Advanced BlackHoling - ABH

François Contat

Agence nationale de la sécurité des systèmes d'information

http://www.ssi.gouv.fr/en

RIPE 73 - October 25th, 2016

Your situation

Ongoing DDoS

Backbone admin

Enough transit bandwidth

Service(s) down

RTBH is not acceptable

DIY solution

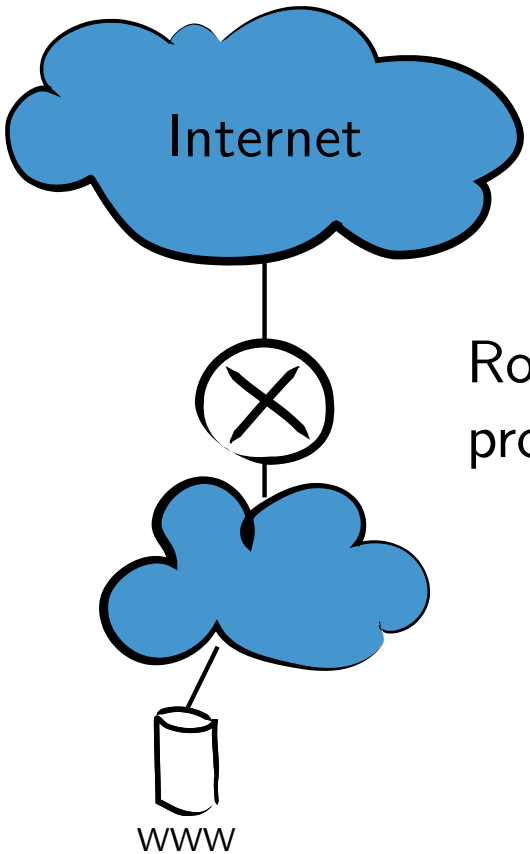
Anti-DDoS Solutions

	Scalability	CPU	Cost	Ease of deployment
ACLs	No	Low	Free	Hard
FlowSpec	Depends	Low	Free	Depends
Vendor-specific	Depends	N/A	High	Easy

Source-Based RTBH - RFC 5635

uRPF strikes again!

