35 responses

SUMMARY INDIVIDUAL

Accepting responses

Name of your organization (optional) (23 responses)

Indiana University

University of California, Los Angeles

University of Washington

Pacific Northwest Gigapop

KanREN

University of Minnesota

Rutgers University

Florida LambdaRail

AS 3128

Indiana University of Pennsylvania

University of California, Santa Cruz

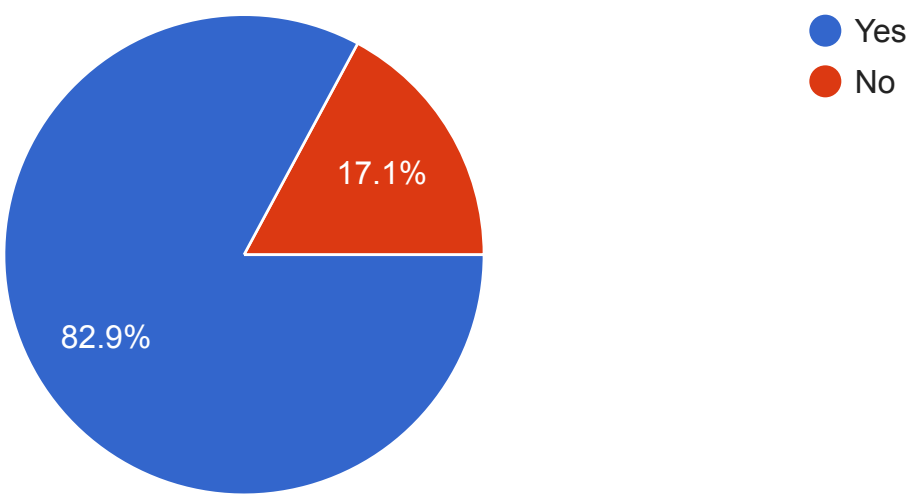
Colby College

Indiana University Campus Networks

University of Northern Iowa

University at Albany
UNC-CH
University of Iowa
UCI
Williams College
California State Polytechnic University, Pomona
University of Illinois - ICCN
NCSA AS1224
University of Illinois at Urbana-Champaign (AS 38)

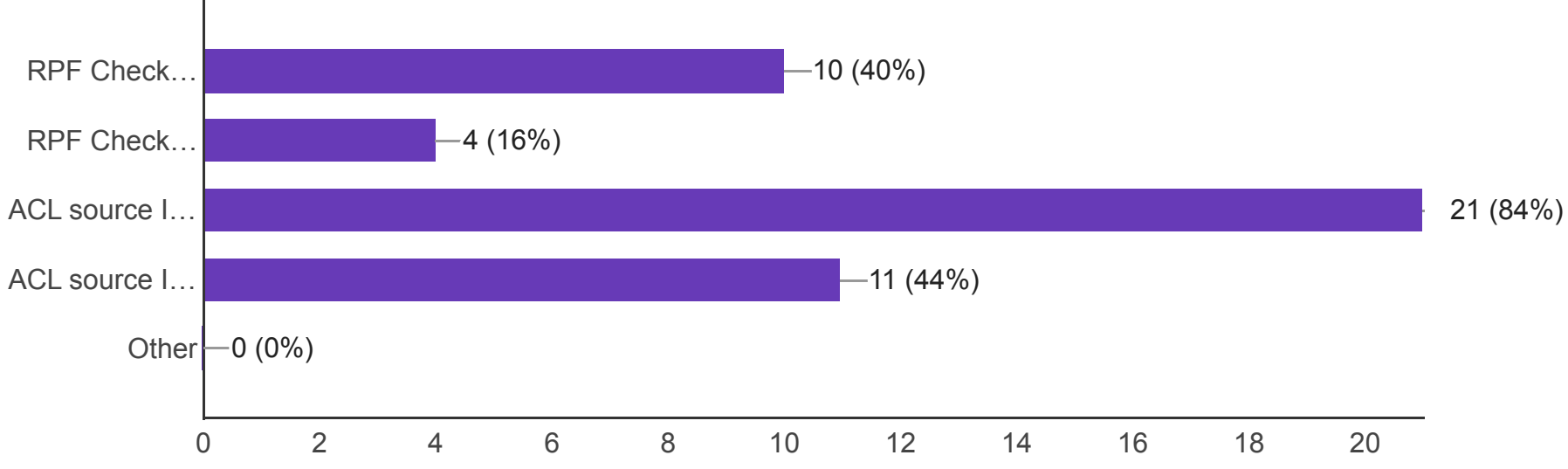
Does your organization implement source address validation? (35 responses)



