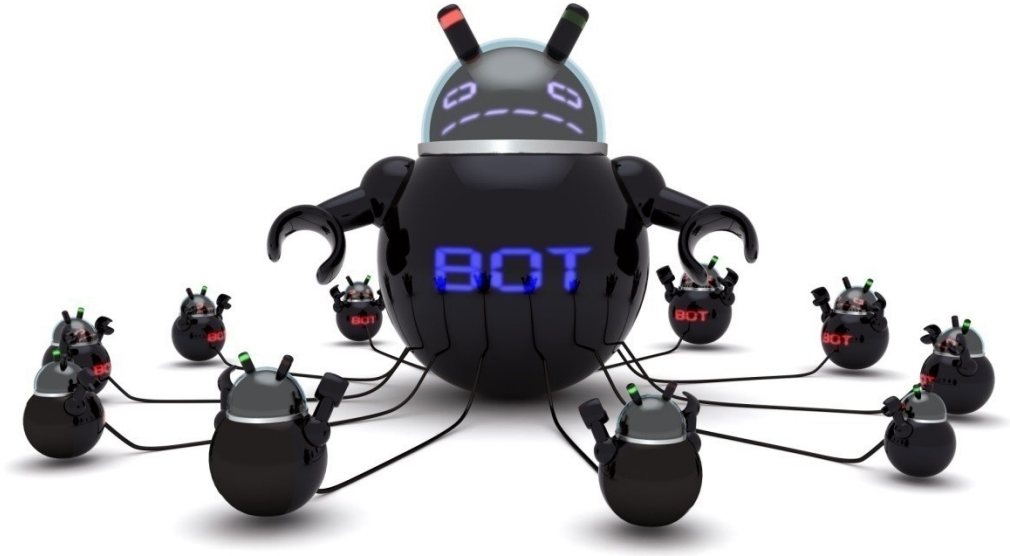
A General-purpose Laboratory for Large-scale Botnet Experiments

Thomas Barabosch, *Sebastian Eschweiler, Mohammad Qasem, Daniel Panteleit, Daniel Plohmann and Elmar Gerhards-Padilla*



http://images.techhive.com/images/article/2013/04/botnet-100034898-orig.jpg

http://michaelhyatt.com/wp-content/uploads/2009/06/the-wow-is-in-the-details1.jpg

http://www.doc.govt.nz/pagefiles/58827/big-picture-223.jpg

Fraunhofer FKIE

Botnet Analysis Approaches

- *Mathematical modelling*
- *Stochastic simulation*
- *Real world data analysis*
- *In-laboratory emulations*

Reasons for us to design a new laboratory

- *Previous work already exists, e.g. Deter or SecSI/LHS labs*
- *Need for own laboratory due to confidentiality requirements*
- *Complementary analysis to our in-house reverse engineering process*
- *Long term goal: improving the state-of-the-art*

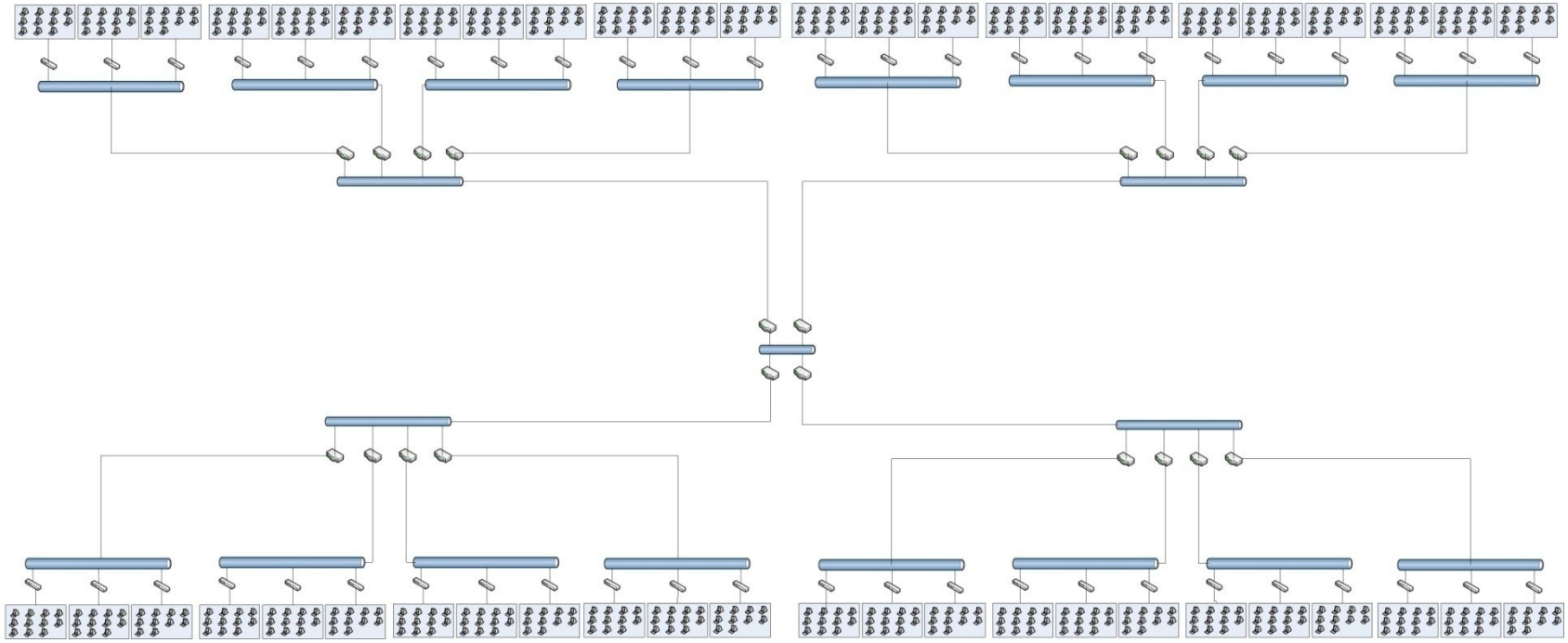
Design of our Botnet Analysis Laboratory