Source-Based RTBH - Step #1

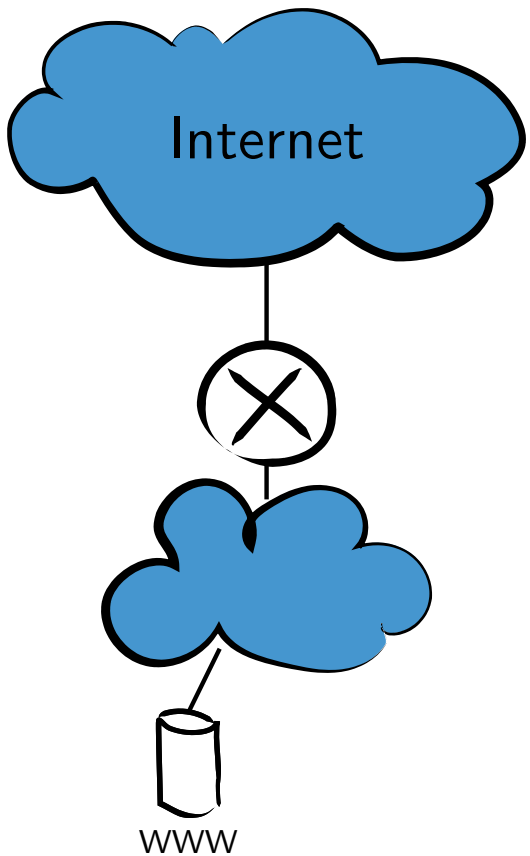


Router connected to a transit provider

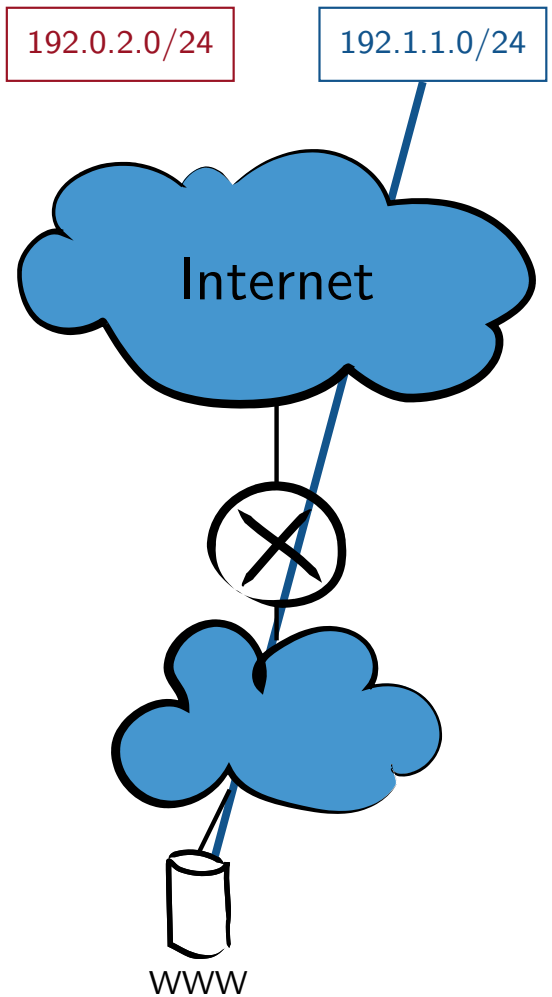
Source-Based RTBH - Step #1

192.0.2.0/24

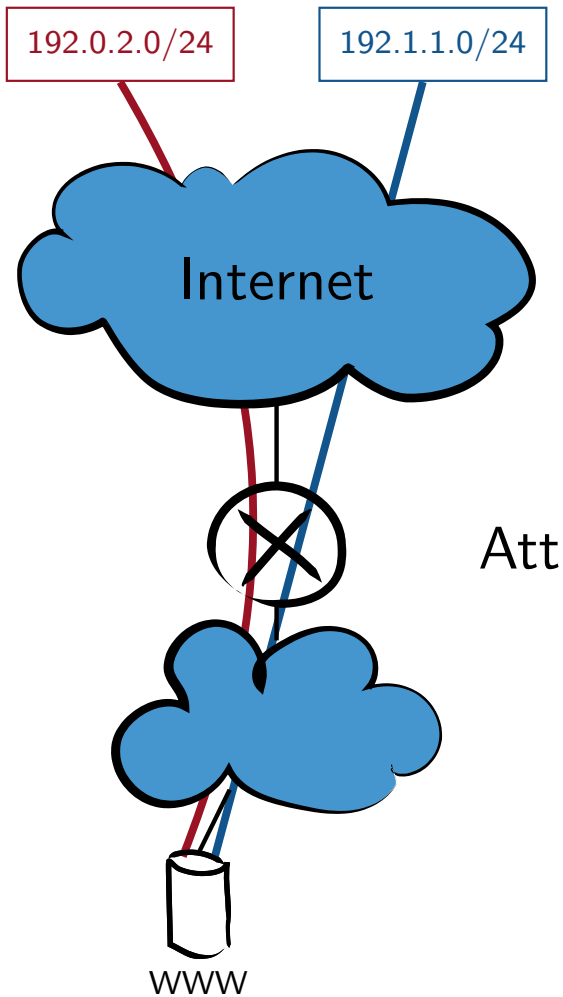
192.1.1.0/24



Source-Based RTBH - Step #1

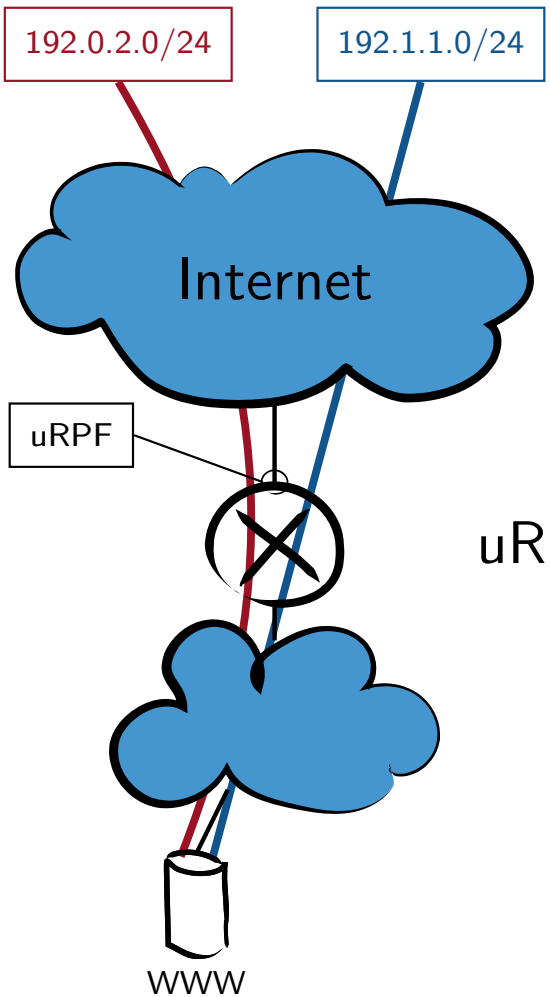


Source-Based RTBH - Step #4



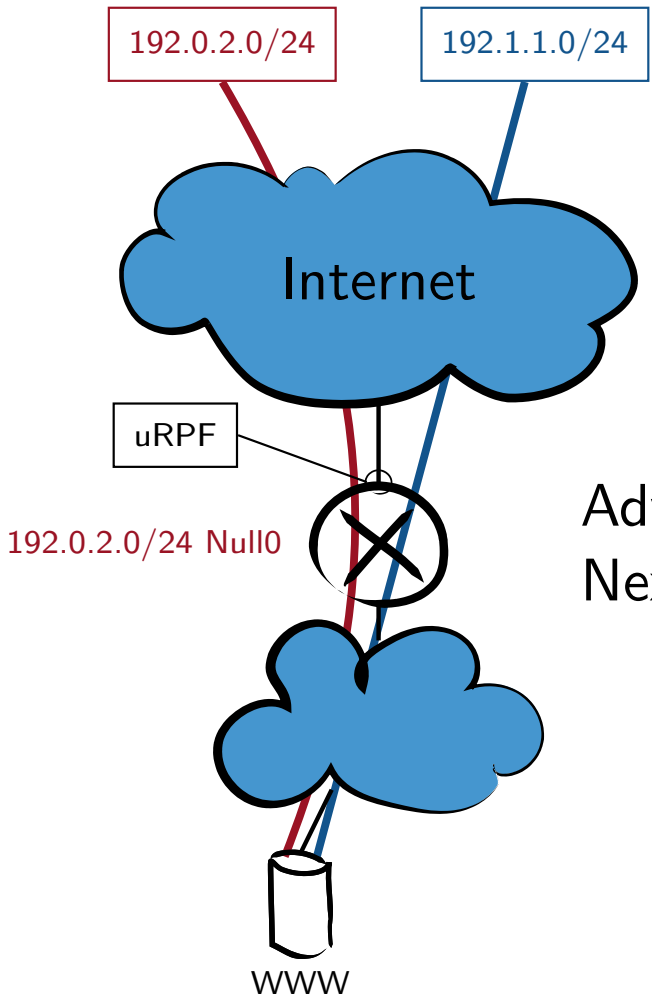
Attack traffic to the web server

Source-Based RTBH - Step #5



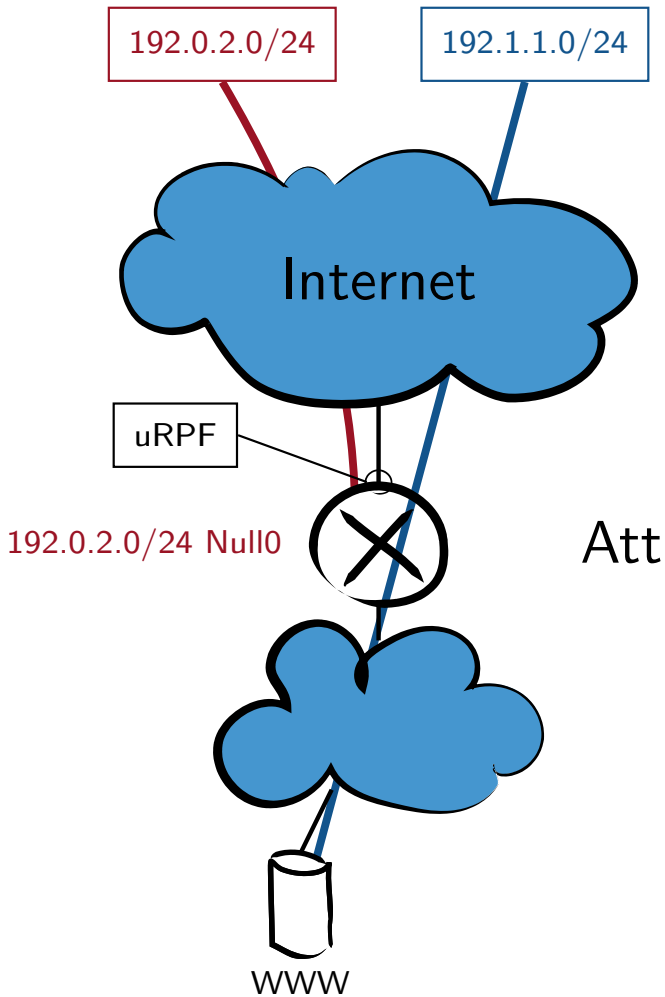
uRPF on the upstream interface

Source-Based RTBH - Step #6



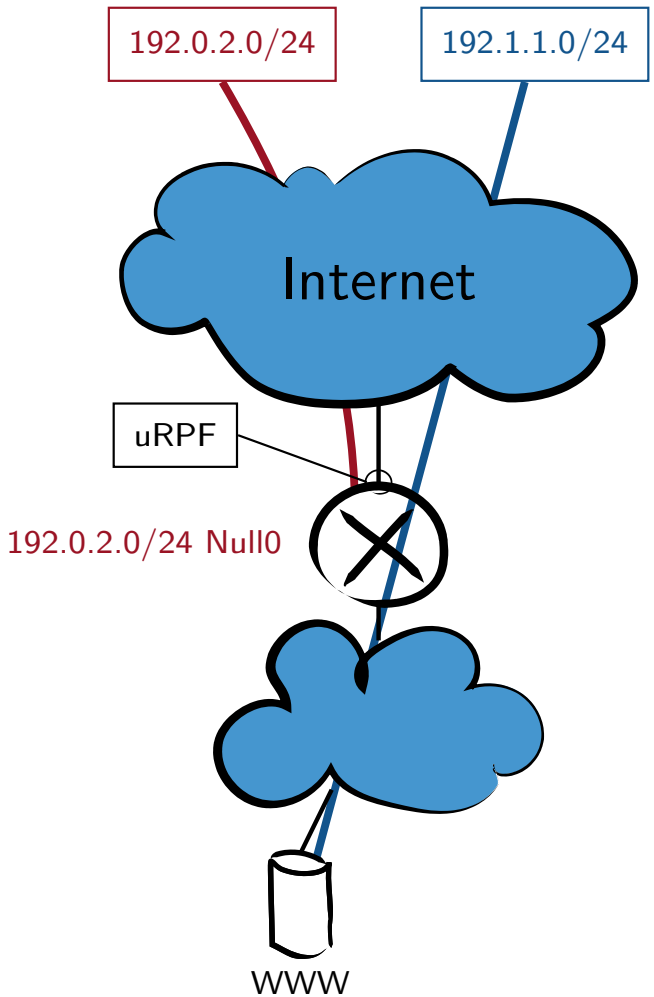
Advertisement of attacker prefix with Next-Hop Null0

Source-Based RTBH - Step #7



Attack mitigated => Beer time \o/

Source-Based RTBH - Summary

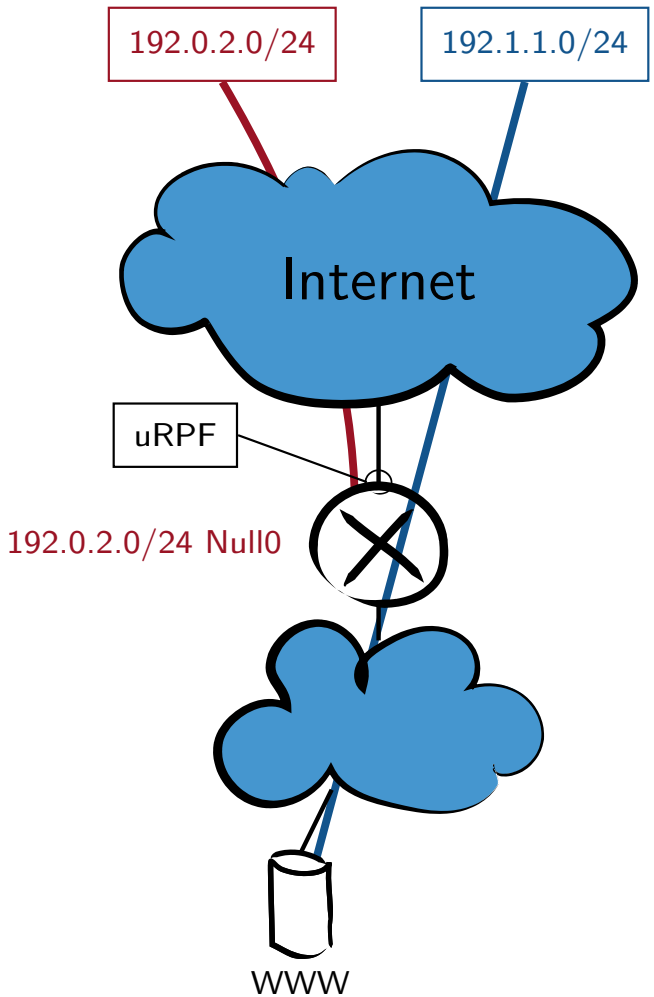


Attack prefix advertisement

Line rate performance!

If multihoming => loose mode

Source-Based RTBH - Summary



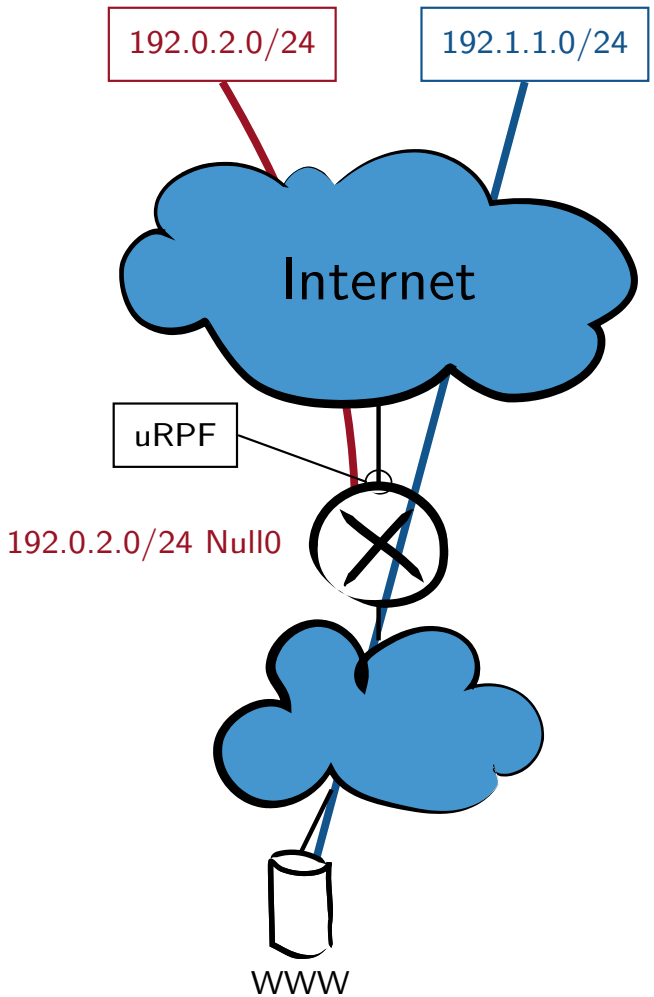
Attack prefix advertisement

Line rate performance!

If multihoming => loose mode

Block ALL traffic from the prefix

Source-Based RTBH - Summary



Attack prefix advertisement

Line rate performance!

