REN-ISAC

Research and Education Networking Information Sharing and Analysis Center

REN-ISAC

What I'll be talking about:

- REN-ISAC introduction
- Expanded Participation
- SES (Security Event System)
- Passive DNS project
- Project CHUM

REN-ISAC

Mission

The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities. The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

REN-ISAC

Mission

The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities.

The mission is conducted within the context of a private community of trusted representatives at member institutions,

and in service to the R&E community at-large.

REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

REN-ISAC

<COMPONENTS>

- Private Trust community
- CSIRT for .edu
- Sector ISAC
- R&D

REN-ISAC

Components

- Private Trust community
  - CSIRT for .edu
  - Sector ISAC
  - R&D

REN-ISAC

Private Trust Community

- A community of trusted security staff at R&E institutions sharing actionable information for operational protection and response; among the trusted R&E members, cross-sector, and with external trusted partners.

REN-ISAC

Private Trust Community - Membership

- Membership is open to:
  - colleges and universities,
  - teaching hospitals,
  - R&E network providers, and
  - government-funded research organizations.
- Member representative eligibility:
  - Very specific job responsibility requirements: institution-wide operational protection and response (essentially the IT Security Office (or alike) security engineers, architects, and direct managers)
  - Tightly circumscribed to maintain a high level of trust and interaction among the representatives
- 2 tiers, differing in eligibility criteria, trust vetting, sensitivity classification, and the commitment-level of the institution

REN-ISAC

Private Trust Community - Reach

- As of November 2013, there are over
  - 445 member institutions
  - represented by 1364 member representatives
- A list of member institutions is on the Membership web page
  - http://www.ren-isac.net/memberlist.html

REN-ISAC

Private Trust Community - Benefits of Membership

- Receive and share actionable information among trusted peers
- Have access to threat indicator resources that can be used to identify local compromised machines, block known threats, and aid incident response (SES aka CIF)
- Information products (e.g. Daily Watch, Advisories, and Alerts)
- Benefit from REN-ISAC relationships in broad security community
- Benefit from REN-ISAC / vendor security cooperation relationships
- Participate in technical educational security webinars
- Participate in REN-ISAC meetings, workshops and training
- Access to the 24x7 REN-ISAC Watch Desk
- Develop relationships with known and trusted peers

REN-ISAC

Components

- Private Trust community
- CSIRT for .edu
- Sector ISAC
- R&D

REN-ISAC

CSIRT for .edu

- Daily notifications, directly and privately to abuse contacts at .edu institutions concerning compromised or vulnerable systems, credentials, and other incident involvement
  - In service to all of US .EDU regardless of membership, and international members
  - Over 12,000 notifications per month
  - Over 1,800 institutions notified
- 24x7 Watch Desk
- Represent the sector in forums of private, commercial, and governmental CERT/CSIRTS

REN-ISAC

Components

- Private Trust community
- CSIRT for .edu
- Sector ISAC
- R&D

REN-ISAC

EDU Sector ISAC

- Trusted partner for the R&E community
- Member, National Council of ISACs
- Formal relationship with DHS/US-CERT
- Cross-sector information sharing
- Public alerts aimed at R&E security practitioners, CIOs and business officers

REN-ISAC

Components

- Private Trust community
- CSIRT for .edu
- Sector ISAC
- R&D

REN-ISAC

R&D

- SES (visited later in the presentation)

- CSIRT Tools
  - RINO (Ren-Isac NOtification system)
    - Receives, collates, and distributes notifications concerning observed compromised or vulnerable systems
  - RIHF (Ren-Isac Human Filter)
    - Process notifications based on data that requires operator vetting and interaction.

- RINO and RIHF aren't currently released open-source but we're hoping to get there.

REN-ISAC

</COMPONENTS>

REN-ISAC

Relationships

- APWG (Anti-Phishing Working Group)
- DHS/US-CERT and other national CERTS and CSIRTS
- EDUCAUSE
- Global Research NOC at IU
- Higher Education Information Security Council
- Internet2
- LE (various)
- National Council of ISACs
- NCFTA
- Private threat sharing, analysis & mitigation communities (various)
- Other sector ISACs
- Vendors

REN-ISAC

Organization

- Hosted by Indiana University (fiscal and administrative agent)
- Eight full-time staff
- Governed by a Board formed from among the members (2/3) plus sponsoring and host organizations
- Relationship with the Higher Education Information Security Council (HEISC, similar in concept to a Sector Coordinating Council (SCC))

REN-ISAC

Organization – Member Participation

- Member participation is a cornerstone of REN-ISAC
- Member contributions through participation:
  - Board
  - Technical Advisory Group
  - Microsoft Analysis Team
  - Membership Committee
  - Member Orientation and Engagement Committee
  - Technical webinars
  - Services development
  - Projects, e.g. sensor development
  - Special Interest Groups, e.g. SIEM, Forensics, Bro, etc.

REN-ISAC

Sustainability

- Membership fee, tiered $1250 – $2500 per institution per year
- Financial contributions from IU, LSU and Internet2, and in-kind support from EDUCAUSE
- Member contributions in projects, services, and activities

REN-ISAC

Selected Successes

- Rich and active sharing among the members
- Rich and high quality external relationships (to private, commercial, and governmental partners) brings substantial value to members
- High quality indicator information for threat mitigation and IR
- High quality and high volume remediation (CSIRT notifications of compromised machines) to entire .edu sector
- Substantial contribution to cleaning up .edu space (e.g. no longer an attractive location for miscreant C&C)
- Automated machine-based threat indicator sharing (SES aka CIF) within REN-ISAC and to external partners
- Participation of the sector (although there's more to be reached)

REN-ISAC

References

- Joining
  - http://www.ren-isac.net/membership.html
- REN-ISAC Organizational Documents
  - http://www.ren-isac.net/about/index.html
    - Charter
    - Membership Document
    - Terms and Conditions
    - Fees
    - Information Sharing Policy
    - Disclaimer
- Overviews
  - http://www.ren-isac.net/about/index.html
    - Flier
    - Executive Overview

REN-ISAC

What I'll be talking about:

- REN-ISAC introduction
- Expanded Participation
- SES evolution
- Passive DNS project
- Chum

REN-ISAC

Expanded Participation

Background : Historical focus of REN-ISAC membership

Participation as a REN-ISAC member representative is purposefully limited to persons who

are

in the institution-wide IT Security Office or Team, and

manage or conduct operational protection and response;

or,

in the absence of an Office or Team, the person(s) who perform that sort of role for the institution

REN-ISAC

Expanded Participation

Background: Changing landscape since REN-ISAC beginning:

- IT Security Offices have grown in responsibilities and staff;
- Leadership is at or among the executive level;
- Enterprise risk-based approaches;
- Full-time policy and compliance officers;
- Awareness programs;
- Full-time roles based on what used to be part of a Generalist's portfolio: e.g. vulnerability mgmt., awareness, firewall/IDS admin
- There are evolving organizational approaches such as the diminishment of centrally-staffed offices in favor of virtual security teams formed from across the organization.