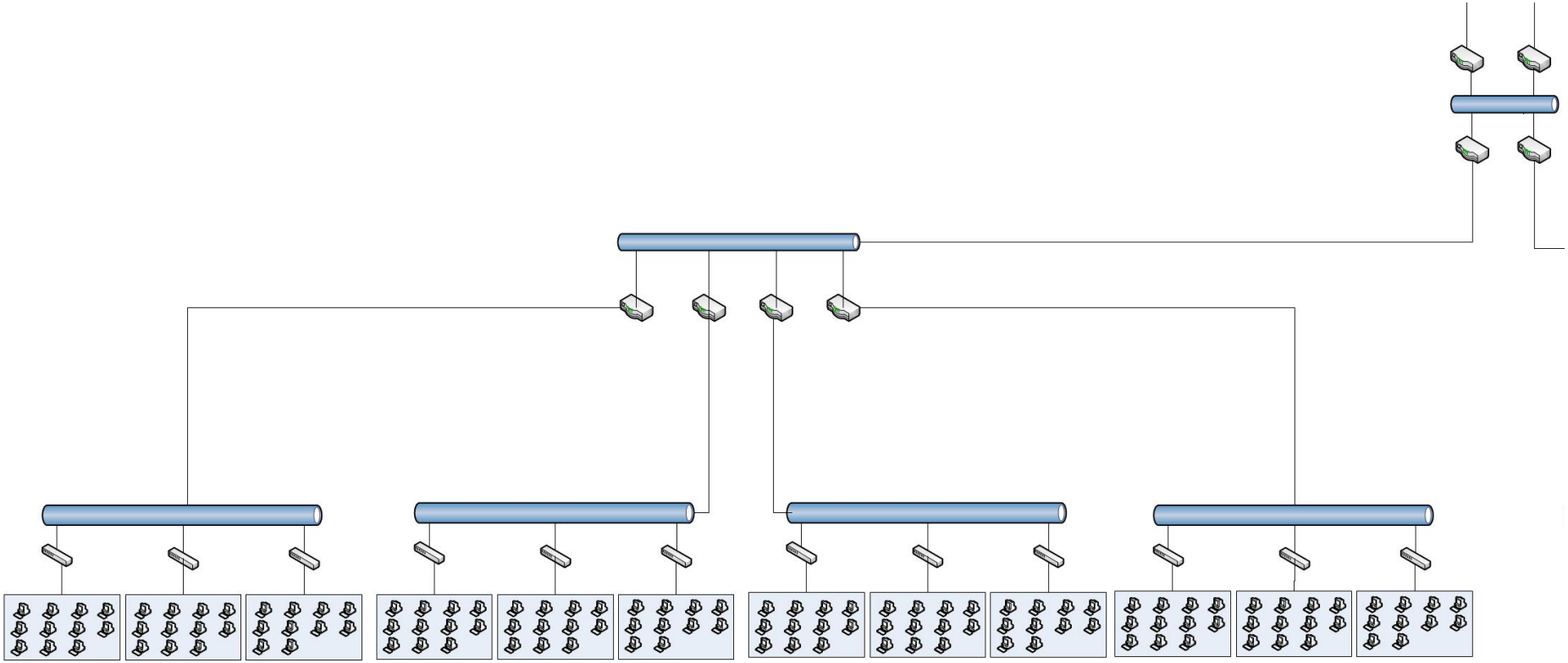
Design Criteria

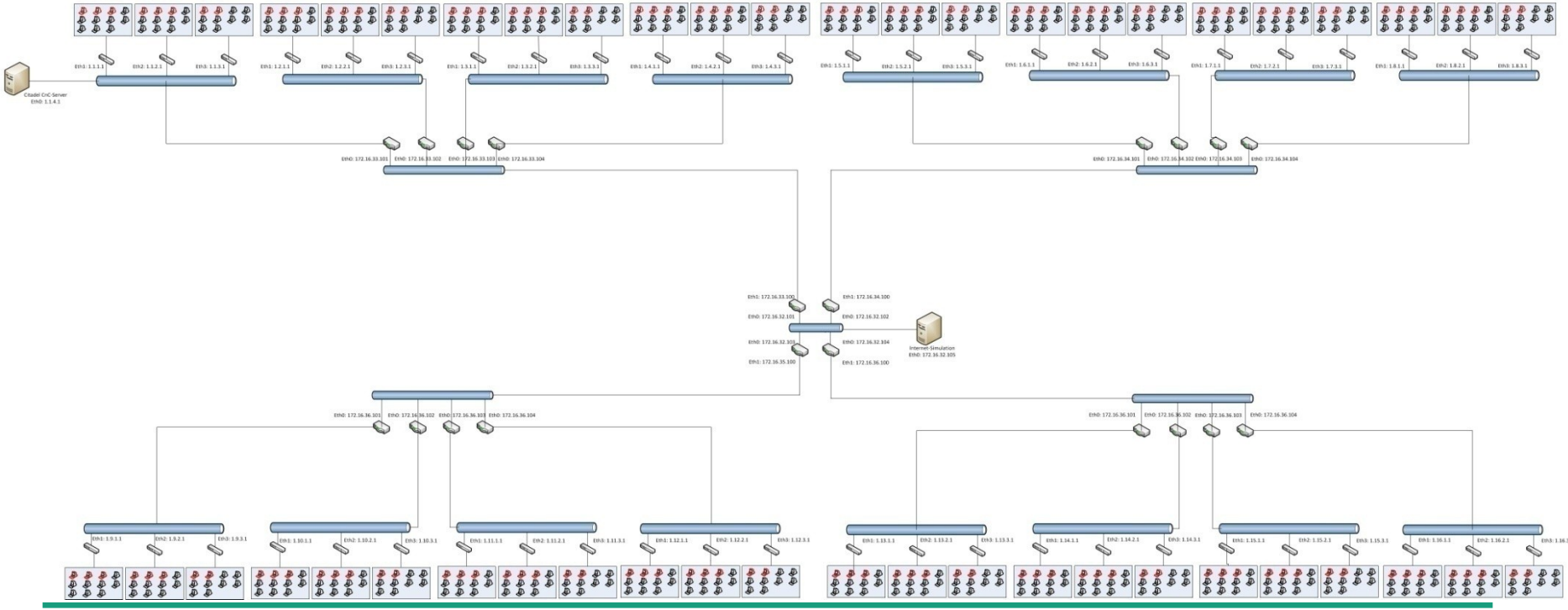
- *Design criteria based on Calvet et. Al, "Isolated virtualised clusters: testbeds for high-risk security experimentation and training*
  - *Security*
  - *Scale*
  - *Realism*
  - *Flexibility*
  - *Sterilizability*

