DE·CIX

Awesome for 20 years

Blackholing at IXPs

DDoS Mitigation at the Core of the Internet

Daniel Kopp

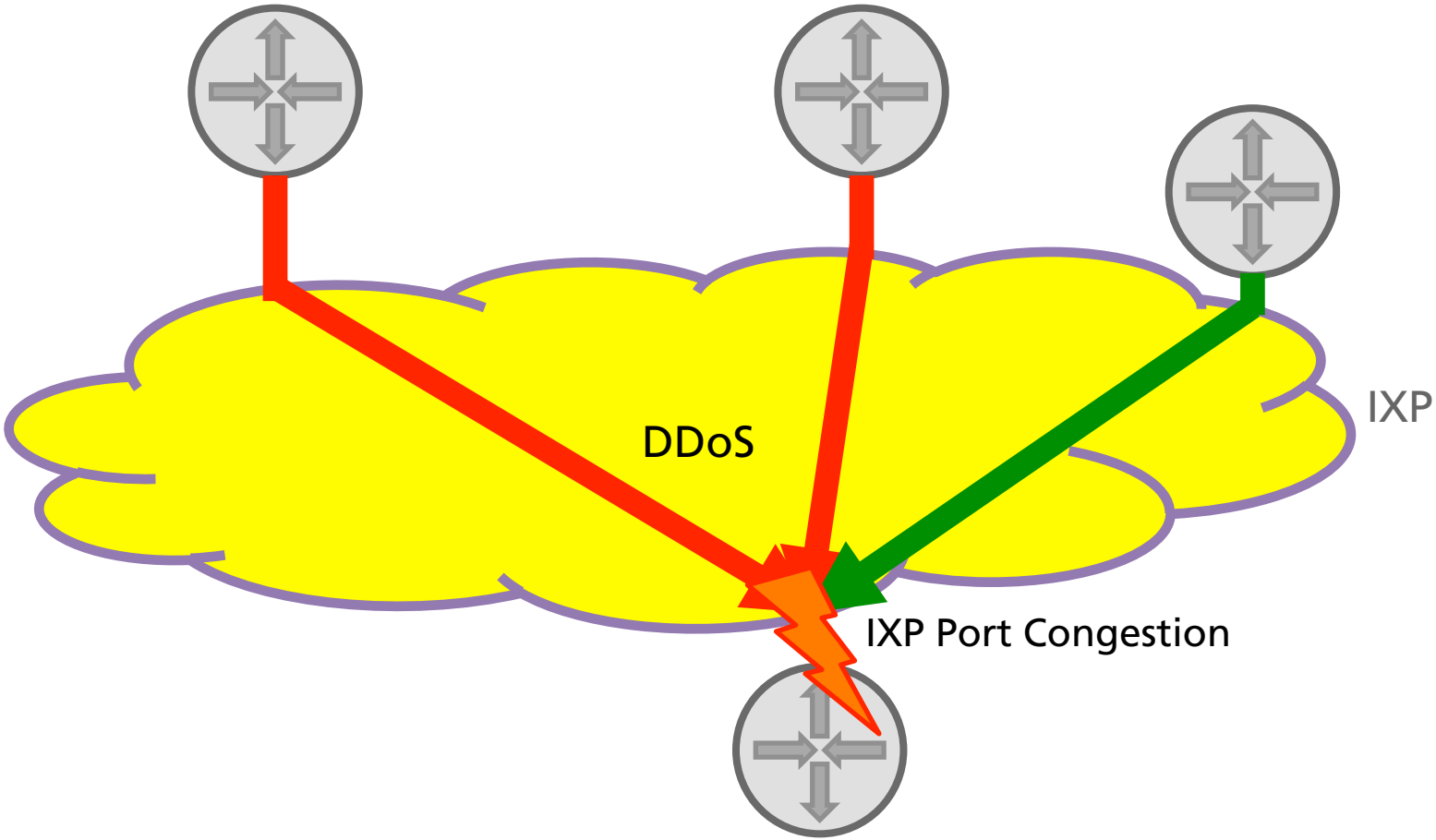
Junior Researcher

Contents

- How does Blackholing Work (at DE-CIX)?
- Using Blackholing at an IXP
- Usage Statistics at DE-CIX Frankfurt
- New Developments

How does Blackholing Work?