REN-ISAC

Expanded Participation

Background: Security is EVERYONE's responsibility:

It's not just the IT Security Office's job! Positions with institution-wide security responsibilities may be homed in other IT organizations, research offices and projects, or functional offices.

- Enterprise applications
- Networks
- DNS admin
- Enterprise systems
- Etc!

REN-ISAC

Expanded Participation

The Challenge:

Provide value for our Members commensurate with their needs!

- private information sharing among trusted peers
  - not just about and for the IT Security Office
- a more widely defined scope of participation
- executive awareness

BUT if we dilute the core – the institution-wide security engineers – they'll be less inclined to share sensitive operational information

PROTECT THE CORE!

REN-ISAC

Expanded Participation

The Response

Still in planning; a fall 2015 objective. Thoughts are:

- A participation model that encompasses additional roles while maintaining a distinct community of service for the “classic” REN-ISAC member rep engaged in institution-wide operational protection and response
- Horizontal expansion (depts/divs/roles)
- Upwards expansion (information product and engagement aimed at the executive level)

Thoughts and idea welcome! membership@ren-isac.net

REN-ISAC

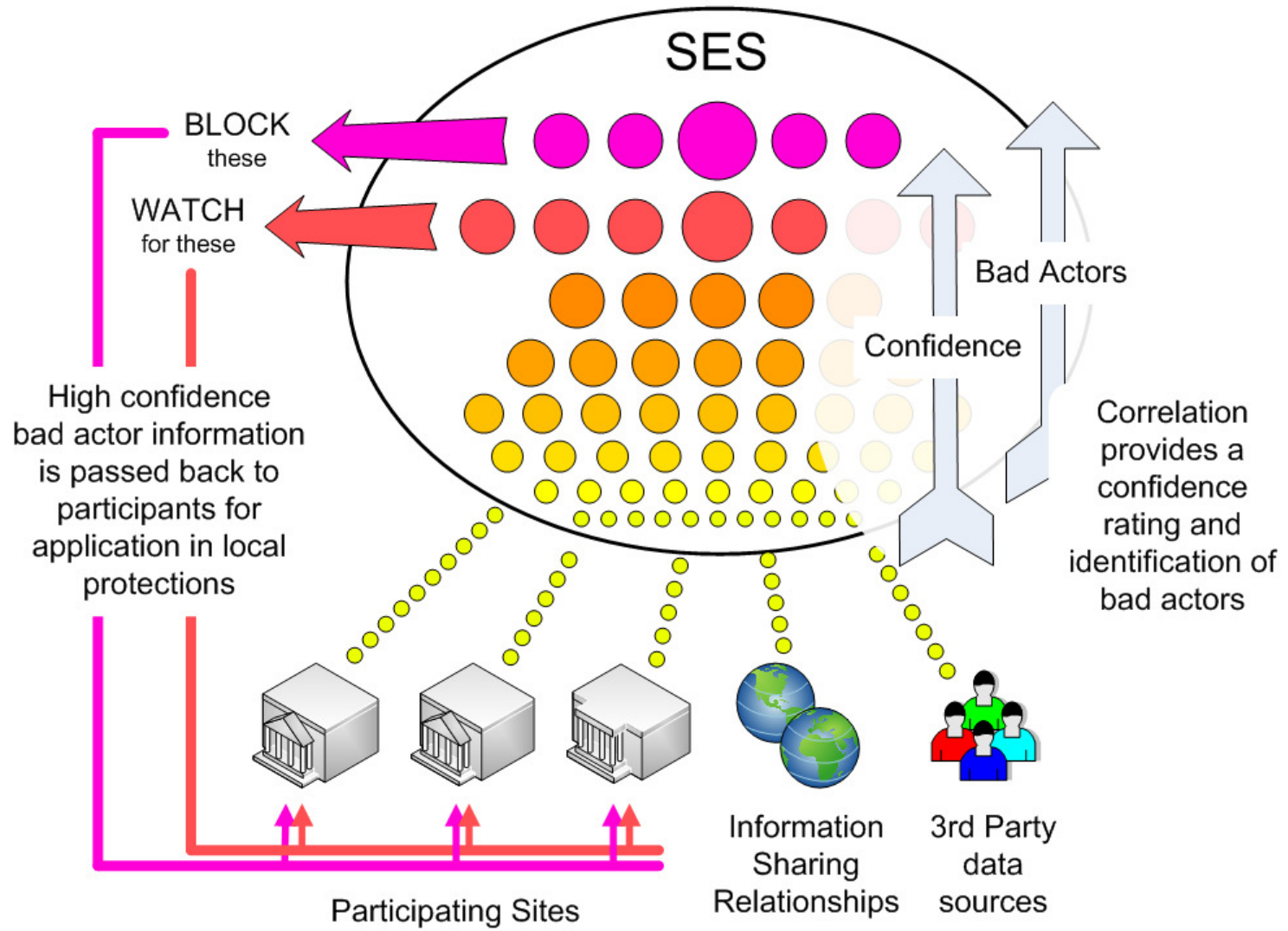
- REN-ISAC introduction
- Expanded Participation
- SES evolution
- Passive DNS project
- Chum

