Towards Autonomic DDoS Mitigation using Software Defined Networking

Authors: *Rishikesh Sahay*, Gregory Blanc, Zonghua Zhang, Hervé Debar

NDSS Workshop on Security of Emerging Networking Technologies (SENT 2015), San Diego, California, US, 8th February 2015

Outline

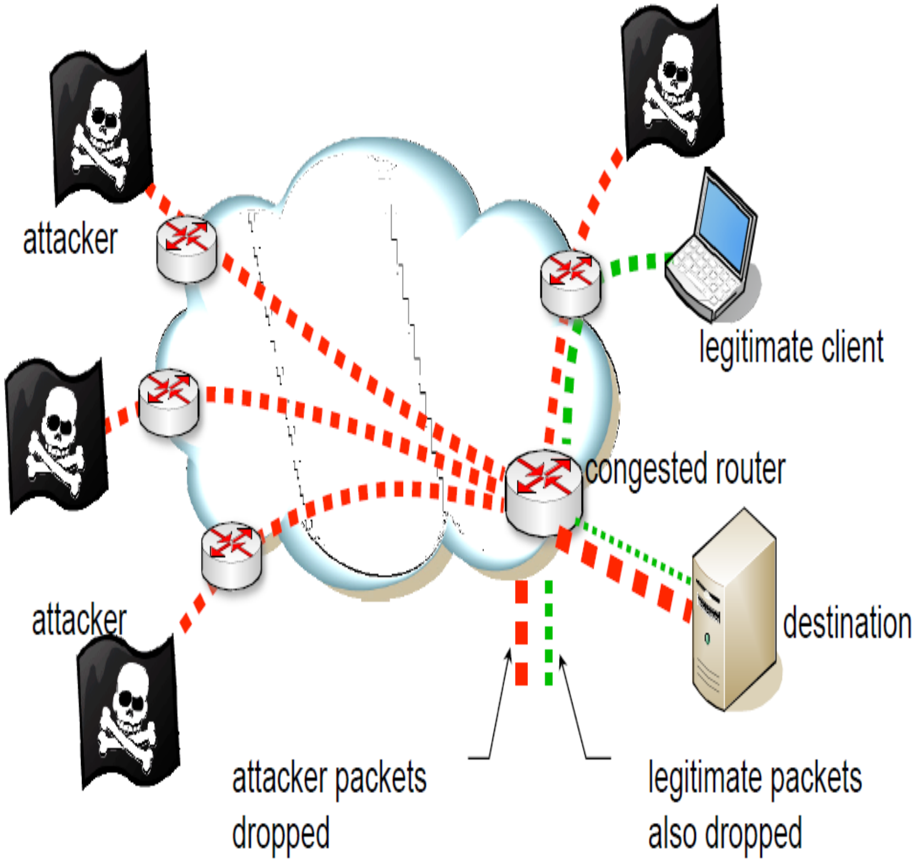
- Key Observations and Motivation
- Towards Autonomic DDoS Mitigation
- Our Proposed Framework
- Related Works
- Conclusion and Future Work

Outline

- Key Observations and Motivation
  - DDoS Attack
  - Key Observation about DDoS
  - Main Attack Vectors
  - Survey of DDoS Mitigation Schemes
  - Lack of Autonomic Properties
- Towards Autonomic DDoS Mitigation
- Our Proposed Framework
- Related Works
- Conclusion and Future Work

DDoS Attacks

- Exhaust resources of a target, by flooding the target with spurious packets.