Campuses that implement source address validation

How are you preventing spoofed IPs from leaving your network? (select all that apply)

(25 responses)



Please describe any techniques not listed above (3 responses)

- irr data used by upstream isp's for their ingress filters
- loose uRPF applied to world->campus traffic (use of dark space overlaps with spoofing)
- We are actually using ACLs on the edge and at the border

How do you preventing outside entities from spoofing your own IP addresses as sources coming into your network?

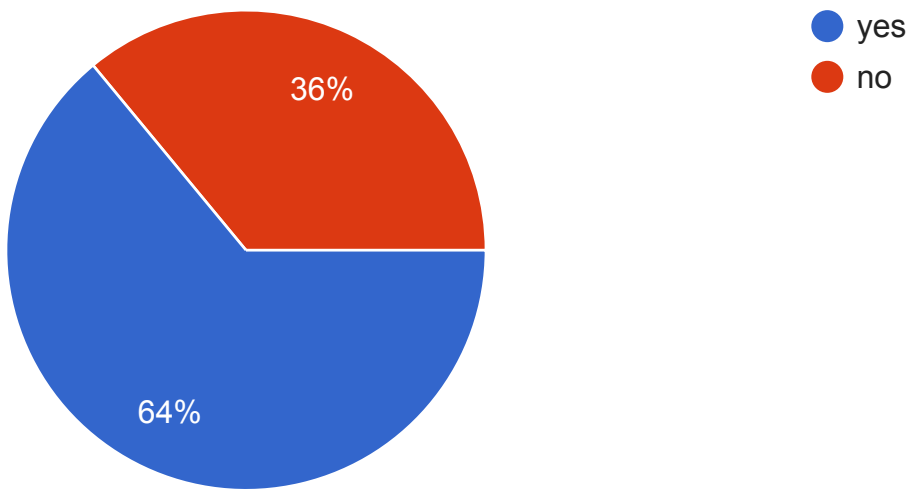
(22 responses)

- ACL blocking own IPs as a source inbound.
- ACLs on external connections
- ACL's
- We do not currently prevent this.
- Yes have ACL to prevent our addresses from coming into our network from the outside
- Split horizon BGP and ACLs
- Ingress ACLs
- Ingress ACL at campus border to eliminate campus addresses, bogons, and other cruft source addresses

ACL
ACLs that drop packets with our own IPs as as source.
bgp prefix filters with external neighbors and interface acls at the border
inbound ACL
ACL source IP filtering on inbound traffic blocks my netblocks from being the source on inbound traffic
Routing filters at edges.
ACLs
filter world->campus traffic to disallow that sourced with our address space
We filter our own addresses as source addresses at the border by ACL
ACL source ip filters and BGP advertisement filters
Inbound traffic with our IPs is blocked at the border
ACL on border router
Firewall policies at edge.
URPF on the provider peering interface

Do you have a Remotely-Triggered Black Hole (RTBH) solution established with your provider(s)?

(25 responses)