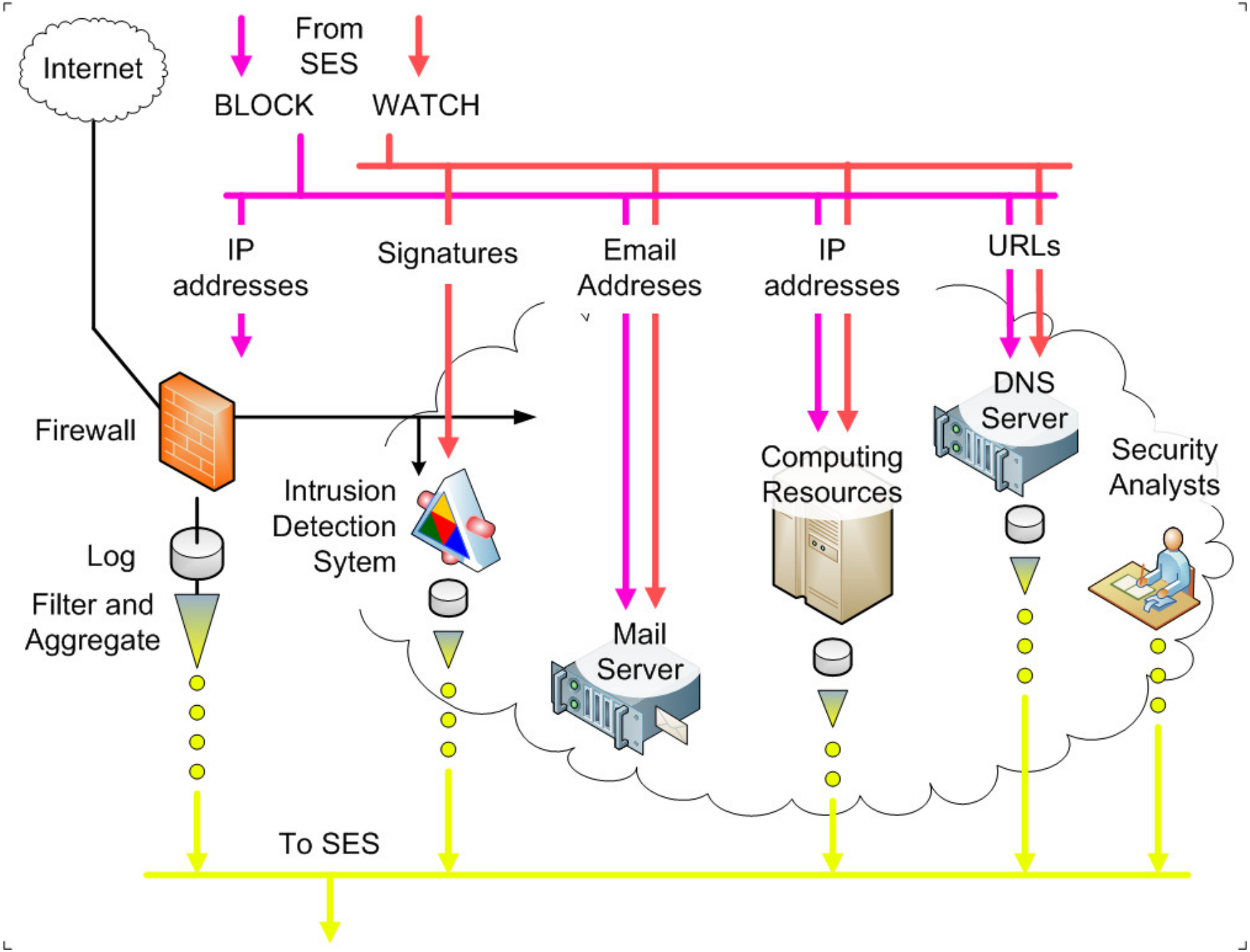
REN-ISAC

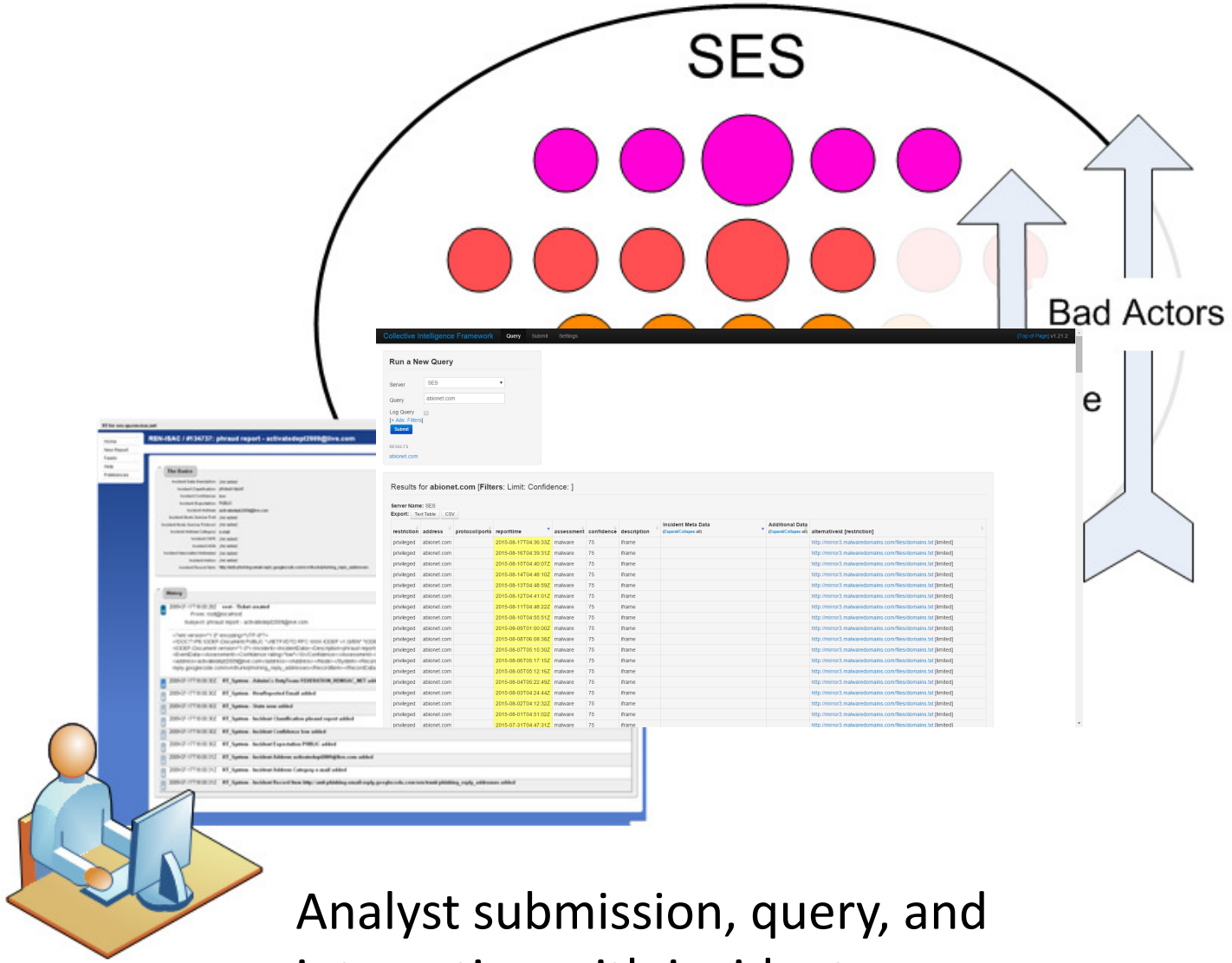
SES (aka CIF) threat intel management & sharing

