Bohatei: Flexible and Elastic DDoS Defense

Seyed K. Fayaz, Yoshiaki Tobioka,
Vyas Sekar, Michael Bailey

Carnegie Mellon University

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

https://github.com/ddos-defense/bohatei

Full paper: USENIX Security Symposium 2015

DDoS attacks are getting worse

High cost on victims

Increasing in *number*

Increasing in *volume*

Increasing in *diversity*

DDoS Attacks Cost $40,000 Per Hour

Incapsula, 11/12/2014

FBI WARNS OF INCREASE IN DDOS EXTORTION SCAMS

Threatpost, 7/31/2015

China Appears to Attack GitHub by Diverting Web Traffic

The New York Times, 3/30/2015

Half of companies experience more than five DDoS attacks a year.

Neustar, 2014

The DDoS That Almost Broke the Internet

Cloudflare, 3/27/2013

Wave of 100Gbps 'mega' DDoS attacks hits record level in 2014

Techworld, 7/16/2014

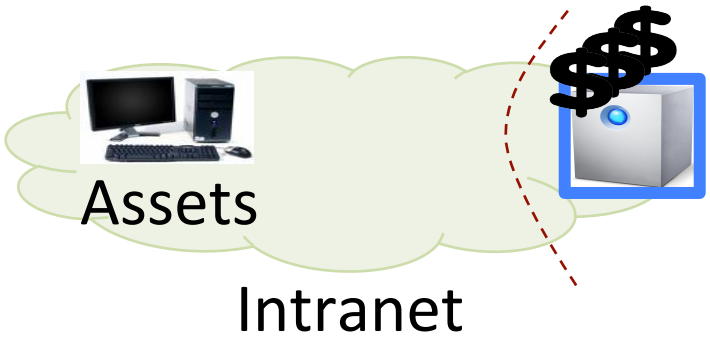
NTP ATTACKS: Welcome to The Hockey Stick Era

Arbor Networks, 2/14/2014

Tsunami SYN Flood Attack

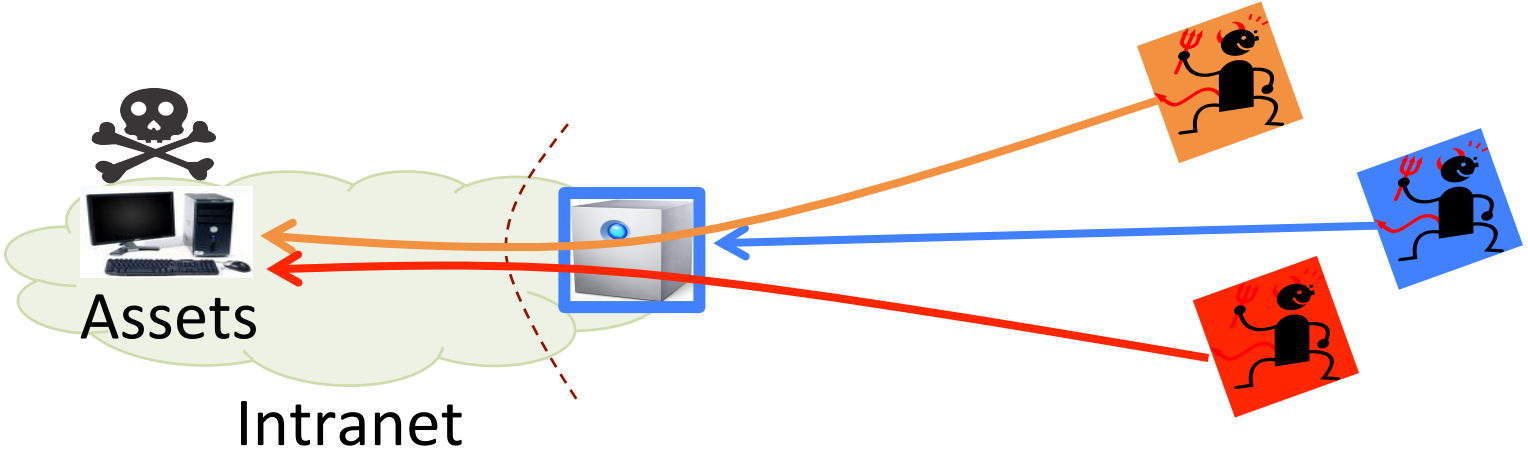
Radware, 10/7/2014

DDoS Defense Today: Expensive Proprietary Hardware

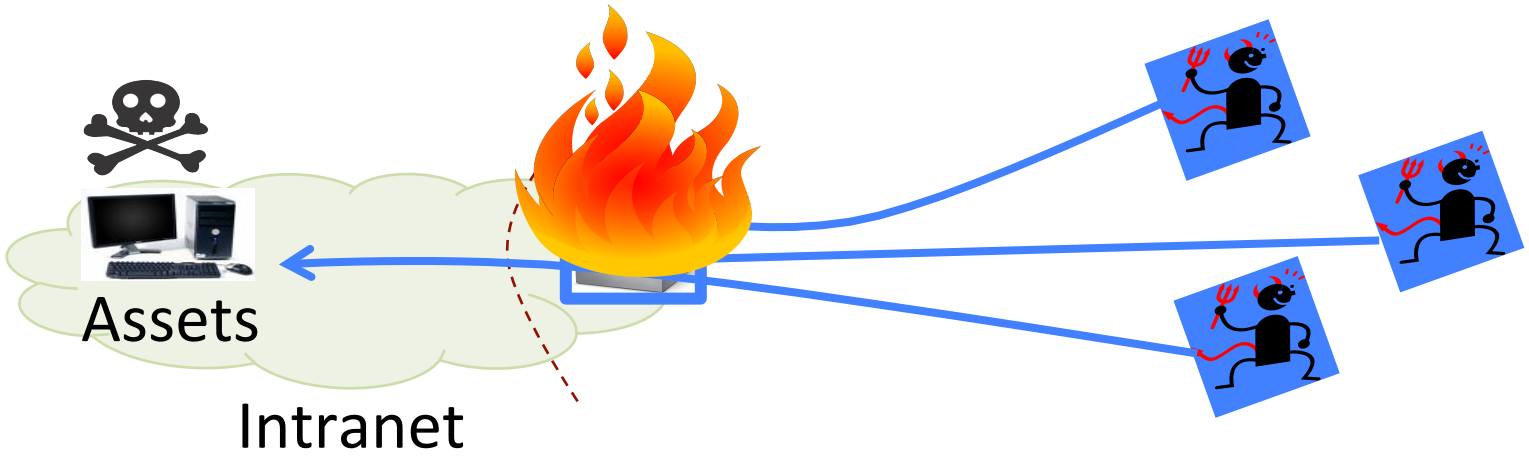


Limitation: Fixed functionality

What if new types of attacks emerge?

