TEAM CYMRU

DDoS Mitigation by Community Cooperation

... and other fun

$whoami

James Shank, jshank@cymru.com

Chief Architect, Community Services
Senior Security Evangelist

12 years at Team Cymru

Make no-cost solutions to
Internet-scale problems

Agenda

1) Cooperation and the Internet
2) DDoS and Cooperation
3) Fraud + Abuse and Cooperation

Community Cooperation

What makes the Internet work!

"We set up a telephone connection between us and the guys at SRI ...", Kleinrock ... said in an interview:

"We typed the L and we asked on the phone,

"Do you see the L?"

"Yes, we see the L," came the response.

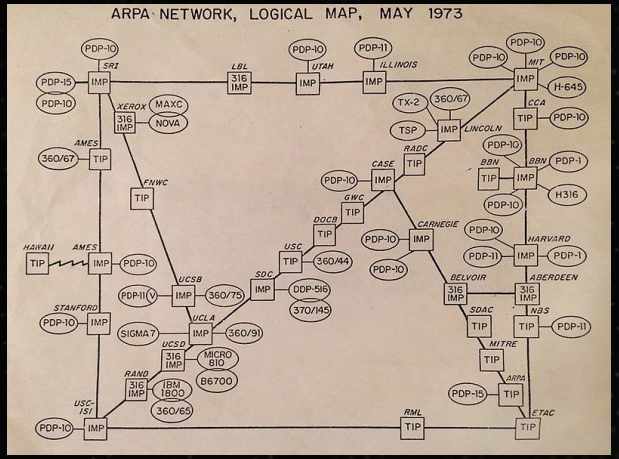
We typed the O, and we asked,

"Do you see the O."

"Yes, we see the O."

Then we typed the G, and the system crashed...

Yet a revolution had begun" ....



ARPANET 1973, Public Domain

Source: http://www.netvalley.com/cgi-bin/intval/net_history.pl?chapter=1

Community Cooperation

You make the Internet work!

Cooperation Today

- Internet Exchanges
- Peering Coordinators
- Private Peering
- Transit

Goal: Forwarding packets

Community Cooperation

Forwarding is good, right?

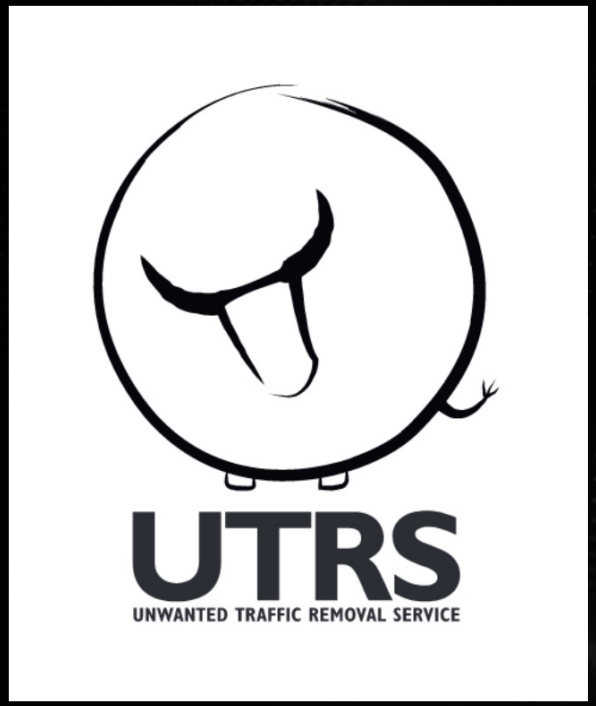
Remote Triggered Black Hole

- RFC 3882
- Don’t forward towards victim IP
- Peers cooperate to filter
- **Completes the attack**

Goal: Forward except to victim IP

Community Cooperation

Better cooperation leads to better results



Unwanted Traffic Removal Service (UTRS)

- No cost, community service
- Started in 2014
- Currently 1,562 BGP sessions!
- Upstream AND Global

Goal: Protect Internet and victim

UTRS v1 compared to UTRS v2

You've got to admit, it's getting better!