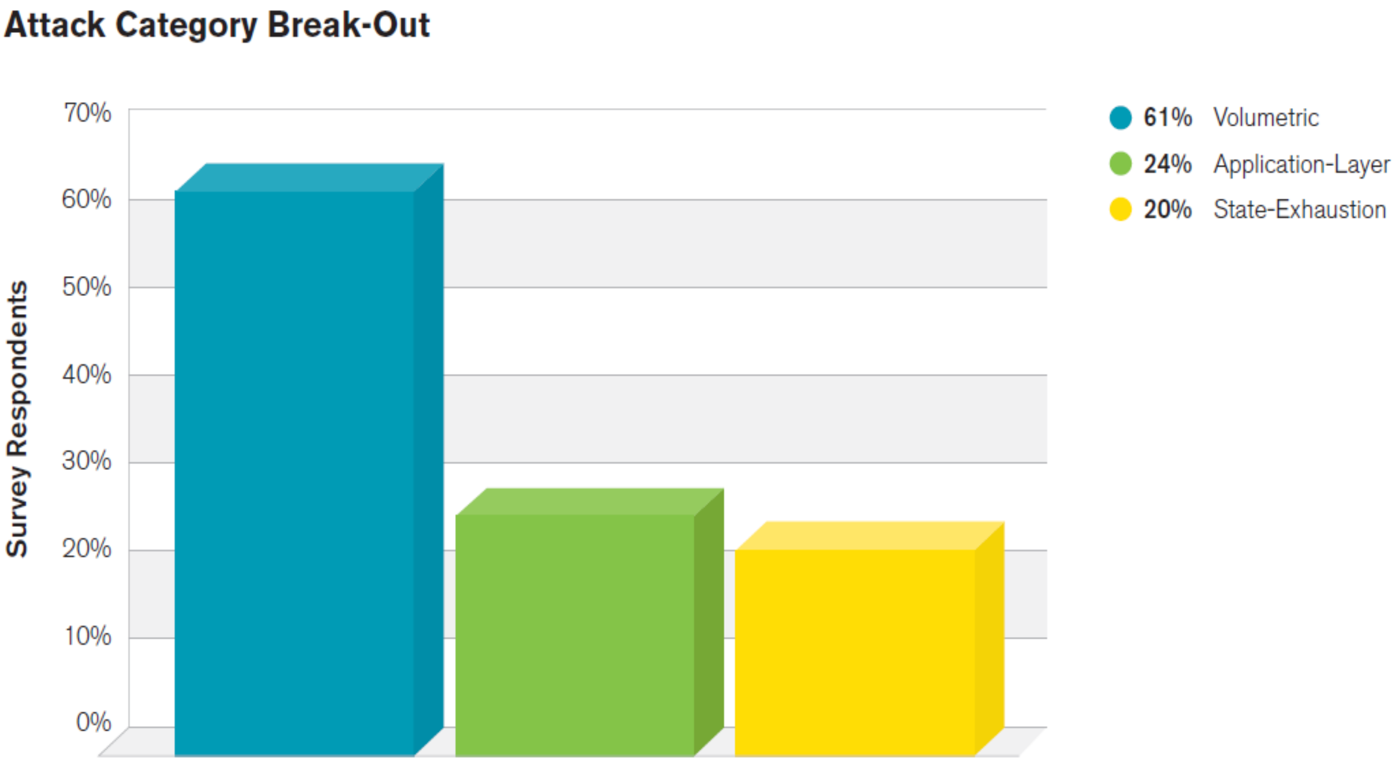


Key Observations about DDoS

- DDoS attacks have become shorter but stronger.
- Average attack bandwidth was up 72 percent.
- Reflection and amplification attack have become more popular.
- 46 percent increase in the Infrastructure attack.

Source: Prolexic Quarterly Global DDoS Attack Report Q2 2014

Main Attack Vectors



Source: Worldwide Infrastructure Security Report, Arbor Special Report 2014.

Survey of DDoS Mitigation Schemes

- **Capability Based Technique[3]:** Capability token is used for secure communication.

- **Congestion Based Technique[4]:** Traffic is rate limited based on given threshold.

- **Packet Marking Techniques[5]:** A mark is inserted in the IP packets by the routers to reconstruct the path from victim to the attack source.