If multihoming => loose mode

Block ALL traffic from the prefix

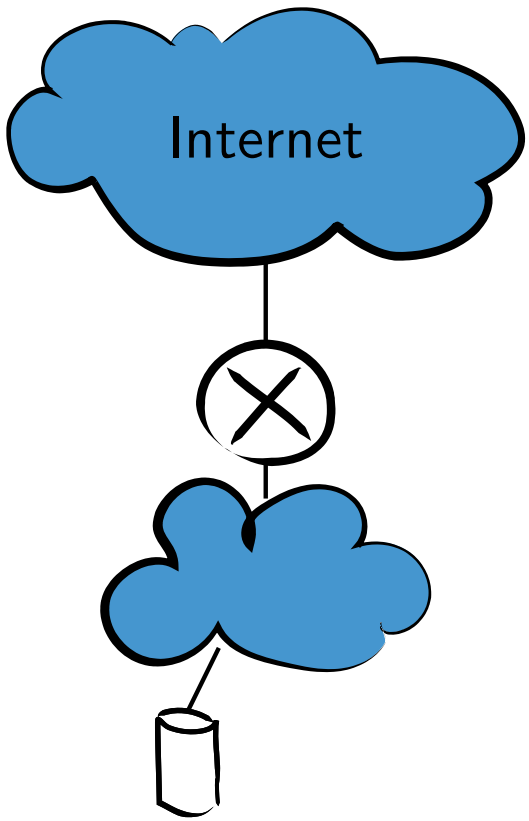
Customer traffic may be dropped

Still good but not ideal

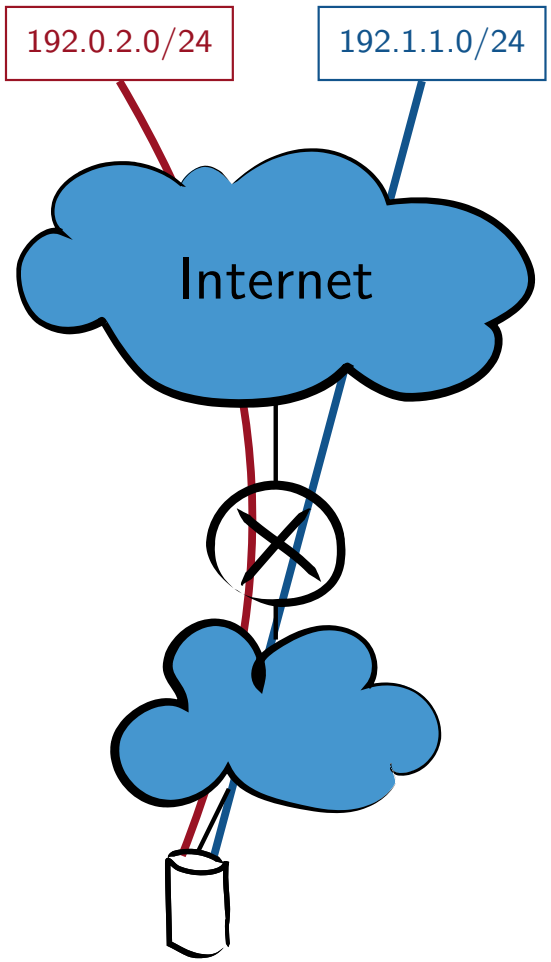
Vendor-Specific

192.0.2.0/24

192.1.1.0/24

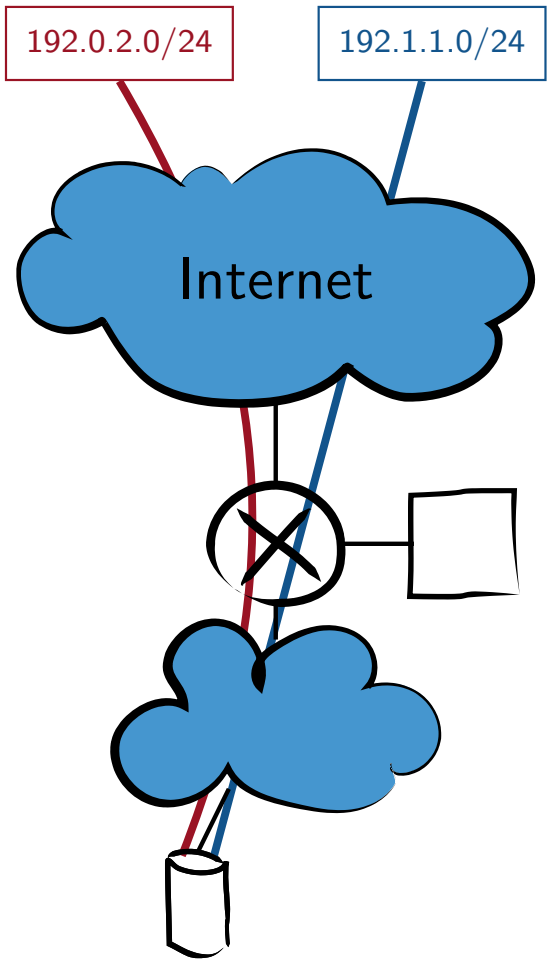


Vendor-Specific



Traffic goes in

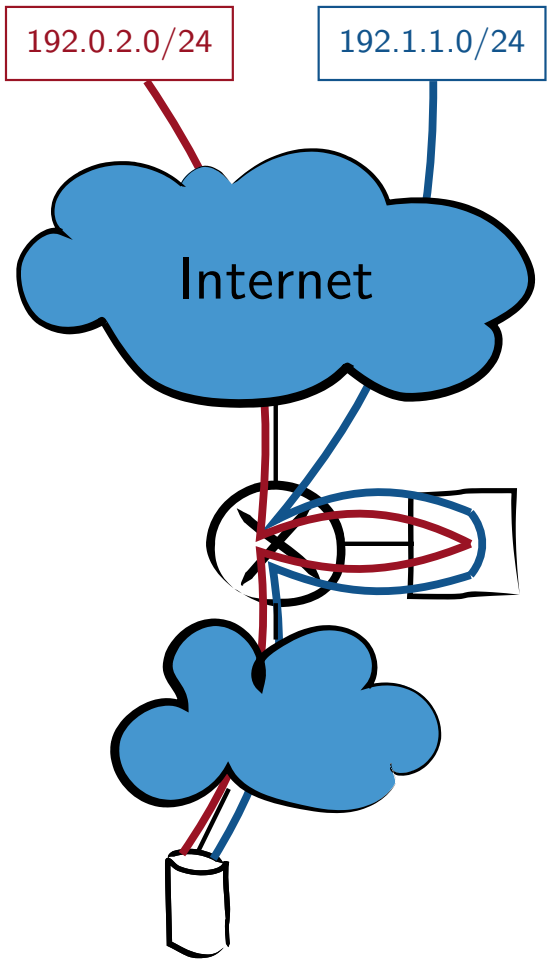
Vendor-Specific



Traffic goes in

Plug a blackbox into iBGP

Vendor-Specific



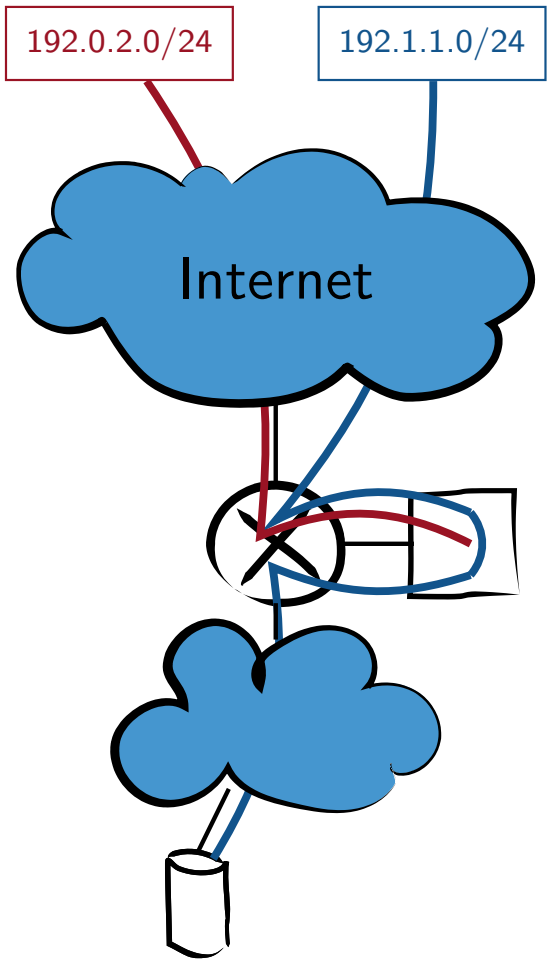
Traffic goes in

Plug a blackbox into iBGP

Divert traffic

Traffic learning

Vendor-Specific



Traffic goes in

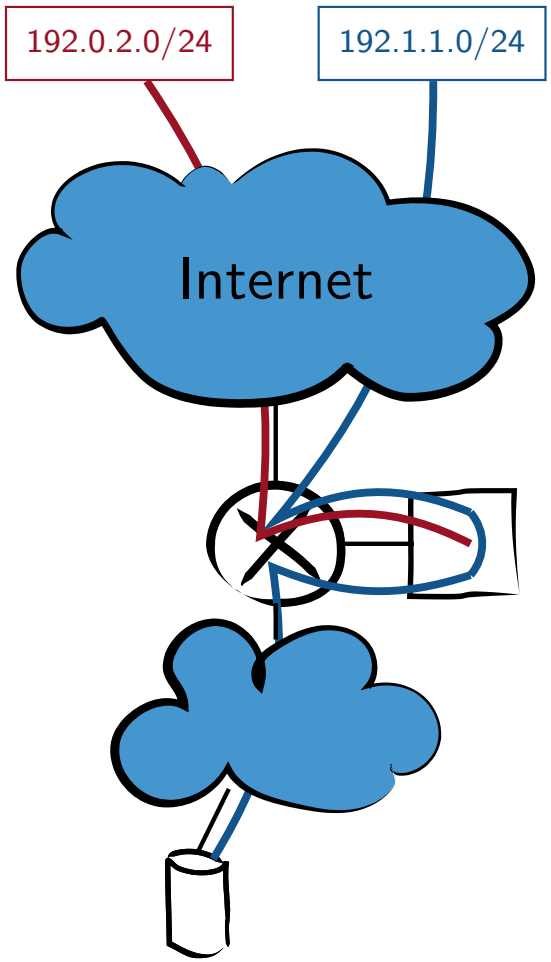
Plug a blackbox into iBGP

Divert traffic

Traffic learning

Scrub traffic

Vendor-Specific



Traffic goes in

Plug a blackbox into iBGP

Divert traffic

Traffic learning

Scrub traffic

Voodoo magic

Capacity depends on license

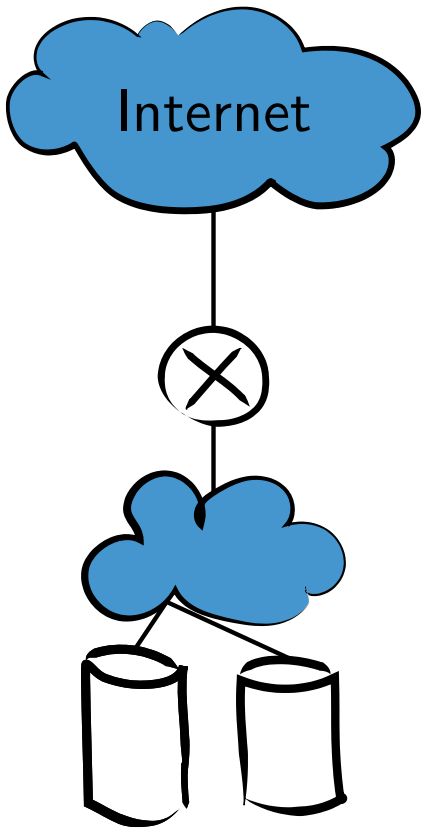
How About Merging both Solutions?

How About Merging both Solution?

