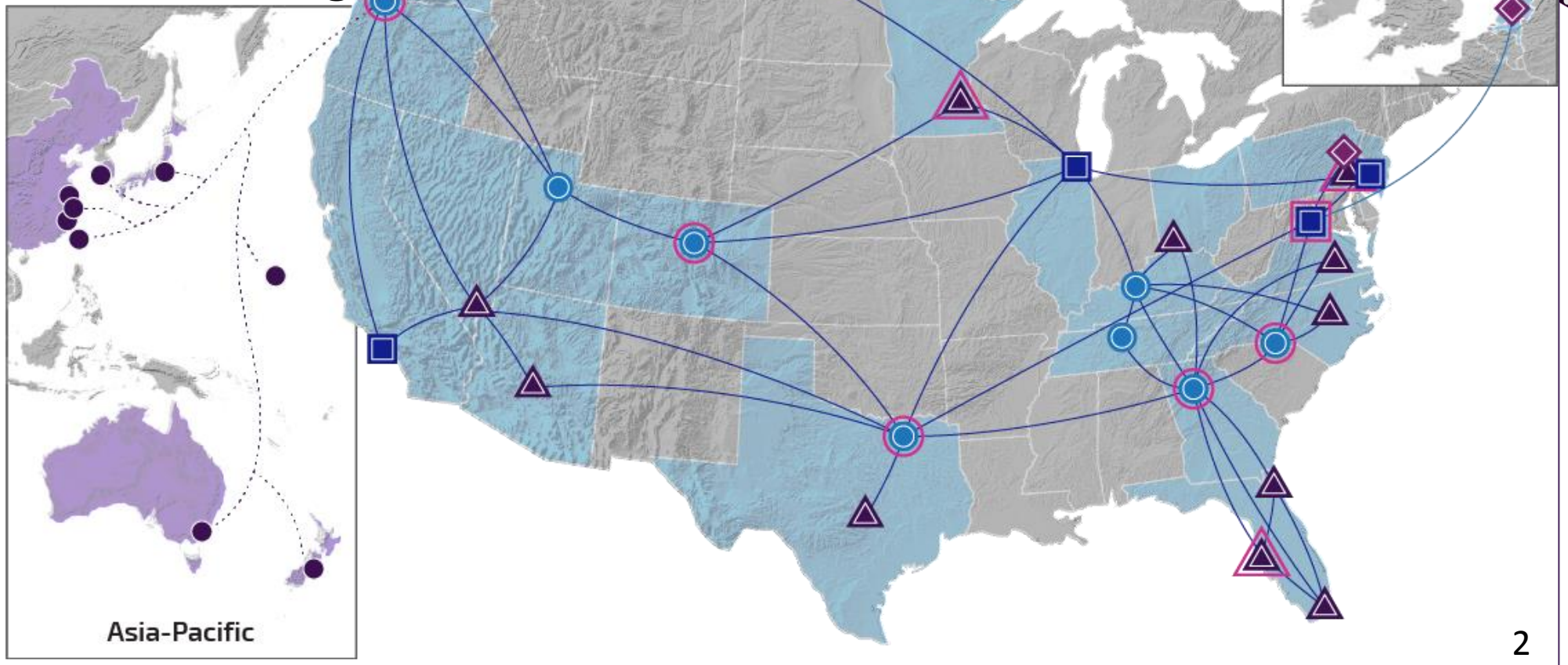
Automated DDOS Protection for our National Service-Provider Backbone

Jeremy Palmer, Senior Backbone Network Engineer

FLEXENTIAL

Flexential Backbone Network

- 3Tb/s Capacity
- 12,000+ Route Miles
- 496 Dark Fiber Pairs
- Automated DDOS Scrubbing



