpu+data+net orchestration

# Secure Policy Enforced Data Processing



- Bringing data and processing software from competing organisations together for common goal
- Docker with encryption, policy engine, certs/keys, blockchain and secure networking
- Data Docker (virtual encrypted hard drive)
- Compute Docker (protected application, signed algorithms)
- Visualization Docker (to visualize output)

Org 1

Org 2

Untrusted Unsecure Cloud or SuperCenter

Secure Virtual PC

Data-1

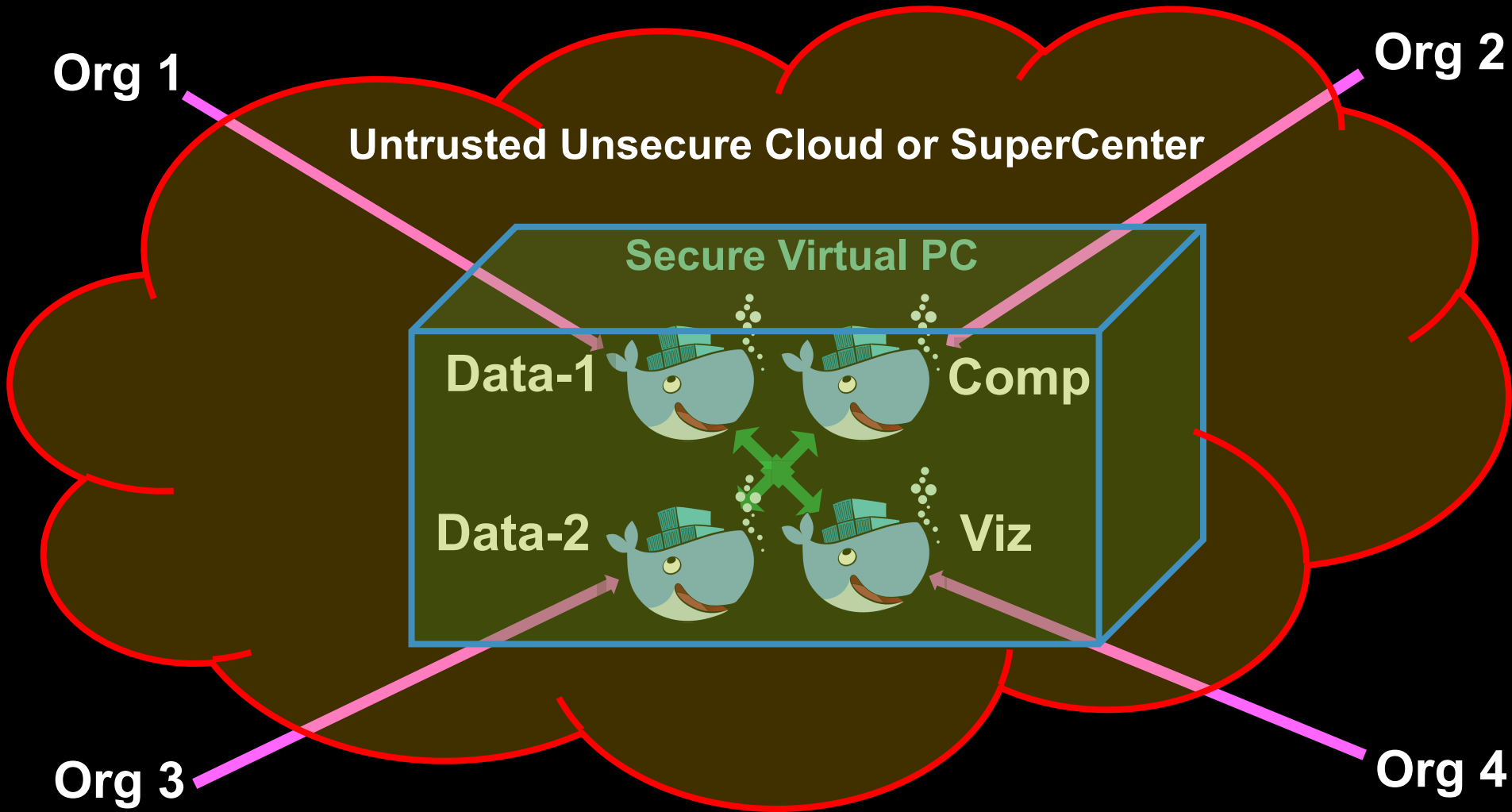
Comp

Data-2

Viz

Org 3

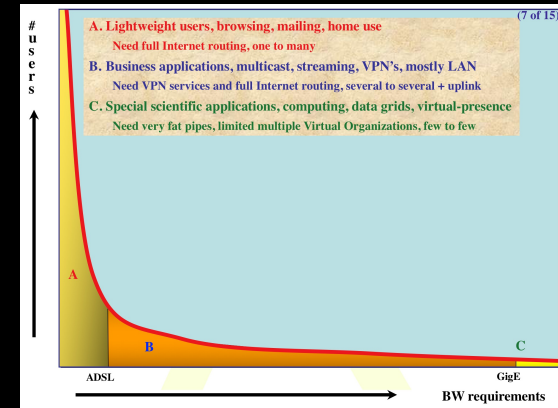
Org 4





# Areas of research

- Each domain its own AI on networks.
  - Multiple AI's fighting on my behalf?
- A-B-C slide
  - Where makes what AI sense?
- Many layers of complexity and abstraction.
  - Can AI help to understand and debug?
  - Can it explicitly understand? Reveal a model?
- Probabilities are badly understood in AI
  - How to deal with false positives?
  - Ethical issues?
  - Trust issues?
  - Intention issues?



# Critical notes

- We created complexity
- Huge number of actors (devices)
- Millions of lines of codes
- We have shrinking trust in the Internet
- Let's throw in another hundred-thousand lines of code! Good luck...
- Complexity encapsulation
- Do we have enough information for RL - ML?
- Do we understand what the Machine needs to learn?

# Acknowledgements

## WP 20.3 SeSI: Security of (Virtual) e-Science Infrastructure

Cees de Laat

Matthijs Koot, Leon Gommans, Guido van 't Noordeinde

overhead  
production



## WP 20.11 SARNET: Security Autonomous Response with programmable NETWORKS

Cees de Laat

Leon Gommans, Rodney Wilson, Rob Meijer  
Tom van Engers, Marc Lyonnais, Paola Grosso, Frank Fransen,  
Ameneh Deljoo, Ralph Koning, Ben de Graaff, Gleb Polevoy

overhead  
production



Why?



**Because we can!**