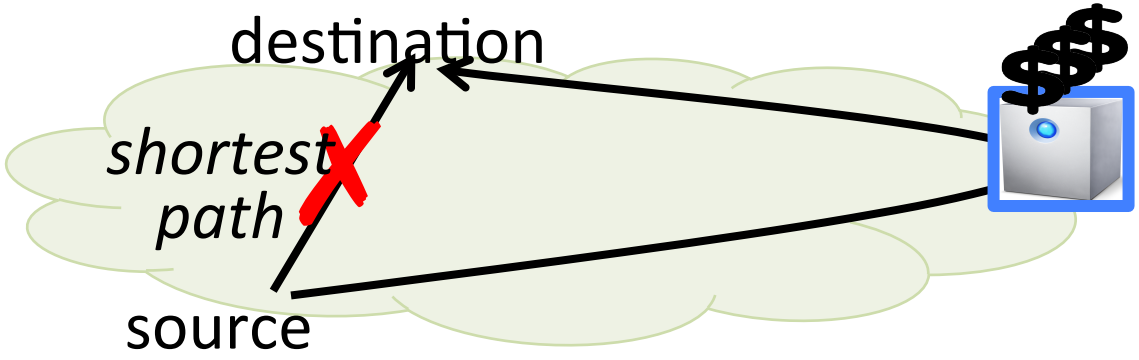


Limitation: Fixed capacity

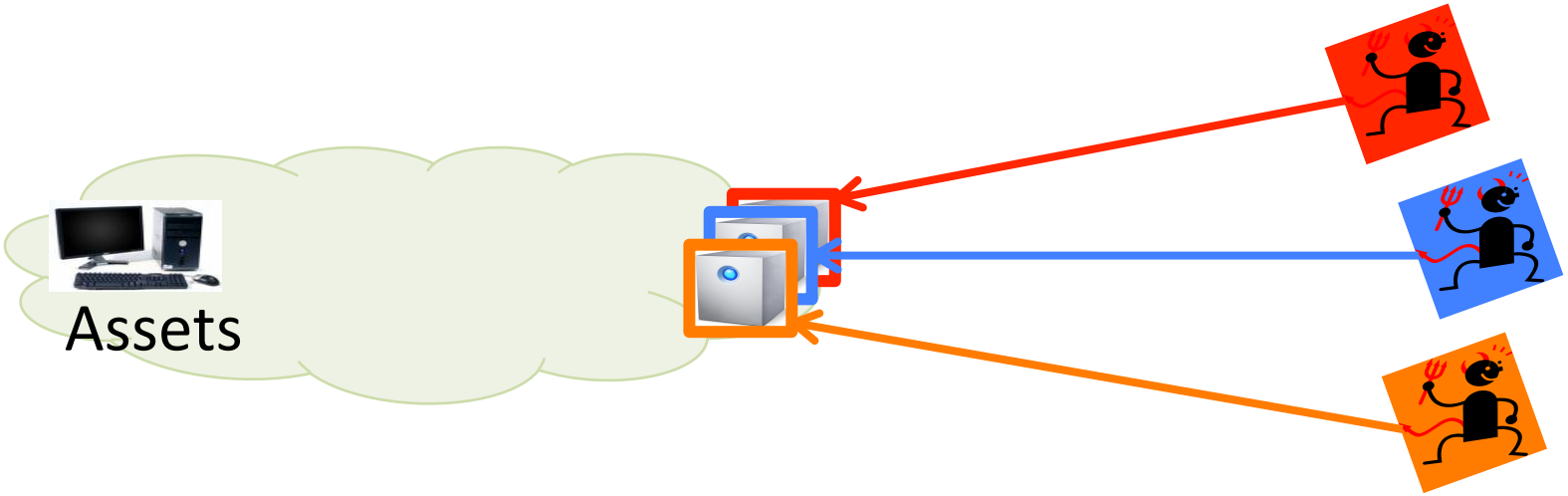


Limitation: Fixed location

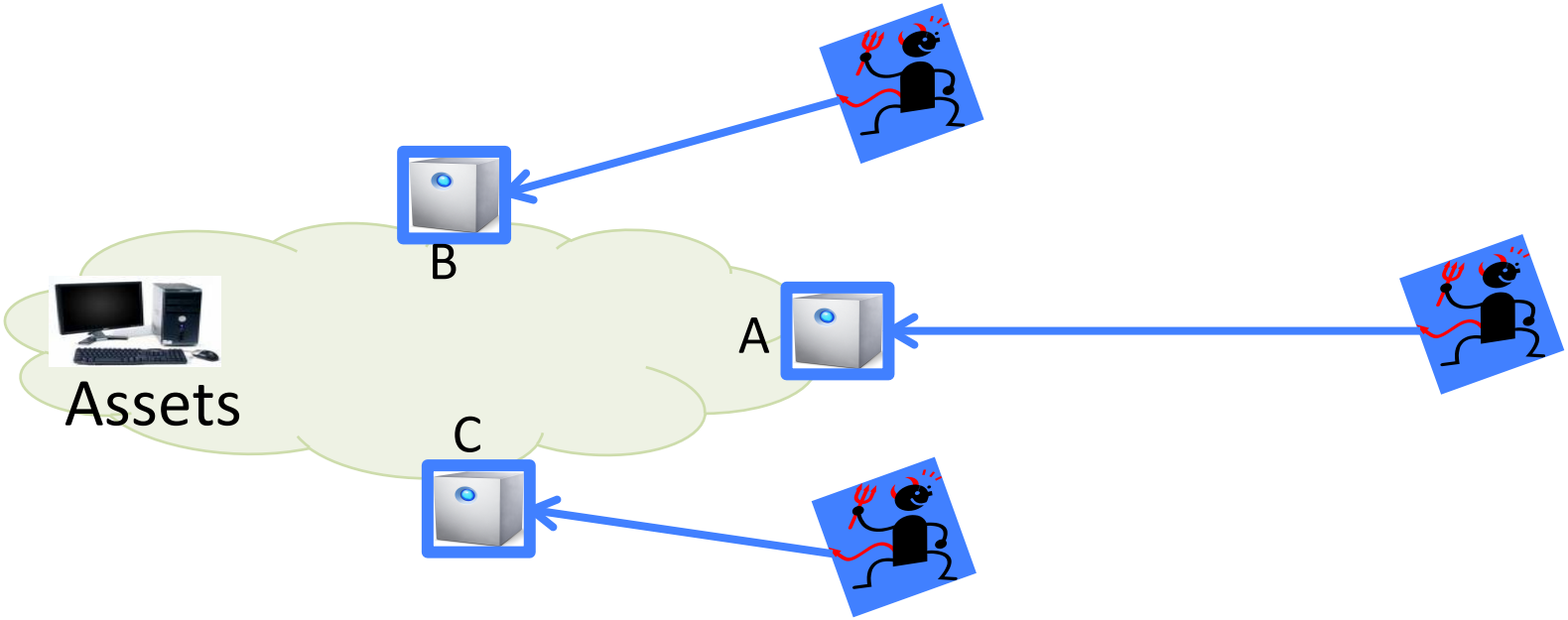
- Additional traffic latency due to waypointing
- Routing hacks to enforce defense



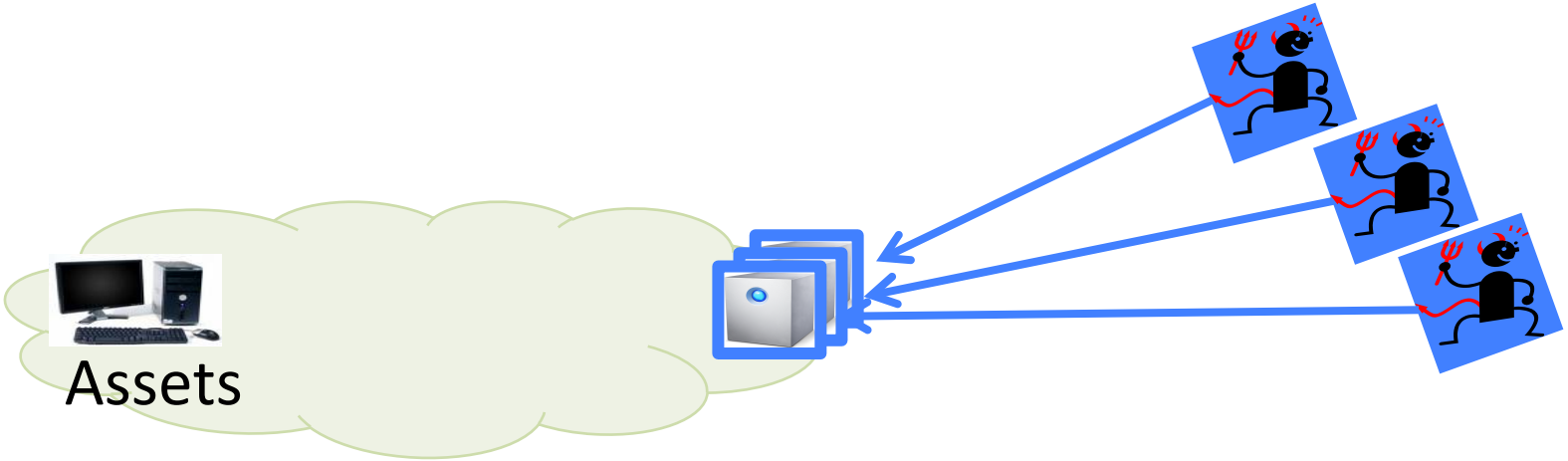
Need flexibility w.r.t. attack type



Need Flexibility w.r.t Attack Locations



Need Elasticity w.r.t. Attack Volume



Bohatei in a nutshell...