UTRS Version One

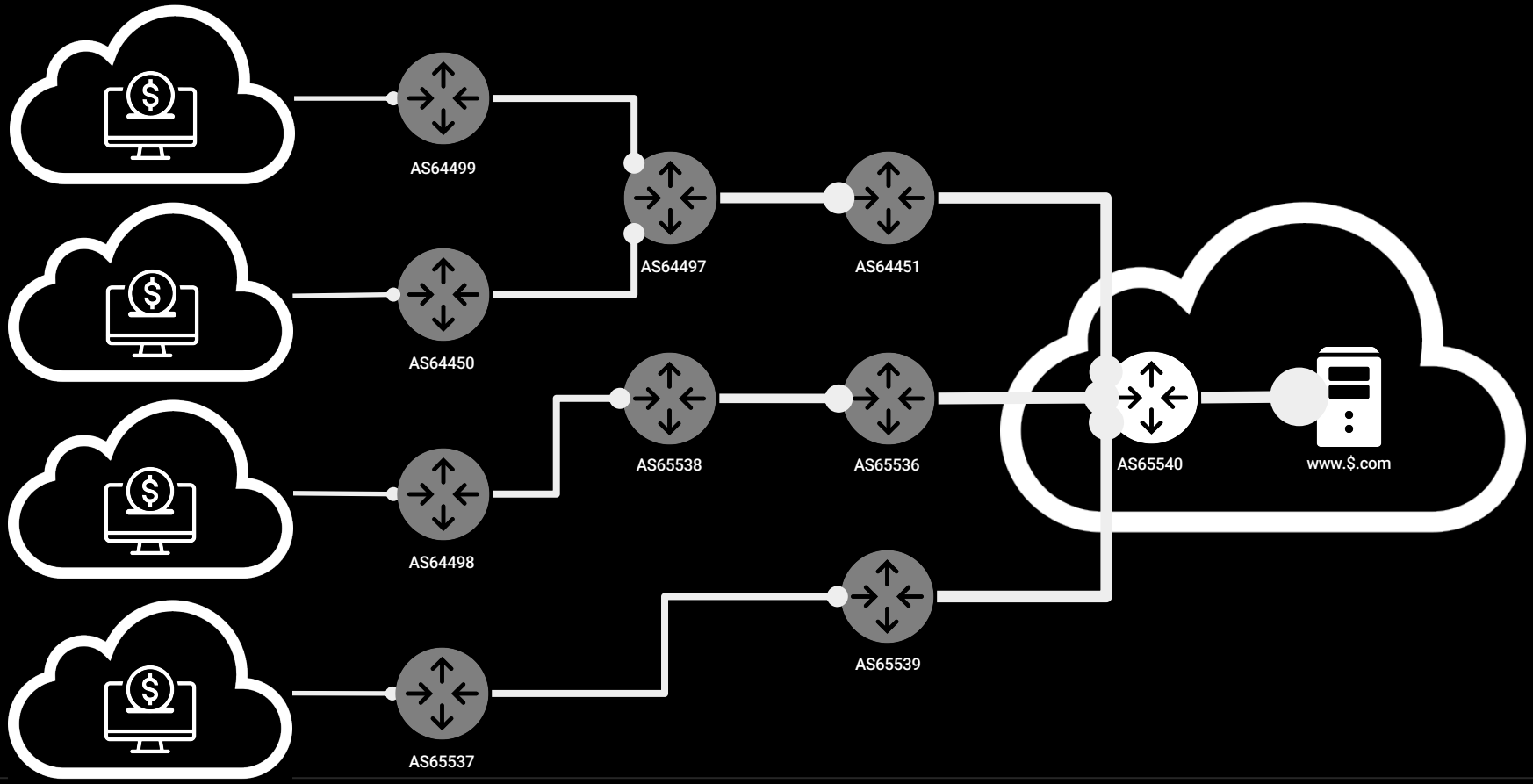
- IPv4 Addresses only
- One router on our side
- BGP support only
- Accepts only /32s