Steps to Mitigate a DDOS Attack

Step1: Attack Detection

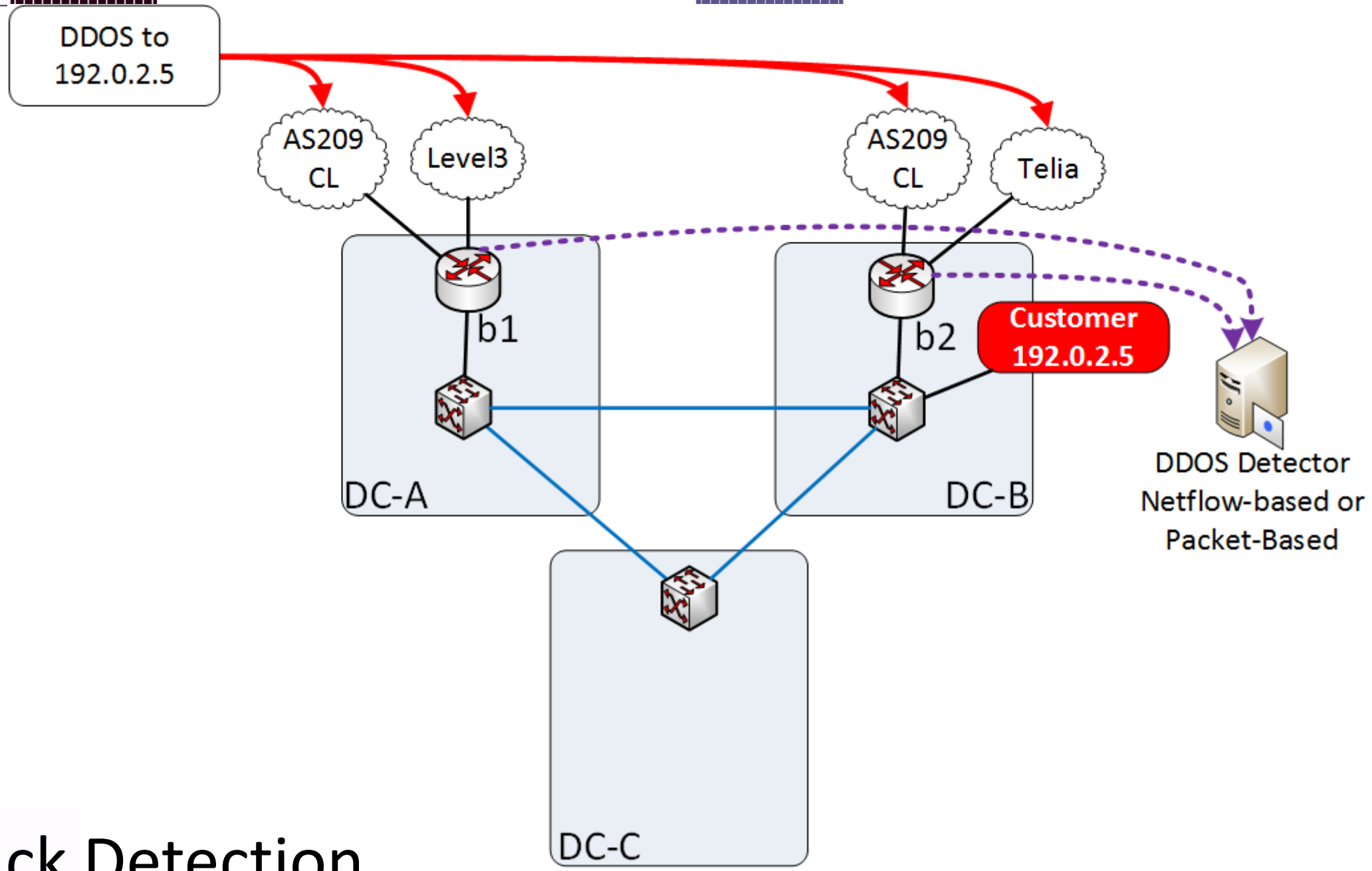
- Netflow-based Detection: Inexpensive to deploy, slower detection
- Packet-based Detection: Fast detection, more expensive deployment