Architectural key aspects

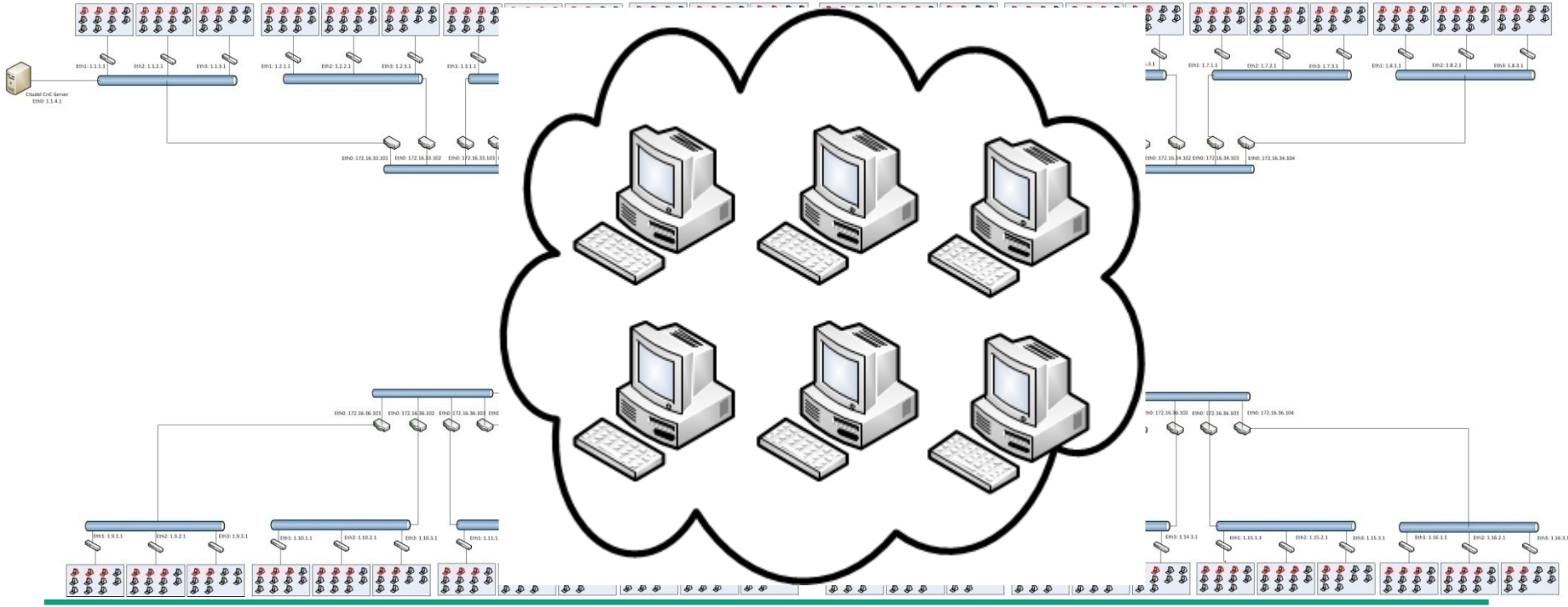
- *Realistic simulation of selected parts of the Internet*
- *Total isolation of the laboratory*
- *Total observability within the laboratory*



