External BGP (D)DoS Diversion

Ruben Valke

Wouter Borremans

Presentation Content

- Why was this project initiated?
- What is a (D)DoS Attack?
- How to detect (D)DoS attacks?
- (D)DoS diversion levels
- Anti (D)DoS mechanisms
- What is external BGP (D)DoS diversion?
- Test environment
- Tests performed
- Future work
- Conclusion

Why was this project initiated

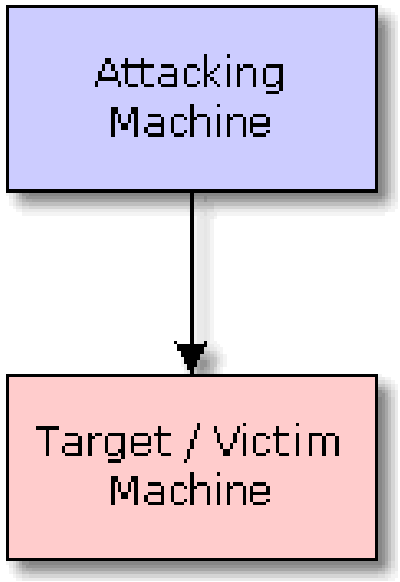
- Fill the increasing need for (D)DoS protection
- Prevention of financial damage
- Reduce the impact of (D)DoS attacks within the Internet core

What is a (D)DoS attack?

- (**D**istributed) **D**enial of **S**ervice attack
- Can use vulnerabilities in TCP/IP stack
- Compromised hosts send traffic to a specific destination
- Result:
  - Backbone is filled up with useless traffic
  - Host becomes unreachable

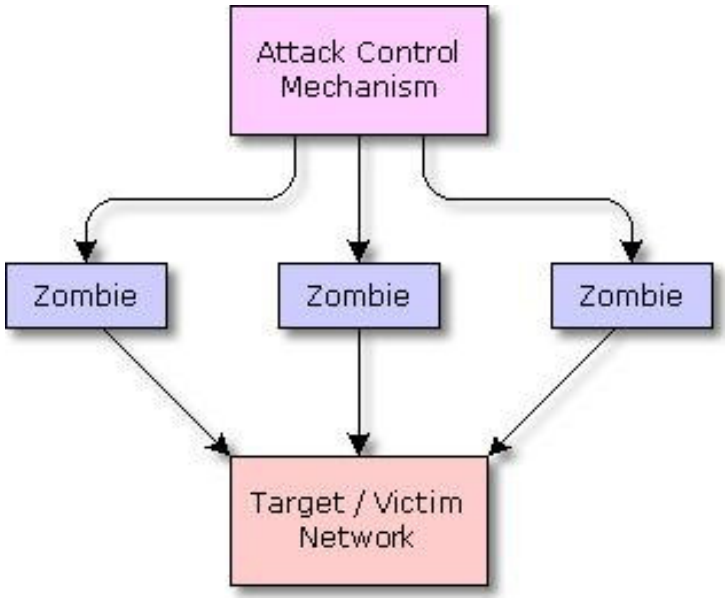
What is a (D)DoS attack?

- Non distributed attack



What is a (D)DoS attack?