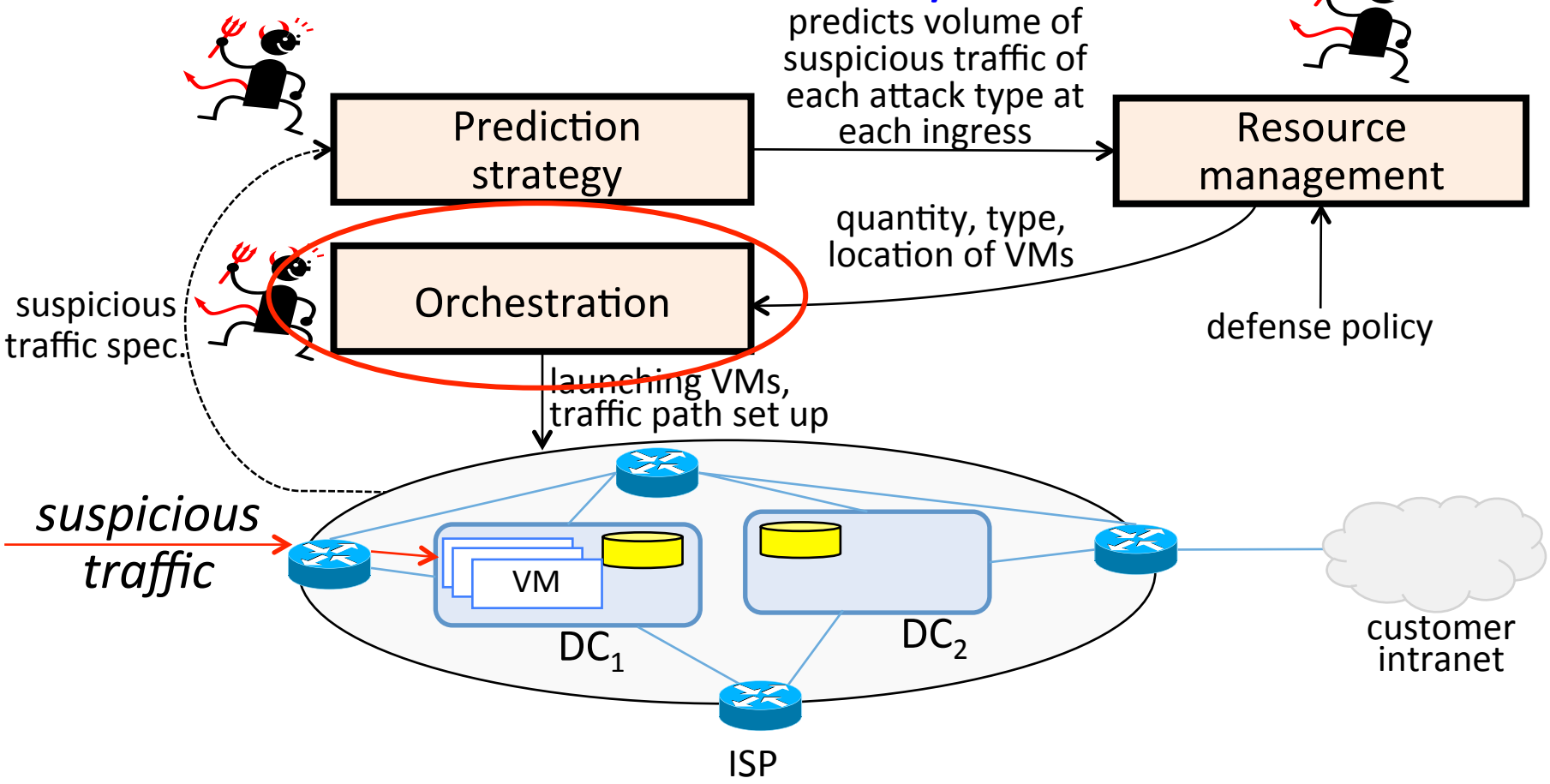
A practical ISP-scale system

for Flexible and Elastic DDoS Defense via

- Software-Defined Networking (SDN) &
- Network Functions Virtualization (NFV)

→ React to 500 Gbps scale attacks in 1 min!

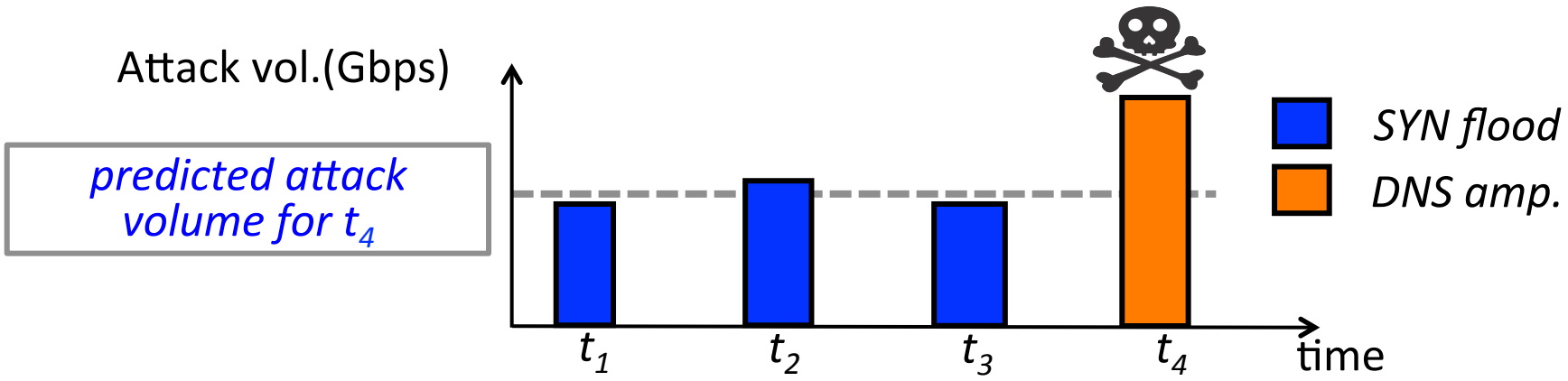
Bohatei Vision:
Flexible + Elastic Defense via SDN/NFV



Dynamic adversaries can game the defense

Adversary's goals:

1. Increase defense resource consumption
2. Succeed in delivering attack traffic



Simple prediction (e.g., prev. epoch, avg) can be gamed

Our approach: Online adaptation

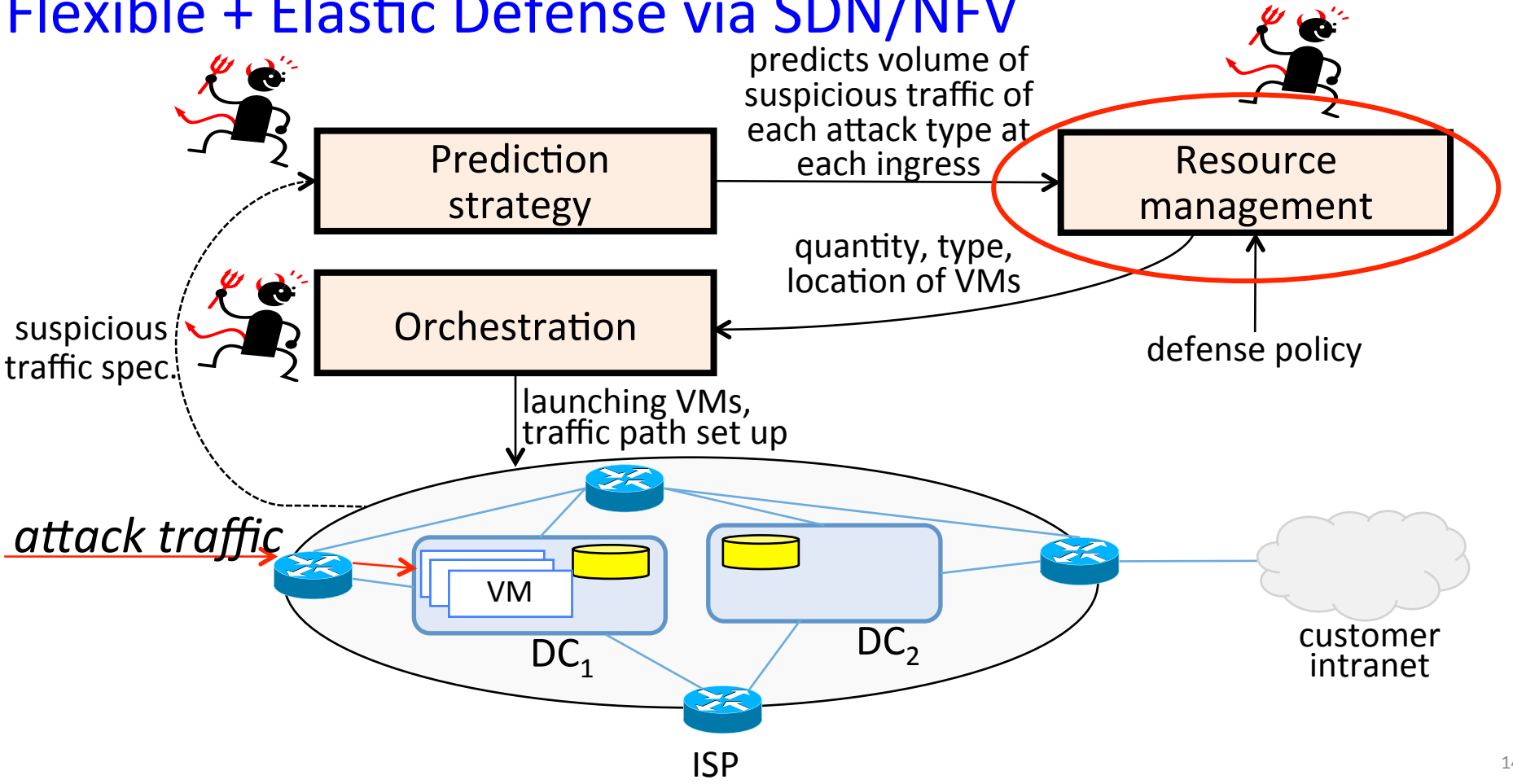
- Metric of Success = "Regret minimization"
  → How worse than best static strategy in hindsight?