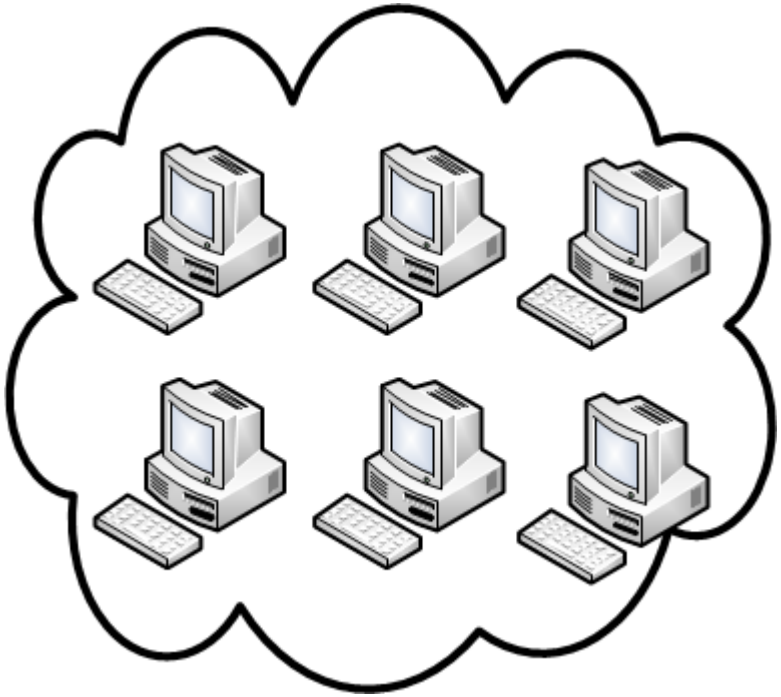




Fraunhofer FKIE

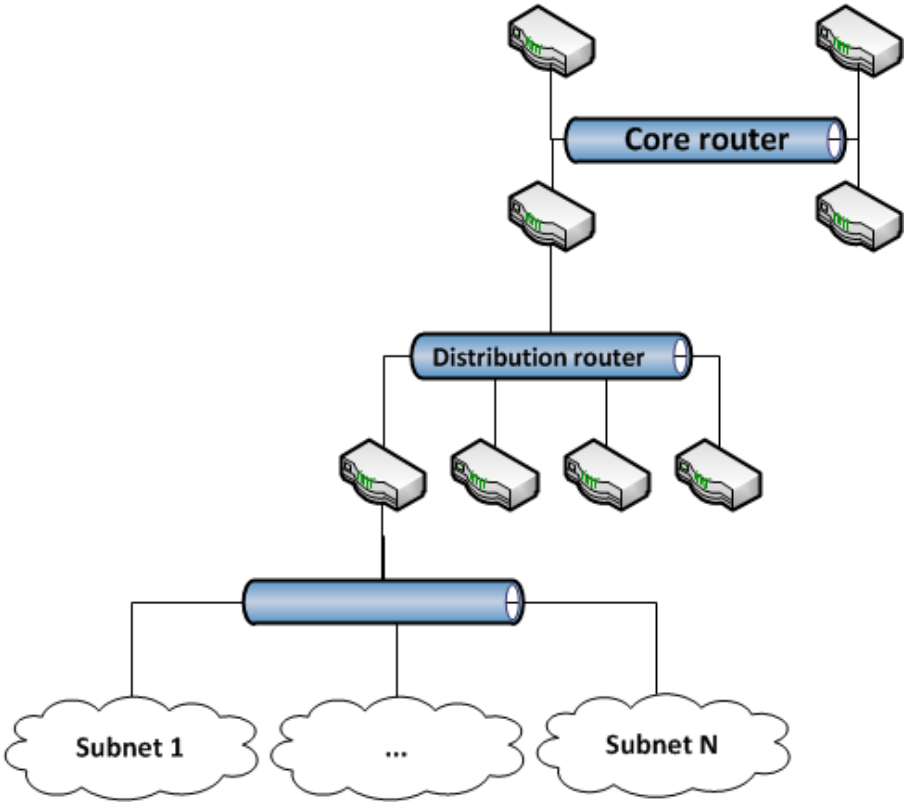


Network nodes



Virtualization

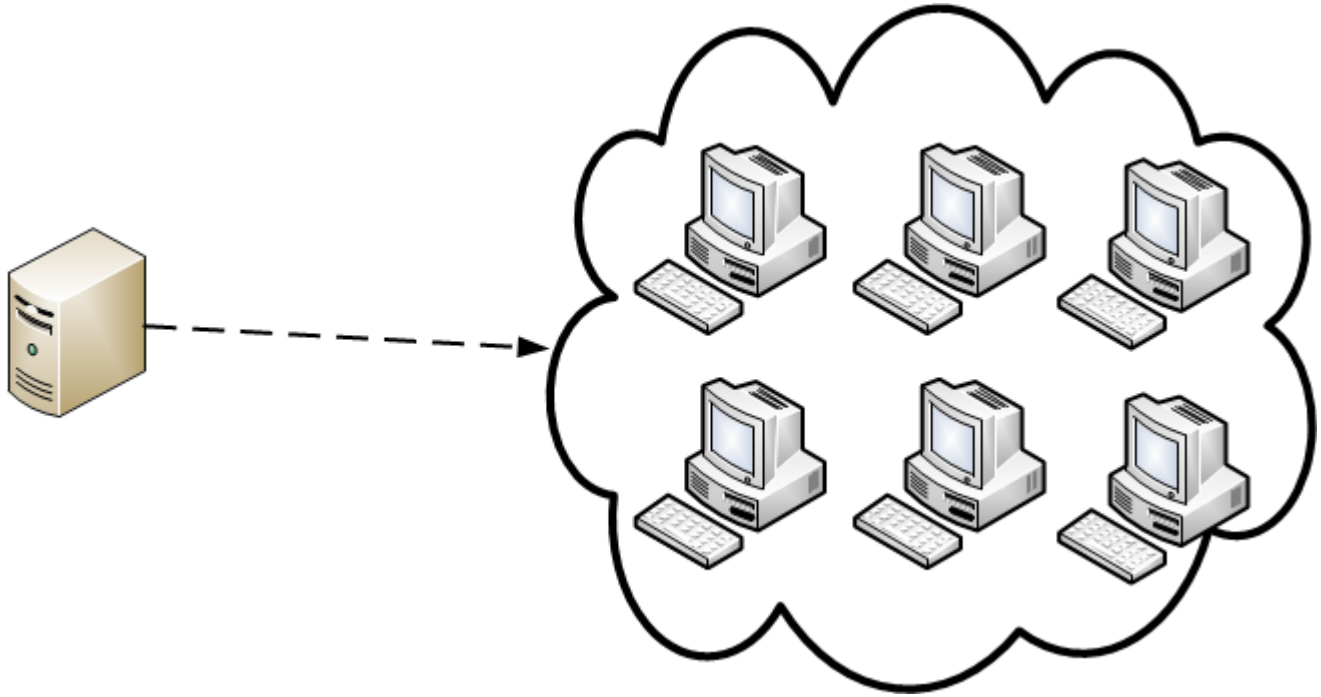
Network topology



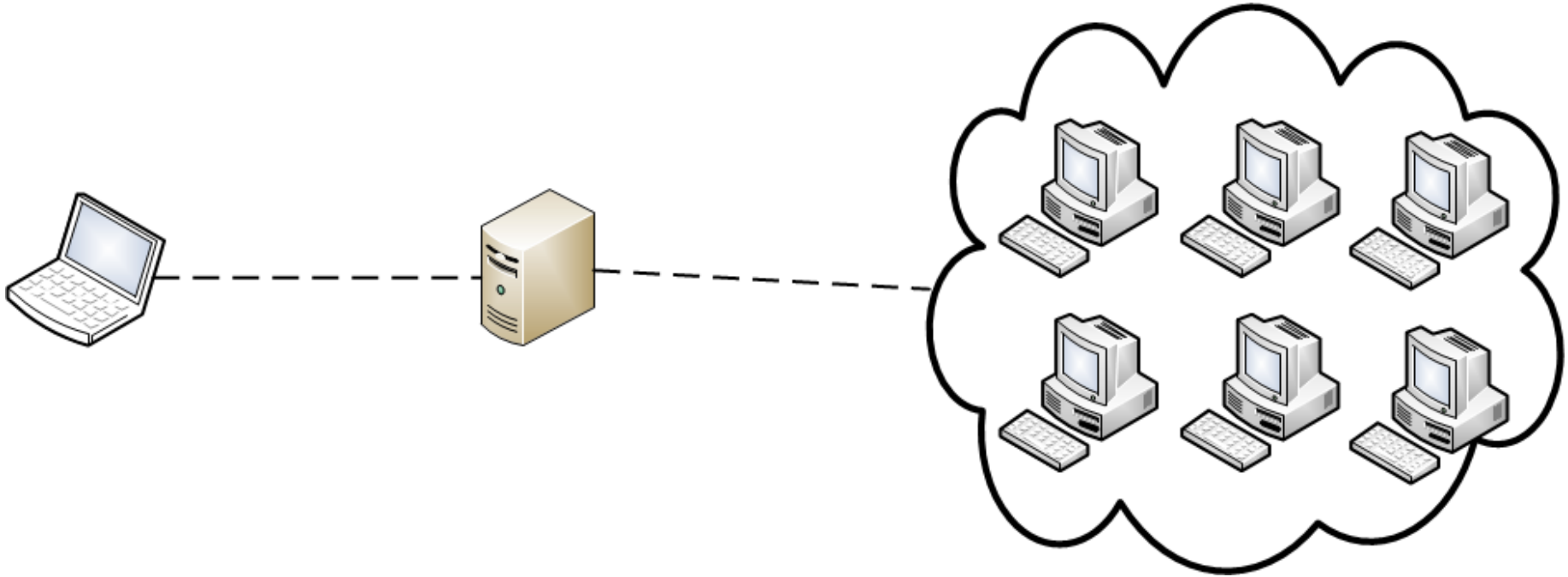
Architectural key aspects

- *Realistic simulation of selected parts of the Internet* ✓
- *Total isolation of the laboratory*
- *Total observability within the laboratory*