- Name disambiguation:
  - CIF = the open source system
  - SES = implementation of that tool in REN-ISAC community
- Combine malicious threat information from many sources; perform discovery of related information (e.g. IPs related to domains, name servers, ASNs, &c); and use that information for identification, detection and mitigation.
- The most common types of threat intelligence warehoused in CIF are IP addresses, domains and URLs observed to be related to malicious activity.
- CIF helps you to parse, normalize, store, post process, query, share and produce data sets of threat intelligence.
- Intra- and Inter-federation sharing capability.

REN-ISAC


SES
BLOCK
these
WATCH
for these
Bad Actors
Confidence
High confidence bad actor information is passed back to participants for application in local protections
Correlation provides a confidence rating and identification of bad actors
Participating Sites
Information Sharing Relationships
3rd Party data sources


Internet
From SES
BLOCK
WATCH
IP addresses
Signatures
Email Addreses
IP addresses
URLs
Firewall
Intrusion Detection Sytem
Log
Filter and Aggregate
Mail Server
Computing Resources
DNS Server
Security Analysts
To SES



Analyst submission, query, and integration with incident response tools

REN-ISAC

- Removes the human interrupt from the observe – protect cycle
- Provides collection, storage, and access to security event information within a trust community (e.g. the REN-ISAC membership)
- Incorporates observations sourced from within the trust community, and from external public sources, and private, commercial, and governmental information sharing partners
- Works with a wide variety of indicators (IP addresses, domains, URLs, e-mail addresses, hashes, etc.)
- Correlates and weights observations to develop confidence in the identification of malicious actors, and reputation of Internet elements
- Provides query access (supporting analysts), and feeds (supporting local protection systems, e.g. IDS, firewalls, sinkholes, etc.)
- Utilizes advanced, standard, and evolving practices for storage, access, and data sharing
- Supports inter-federated sharing between trust communities via data marking (e.g. “share w/trusted partners”, “share w/LE”), and policy controls
- Is being used and further developed in the REN-ISAC community.
- Is being deployed in communities external to REN-ISAC

REN-ISAC

Fall 2015 implementation of SESv3

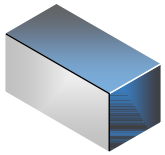
- API changes (current users will have to migrate)
- Faster API; supports more advanced machine-machine interaction
- Metadata tagging
- Faster processing of data, based on elastic search
- Improved capability to rapidly incorporate new feeds
- No more “batched” feed generation. Any combo of tags and confidence in real time; and inter-federation support
- Greater pursuit of member contributions of observations (manual/analyst, and automated e.g. from IDS, logs, etc.)
- Inter-federations (data sharing with other communities)
- Will see more rapid incorporation of new features (via plugin architecture, and rapid development/QA methodologies)
- Native Python, Perl, Ruby, and Javascript SDKs
- Easy Button for server installations

REN-ISAC

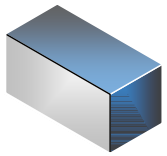
- REN-ISAC introduction
- Expanded Participation
- SES evolution
- Passive DNS project
- Chum