- Borrow idea from online algorithms:
  Follow the perturbed leader (FPL) strategy

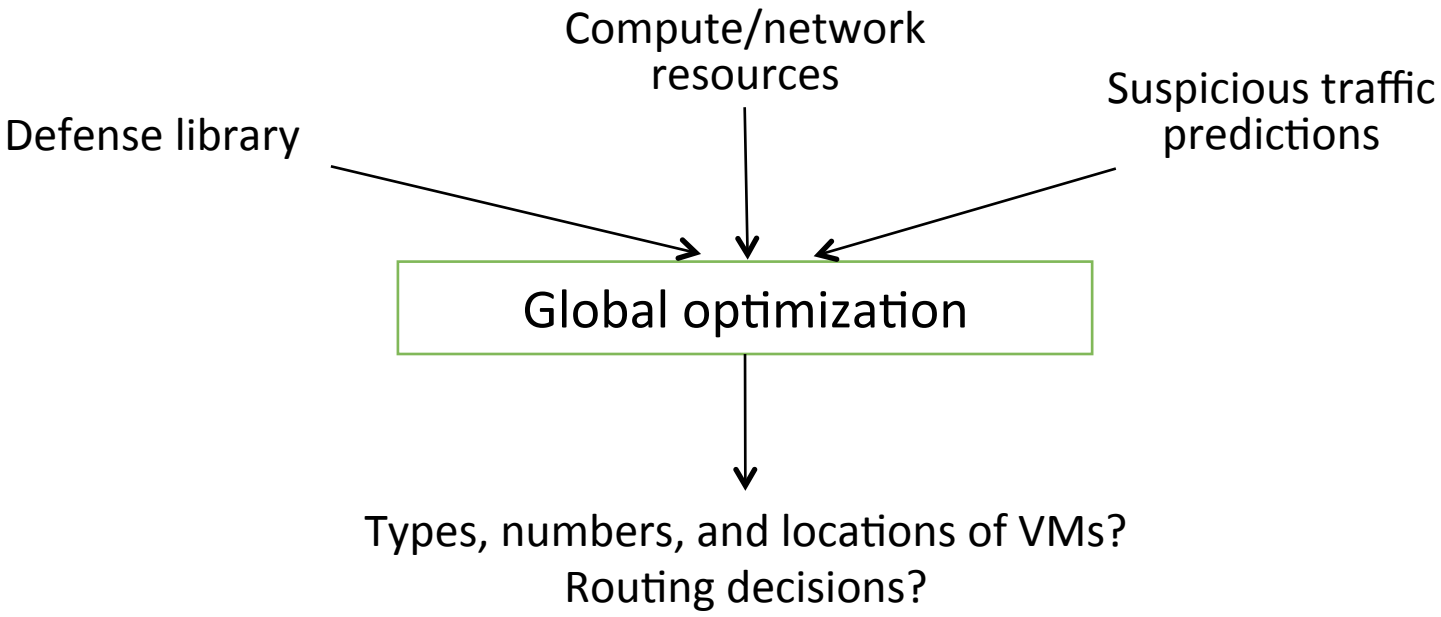
- Intuition: Prediction = F (Obs. History + Random Noise)

- This provably minimizes the regret metric

Bohatei Vision:
Flexible + Elastic Defense via SDN/NFV

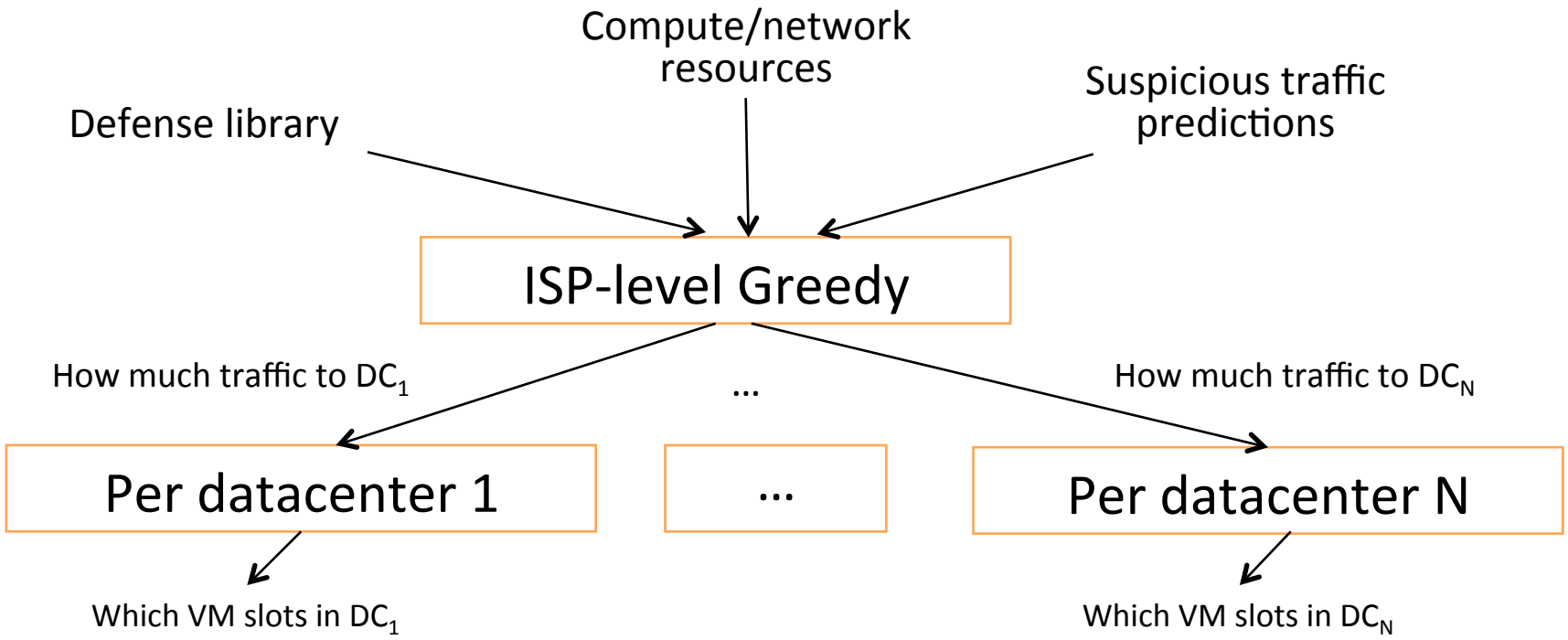


Naïve resource management is too slow!