- **Stateful Policy Technique[6]:** Stateful mitigation policy is specified to redirect the DDoS traffic to the middlebox.

Problems in Existing Schemes

- States to be maintained at the routers and switches.
- Additional devices to be deployed at every routers and switches.
- IDs or mark should be maintained at every routers.
- Information to be coordinated from different devices deployed at different locations in the network.
- Middleboxes should be deployed statically in the network.

Lack of Autonomic Properties

	Self-configuration	Self-optimization	Self-healing	Self-protection
Capability-based DDoS technique	×	√	×	√
Congestion based technique	×	√	×	√
Packet marking	×	√	×	√
Stateful policy technique	×	√	√	√

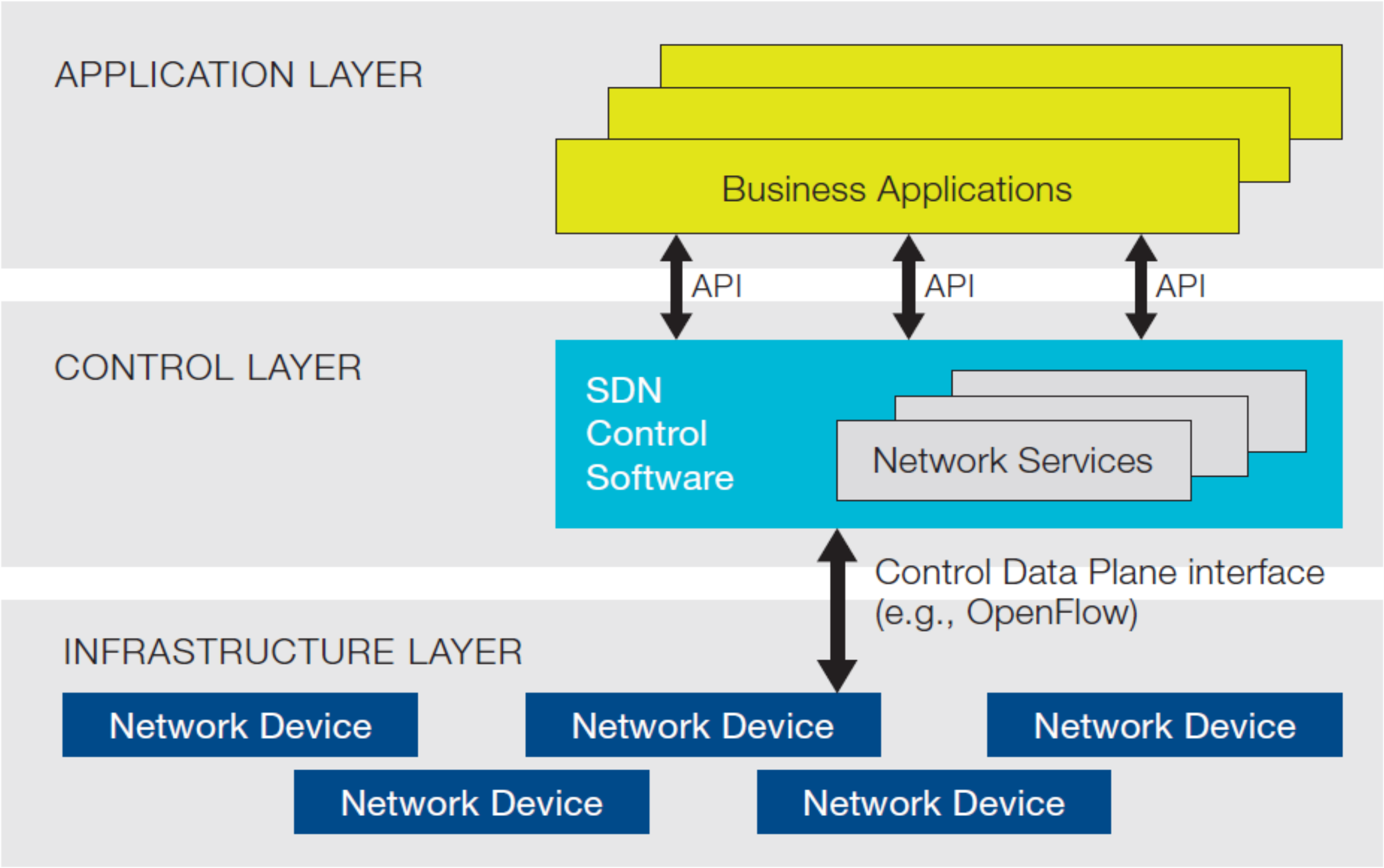
Outline

- Key Observations and Motivation
- Towards Autonomic DDoS Mitigation
  - Autonomic DDoS Mitigation Requirements
  - SDN: Architecture
  - SDN: Towards Autonomic Properties
- Our Proposed Framework
- Related Works
- Conclusion and Future Work

Autonomic DDoS Mitigation Requirements

- It should provide on demand DDoS Mitigation.
- Correlate the information from different devices in the network.
- Network resources should be optimised.
- Four autonomic properties(Self-configuration, optimization, healing, protection) should be preserved.
- Labor cost should be minimized.

SDN: An Overview



Source:Software Defined Networking:The New Norms for Networks. ONF White Paper, 2012.