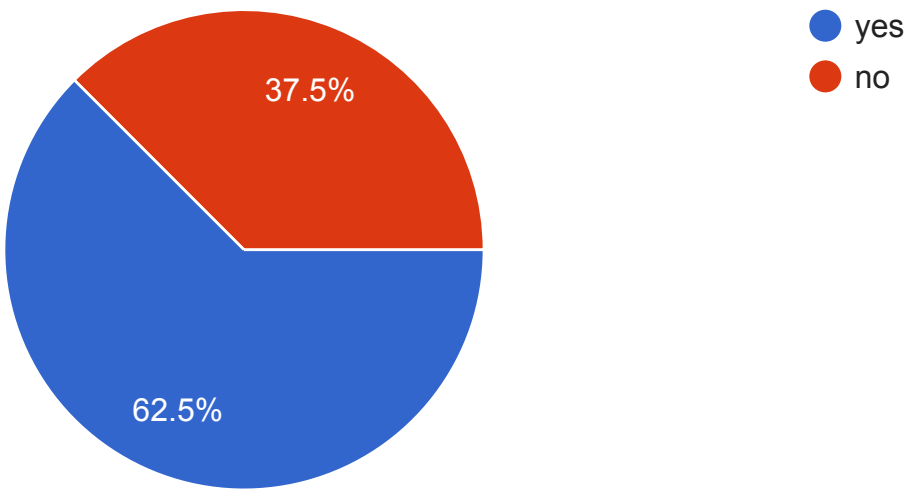


If you don't implement Remotely-Triggered Black Hole (RTBH) please describe why.

(6 responses)

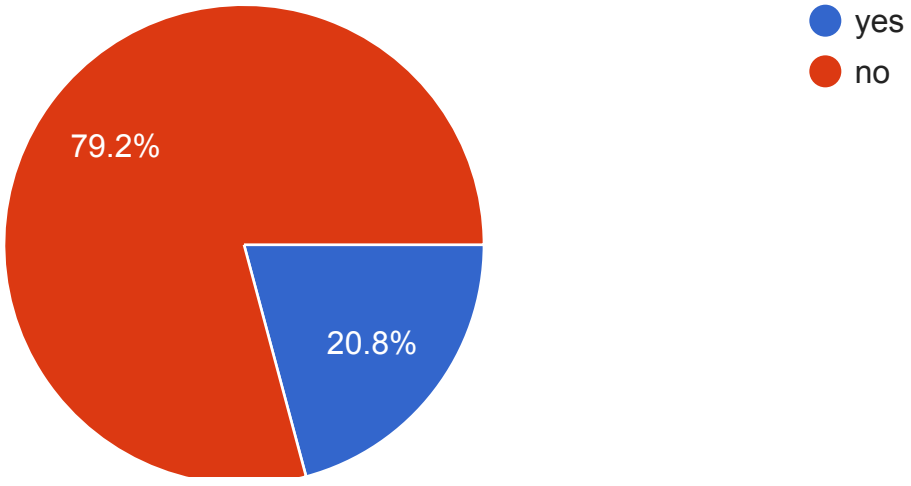
we use it to trigger filters at different areas of the network (first hop router, core, campus Internet border)
lack of available staff time to implement; lack of skills
we can call them and have a good relationship
I'm actually unsure about this.
Not aware of that
you didn't have "kind of". We can manually mark routes to our RON for them to black hole, but they can't do it upstream. None of it is automated.

Have you tested your network to see if it is spoofable? (24 responses)



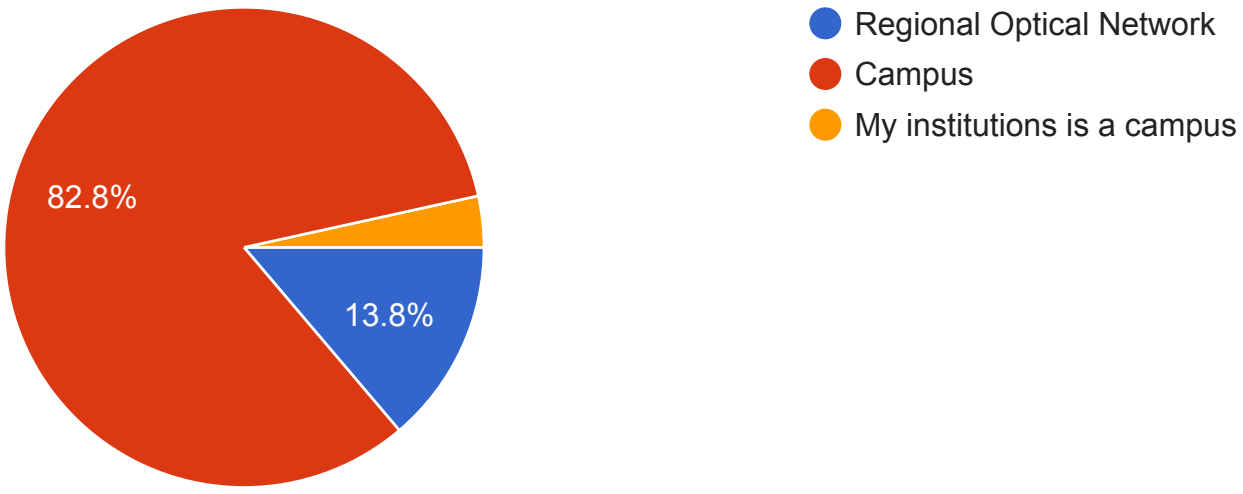
Have you downloaded and run the CAIDA spoofer test and measurement tools? (https://www.caida.org/projects/spoofer/).