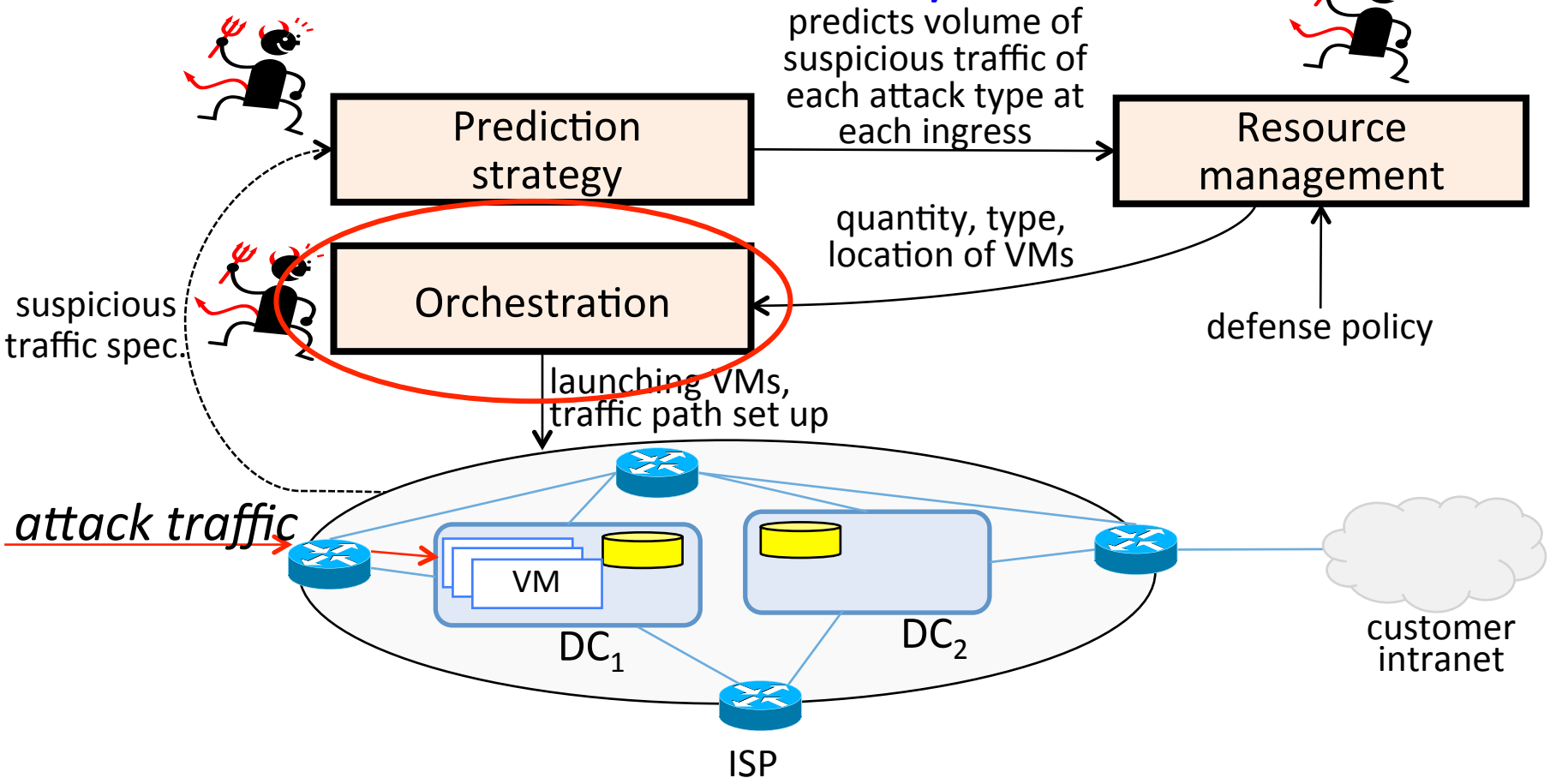


Takes hours to solve…

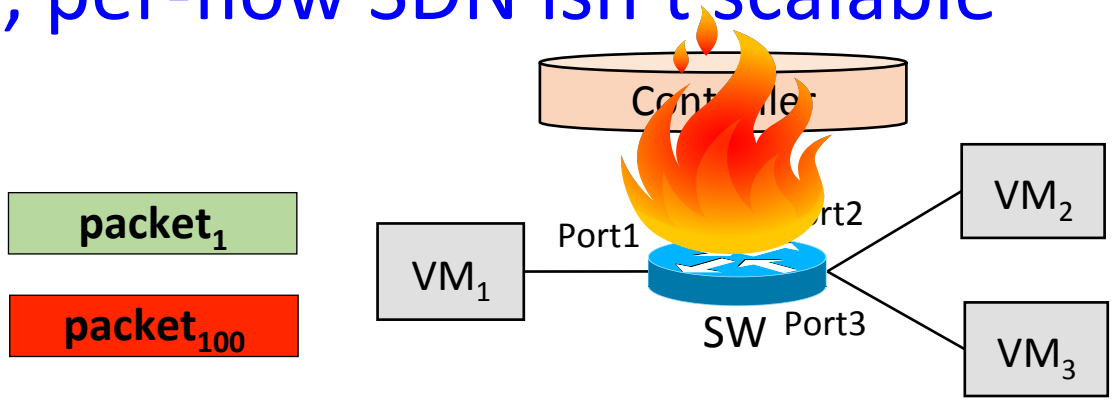
Our Approach: Hierarchical + Greedy



Bohatei Vision:
Flexible + Elastic Defense via SDN/NFV



Reactive, per-flow SDN isn't scalable

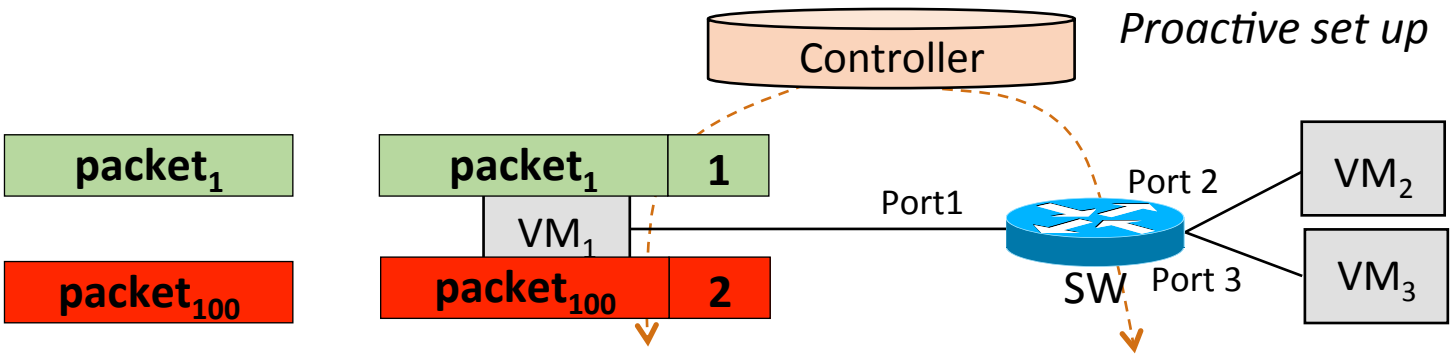


Switch Forwarding Table

Flow	*utPort*
Flow$_1$	2
⋮	⋮
Flow$_{100}$	3

A reactive, per-flow controller will be a new vulnerability

Idea: Proactive tag-based steering



Context	*Tag*
Benign	1
Suspicious	2

Tag	*outPort*
1	Port 2
2	Port 3

Proactive per-VM tagging enables scaling

Implementation and evaluation highlights

Open source implementation

https://github.com/ddos-defense/bohatei

Takeaways:

1. Sub-minute response to various attacks
2. Defense against 500Gbps attacks
3. Successful handling of dynamic attack scenarios

Bohatei: Flexible and Elastic DDoS Defense

Seyed K. Fayaz, Yoshiaki Tobioka,
Vyas Sekar, Michael Bailey

Carnegie Mellon University

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

https://github.com/ddos-defense/bohatei

Full paper: USENIX Security Symposium 2015

Conclusions

- DDoS defense today : Expensive, Inflexible, and Inelastic
- Bohatei: SDN/NFV for flexible and elastic DDoS defense
- Key Challenges: Responsiveness, scalability, resilience
- Main solution ideas:
  - Hierarchical resource management
  - Proactive, tag-based orchestration
  - Online adaptation strategy
- Scalable + Can react to very large attacks quickly!
- Ideas may be applicable to other security problems