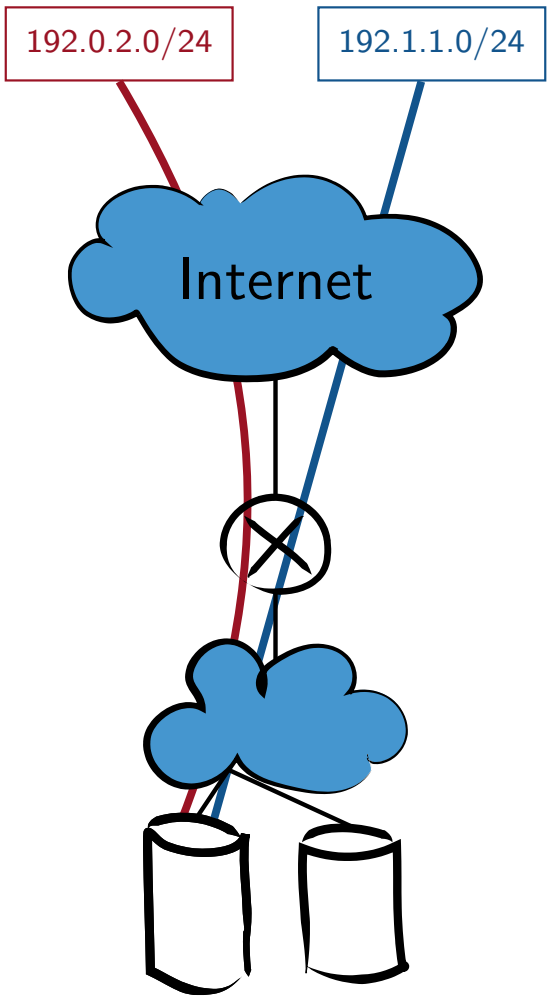
ABH

192.0.2.0/24

192.1.1.0/24

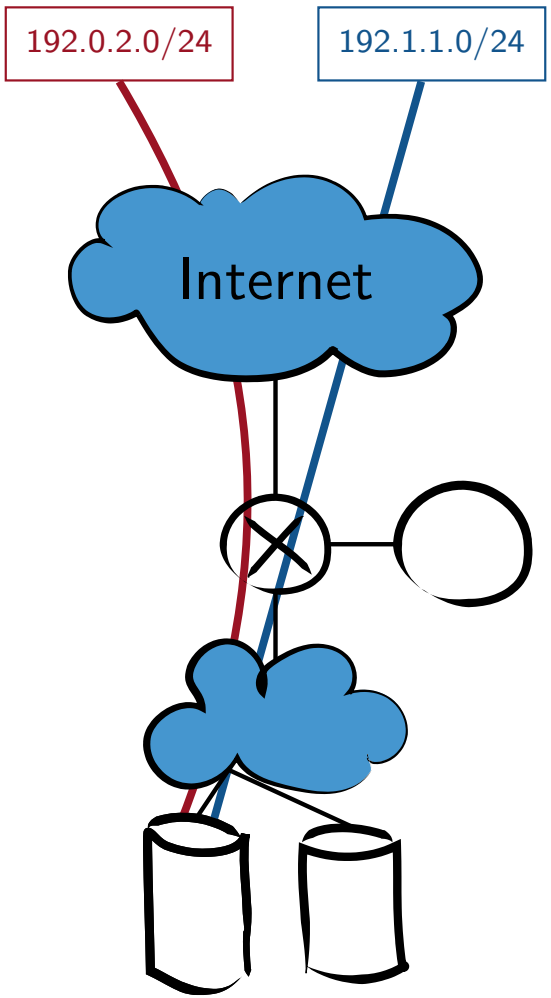


ABH



Web server under attack

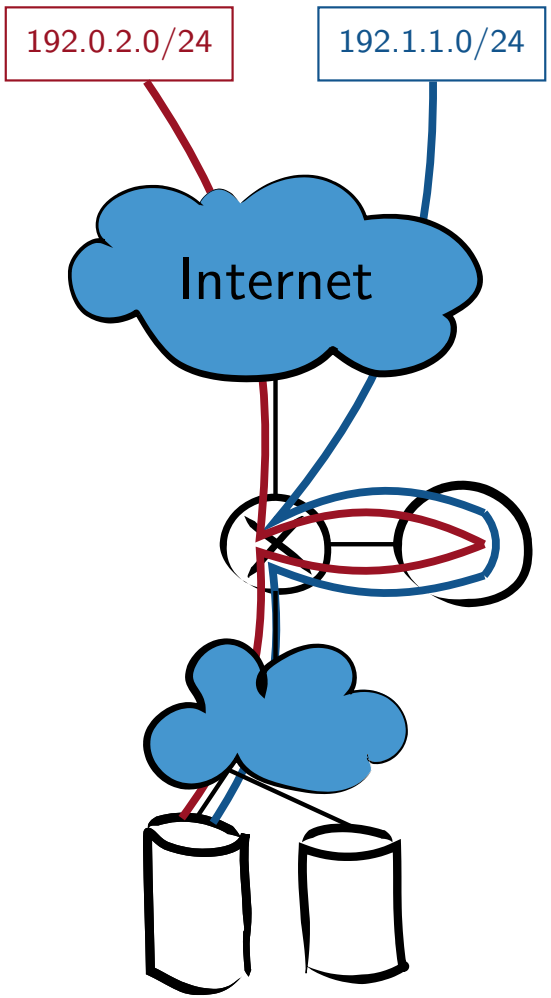
ABH



Web server under attack

Plug a router => ABH

ABH

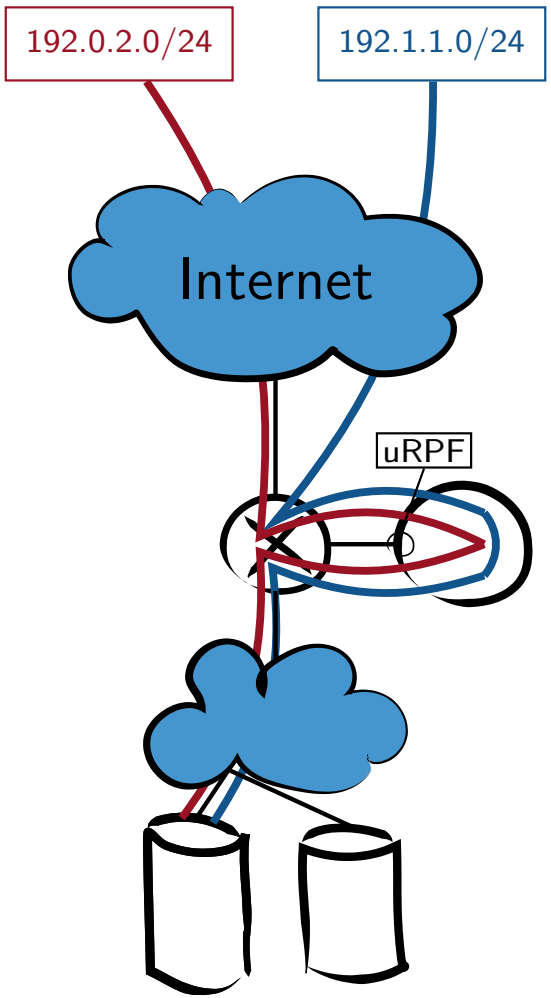


Web server under attack

Plug a router => ABH

Divert traffic to the router

ABH



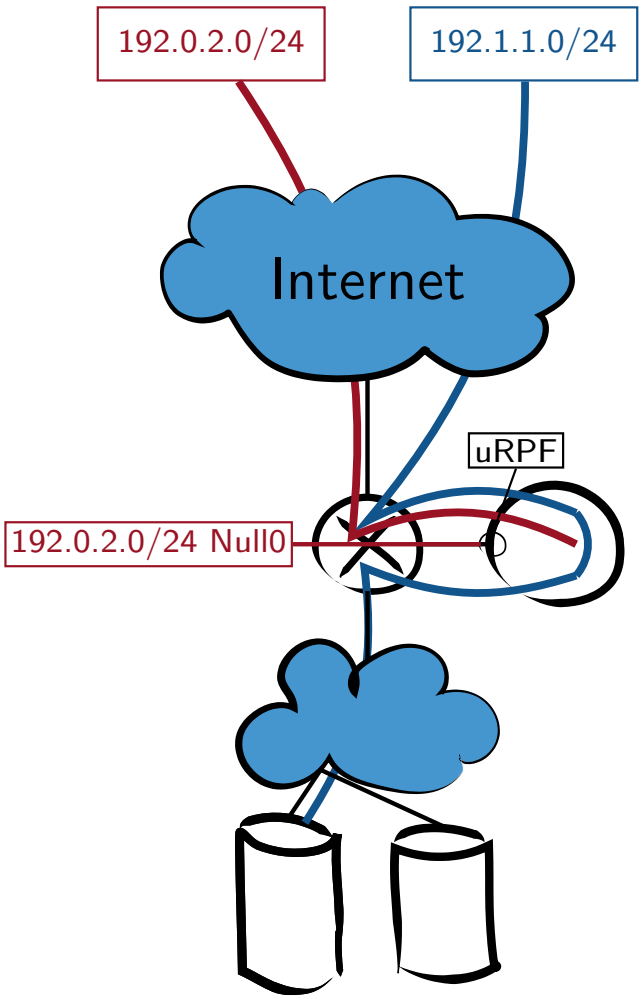
Web server under attack

Plug a router => ABH

Divert traffic to the router

Activate uRPF

ABH



Web server under attack

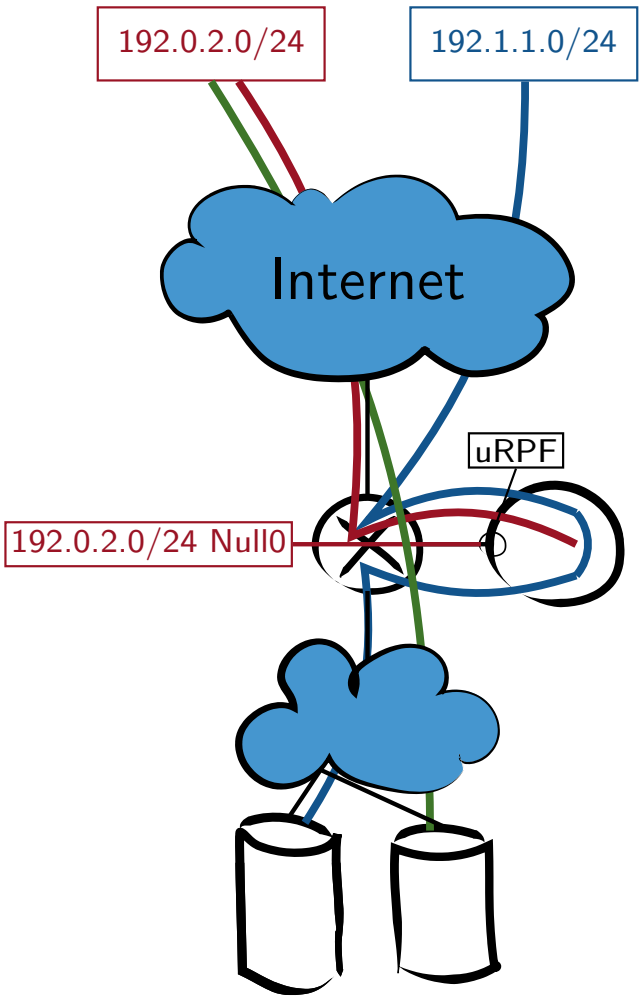
Plug a router => ABH

Divert traffic to the router

Activate uRPF

Set attacker prefix to Null0

ABH



Web server under attack

Plug a router => ABH

Divert traffic to the router

Activate uRPF

Set attacker prefix to Null0

Only attack traffic is dropped

ABH - Summary

- Divert traffic to ABH
  - uRPF
- Set rules to mitigate:
  - Static routes to Null0
  - ACLs
  - Flowspec

ABH - Summary

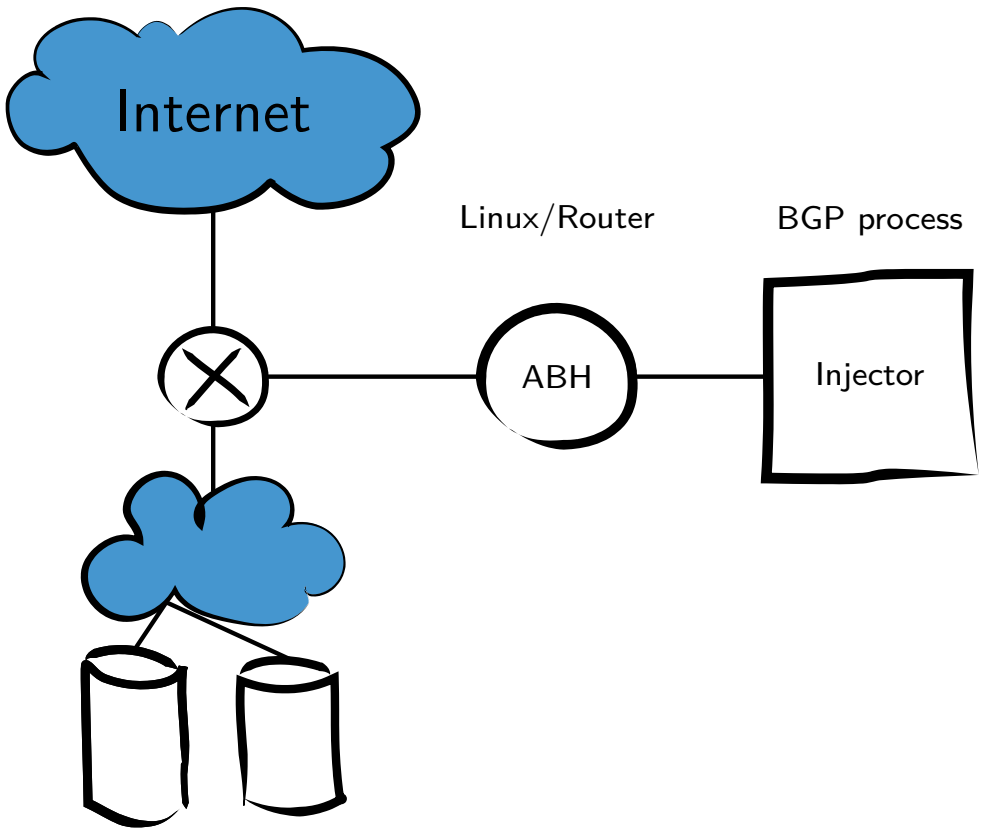
- Divert traffic to ABH
  - uRPF
- Set rules to mitigate:
  - Static routes to Null0
  - ACLs
  - Flowspec

  How about a more flexible mitigation?