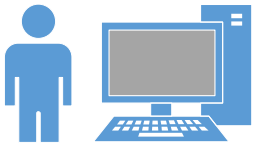
My University

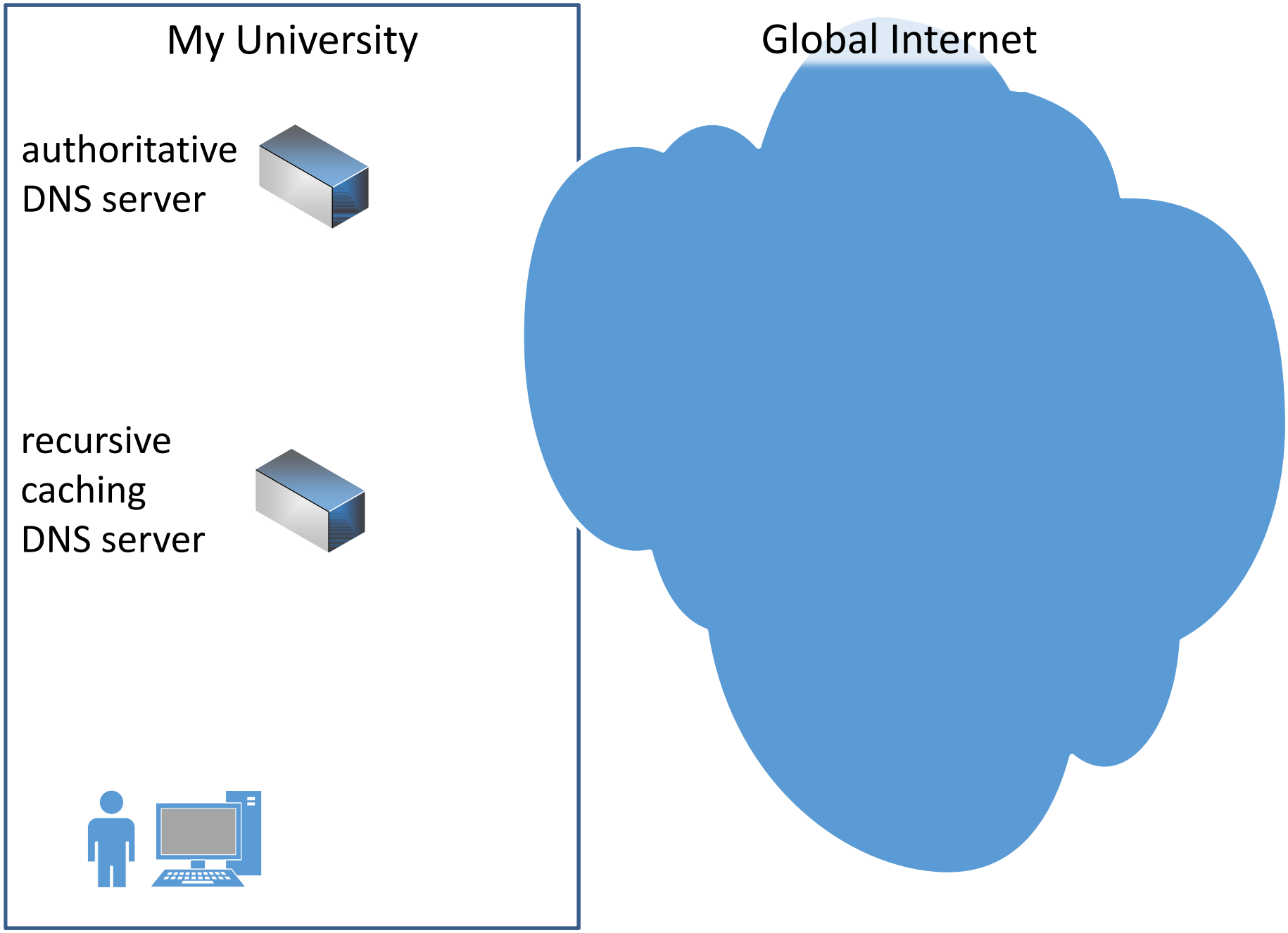
authoritative
DNS server

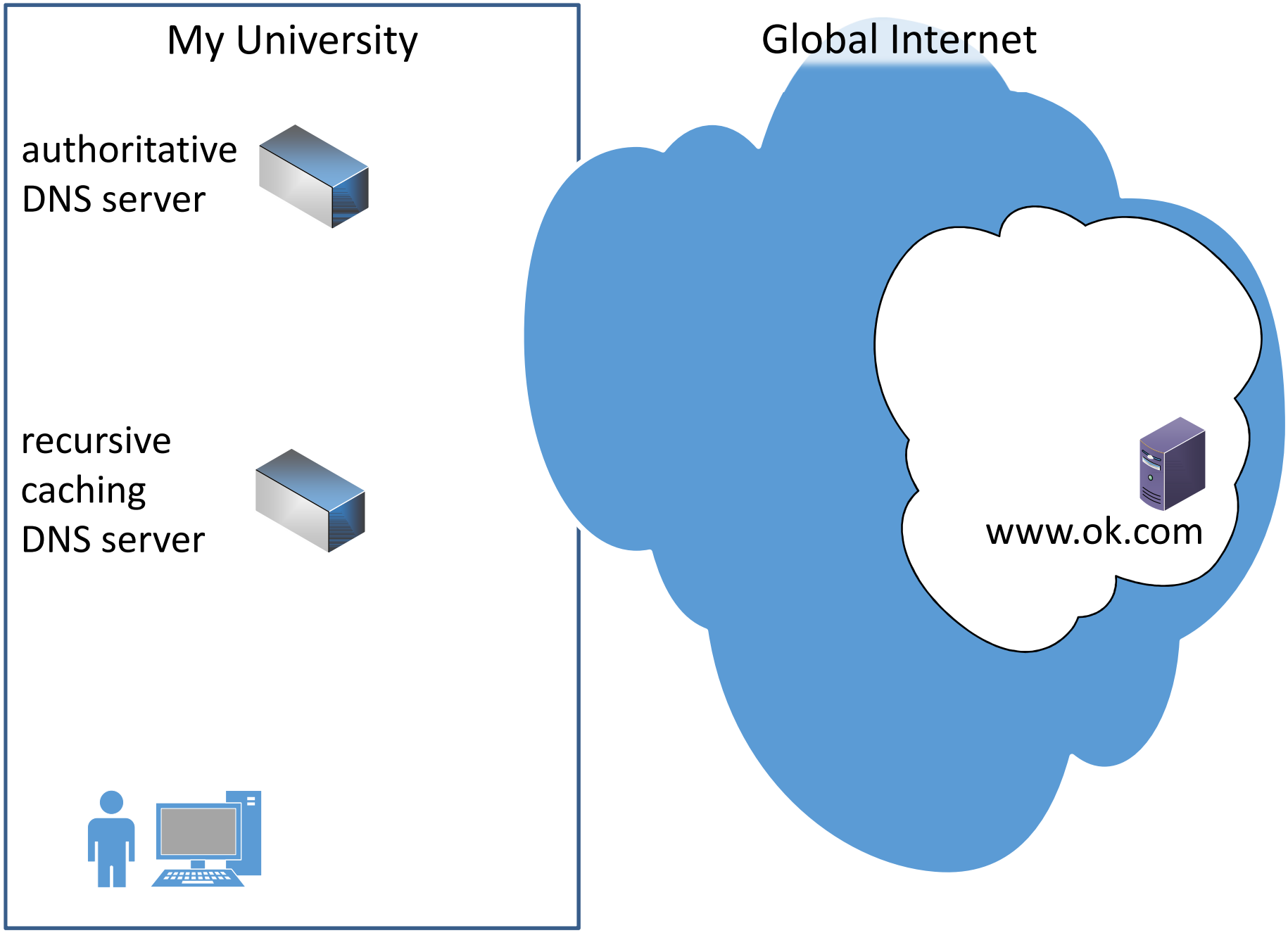