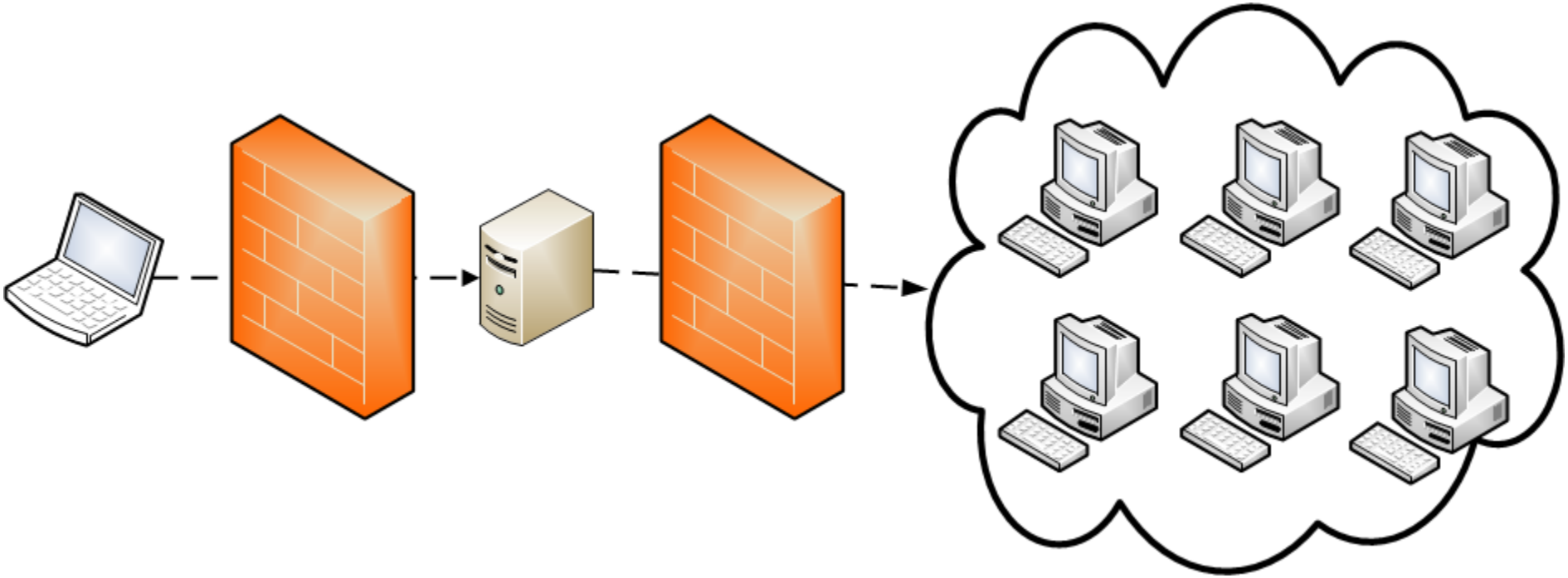
Experiment control



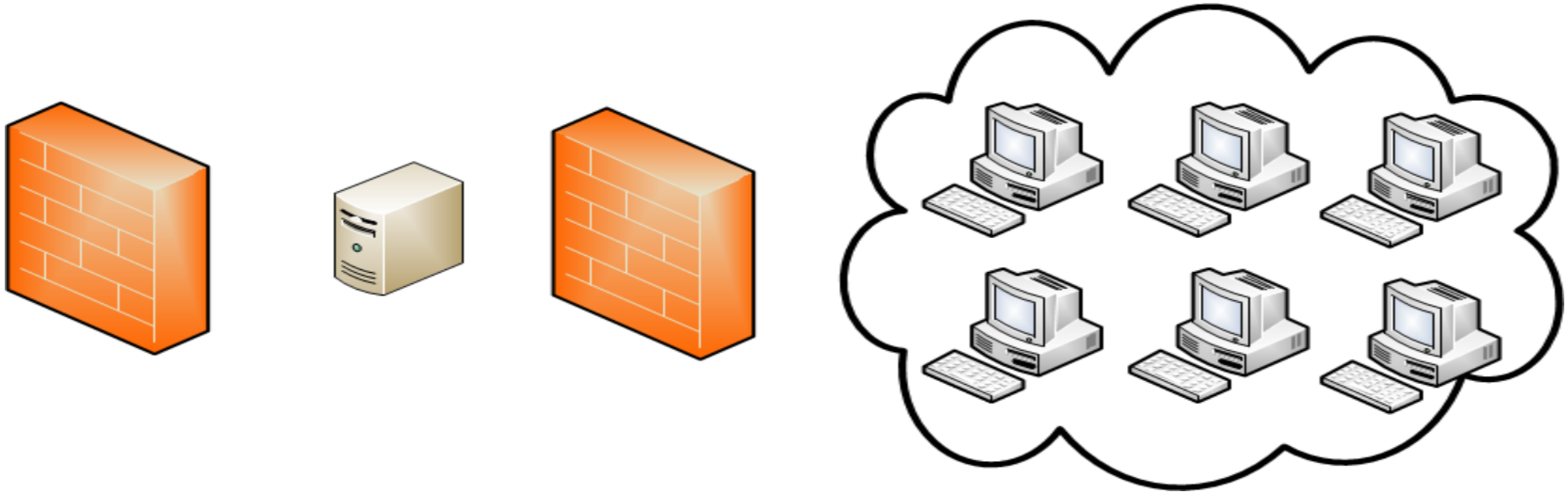
Usability



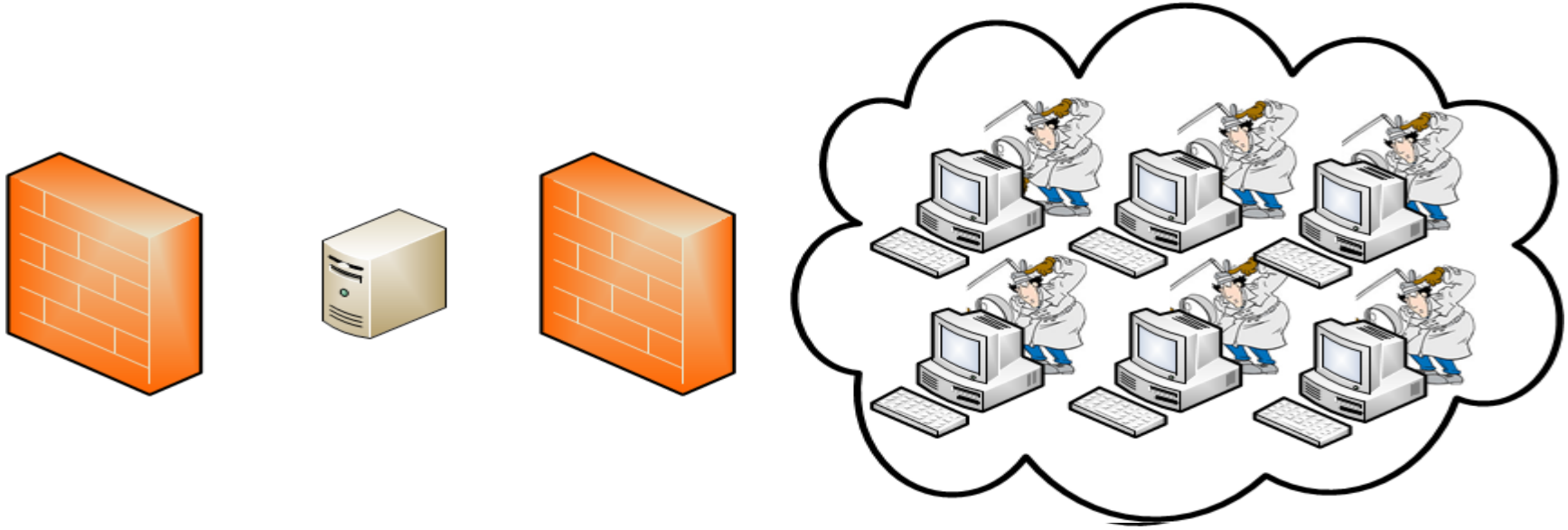
Security



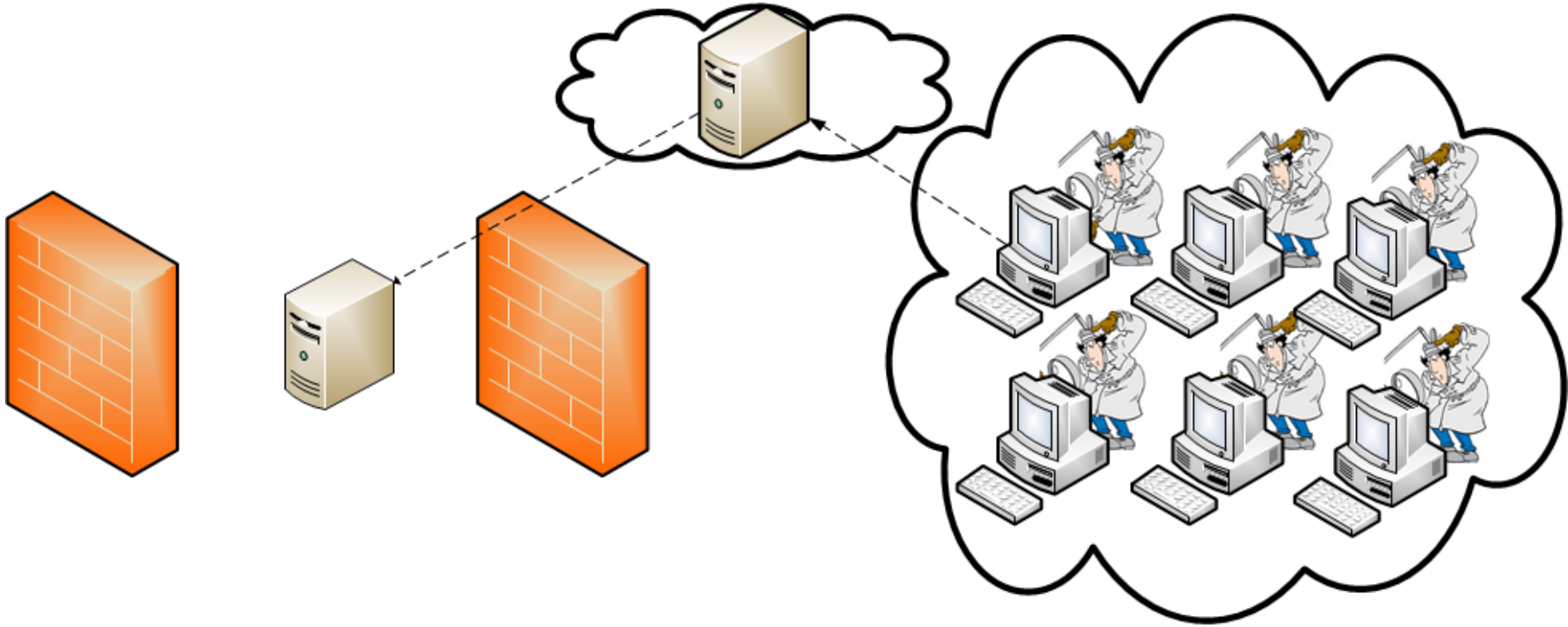
Sensor infrastructure



Sensor infrastructure



Sensor infrastructure



Architectural key aspects

- *Realistic simulation of selected parts of the Internet* ✓
- *Total isolation of the laboratory* ✓
- *Total observability within the laboratory* ✓

Using our Botnet Analysis Labratory