Bohatei Controller Workflow

Strategy layer

Predict attack pattern

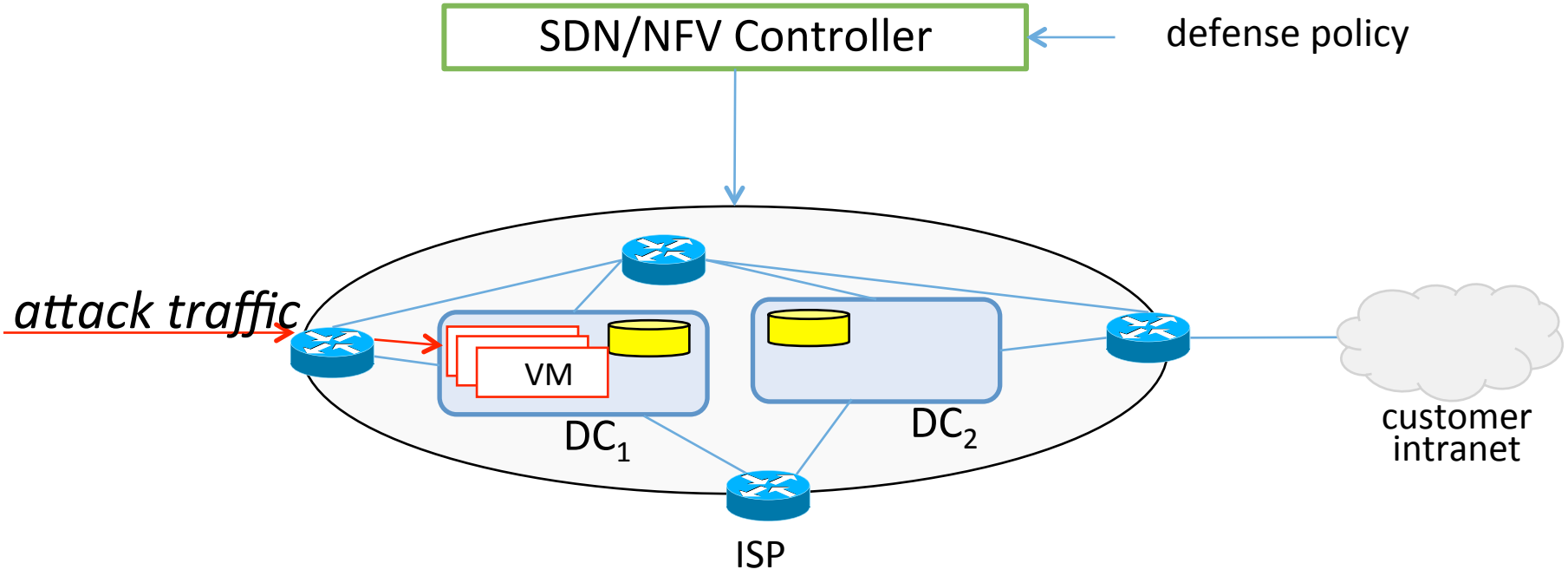
Resource management

Decide how many VMs, what types, where

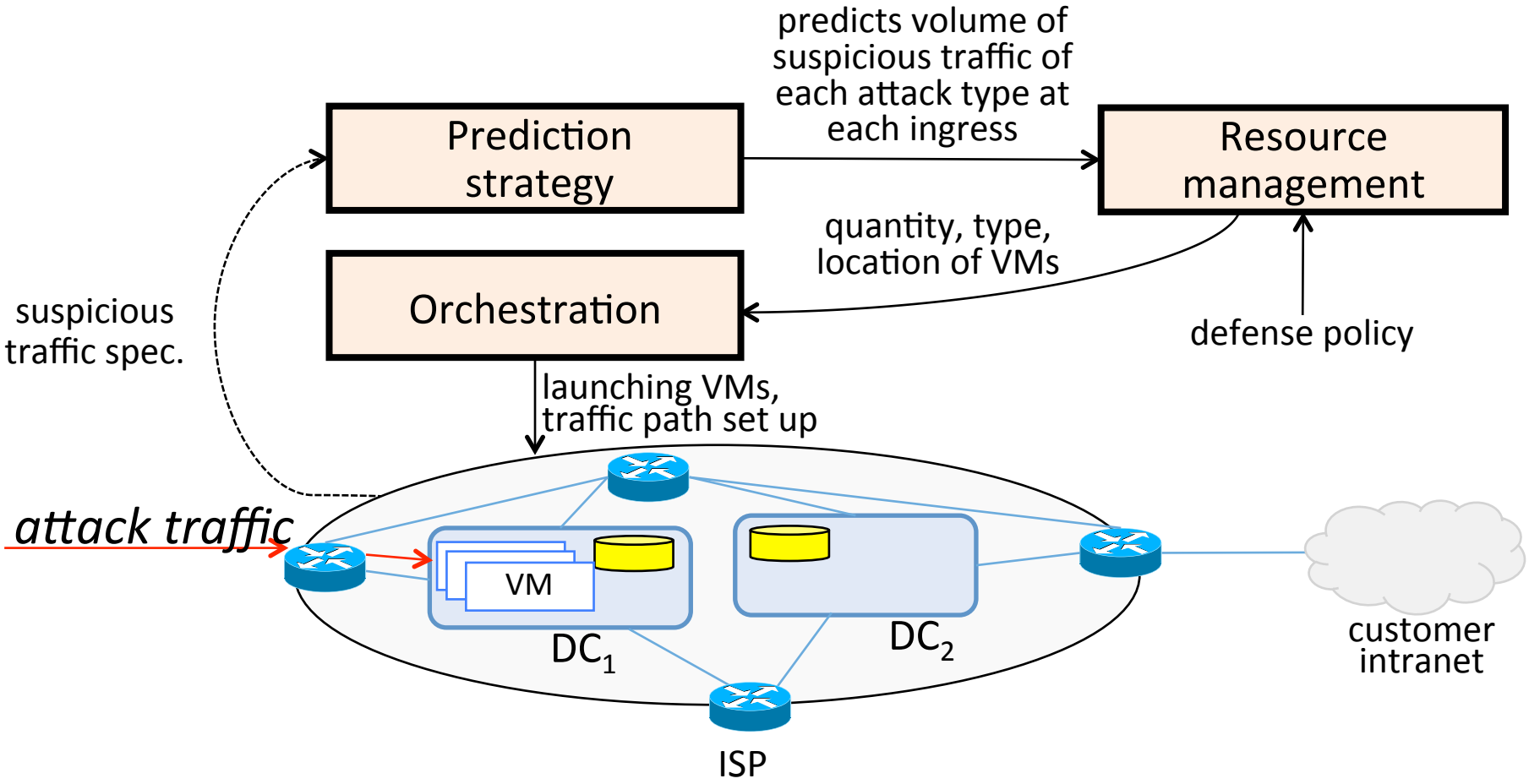
Network orchestration

Configure network to route traffic

Bohatei Vision:
Flexible + Elastic Defense via SDN/NFV



Putting it together



Outline

- Motivation
- Bohatei overview and challenges
- System design
  - Fast resource management
  - Scalable network orchestration
  - Handling dynamic adversaries
- Implementation
- Evaluation
- Conclusions

Outline

- Motivation
- Bohatei overview and challenges
- System design
  - Fast resource management
  - Scalable network orchestration
  - Handling dynamic adversaries
- Implementation
- Evaluation
- Conclusions

Design challenges

Dynamic/General Adversary

→ Need for a responsive resource management

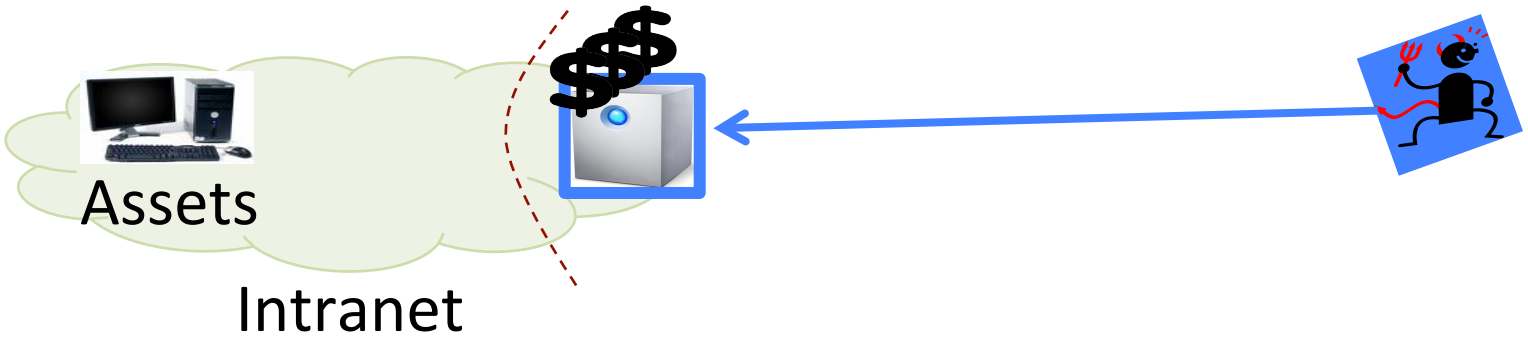
→ Need for resilience to volume adaptation