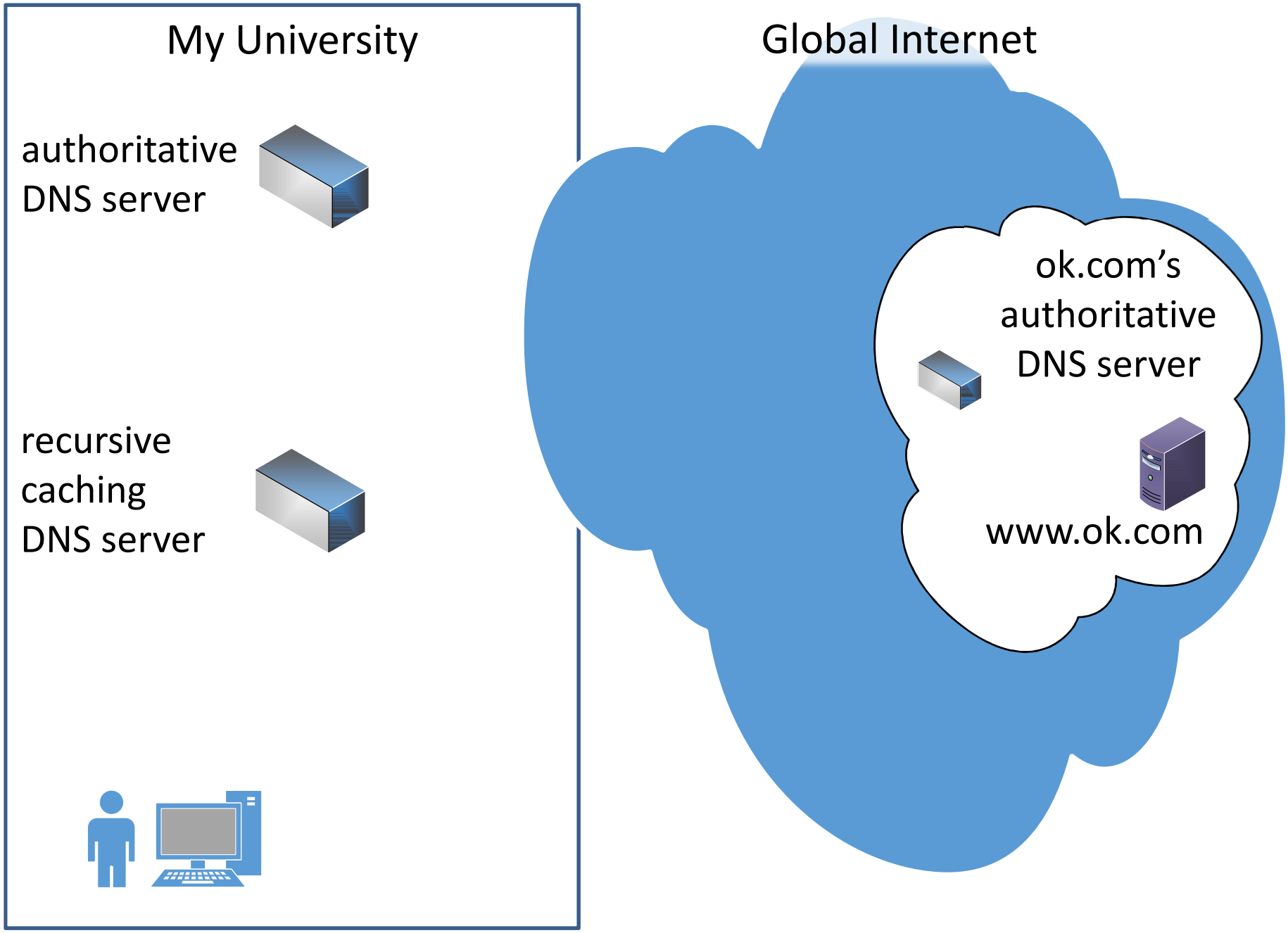
recursive
caching
DNS server

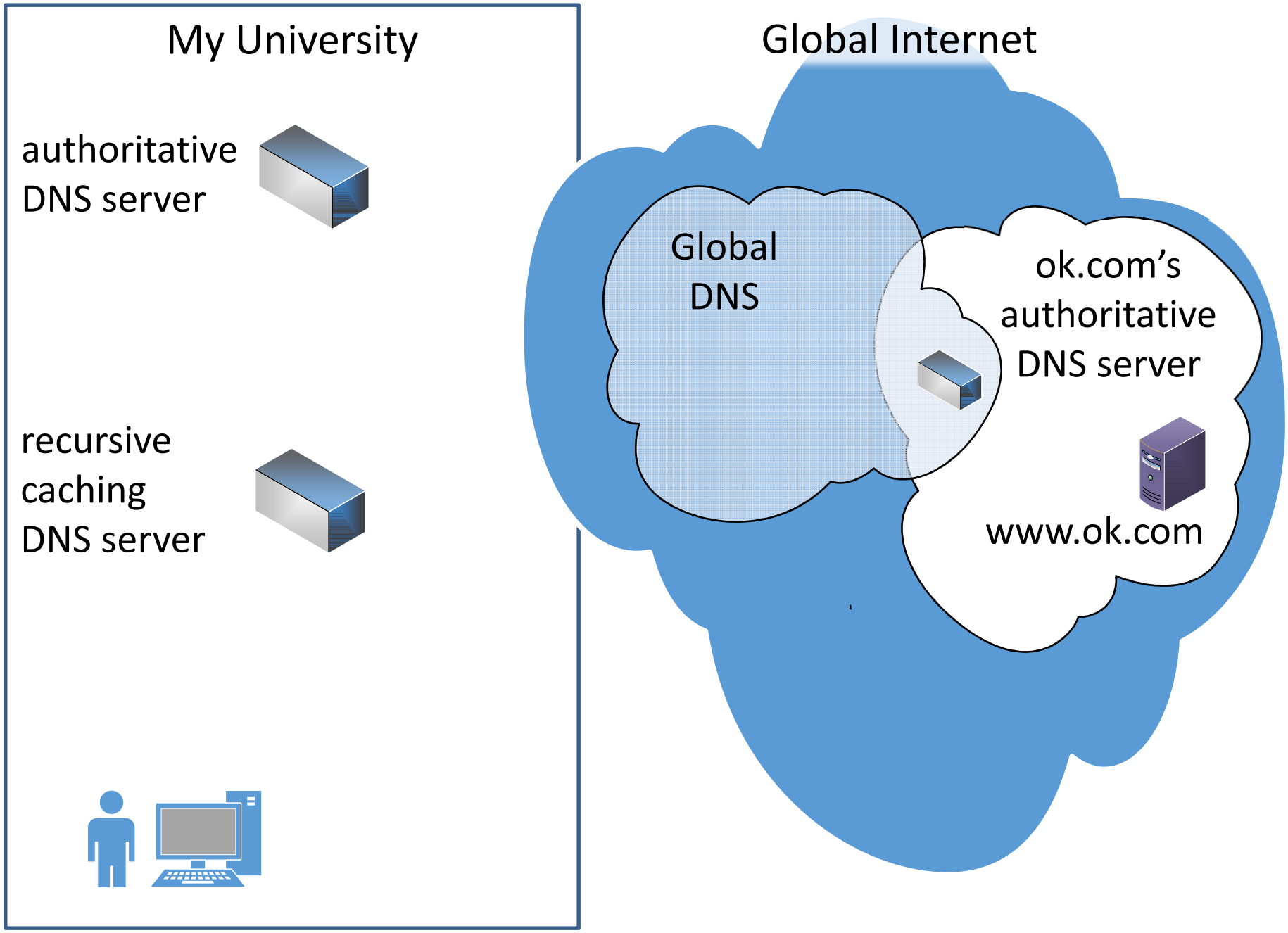