Setting up an experiment: infrastructure

- *Select network-template and VM templates*
  - *Experimenter can also provide his own templates*
- *In case additional infrastructure is needed*
  - *Provide entities*
  - *Adjust DNS*

Setting up an experiment: information gathering

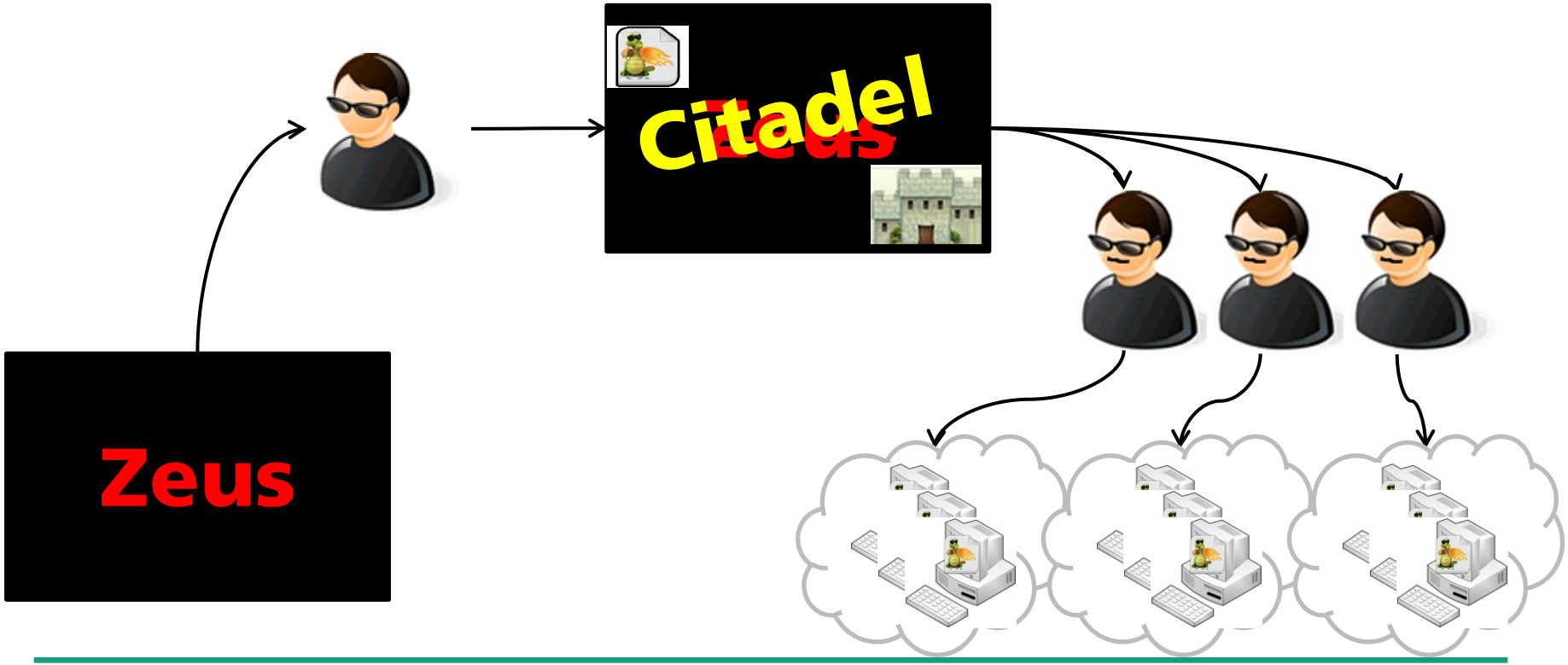
- *Network-based sensors*
  - *Choose routers that should capture network traffic*
  - *Easy adjustment using BPF syntax*
- *Host-based sensors*
  - *Choose/add plugins to Agent*