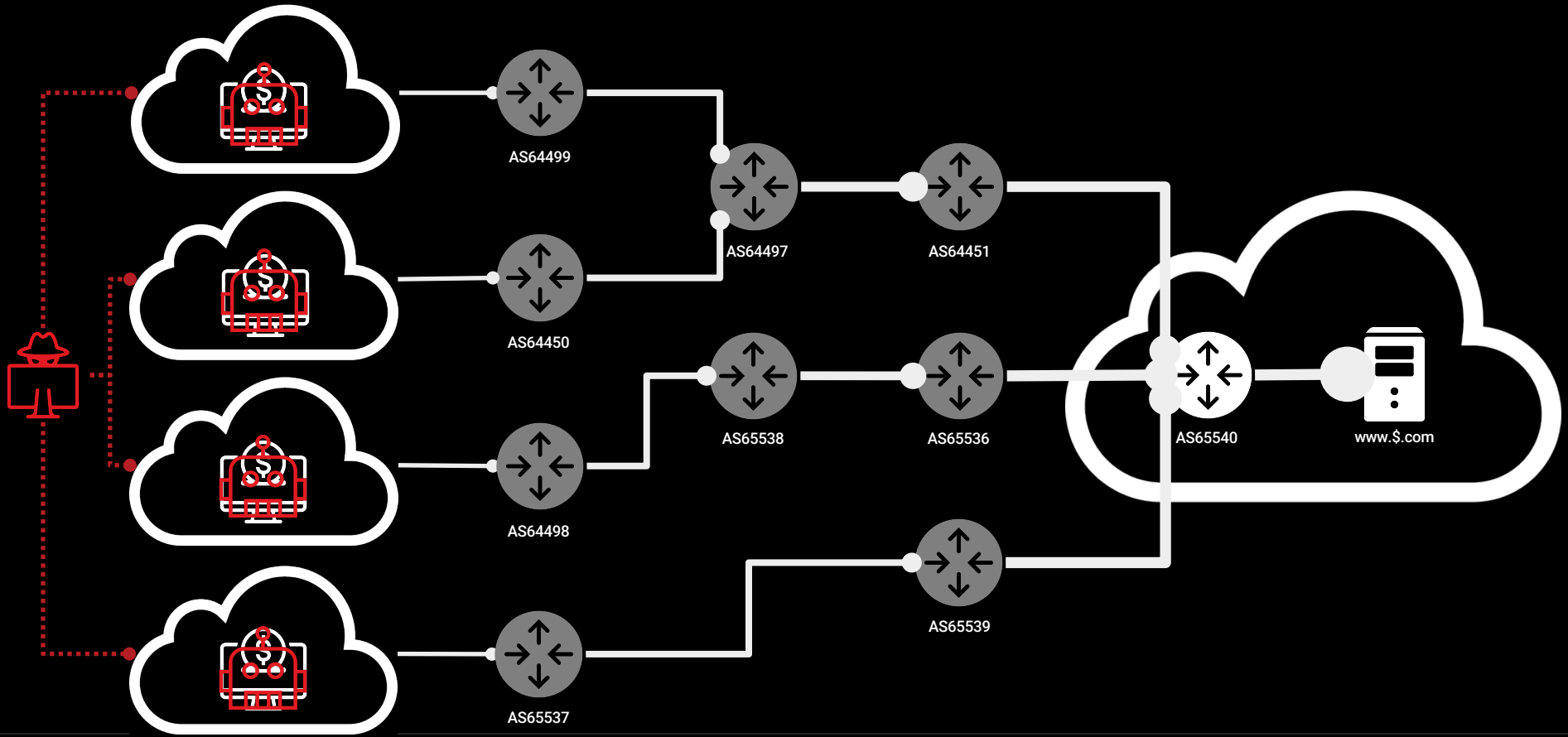
- Validates based on Global Table

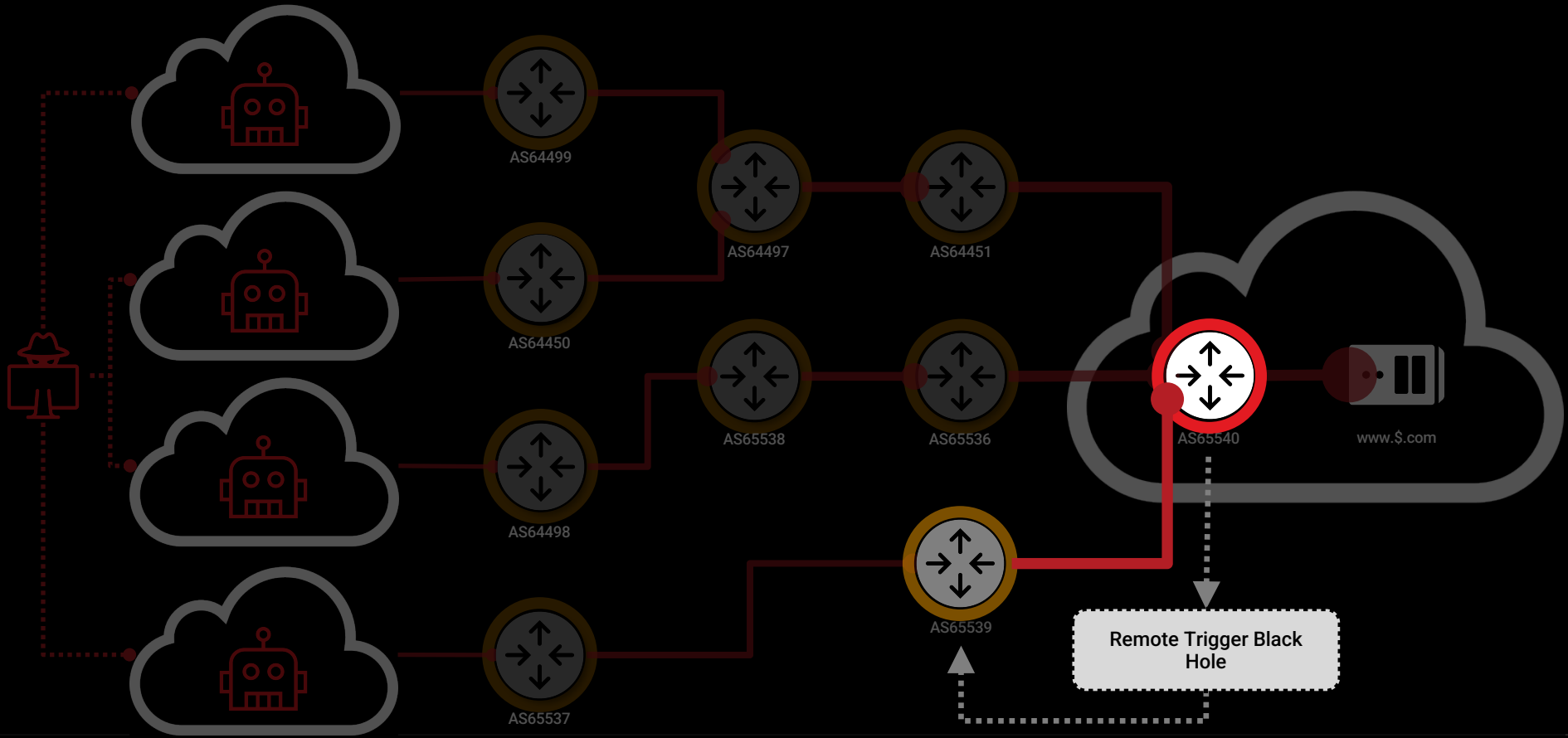
UTRS Version Two

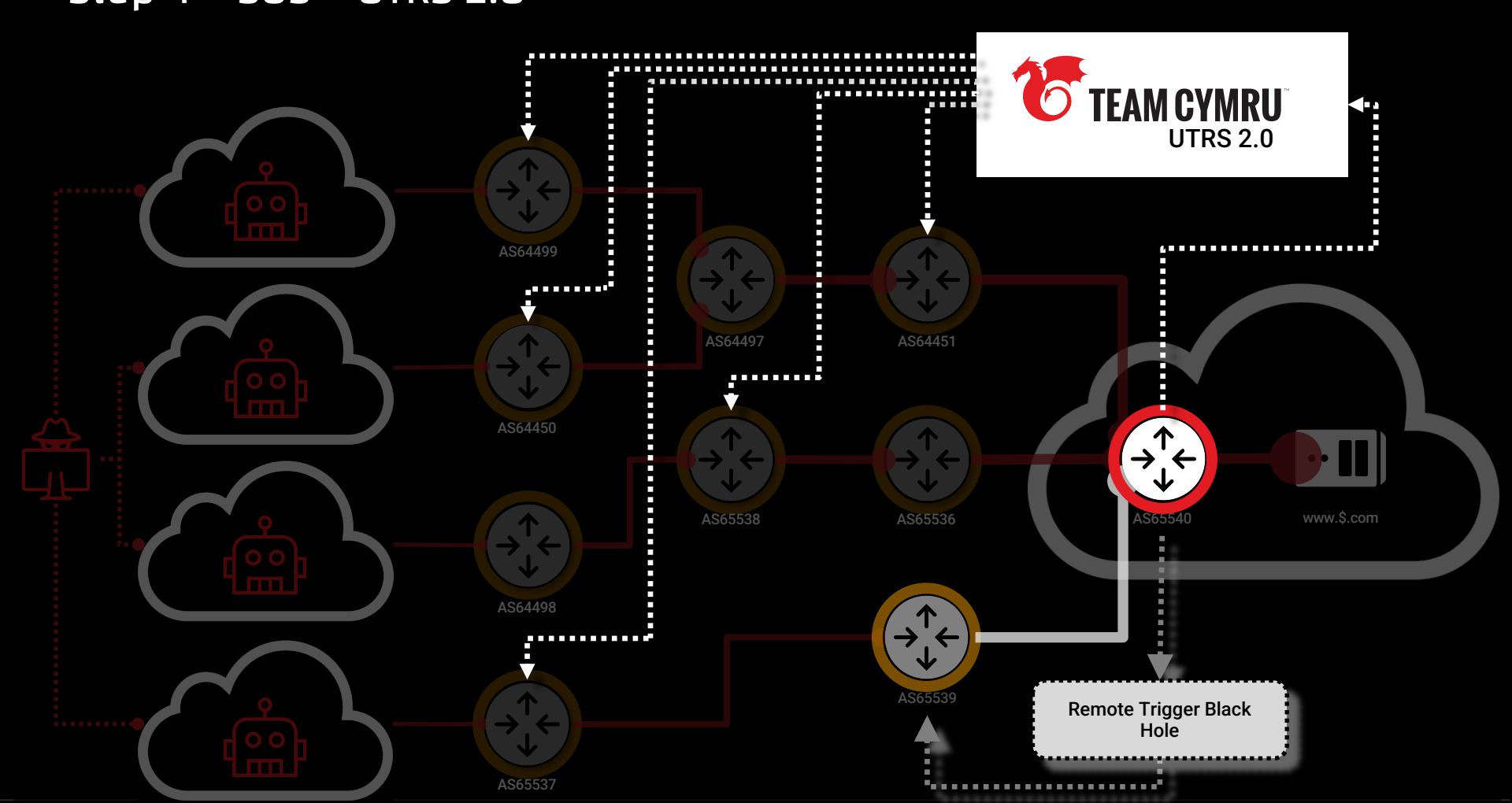
- IPv4 and IPv6 support
- Two geographically distinct routers
- BGP and BGP FlowSpec support
- Accepts /25s and /49s
  - (carpet bombing)
- Global Table or RPKI ROAs
  - (mitigation provider friendly)

Step 1 - Business as Usual









"Safe" BGP FlowSpec

Always practice safe peering!

FlowSpec - Safe with guard rails

- MUST specify destination CIDR
- MAY specify integer only for:
  protocol, src port, dst port
- MUST set action to drop
  traffic-rate 0

Goal: Fine grained filter control

Community Cooperation

Highlighting a noteworthy win!

Biggest Amplification Vector ever discovered

UTRS user network attacked

Then used UTRS to filter the massive attack.

Community Cooperation

What else?

What other hard problems get easier when the community of operators cooperate?

Fraud

- Providers compete on services, not fraud mitigation
- Pattern of fraud
- Big focus, big dollars, for hosting providers

What if they could collaborate on fraud?

Safety, Abuse, and Fraud Exchange (S.A.F.E.)

- Providers submit fraud-related details
- Check details (quick)
- Get full details (audit)
- Refute

Goal: Reduce fraud through collaboration

Coming 2022, interested? Email me: jshank@cymru.com

Community Cooperation

What else?

Ideas? Thoughts?

Always open to chat, and have a conversation

https://calendly.com/cymru-jshank/

Thank You!

Thank You!

jshank@cymru.com
outreach@cymru.com