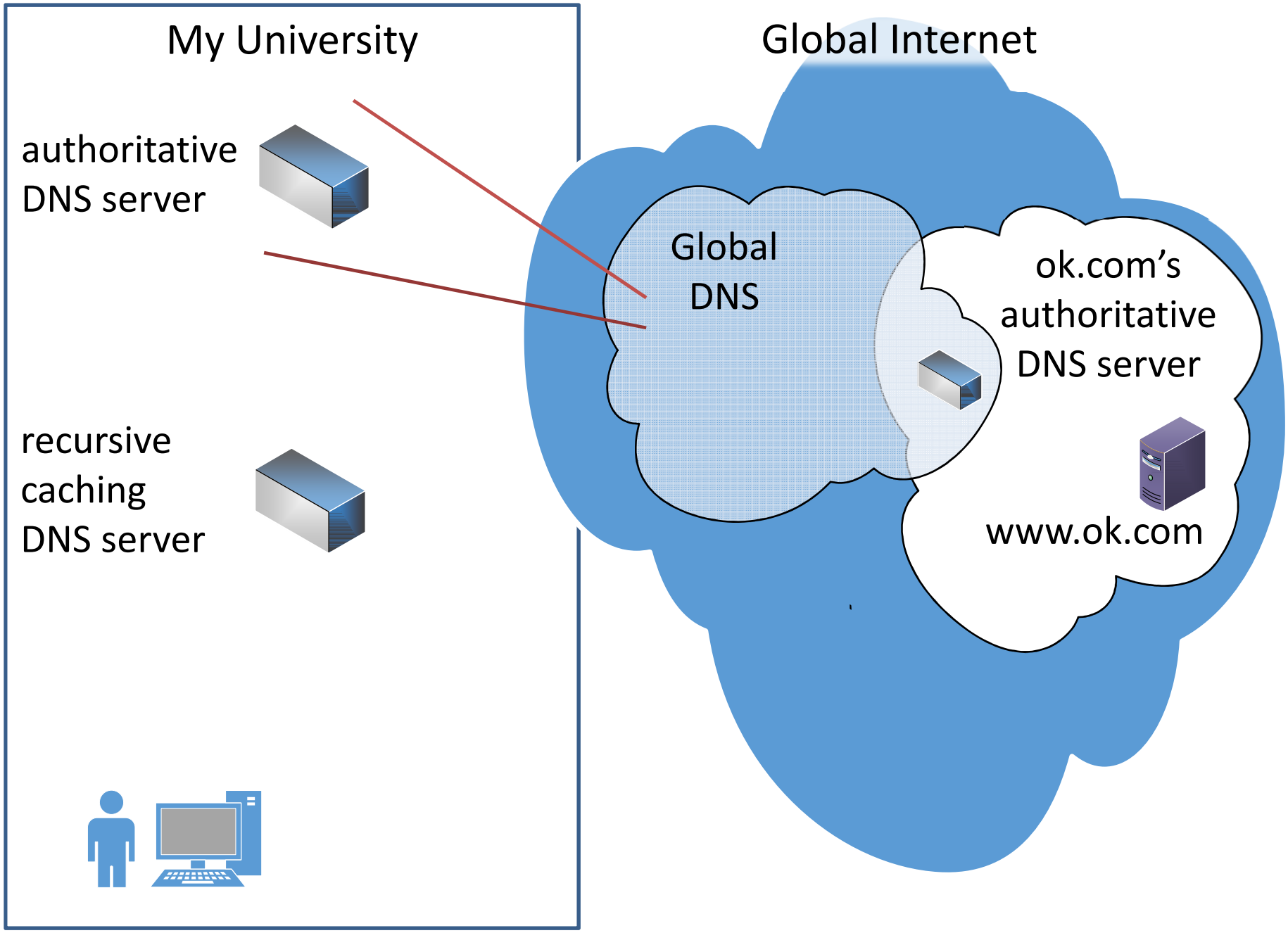


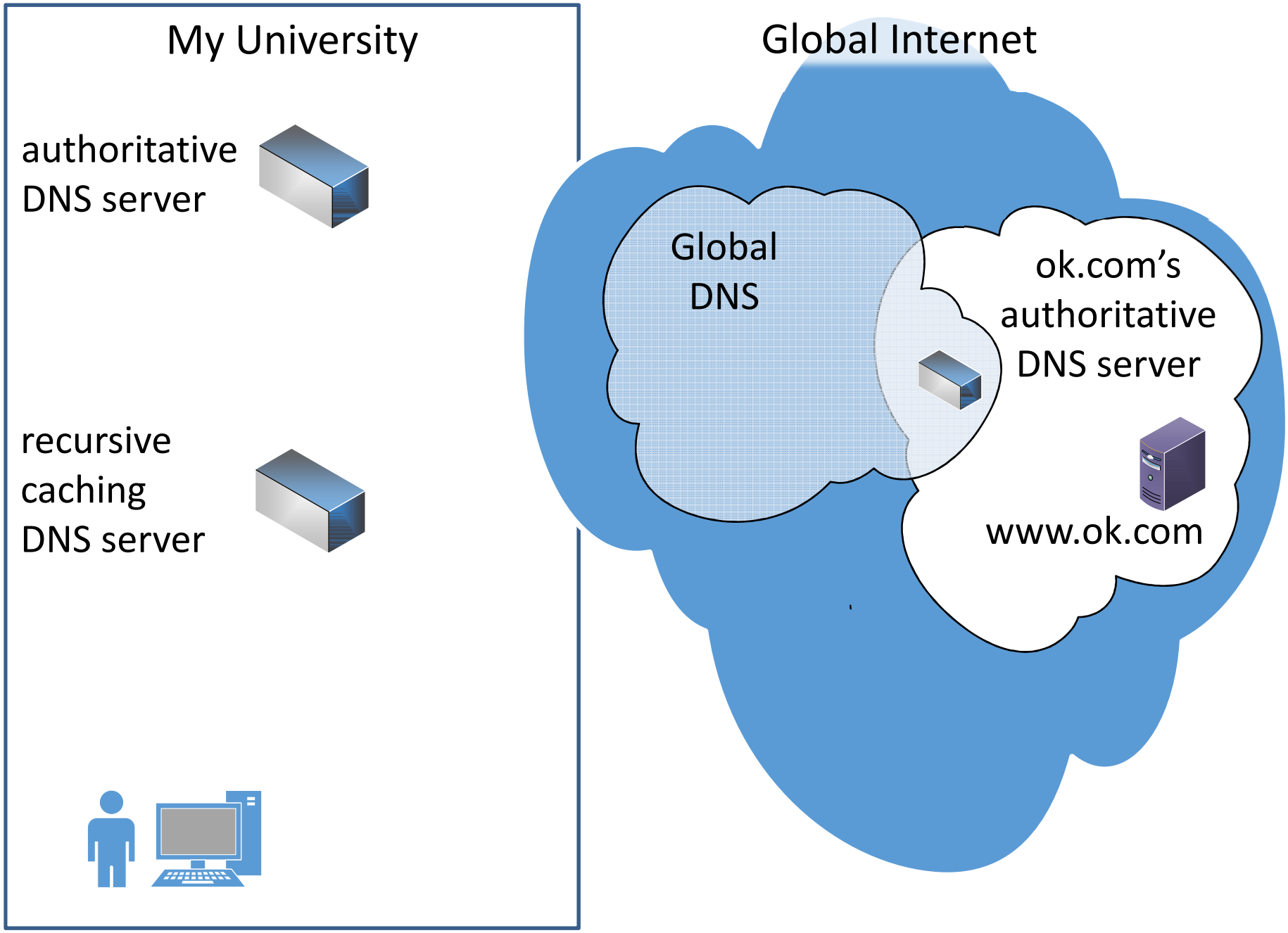

My University
authoritative
DNS server
recursive
caching
DNS server