- Distributed attack



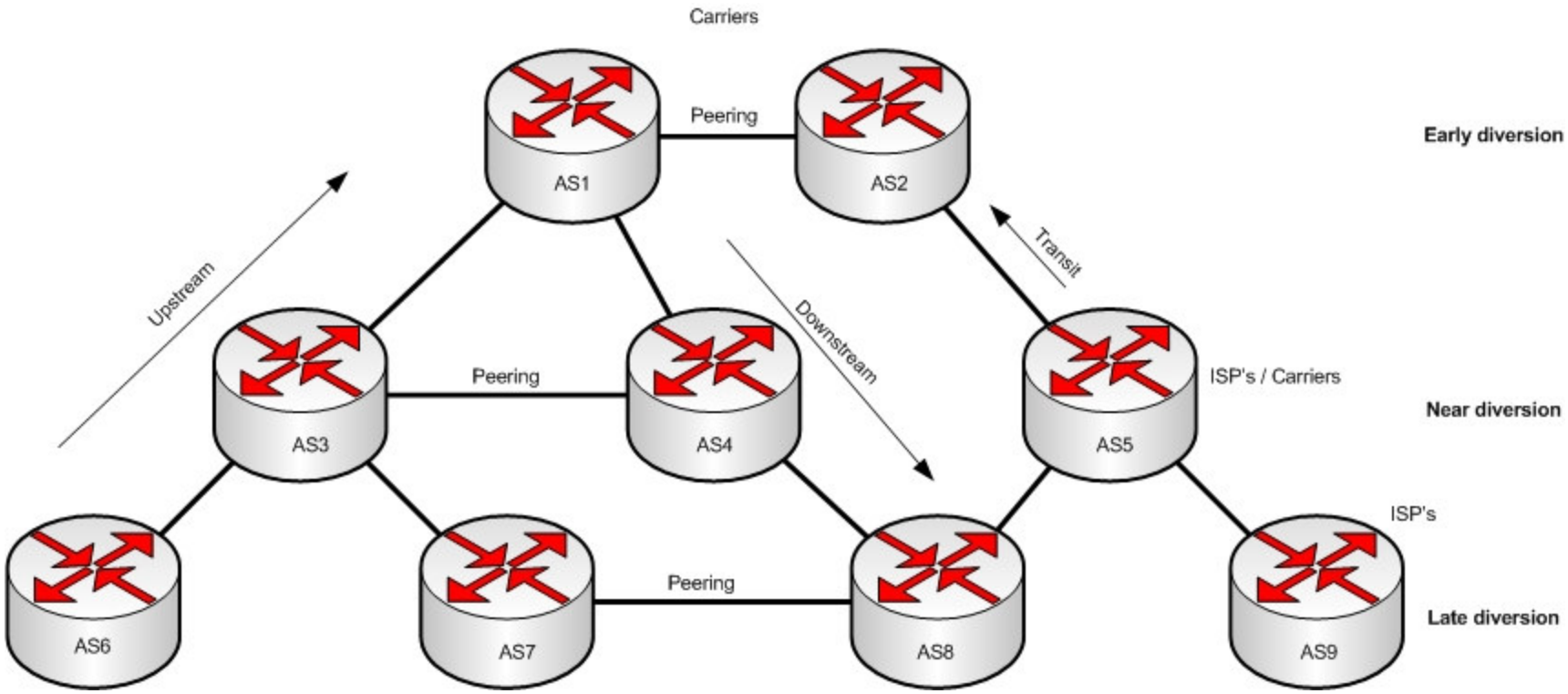
How to detect (D)DoS attacks?

- Detection by traffic patterns
- Detection by sudden traffic increase
- Problem:
  - How to trace back the origin of the (D)DoS attack?

(D)DoS diversion levels

- Early diversion
- Near diversion
- Late diversion

(D)DoS diversion levels



Anti (D)DoS mechanisms

- Rate limiting
- Oversizing
- Firewalling (TCP/UDP blocking)
- Isolation
- External BGP Diversion