Using centralized SDN/NFV control

→ Need for scalable orchestration

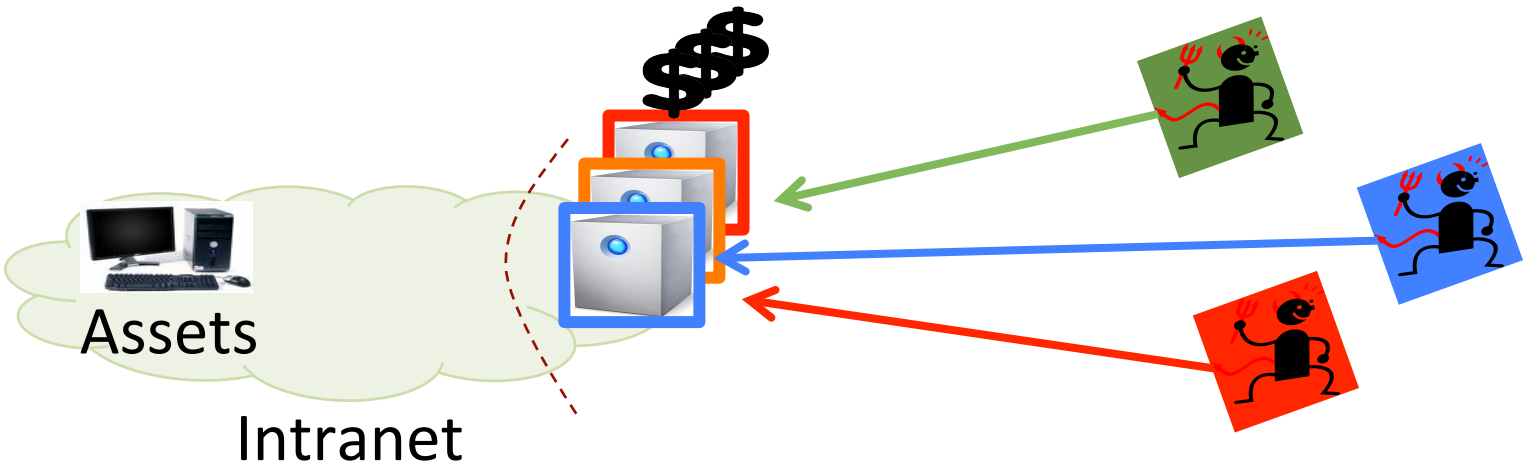
Current approach to DDoS defense

- Expensive
- Fixed functionality
- Fixed capacity
- Fixed location



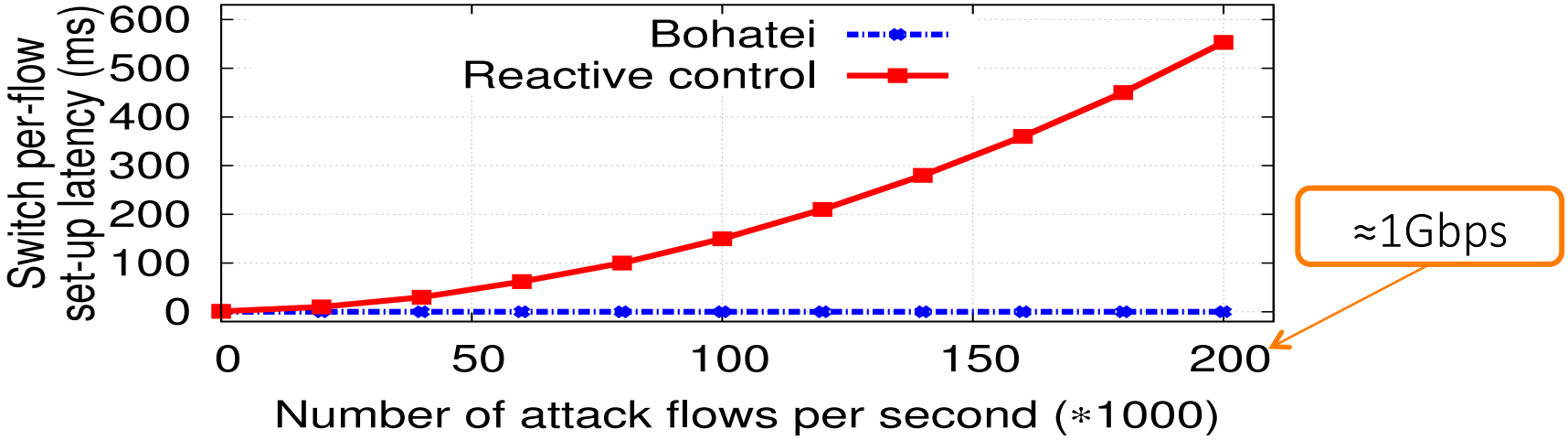
When new attacks emerge…

Today's solution: buy more proprietary appliances.



Scalability: Rule set-up latency

Effect of proactive data plane configuration



In-data plane proactive traffic tagging enables scalability.

Our design contributions

Dynamic/General Adversary

→ Need responsive resource management

→ Need resilience to volume adaptation

Using centralized SDN/NFV control

→ Need scalable orchestration

Outline

- Motivation
- Background on SDN/NFV
- Bohatei overview and challenges
- System design
  - Fast resource management
  - Scalable network orchestration
  - Handling dynamic adversaries
- Evaluation
- Conclusions

Outline

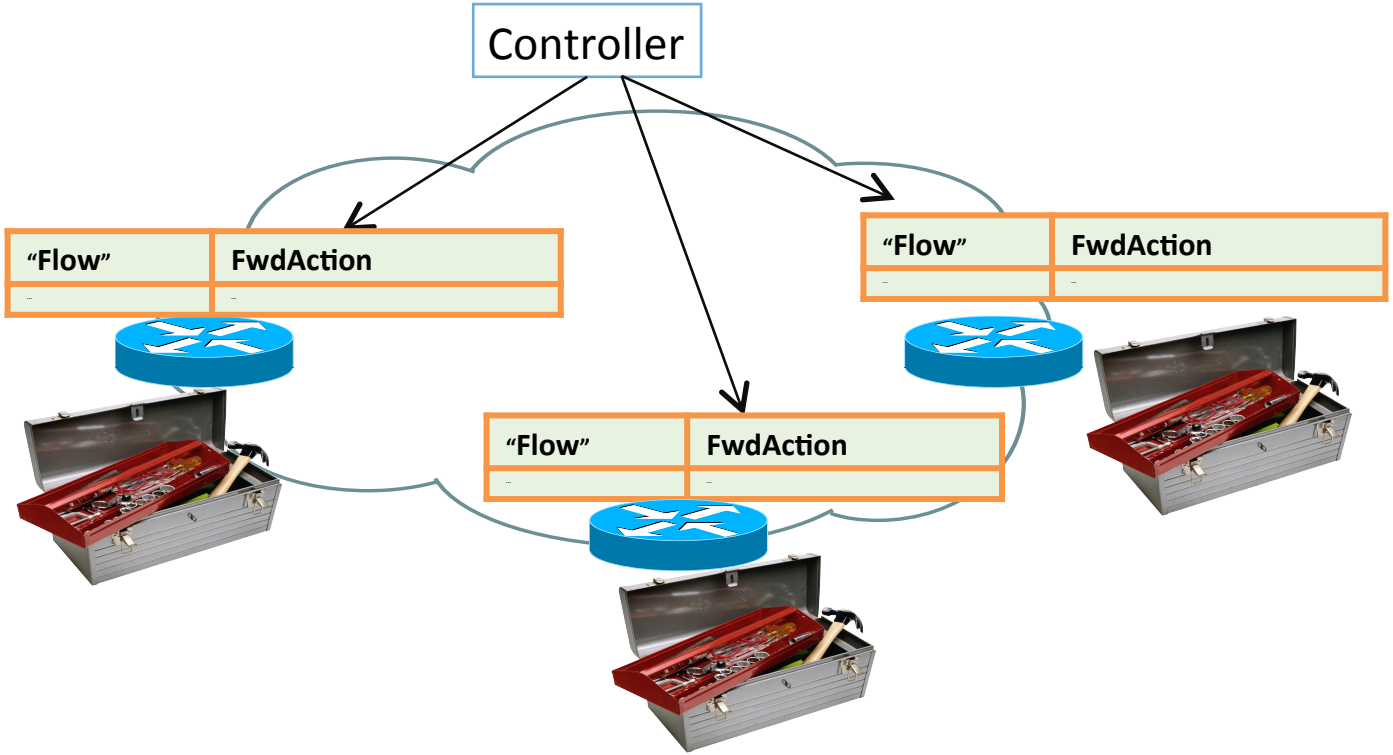
- Motivation
- Background on SDN/NFV
- Bohatei overview and challenges
- System design
  - Fast resource management
  - Scalable network orchestration
  - Handling dynamic adversaries
- Evaluation
- Conclusions