Setting up an experiment: roll out

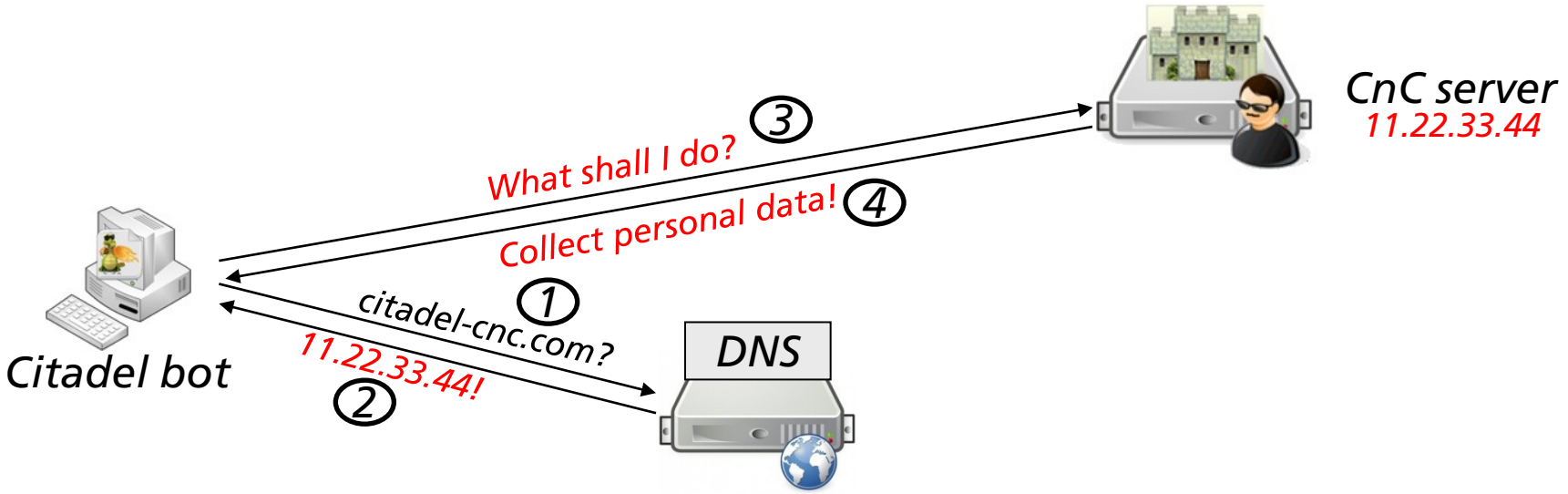
- *Once properly configured: roll it out!*
- *Initial setup time*
  - *32 VMs ~ 50 minutes*
  - *512 VMs ~ 7 hours*

CASE STUDY CITADEL

What is Citadel?