SDN:Towards Autonomic Properties

- Logically Centralized Intelligence

- Flexible Path Management

- On-demand Resource Allocation

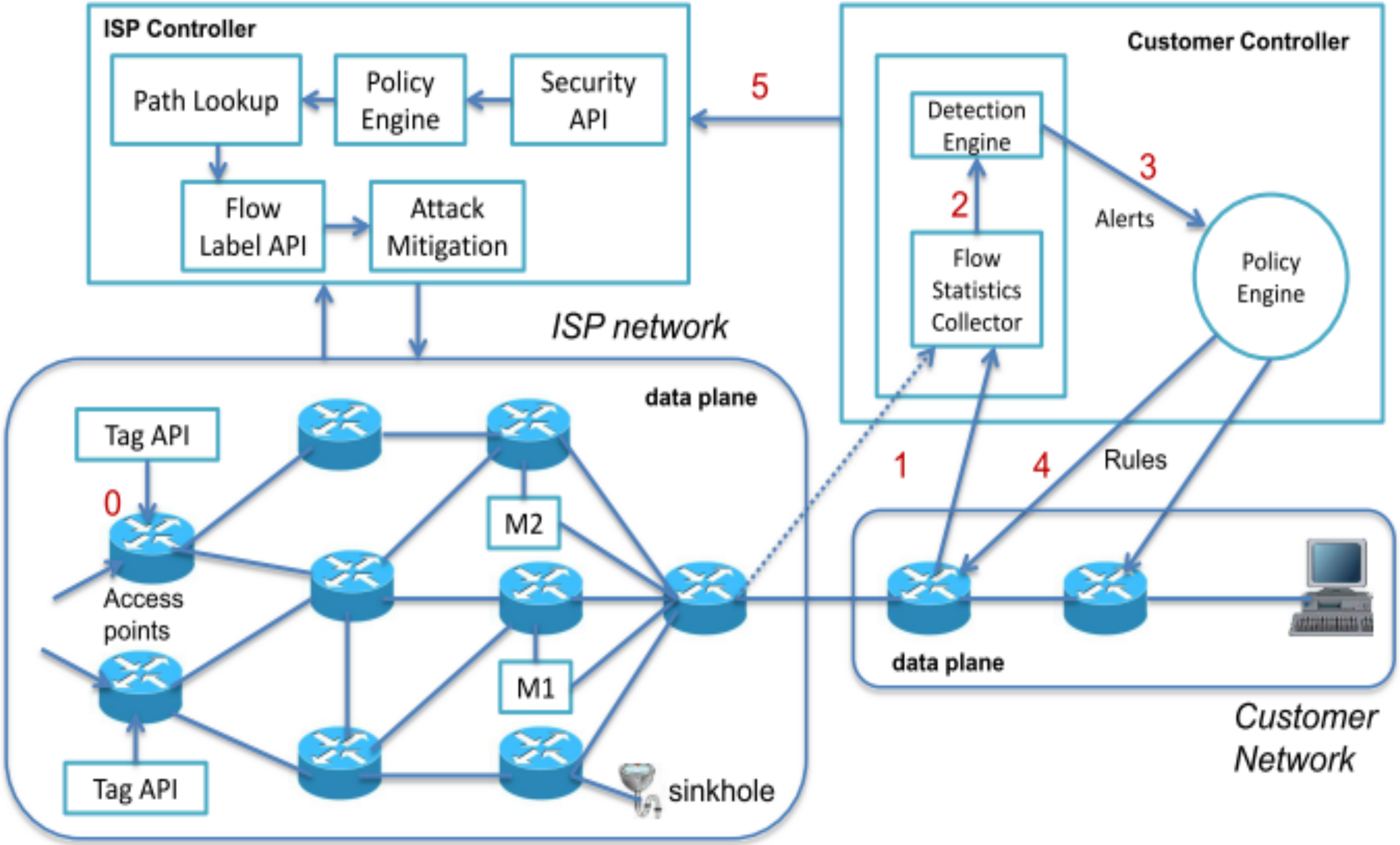
Outline

- Key Observations and Motivation
- Towards Autonomic DDoS Mitigation
- Our Proposed Framework
  - Design Assumptions in Framework
  - Proposed Architecture
  - Use Case
- Related Works
- Conclusion and Future Work