The Problem: Massive DDoS Attack

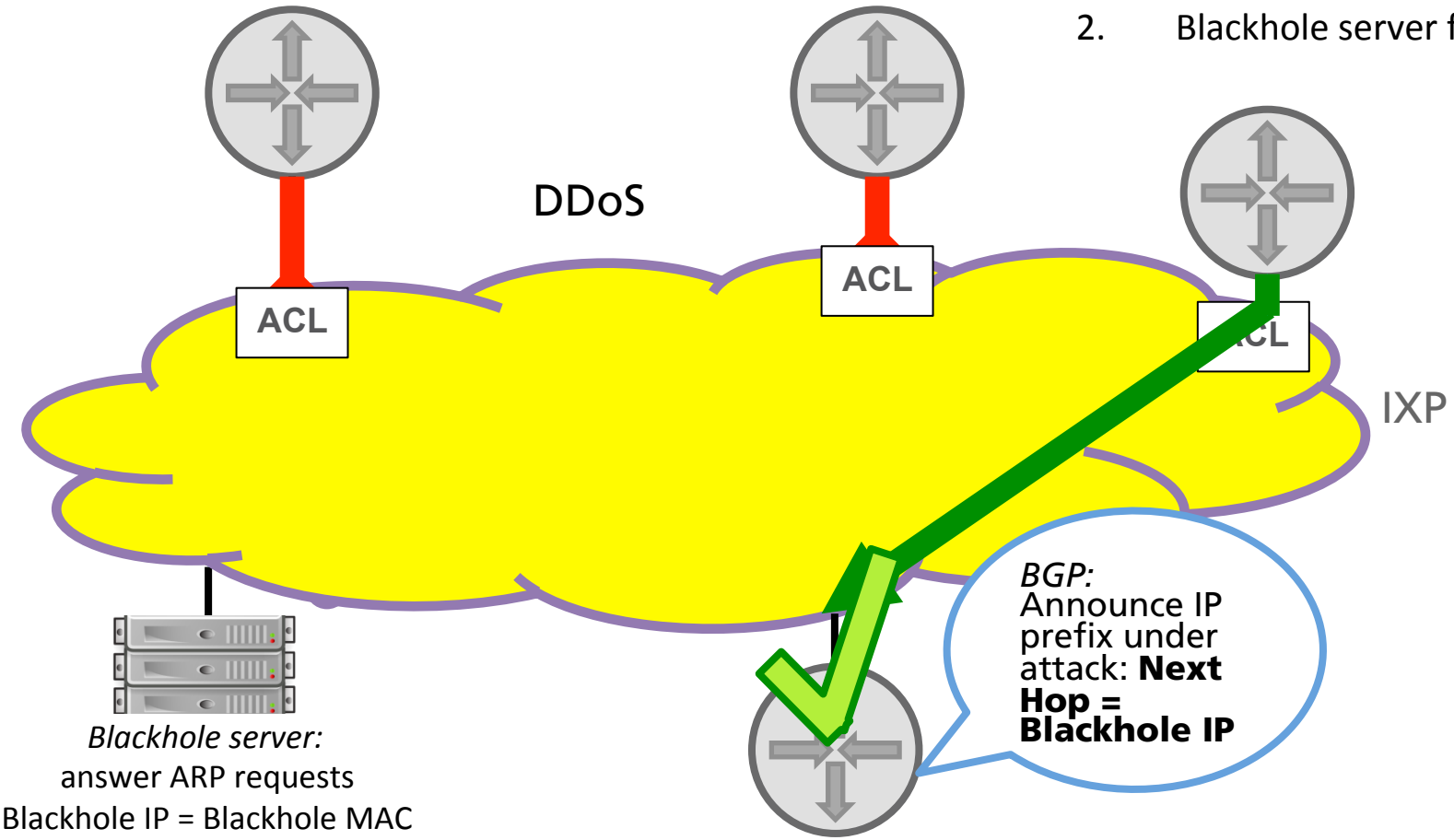


If an IXP customer is hit by a massive DDoS attack its port can get congested and impact legitimate traffic