Step 2: Rerouting Attack Traffic

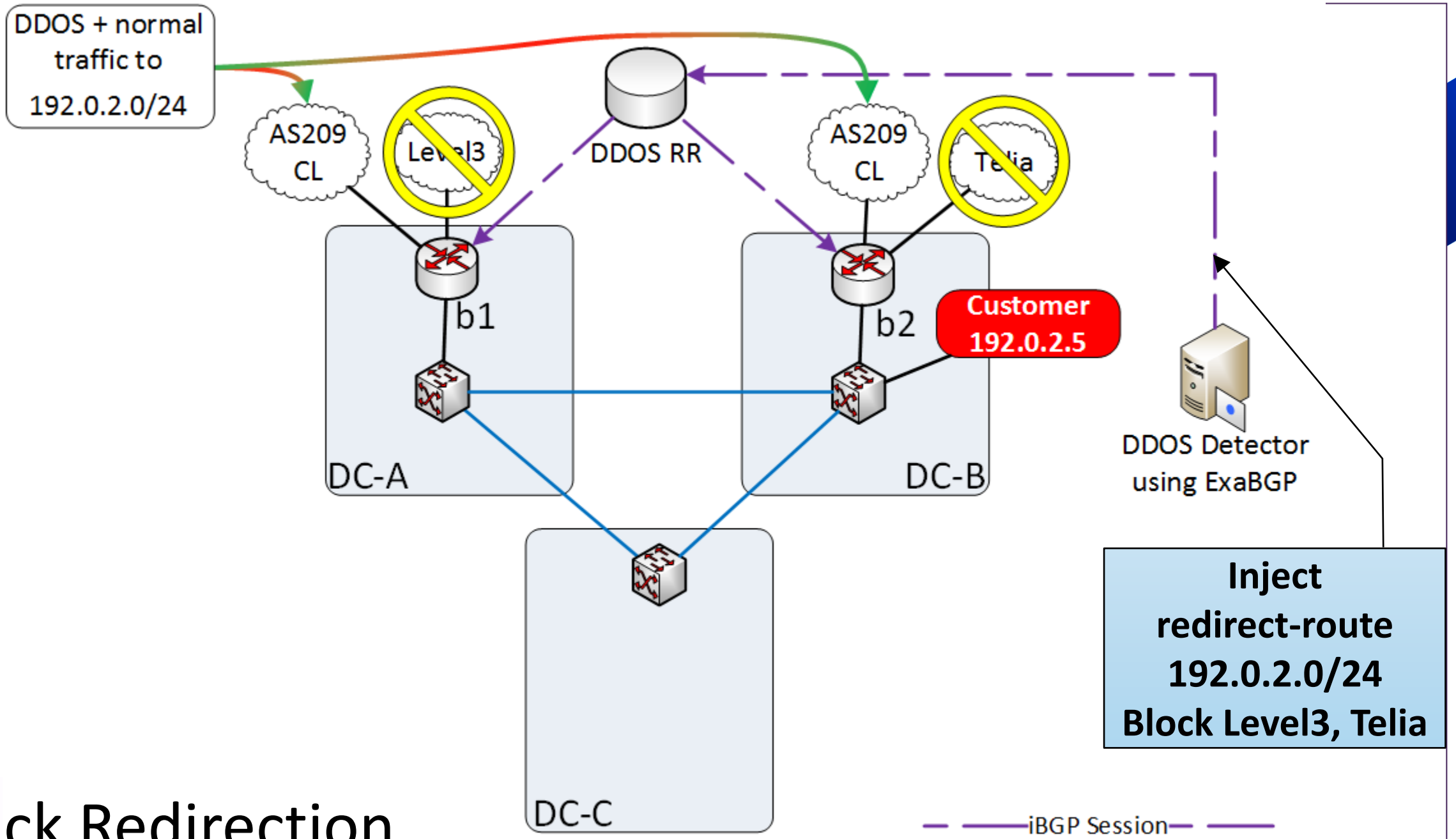
- Announce /24 “redirect-route” using special “blocking” communities
- This withdraws any existing /24 prefix from non-scrubbing provider