Outline

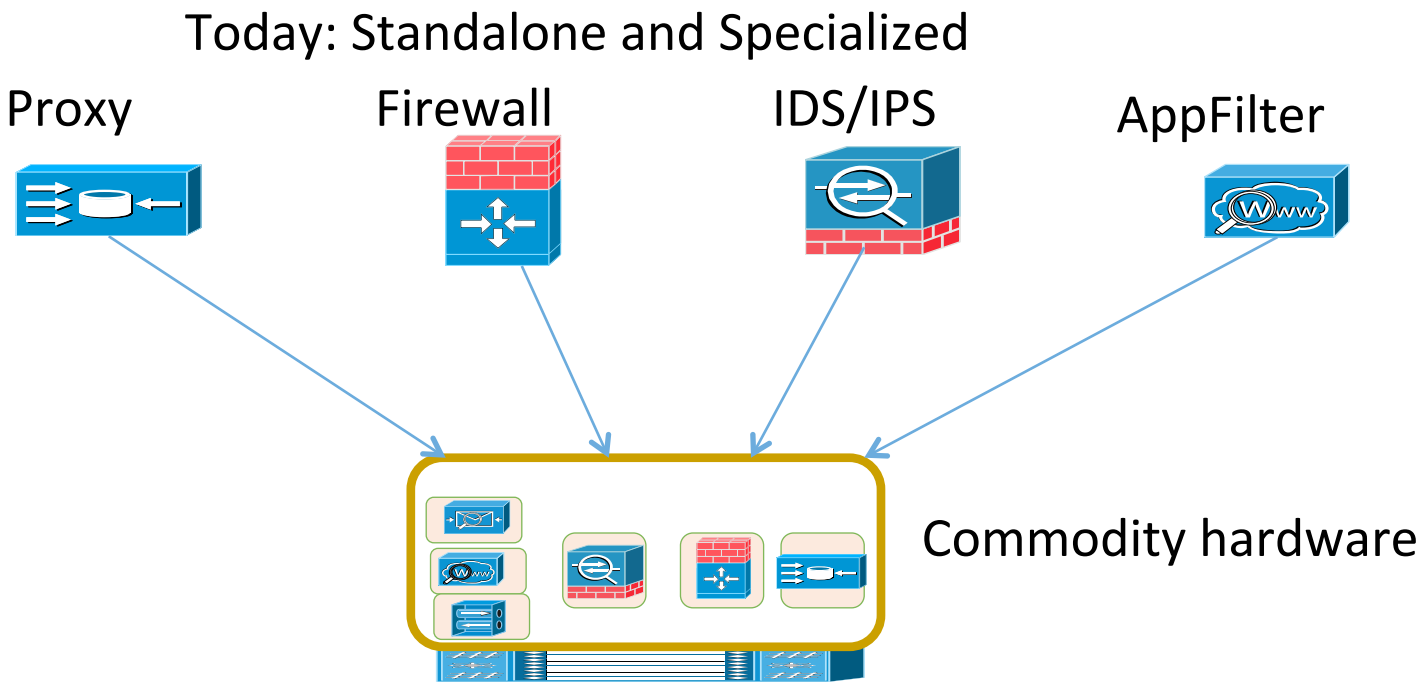
- Motivation
- Background on SDN/NFV
- Bohatei overview and challenges
- System design
  - Fast resource management
  - Scalable network orchestration
  - Handling dynamic adversaries
- Evaluation
- Conclusions

Software-Defined Networking (SDN)

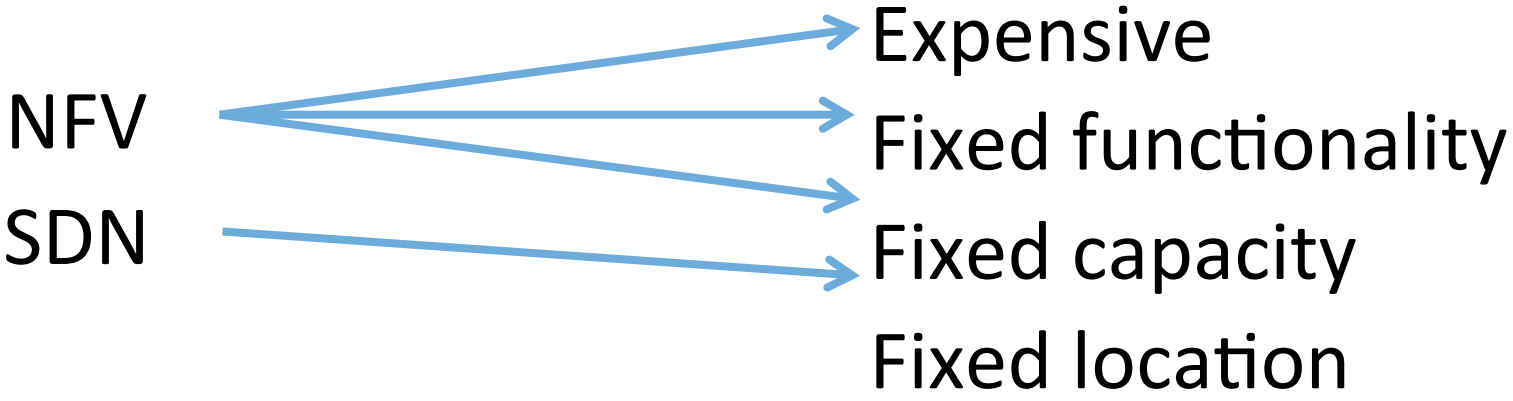
Centralized management + Open config APIs



Network Functions Virtualization (NFV)



Why are SDN/NFV useful for DDoS defense?



Our Work: Bring these benefits to DDoS Defense

Bohatei Design Challenges

Strategy layer

Predict attack pattern

Resilient to adaptation?

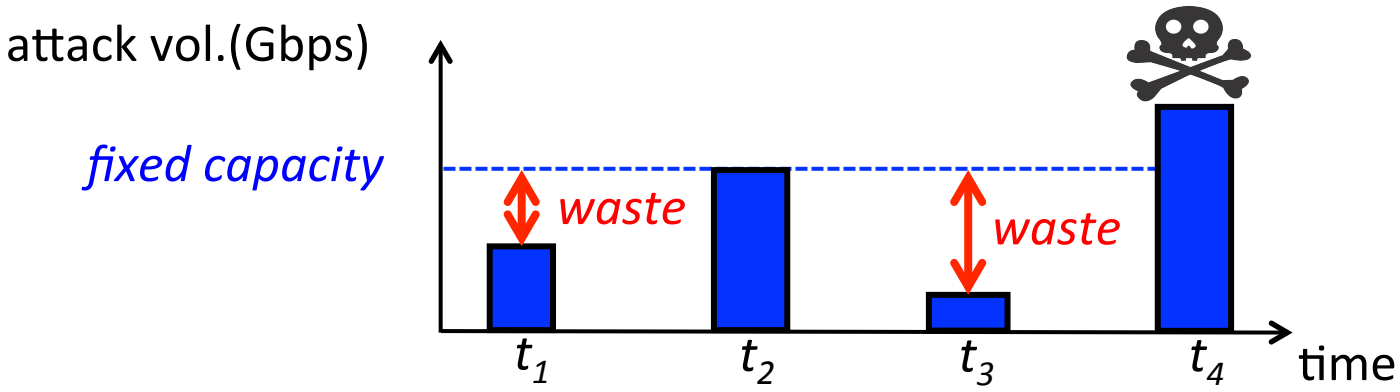
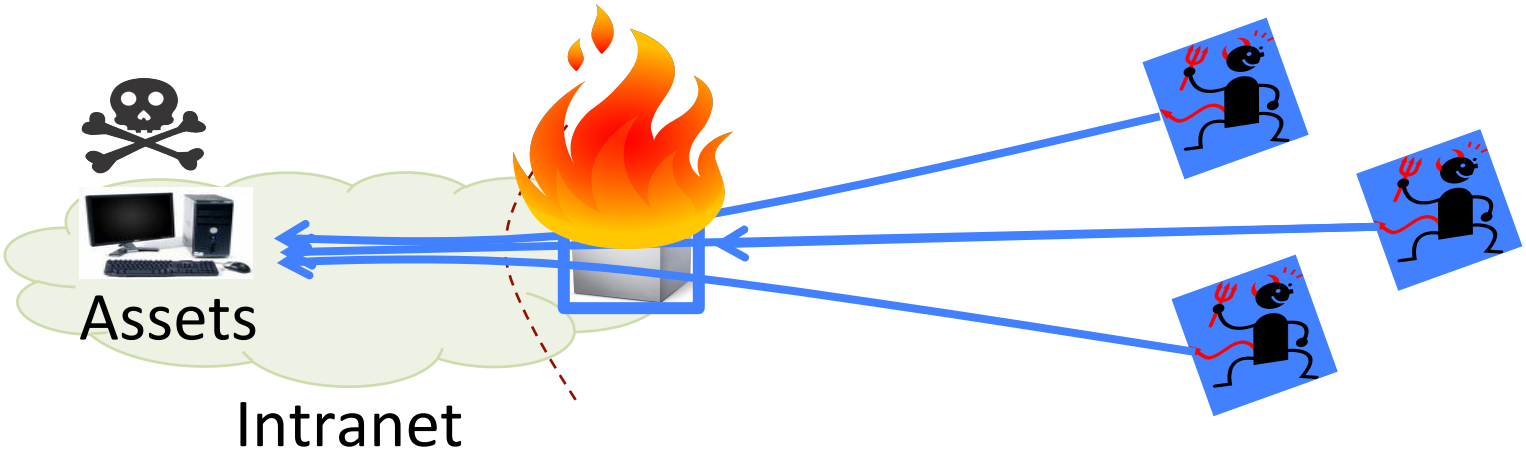
Resource management

Decide how many VMs, what types, where

Fast algorithms?

Network orchestration

Configure network to route traffic

Scalable SDN?

Limitation: Fixed capacity