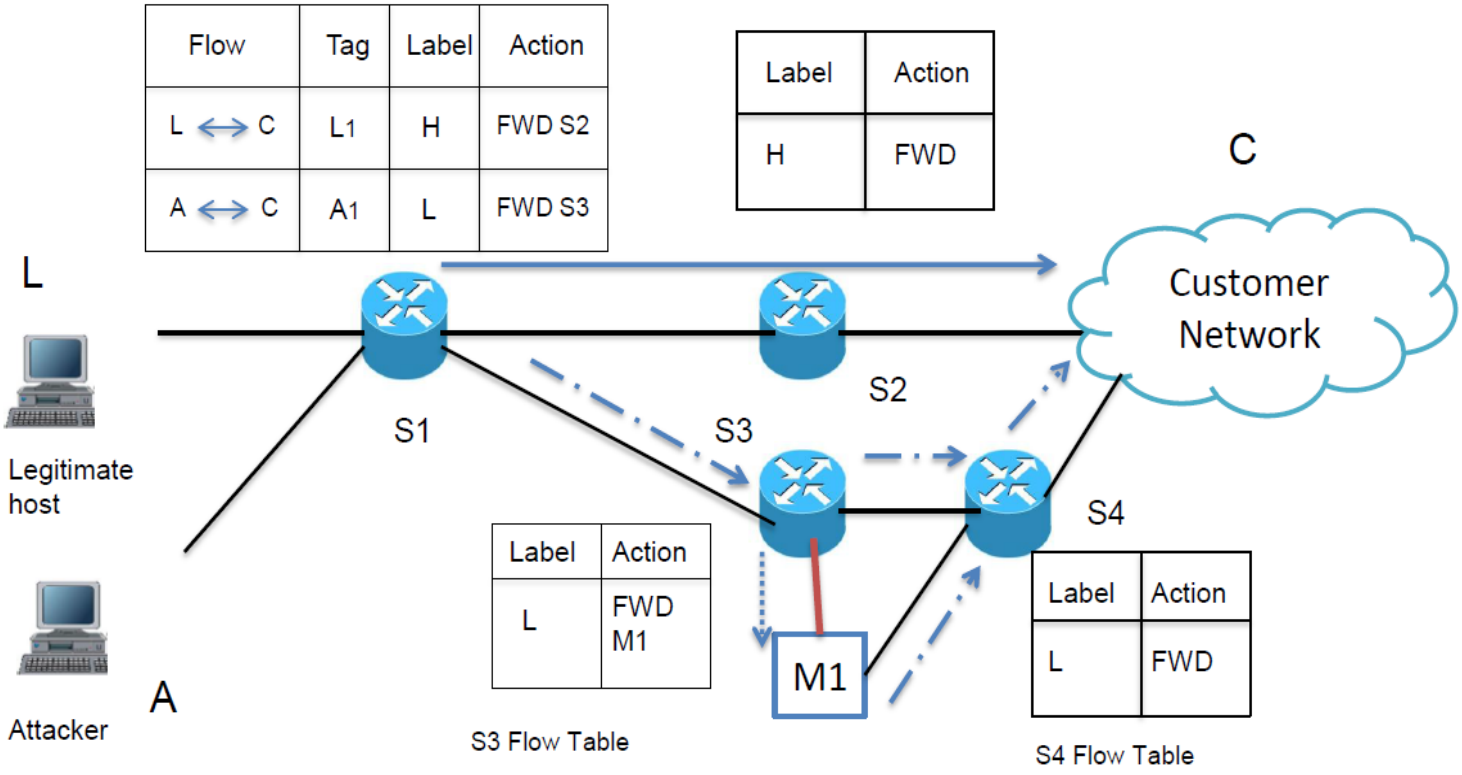
Design Assumptions in Framework

- DDoS mitigation framework is distributed across the ISP and customer network.
- Security API is provided by the ISP to the customer to request for the on demand DDoS mitigation.
- DDoS detection module is running in the customer network and generates the security alerts.