Flexible ABH - System Setup

192.0.2.0/24

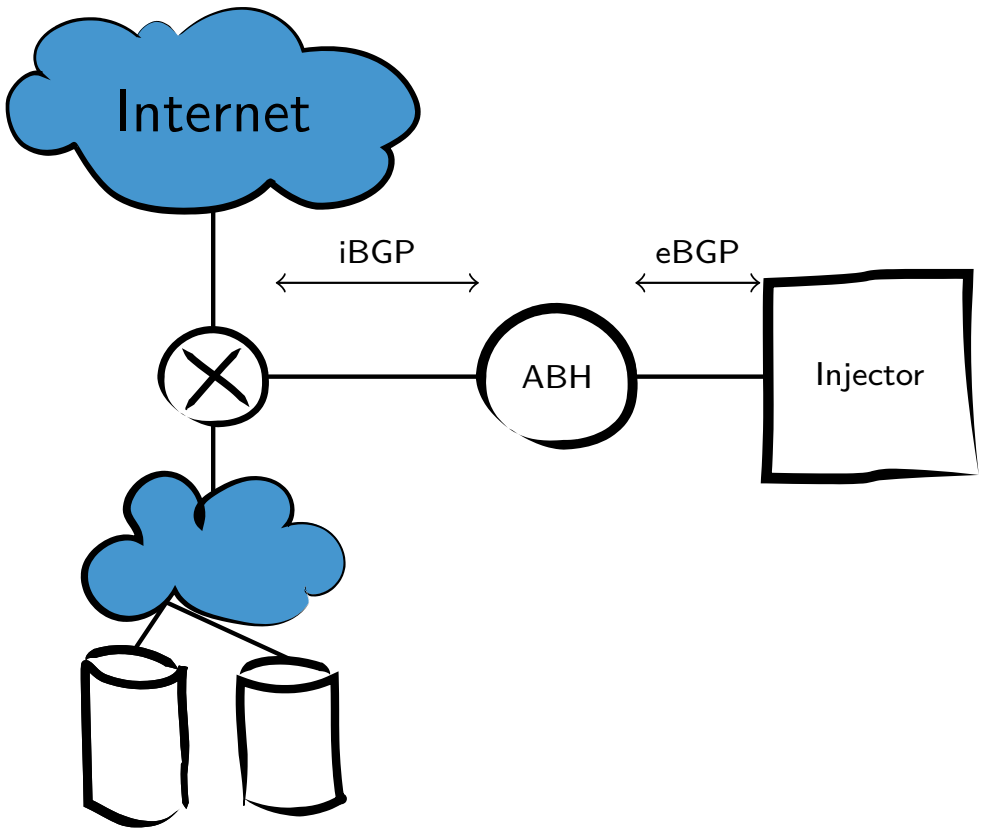
192.1.1.0/24



Flexible ABH - Network Setup

192.0.2.0/24

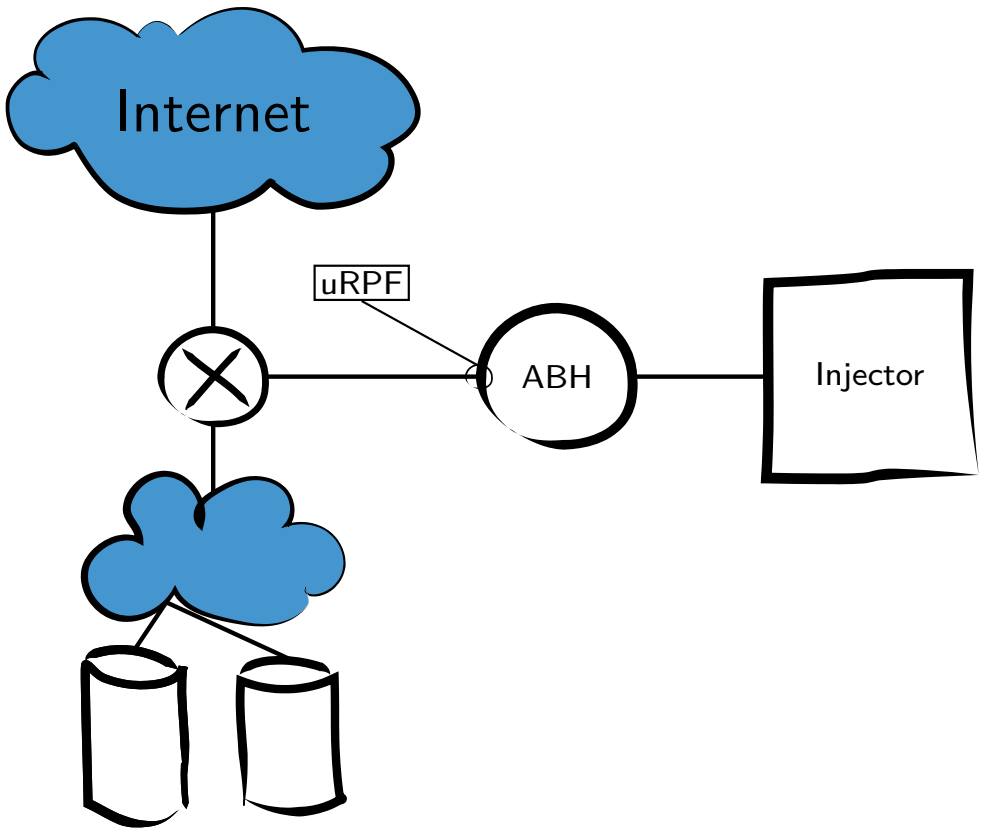
192.1.1.0/24



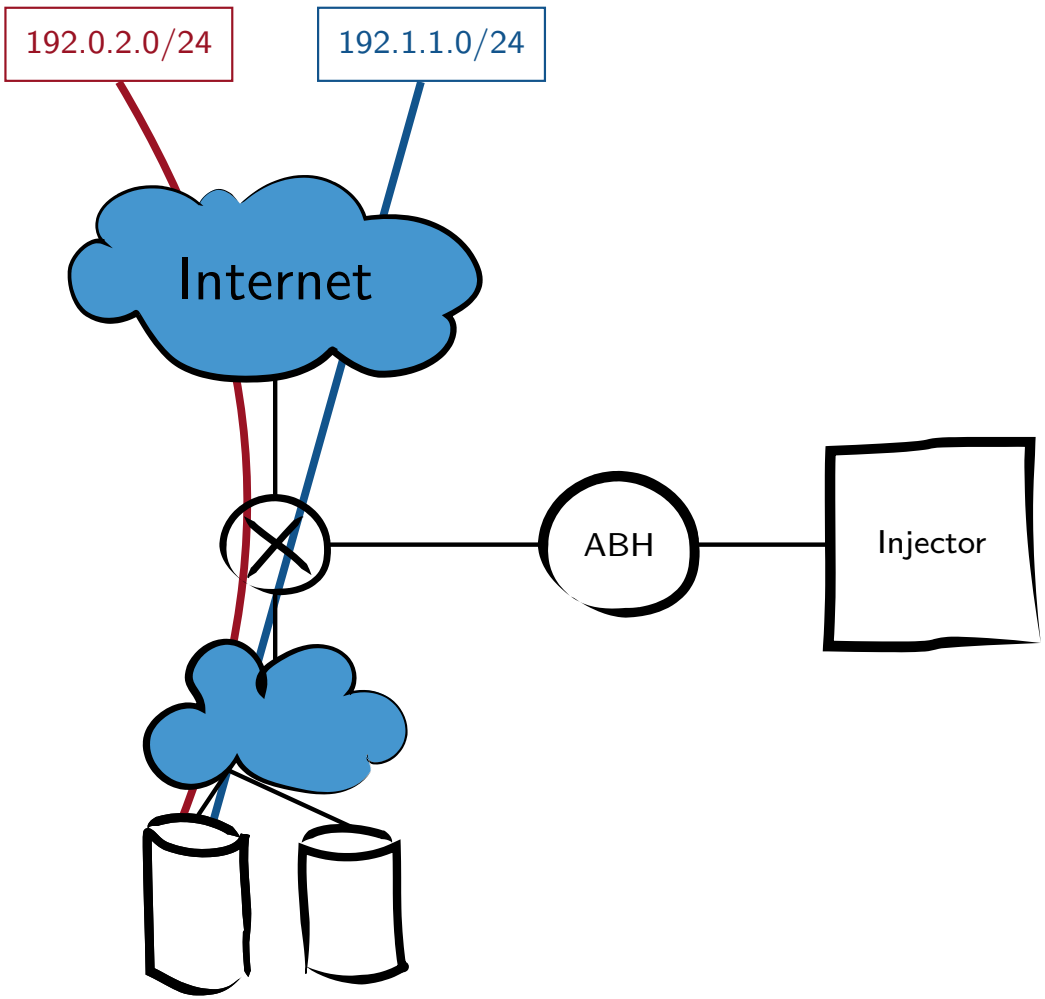
Flexible ABH - Network Setup

192.0.2.0/24

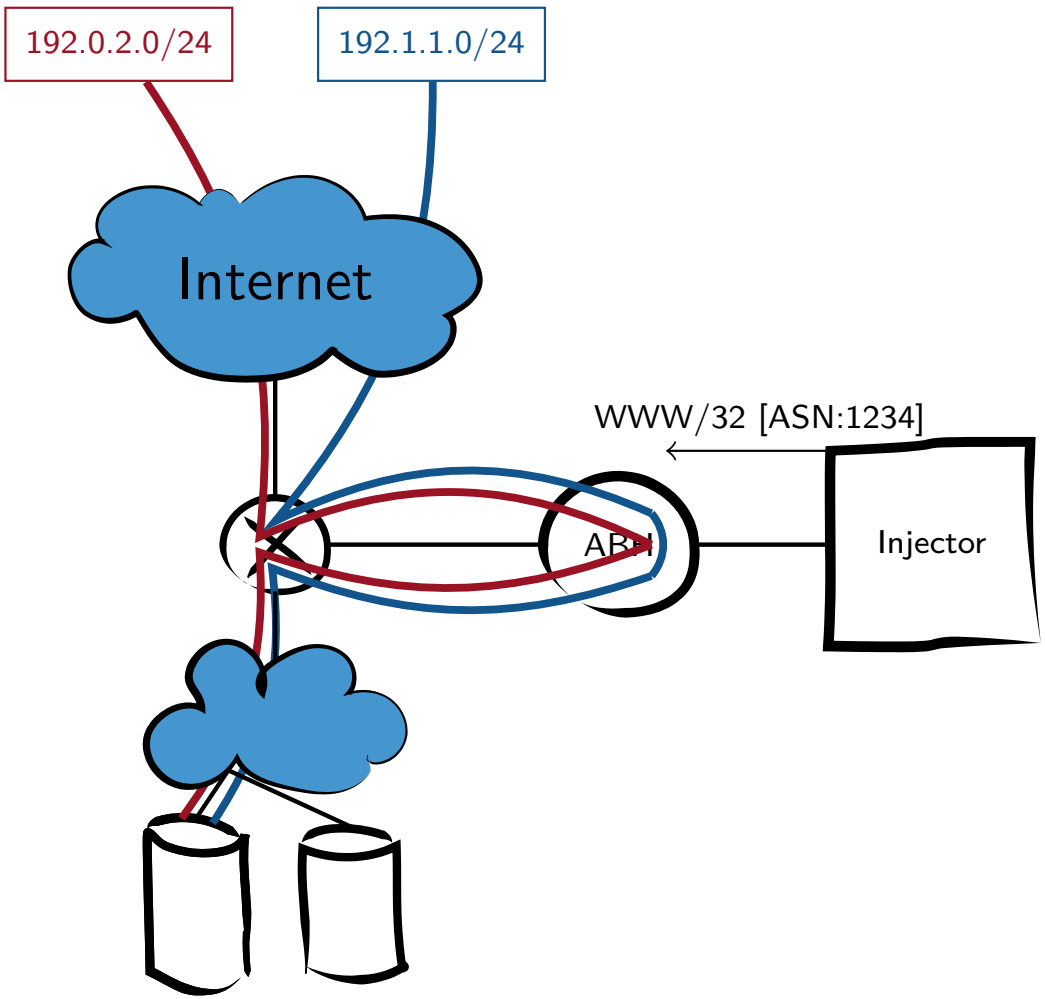
192.1.1.0/24



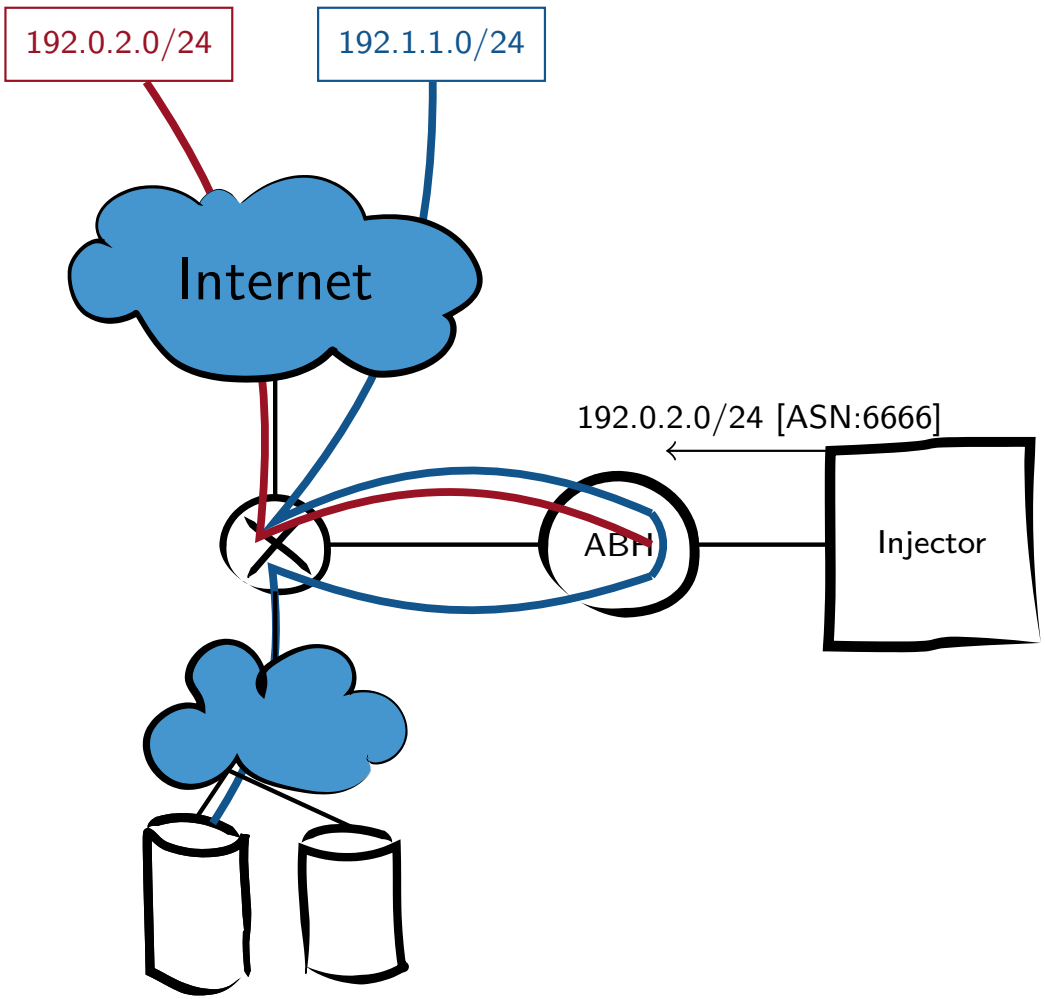
Flexible ABH - Incoming Traffic



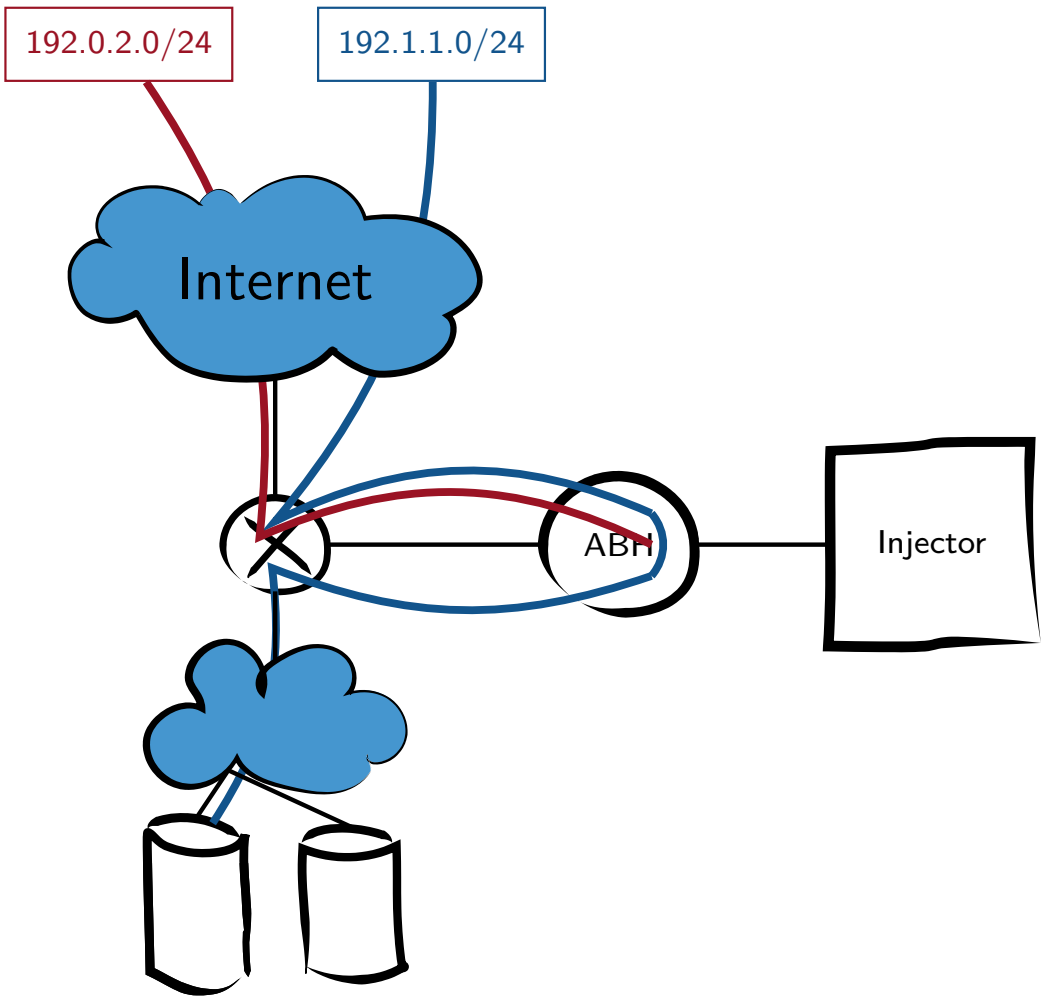
Flexible ABH - Divert Traffic



Flexible ABH - Advertise Bad Prefix



Flexible ABH - Beers!



Feed The Injector

Examples of criteria:

- Well-known IP of exploitable services (DNS, NTP, etc.)
- Geographic community
- Well-know hijack/spam origin AS
- Netflow statistics
- PCAP analysis
- Geographic IP

PoC - ABH Implementation

Router with:

- Add no-advertise community from injector
- Add huge local preference

PoC - Injector Implementation