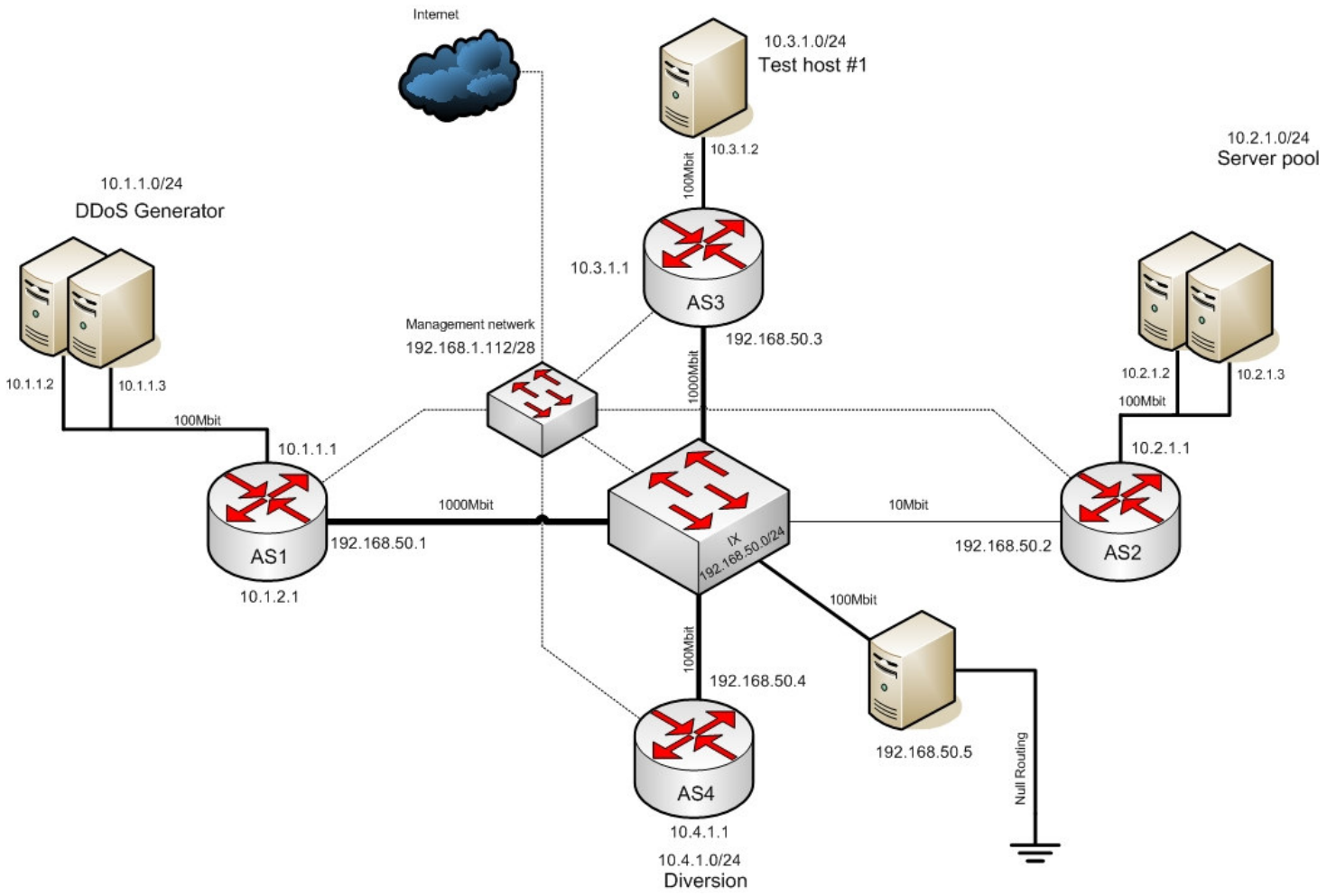
What is external BGP diversion?

- Announcing a more specific network (/32)
- Leading traffic away from a targeted host or network
- Implemented as an AS, representing the anti (D)DoS diversion

Why external BGP (D)DoS Diversion?

- Effective routing decisions to prevent traffic flows end up in an ISP network
- Can be implemented at all layers of the Internet core (Early, Near, Middle)
- Fast convergence to other routers