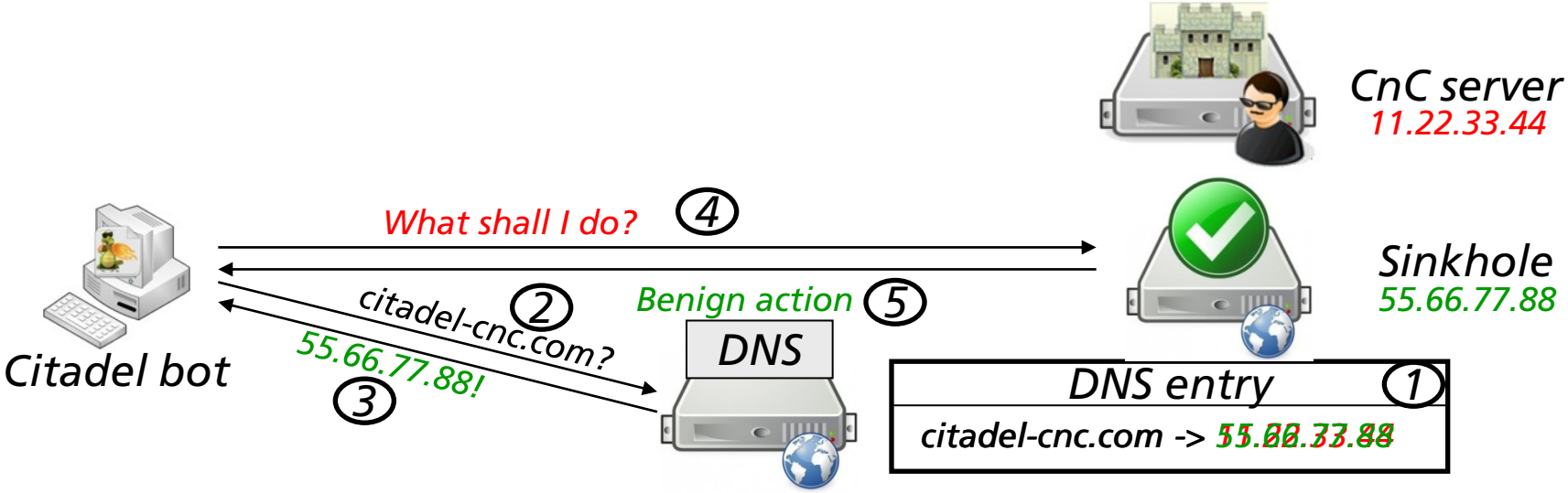


Communication with C&C server



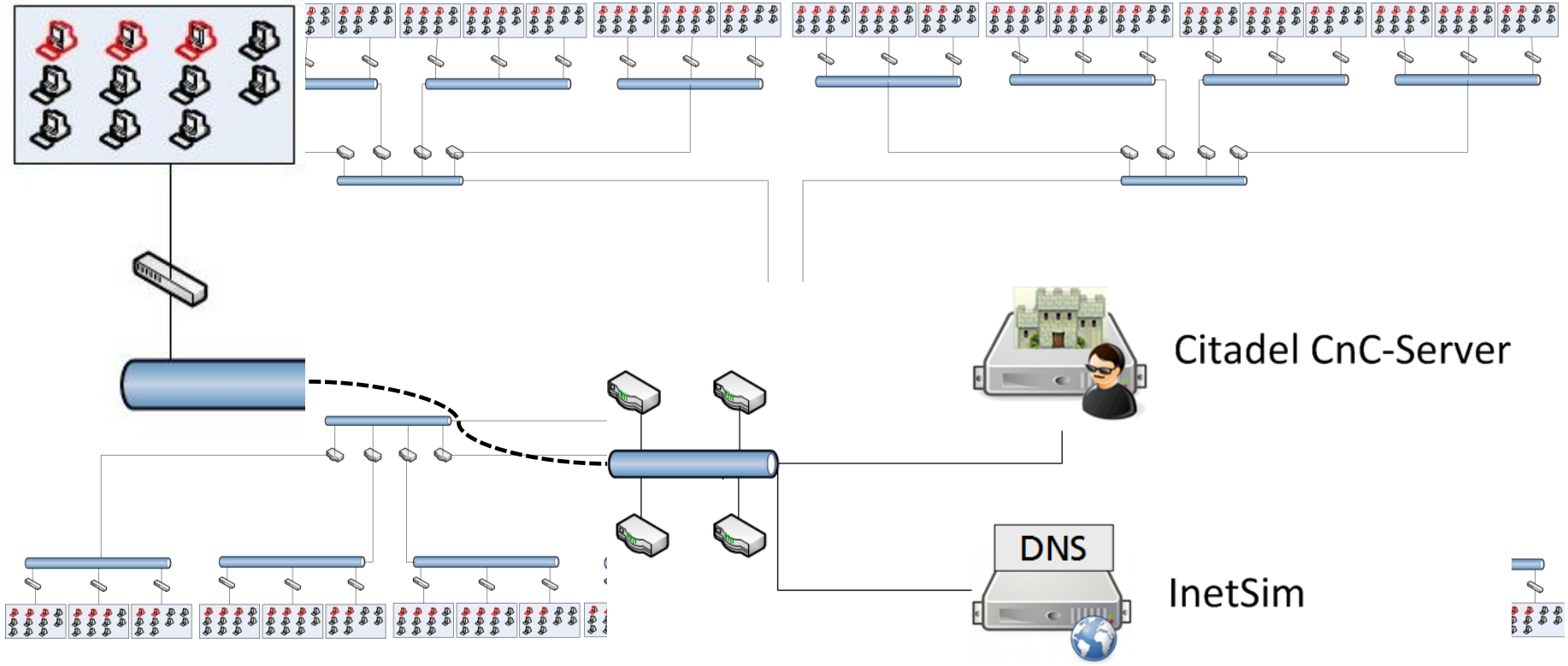
Countermeasure

Takedown via domain replacement



EXPERIMENTS WITH CITADEL

Network infrastructure of the experiment



SETTING UP A BOTNET

Architectural key aspects

- *Realistic simulation of selected parts of the Internet* ✓
- *Total isolation of the laboratory* ✓
- *Total observability within the laboratory* ✓

→ *secure analysis of malware* ✓

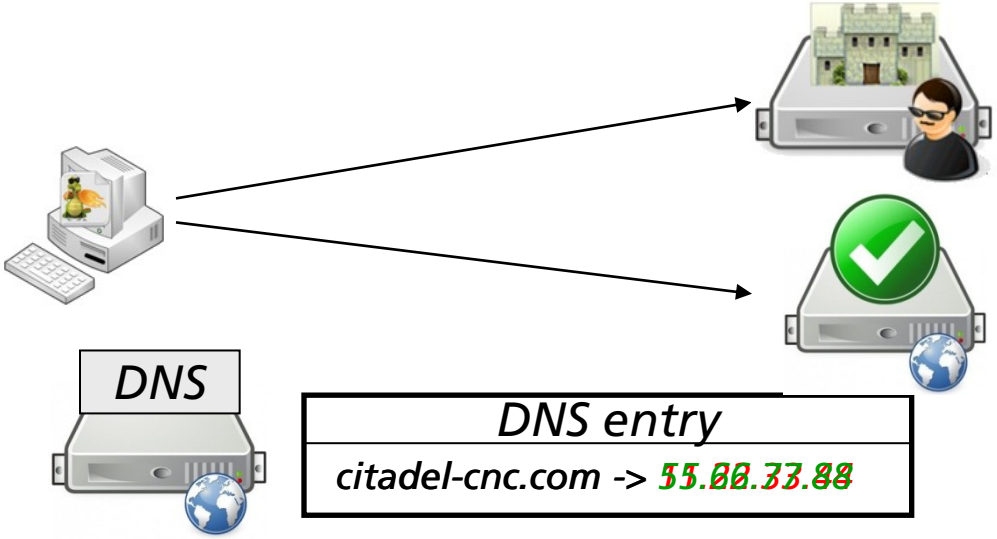
→ *secure testing of countermeasures*

BOTNET TAKEDOWN

Countermeasure

Takedown via domain replacement

- *Malicious DNS entry is replaced by benign DNS entry at certain point in time*



Architectural key aspects

- *Realistic simulation of selected parts of the Internet* ✓
- *Total isolation of the laboratory* ✓
- *Total observability within the laboratory* ✓

→ *secure analysis of malware* ✓

→ *secure testing of countermeasures* ✓

CONCLUSION & OUTLOOK

Conclusion & Outlook

- *Presentation of a general-purpose laboratory for large-scale botnet experiments*
  - *Realistic simulation of selected parts of the Internet*
  - *Total isolation of the laboratory*
  - *Total observability within the laboratory*
- *Future work*
  - *Integration of bare-metal machines*
  - *Automatic provisioning of basis templates*