ExaBGP
Python script to get GRT and:

- Learn routes from eBGP
- Find routes matching criteria
- Inject routes to ABH

ABH - First line of defense

1. ABH filtering
2. TCP SYN Cookies and alike
3. Flowspec
4. Vendor-specific
5. ...

Conclusion 1/2

- Cheap
  - Spare router
  - Linux + 10Gb/s NICs (2.5/3k€)
- Network-based solution
  - Proactivity

Conclusion 2/2

- Scalable
  - BGP equal cost multi-path
  - One injector to rule them all
- Modular
  - First line of defense
  - Flowspec
  - Lower cost of vendor-specific
- Feedbacks
  - Some CDNs and ISPs looking into it
  - Open to yours :)

Thank you for your attention

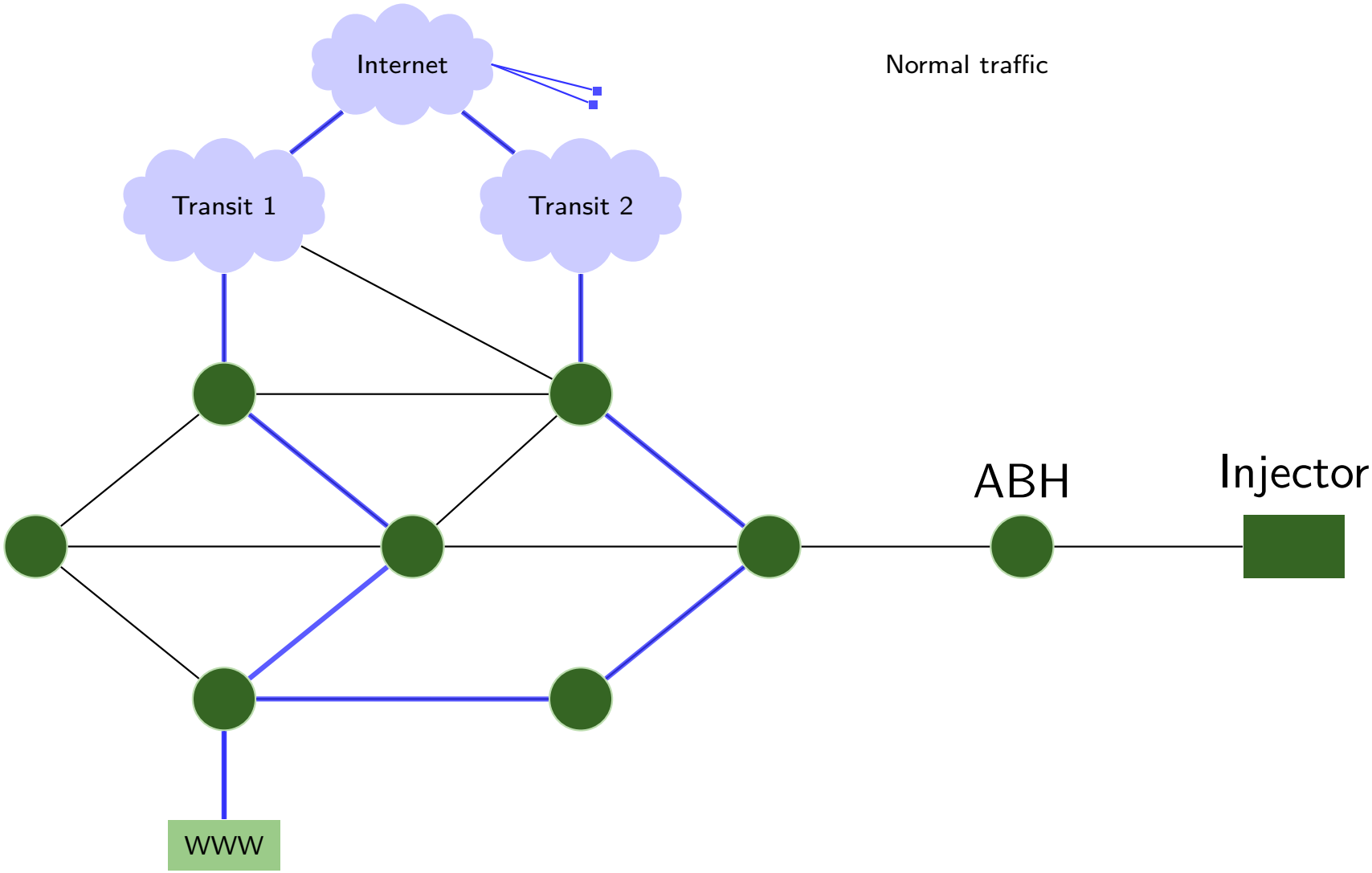
Github Advanced-Blackholing repository (click me)

Observatory 2015 report (click me)
(PDF, Kindle and Epub versions available)

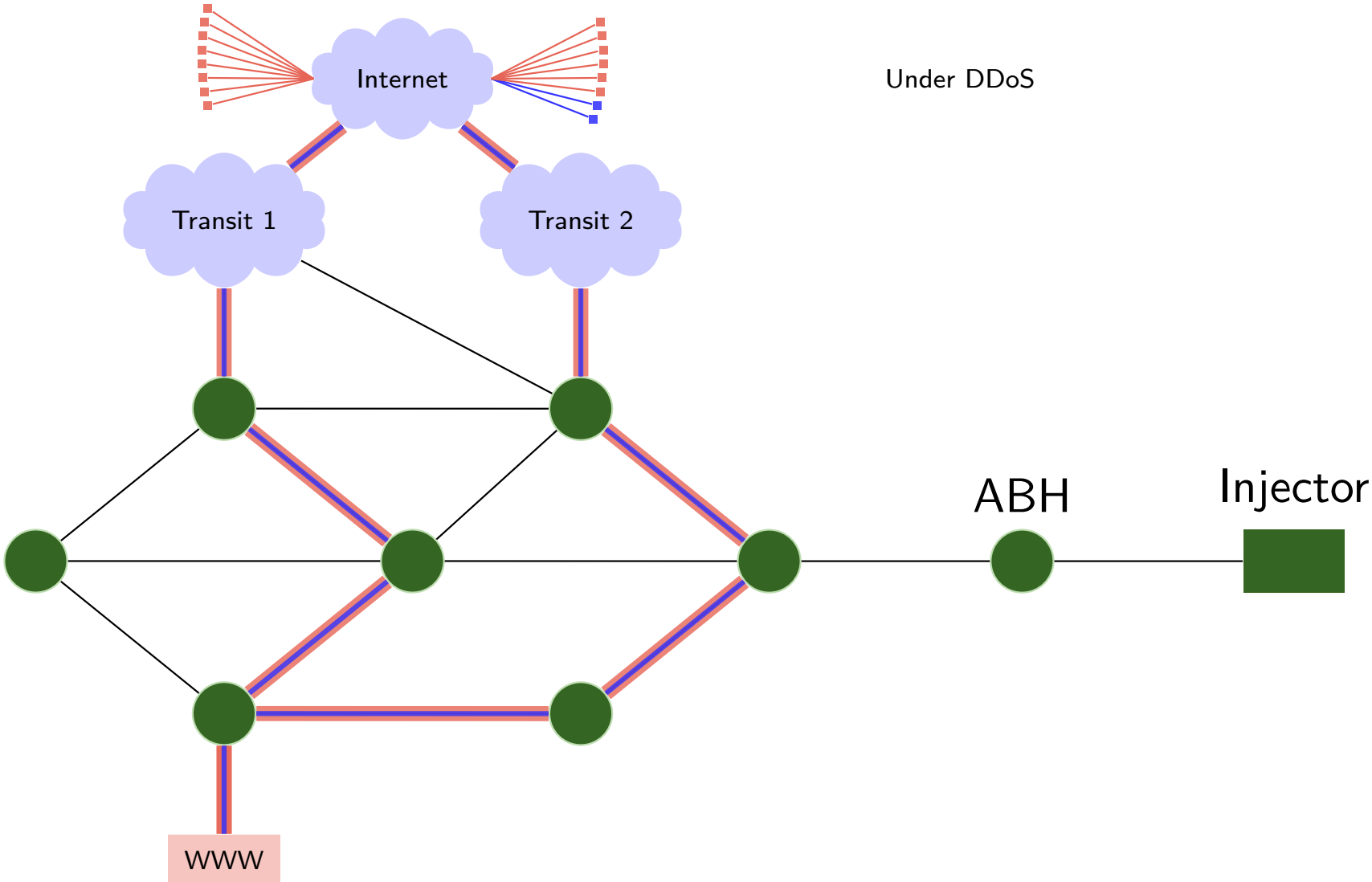
francois[dot]contat[at]ssi.gouv.fr

Questions?