Proposed Framework



Use Case



Flow	Tag	Label	Action
L ↔ C	L1	H	FWD S2
A ↔ C	A1	L	FWD S3

Label	Action
H	FWD

Label	Action
L	FWD M1

S3 Flow Table

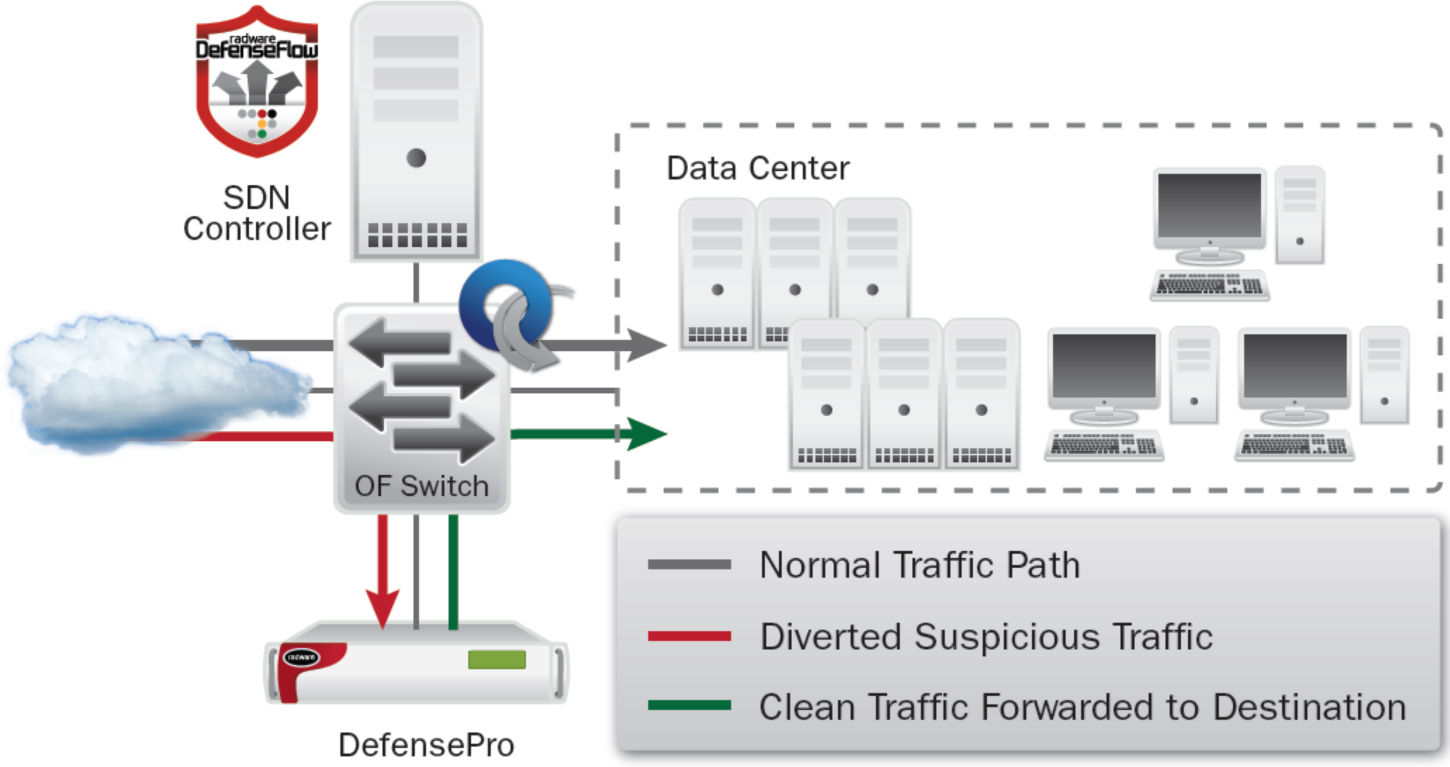
Label	Action
L	FWD

S4 Flow Table

Outline