A Solution: Blackholing

Preparation IXP:

1. ACL: Block Blackhole MAC
2. Blackhole server for ARP



For the IP prefix for which a blackholing is triggered all traffic is discarded at the IXP. Traffic for other IP prefixes gets through without any congestion.

IXP: What is Needed

1. The IXP operator selects an IP address from the Peering LAN as Blackhole IP address (e.g. 80.81.193.66)
2. The IXP operator selects a MAC address as Blackhole MAC address (e.g. de:ad:be:ef:66:95)
3. IXP operator sets up a server that provides ARP responses to the Blackhole IP address
4. IXP operator installs ACL filters on customer ports to drop all traffic with destination Blackhole MAC address
5. IXP operator updates the configuration of the route server to allow next hops to be the Blackhole IP address (and self)

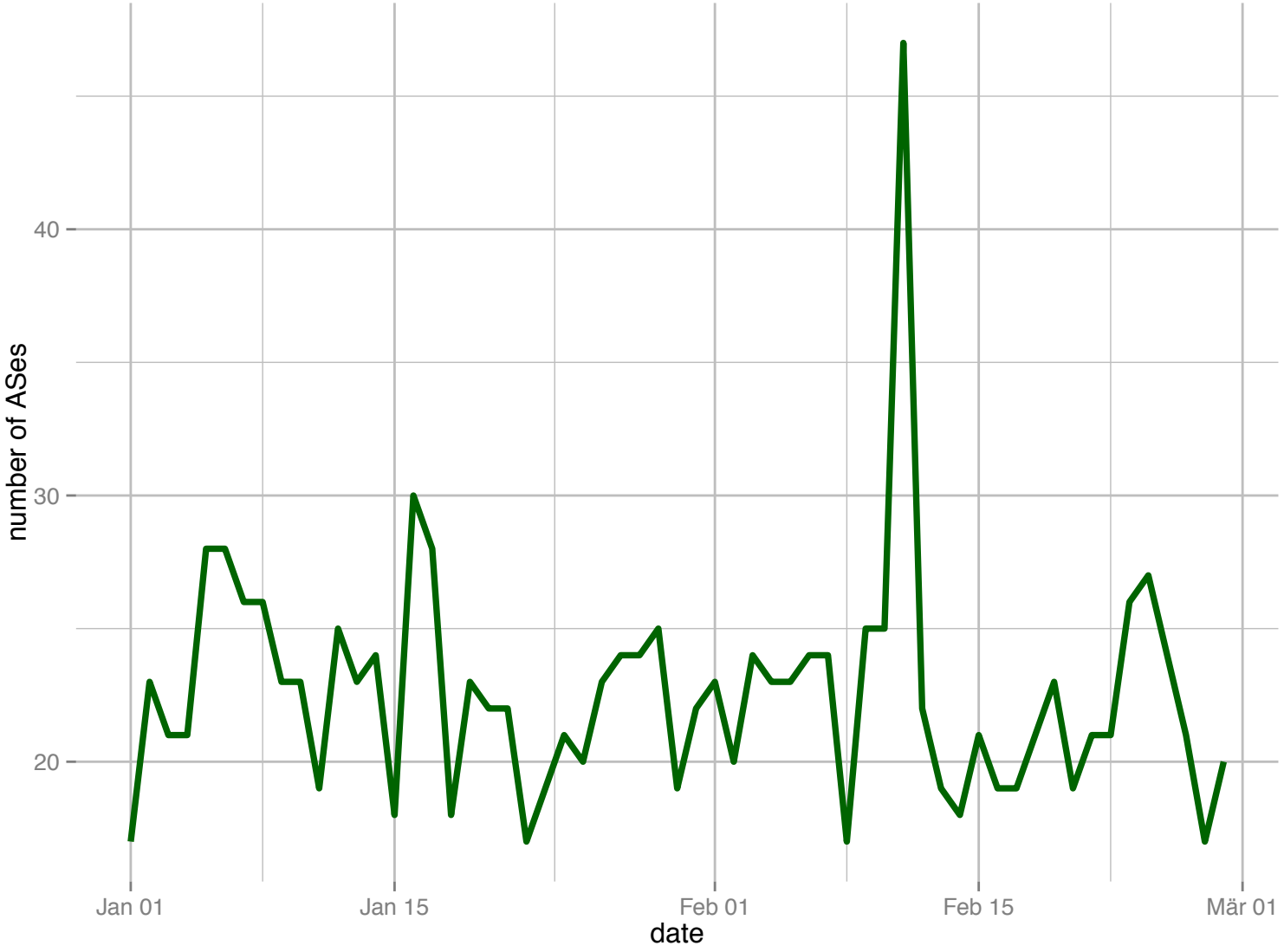
Using Blackholing at an IXP

Customer: How to Trigger a Blackhole

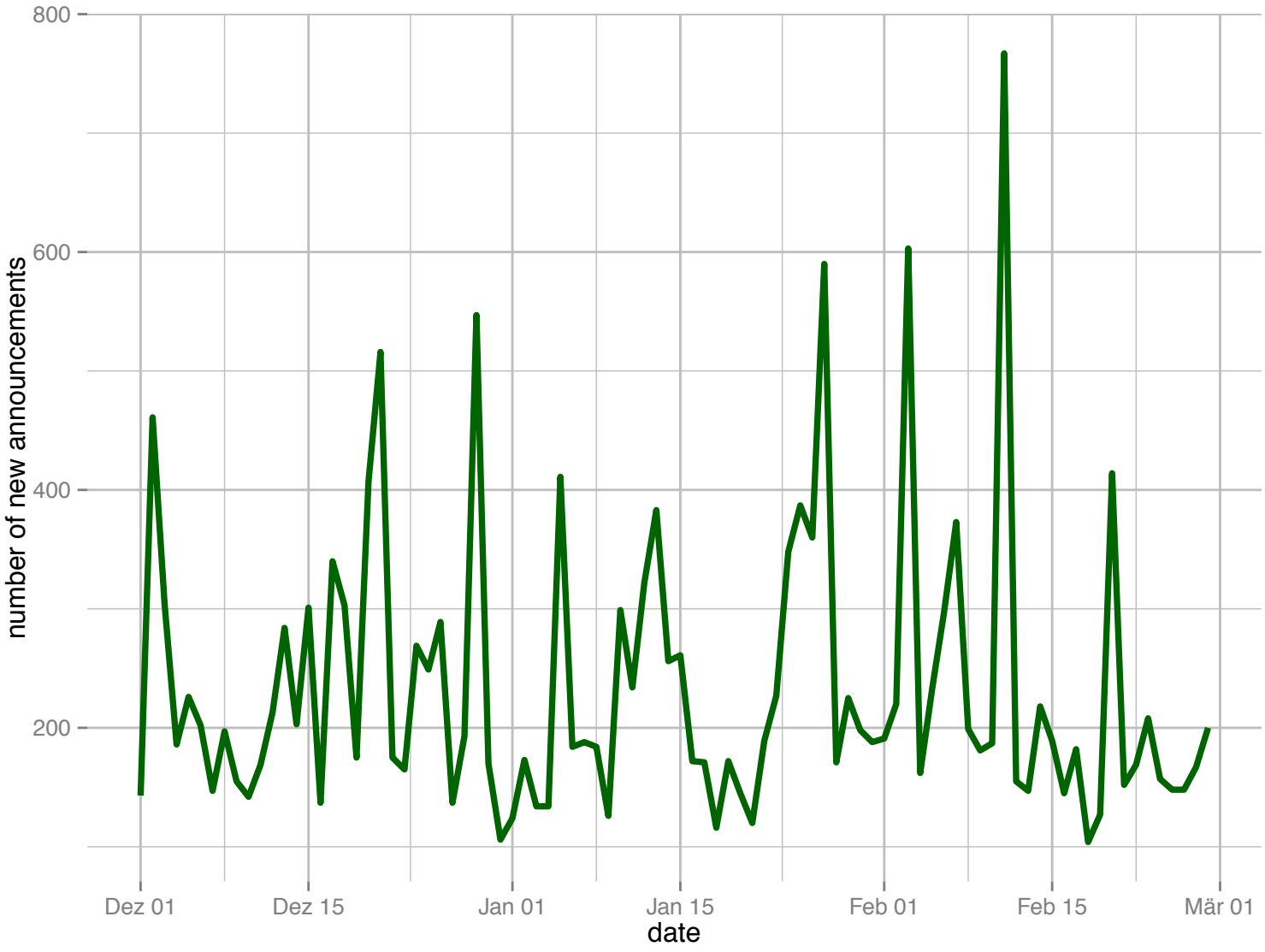
- The customer announces the IP prefix under attack with the next hop IP address set to the blackhole IP address
- Blackholing works with bi-lateral and multi-lateral (route server) peerings
- Limited acceptance of /32 IP prefixes. < /24 is preferred.
- Route server: policy control to whitelist/blacklist a particular ASN can be used