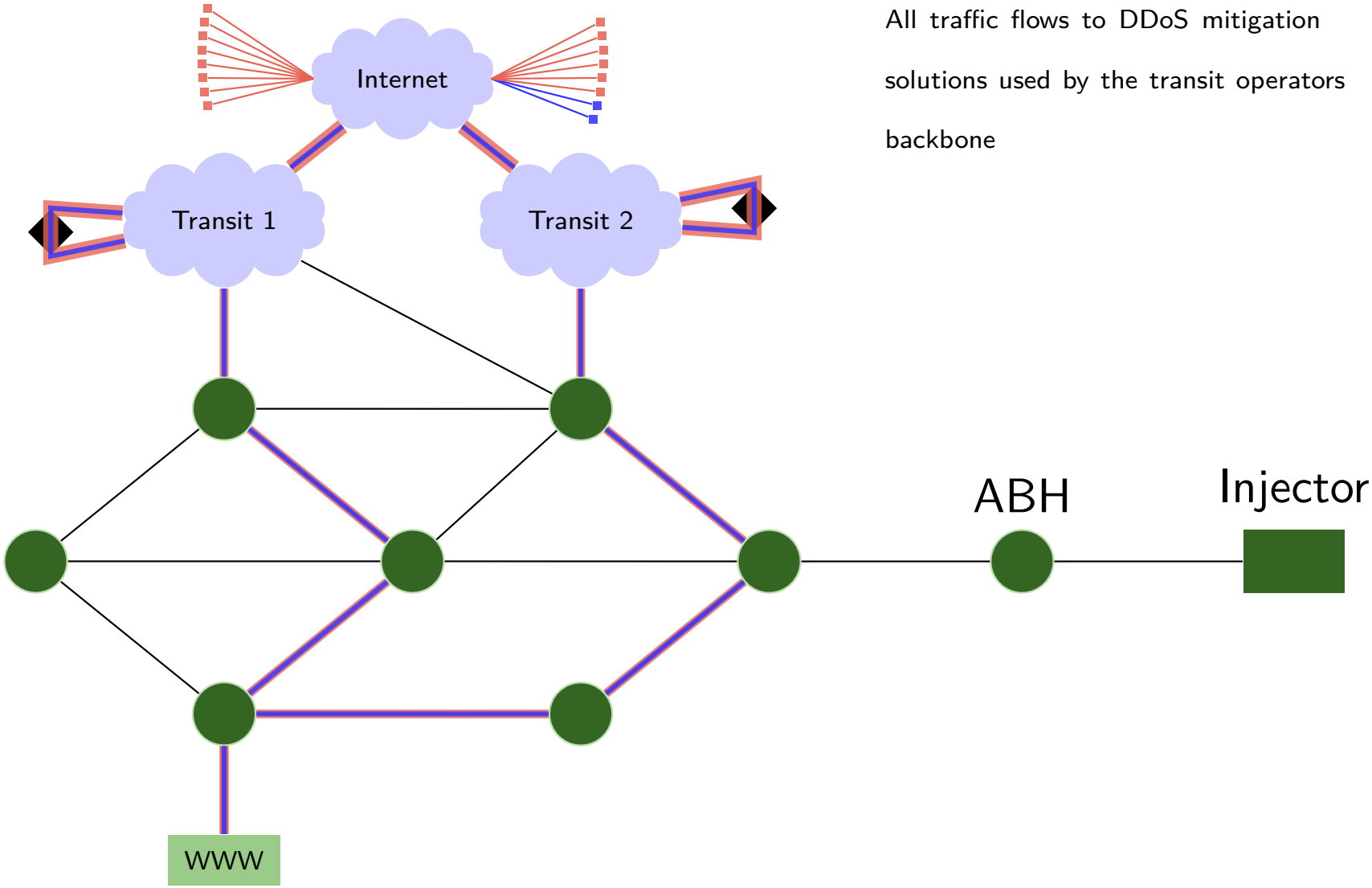
ABH PoC example



ABH PoC example

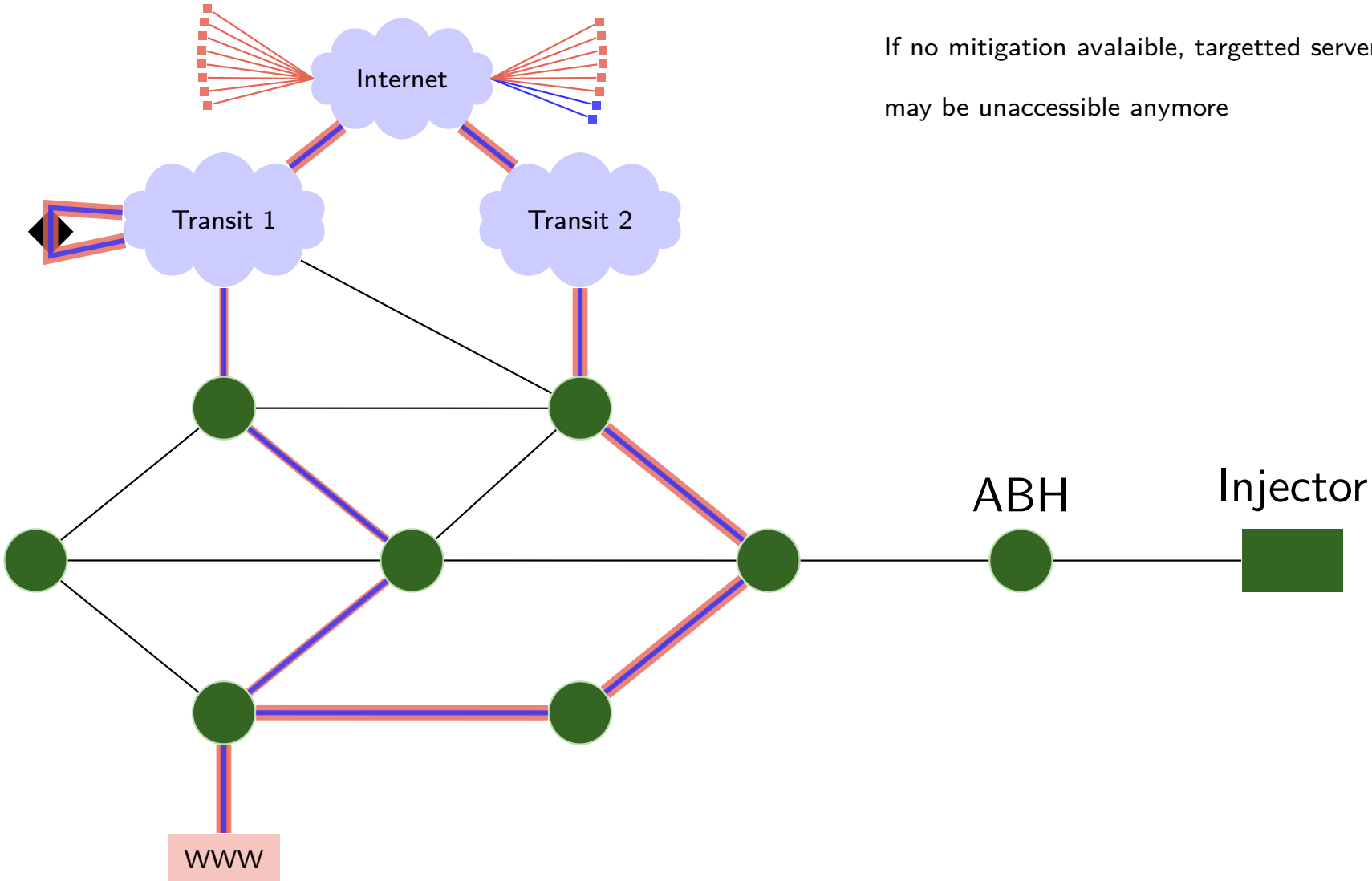


ABH PoC example



All traffic flows to DDoS mitigation solutions used by the transit operators backbone