(24 responses)



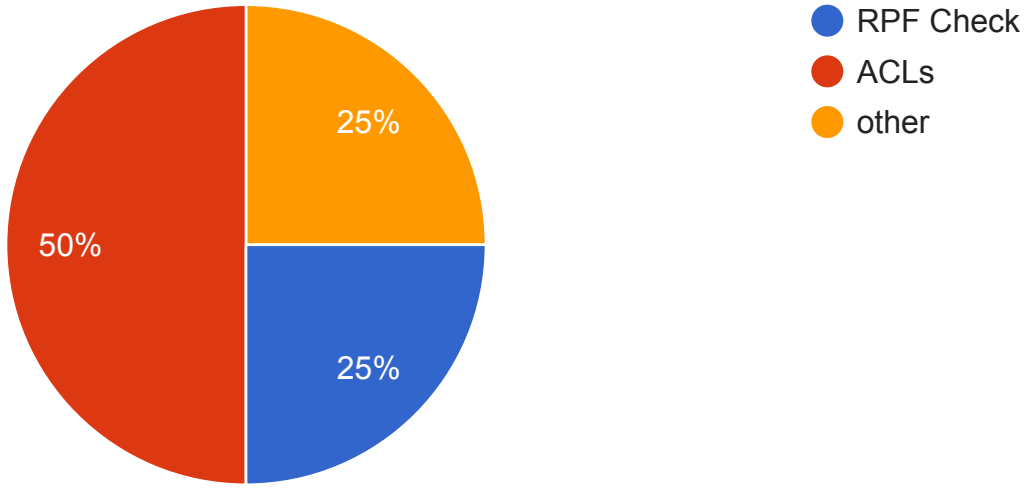
Is your organization a RON or Campus

Do your answers relate to a campus or RON? (29 responses)



RONs that implements source address validation

How are you preventing your connected organizations from spoofing IP addresses through you?
(4 responses)



If other, please describe how you prevent connected organizations from spoofing IP addresses through you.

(1 response)

RPF Check if single homed, ACL if multihomed

How are you preventing outside entities from spoofing your own IP addresses as sources coming into your network?

(4 responses)

We do not currently block this.

ACL on customer edge ports

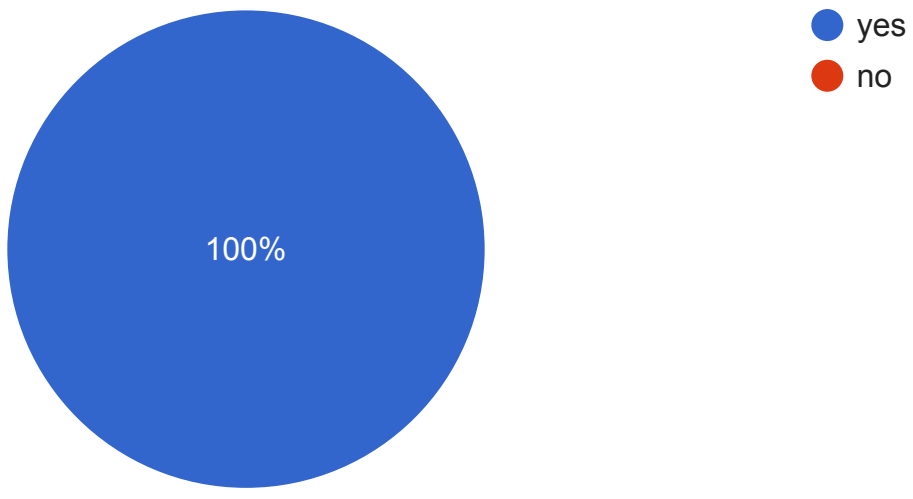
We only do this for our infrastructure and systems networks, not for customers. Via ACLs.