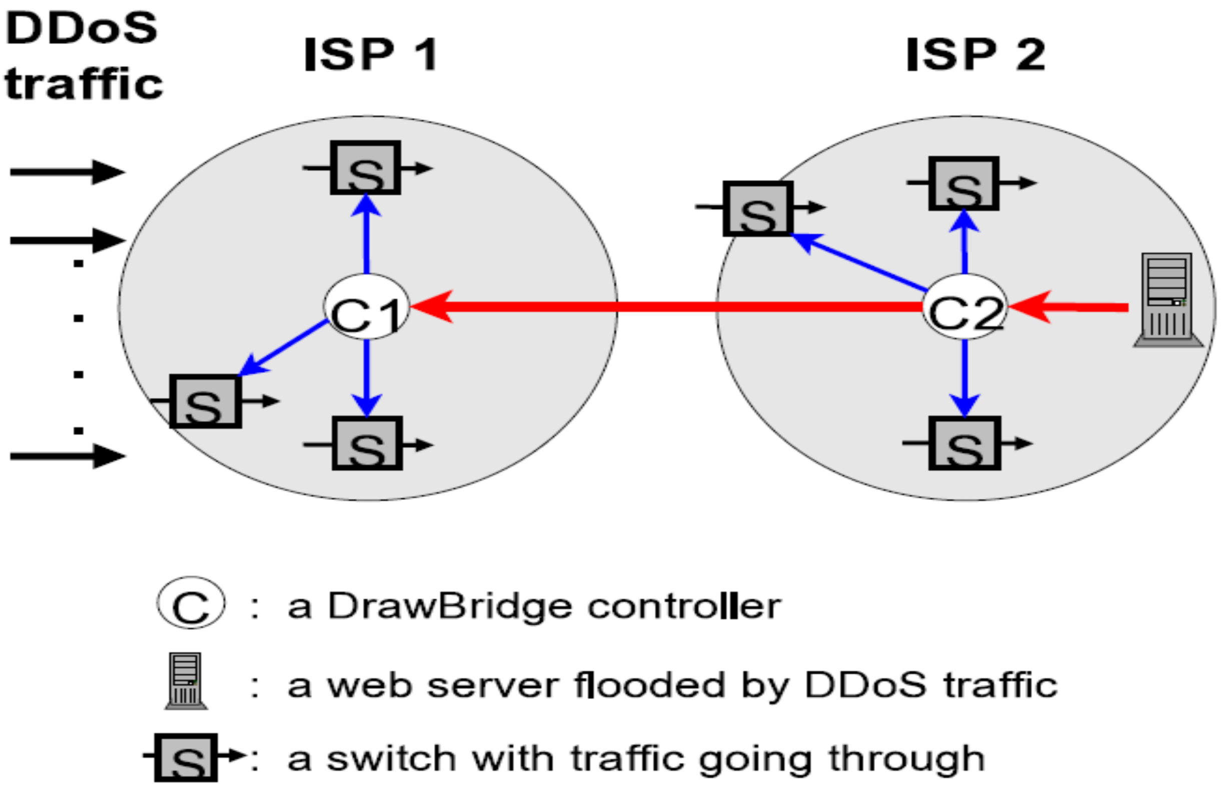
- Distributed Denial of Service Attack and Mitigation
- Towards Autonomic DDoS Mitigation
- Our Proposed Framework
  - Design Assumptions in Framework
  - Proposed Architecture
  - Use Case
- Related Works
- Conclusion and Future Work