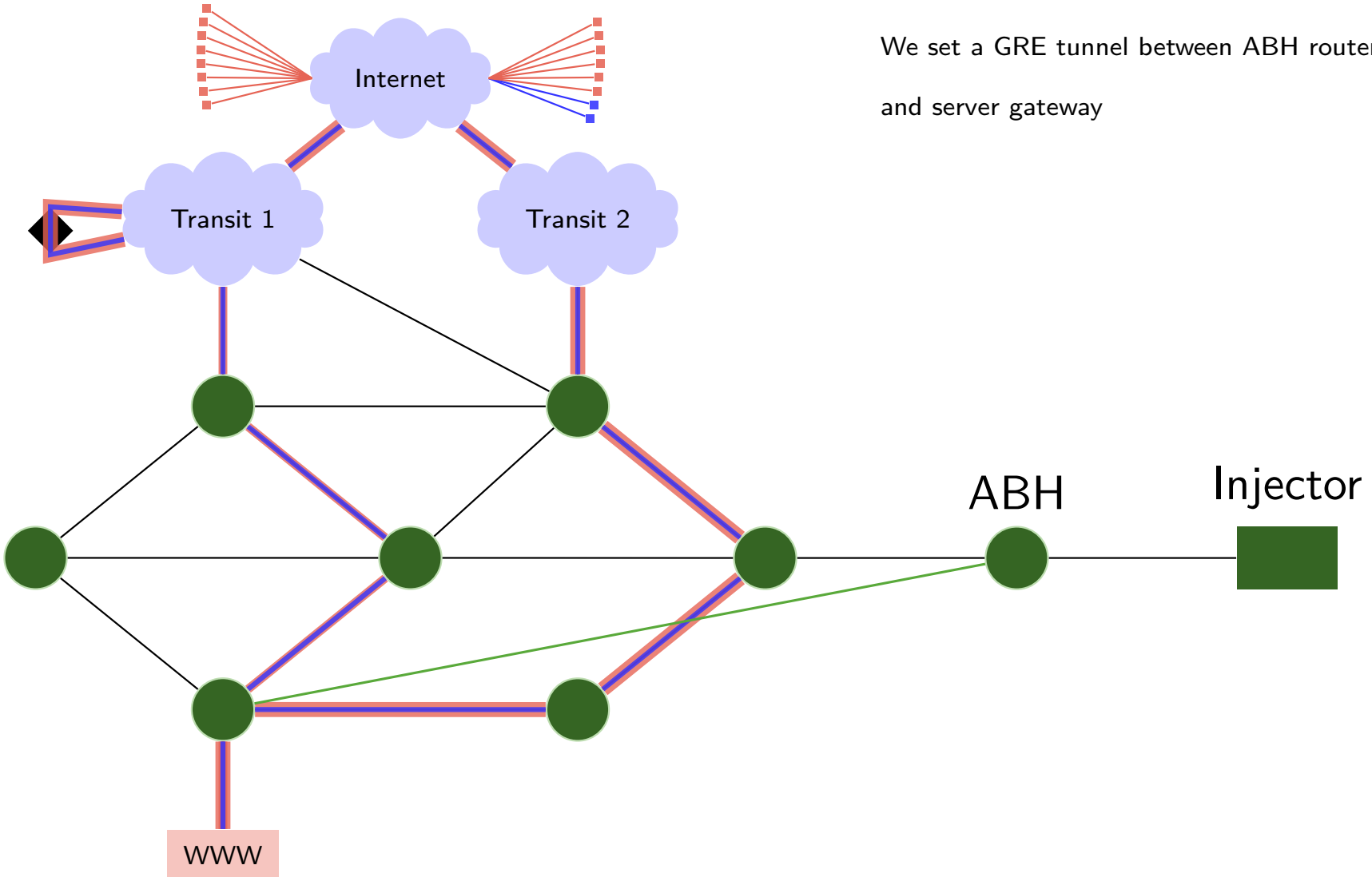
ABH PoC example



If no mitigation avalaible, targetted server

may be unaccessible anymore

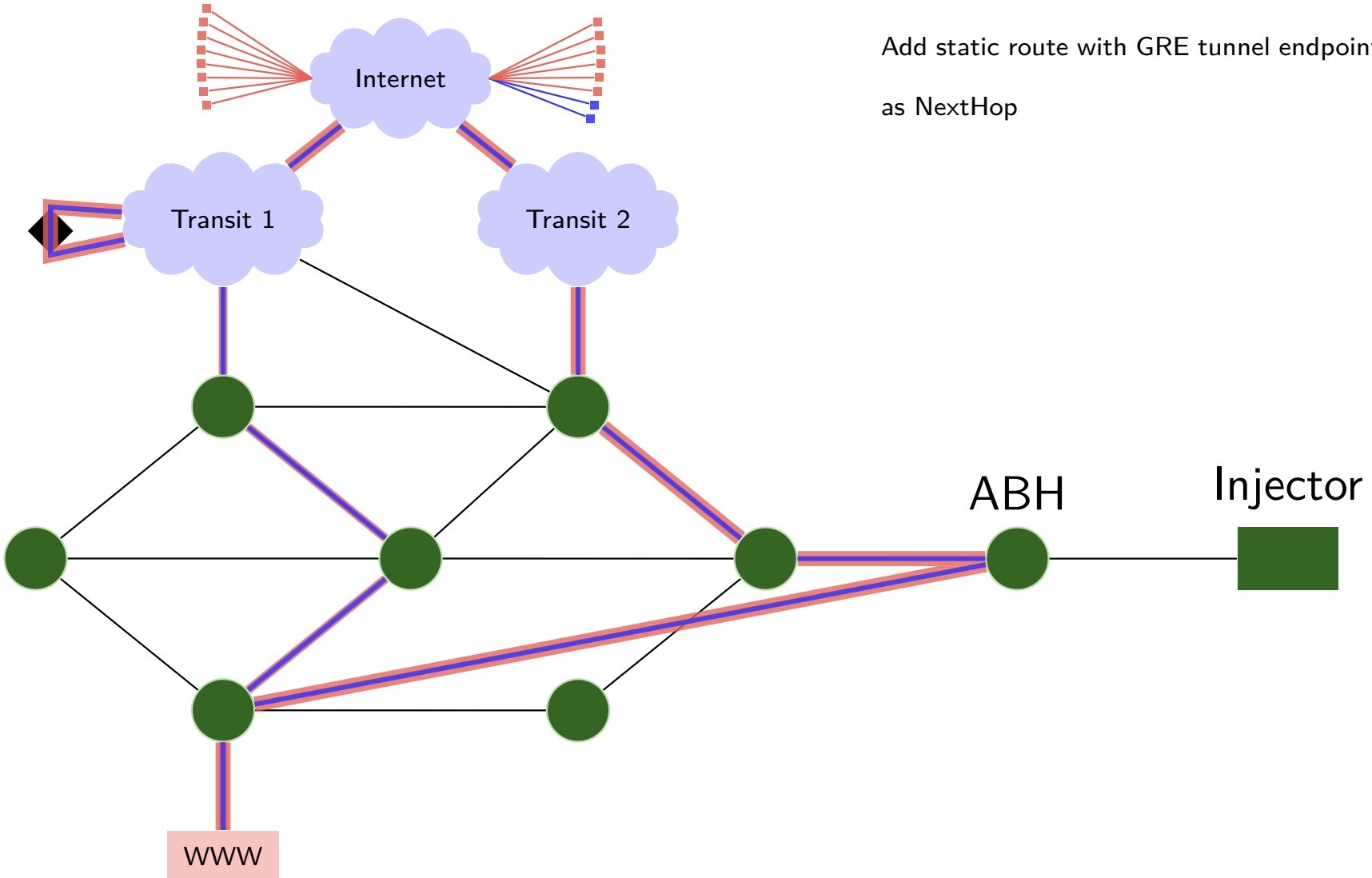
ABH PoC example



We set a GRE tunnel between ABH router

and server gateway

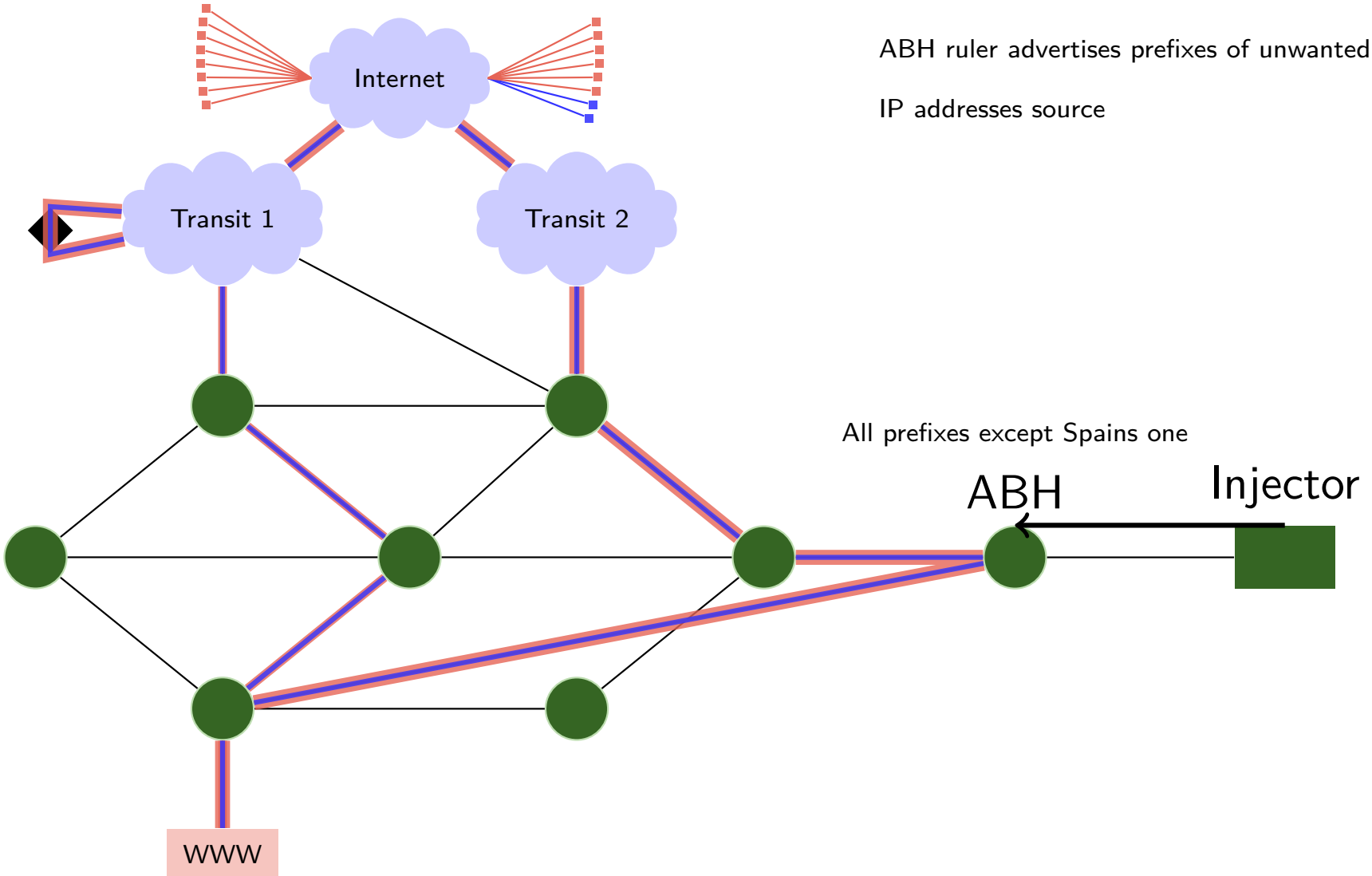
ABH PoC example



Add static route with GRE tunnel endpoint

as NextHop

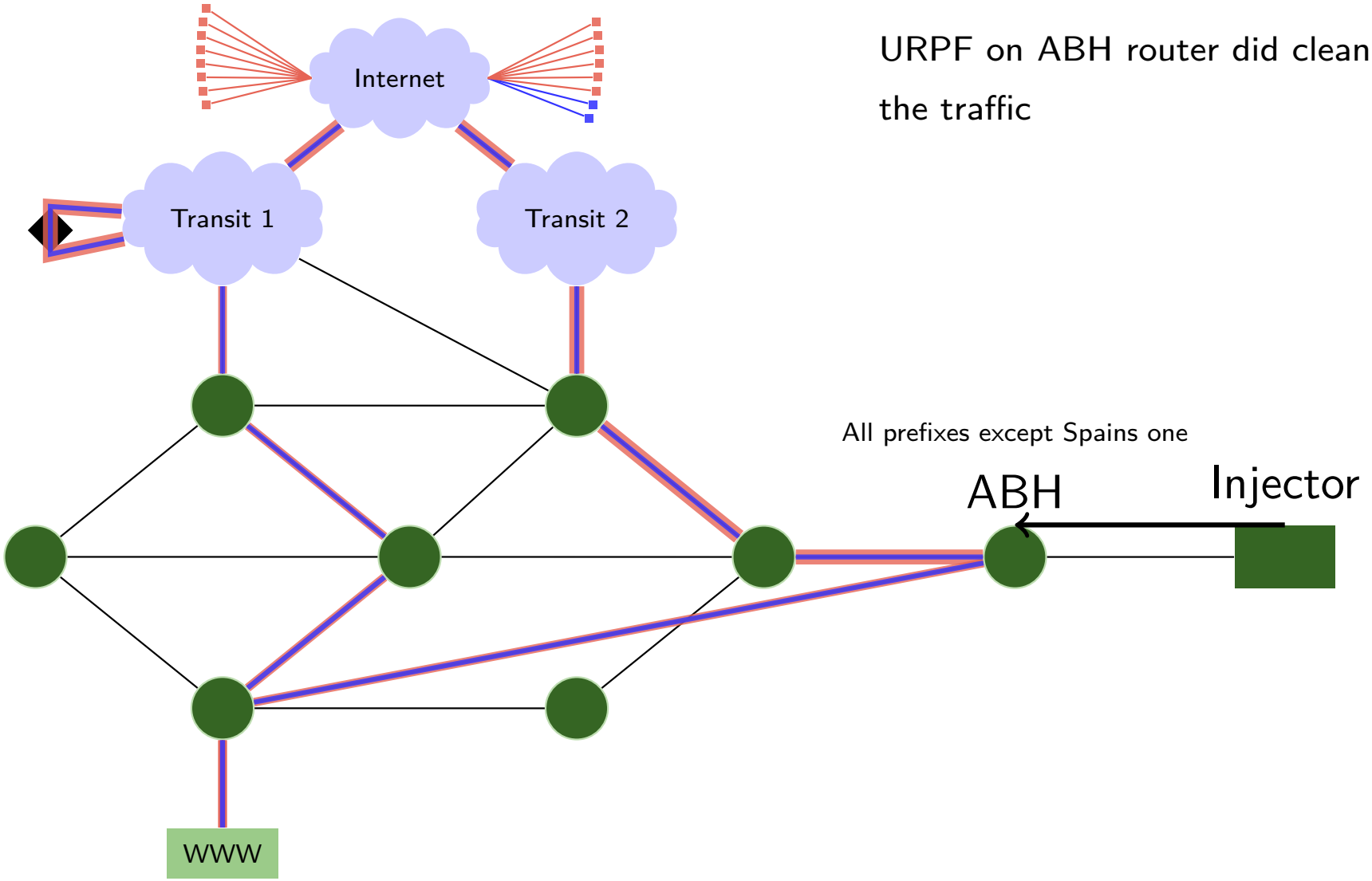
ABH PoC example



ABH ruler advertises prefixes of unwanted IP addresses source

All prefixes except Spains one

ABH PoC example



URPF on ABH router did clean the traffic

exaBGP

exaBGP configuration

```
process parsed-route-backend {
    encoder json ;
    parse-routes ;
    run /usr/bin/python /home/exabgp/ruler.py ;
}
```

Cisco

Cisco configuration

```
ip community-list standard drop-via-urpf permit 66:6666
ip community-list standard protect permit 66:1234
!
route-map from-injector permit 10
 match community protect
 set ip next-hop Null0
 set local-preference 1500
!
route-map from-injector permit 20
 match community drop-via-urpf exact-match
 set community no-advertise
 set local-preference 6666
```