We cannot, some of our connectors are multihomed. We discard bogons on ingress. We also discard IPs related to the network management of our backbone, which is on public space. This includes point to points that we allocate, loopbacks, our servers for network management, etc

Do you have a Remotely-Triggered Black Hole (RTBH) solution established

with your provider(s)?

(4 responses)

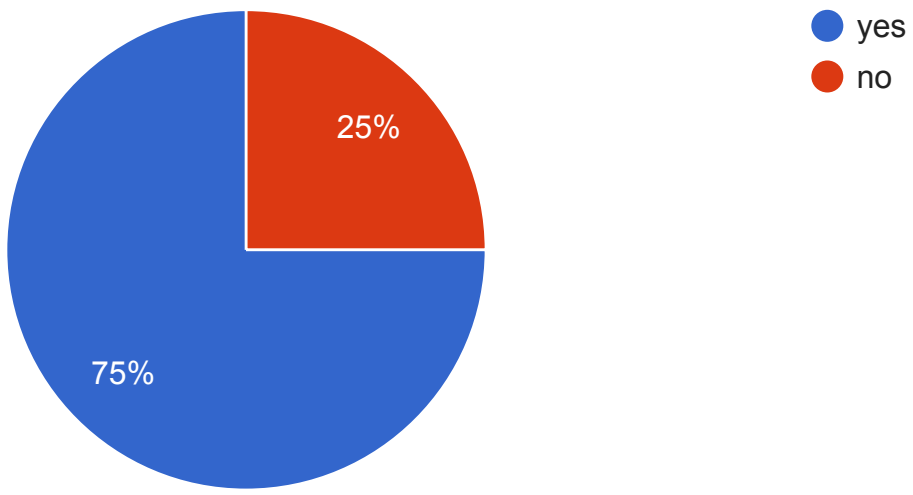


If you don't implement Remotely-Triggered Black Hole (RTBH) please describe why.

(0 responses)

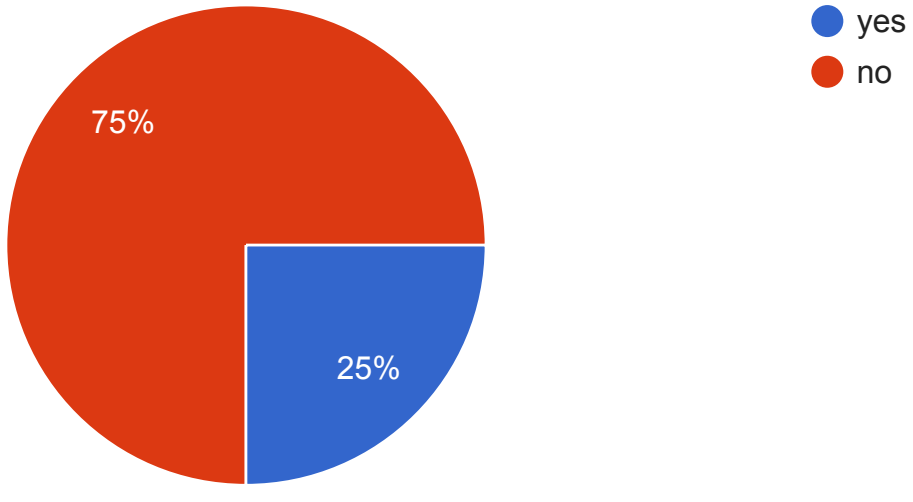
No responses yet for this question.

Have you tested your network to see if it is spoofable? (4 responses)



Have you downloaded and run the CAIDA spoofer test and measurement tools? (https://www.caida.org/projects/spoofer/).

(4 responses)



Doesn't implement source address validation

What are the barriers that prevent your institution from implementing source address validation?

(6 responses)

Time and knowledge
has only been possible since new routers installed this summer - planning on it!
None. I am not aware of why it was not implemented but I plan to do so.
We have delayed SAV without enabling blocking to better understand what, if any, impact it will have on campus.
too many static ip addresses
Not supported for certain network designs

Would assistance from the community for implementing source address

validation be helpful?

(6 responses)