DefenseFlow:Industry Product



Source: DefenseFlow:The SDN Application that Program Network for DoS Security, 2013.

DrawBridge


DDoS traffic
ISP 1
ISP 2
S
C1
C2
C : a DrawBridge controller
: a web server flooded by DDoS traffic
S : a switch with traffic going through

Source: J.Li ,DrawBridge: Software-defined DDoS-resistant Traffic Engineering,in *Proceedings of the 2014 ACM Conference on SIGCOMM*. ACM, 2014.

Conclusion and Future Work

- We will implement the major components of the framework.

- We will evaluate the framework on its scalability on handling large number of requests from customers.

- We will also evaluate the response latency in redirecting the suspicious flow to the middleboxes.

References

- [1]. Prolexic Quarterly Global DDoS Attack Report Q2 2014.
- [2]. Worldwide Infrastructure Security Report, Arbor Special Report 2014.
- [3]. Abraham Yaar, SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks, *in Proceedings of the 2004 IEEE Symposium on Security and Privacy, 2004.*
- [4]. J.Ioannidis, Implementing Pushback: Router Based Defense Against DDoS Attacks, *in Proceedings of Network and Distributed Security Symposium (NDSS)*, 2002.
- [5].A.Yaar, Pi: A Path Identification Mechanism to Defend against DDoS Attacks, in *Security and Privacy*, 2003.
- [6]. A.Mahimkar, dFence:Transparent Network-based Denial of Service Mitigation, *in Proceedings of the 4th USENIX Conference on Networked Systems Design Implementation (NSDI)*,2007

References

- [7]. Software Defined Networking:The New Norms for Networks. ONF White Paper, 2012.

- [8].DefenseFlow:The SDN Application that Program Network for DoS Security, 2013.

- [9]. J.Li ,DrawBridge: Software-defined DDoS-resistant Traffic Engineering,in *Proceedings of the 2014 ACM Conference on SIGCOMM*. ACM, 2014.

- [10]. Seyed Kaveh Fayazbakhsh, FlowTags: Enforcing Network-Wide Policies in the Presence of Dynamic Middlebox Actions, in *HotSDN*, 2013.

Acknowledgment

- The research project (NECOMA) is funded by Ministry of Internal Affairs and Communication Japan and by the European Union Seventh Framework Programme. The link of the project is:

http://www.necoma-project.eu/

Thanks for your Attention