Step 3: Attack Scrubbing and Clean Traffic Return

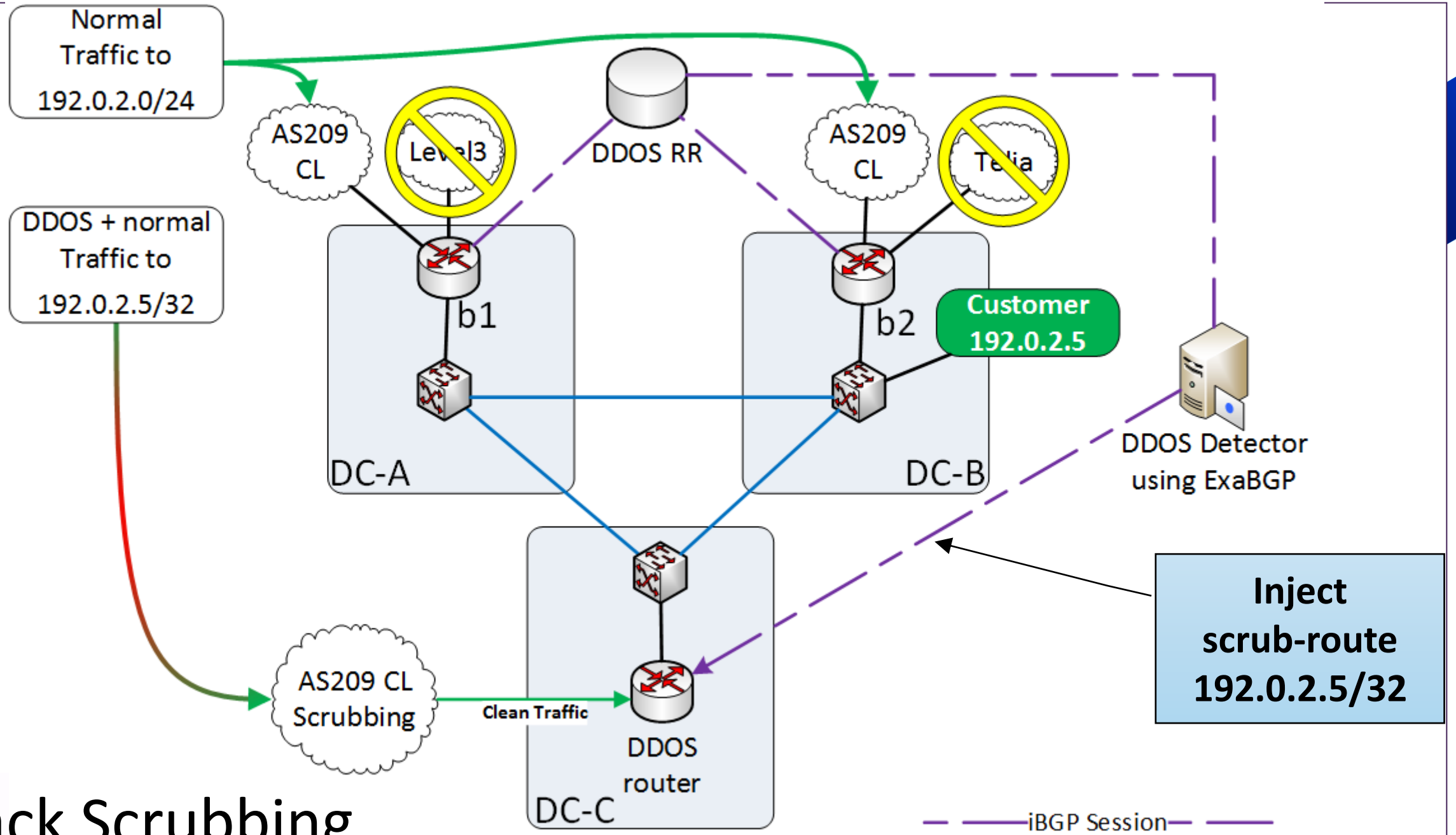
- Inject /32 “scrub-route” to scrub-AS scrub service, bring clean traffic back in via dedicated “DDOS” routers/circuits.



Attack Detection



Attack Redirection



Attack Scrubbing

BGP Route Visual

Normal connectivity to transit/peers

“Before”

BGP Route Visual

All Roads Lead to Scrubbing AS

“After”

DDOS Mitigation: One size does not fit all…

- This method of DDOS redirect works best with prefixes originated from own ASN
- Can also work well for BGP single-homed customers who announce their own prefixes from their own ASN to you.
- Downstream customers who BGP multi-home to you AND other transit ASNs need special care:
  - Traffic may normally ingress via other Transit ASN, bypassing detection.
  - They should filter their own prefixes inbound to prevent learning the redirect-route from other Transit peers.

Questions? Send me an email!

Jeremy.Palmer@flexential.com