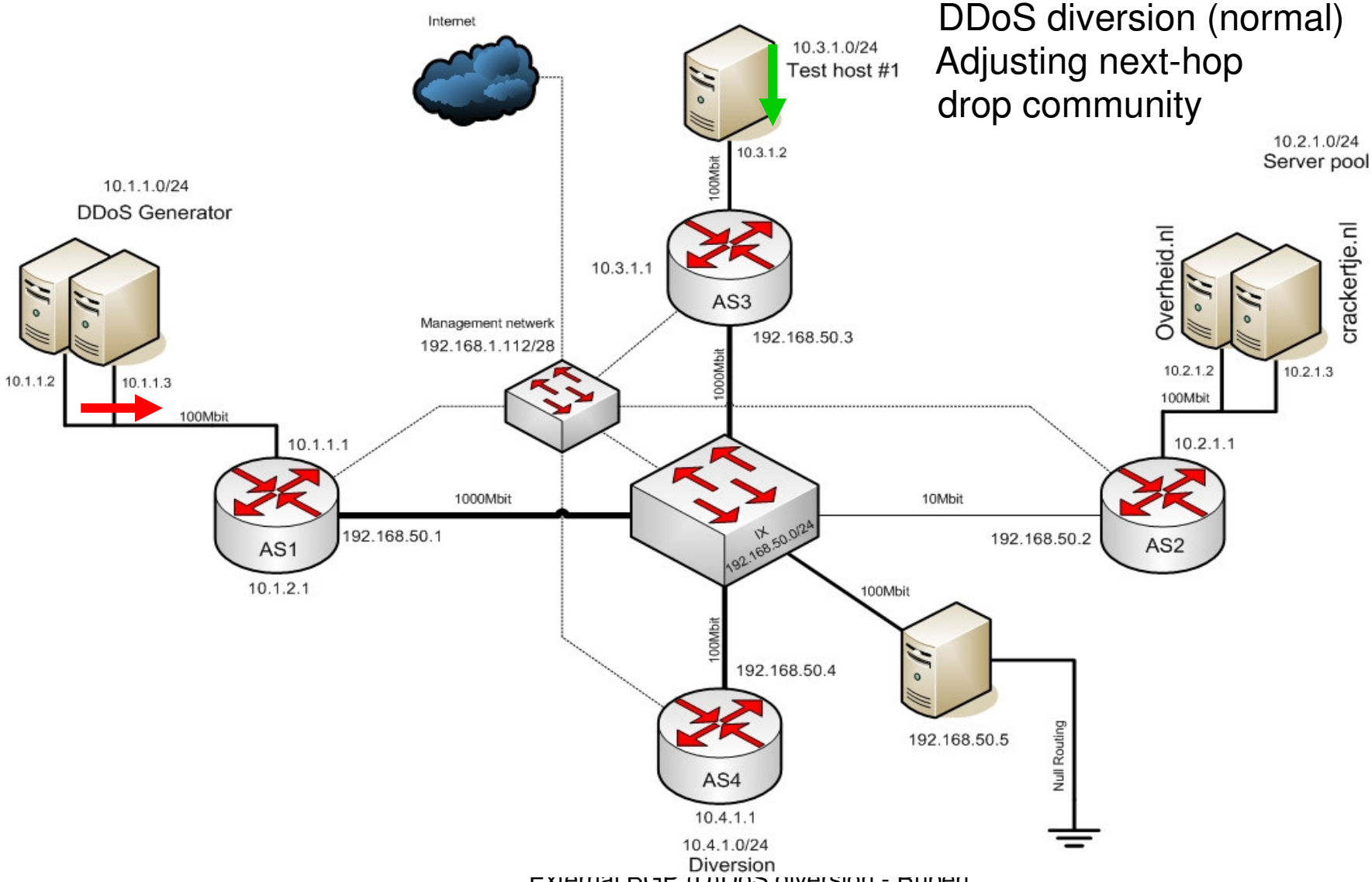
Test environment



Tests performed

- Diversion (Demo)
- Adjusting next-hop
- Drop community
- Null routing

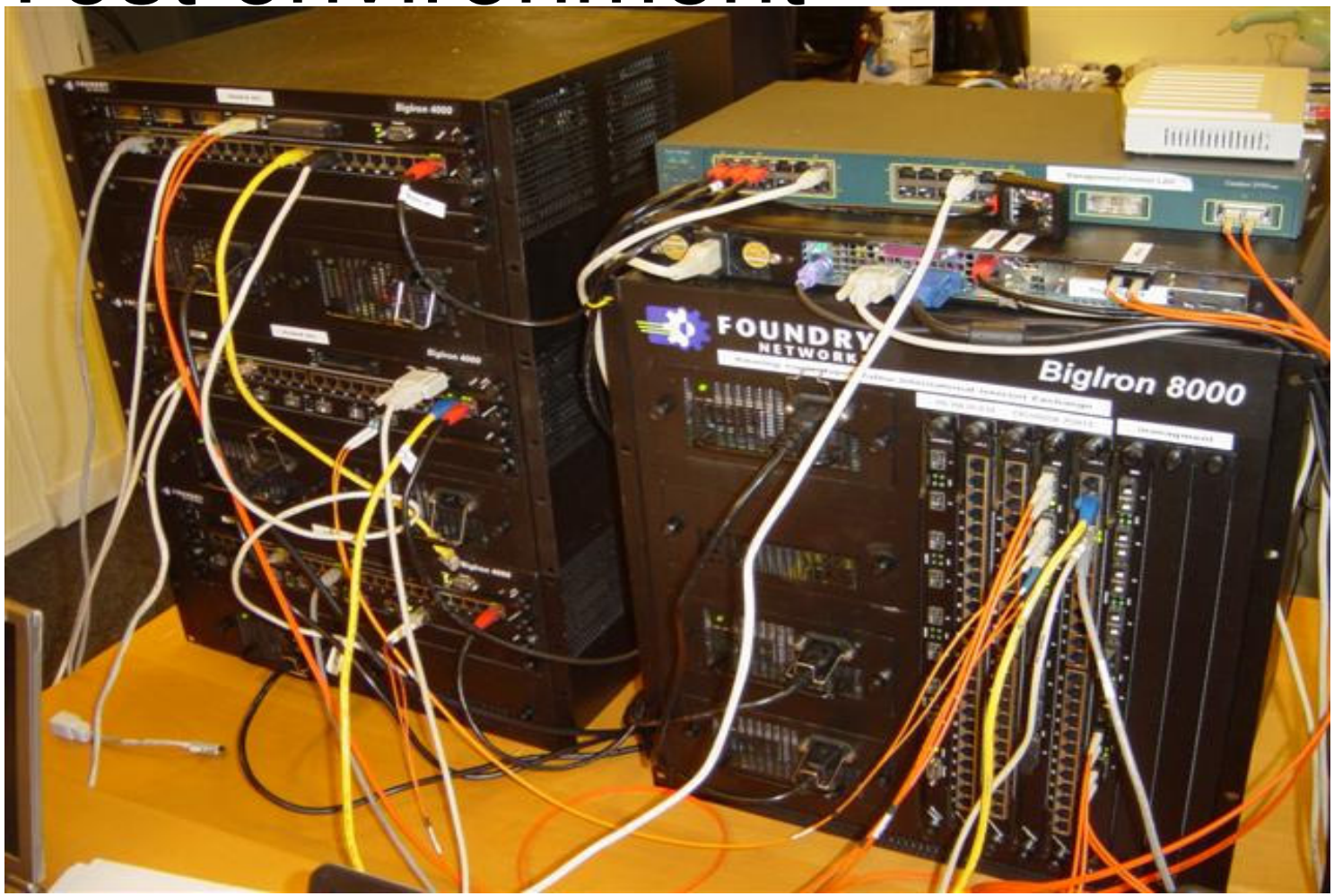
Normal Traffic flow
DoS attack initiated
DDoS diversion (normal)
Adjusting next-hop
drop community



Test environment

- 3 x Foundry BigIron 4000 router
- 1 x Foundry BigIron 8000 switch
- 1 x Server debian linux / zebra router
- 2 x laptops for ddos generation
- 2 x laptops as target hosts
- 1 x laptop as reference machine
- 1 x pc as blackhole

Test environment



Future work

- Phyiscal implementation
- Traffic learning and measuring
- Writing a RFC

Conclusion

- Very effective way
- Can be implemented fast
- Unfortunately not a 100% solution
- Futher research would be nice