Usage Statistics at DE-CIX Frankfurt

Number of ASNs (≈ Customers)

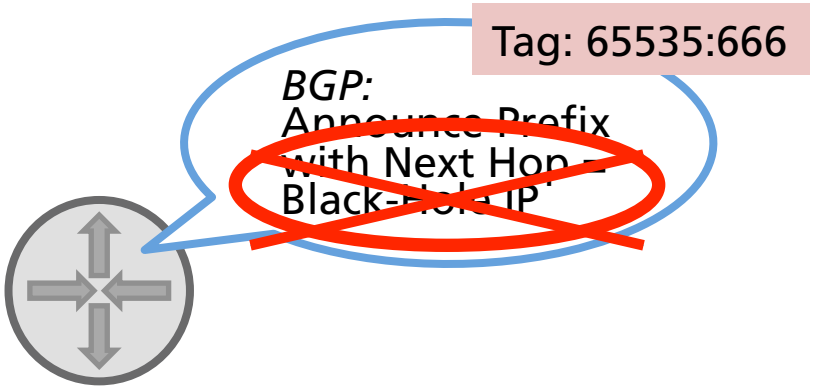


Number of Prefixes Blackholed



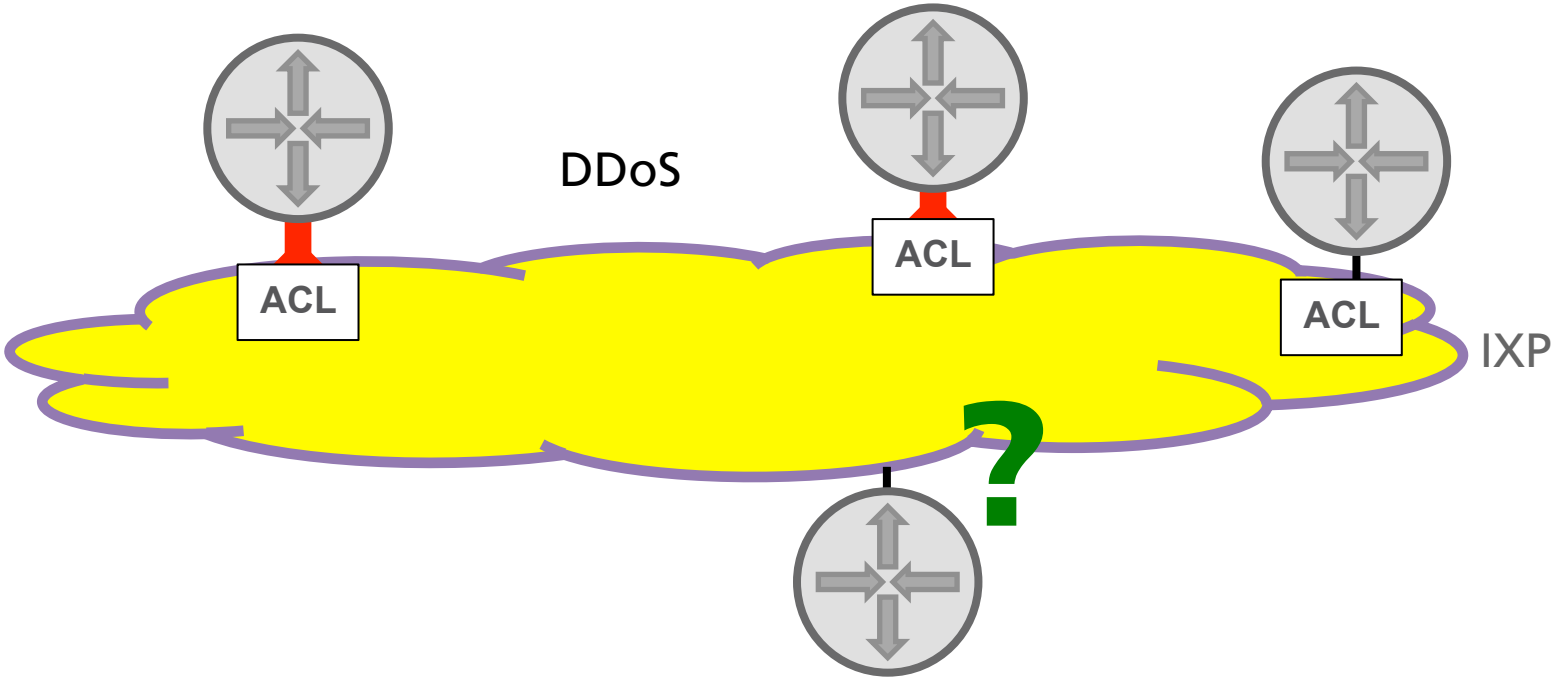
New Developments

Well-Known BGP Community for Blackholing



- Currently, many IXPs provide the blackholing feature
- Triggering is implemented differently at different IXPs (e.g. BGP community, next hop IP address)
- A commonly agreed trigger is preferred: Well-known BGP community for blackholing
- All IXPs offering the blackholing feature voted on the Euro-IX tech mailing list for: **65535:666**
- An Internet Draft is currently coined – support is highly appreciated
  - draft-ymbk-grow-blackholing-00

DDoS Attack State Change Notification



- How to monitor state changes of DDoS attack traffic if the traffic is discarded by an active blackhole? Current situation: switching on and off blackholing is a sup-optimal solution.
- DE-CIX started a research project on DDoS state change notification by analyzing IPFIX data from blackholed traffic
- Customer will be notified by mail/API if the DDoS traffic characteristics for their blackhole changes

Federal Ministry of Education and Research

BGP-ACL

- Why limiting blackholing to IP prefixes?
- Why not providing a mechanism to customers to control certain types on ACLs on the IXP-side?
- Idea: define BGP communities (or other API) to trigger blackholing depending on
  - Source and destination MAC address
  - Source and destination IP address
  - Source and destination TCP/UDP port
- BoF during RIPE 68 about this idea
- Current state: Implementing this with existing gear does not scale

DE·CIX

Awesome for 20 years

Thank you!

Any Questions?

Visit: de-cix.net → Products & Services → Blackholing

DE-CIX Management GmbH
Lindleystr. 12
60314 Frankfurt
Germany
Phone +49 69 1730 902 0

daniel.kopp@de-cix.net

www.de-cix.net