Global Internet

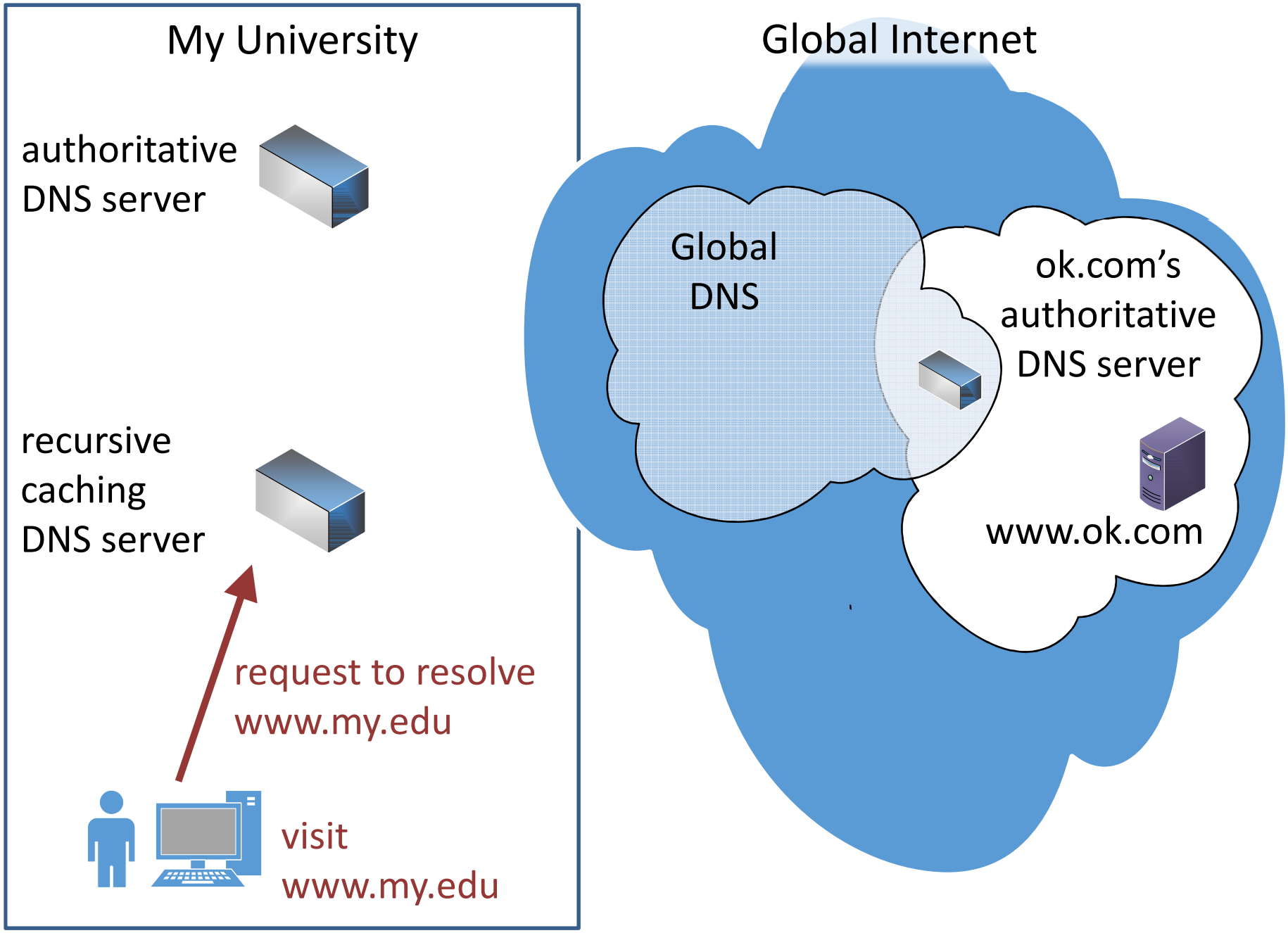

My University
authoritative
DNS server
recursive
caching
DNS server
Global Internet
www.ok.com

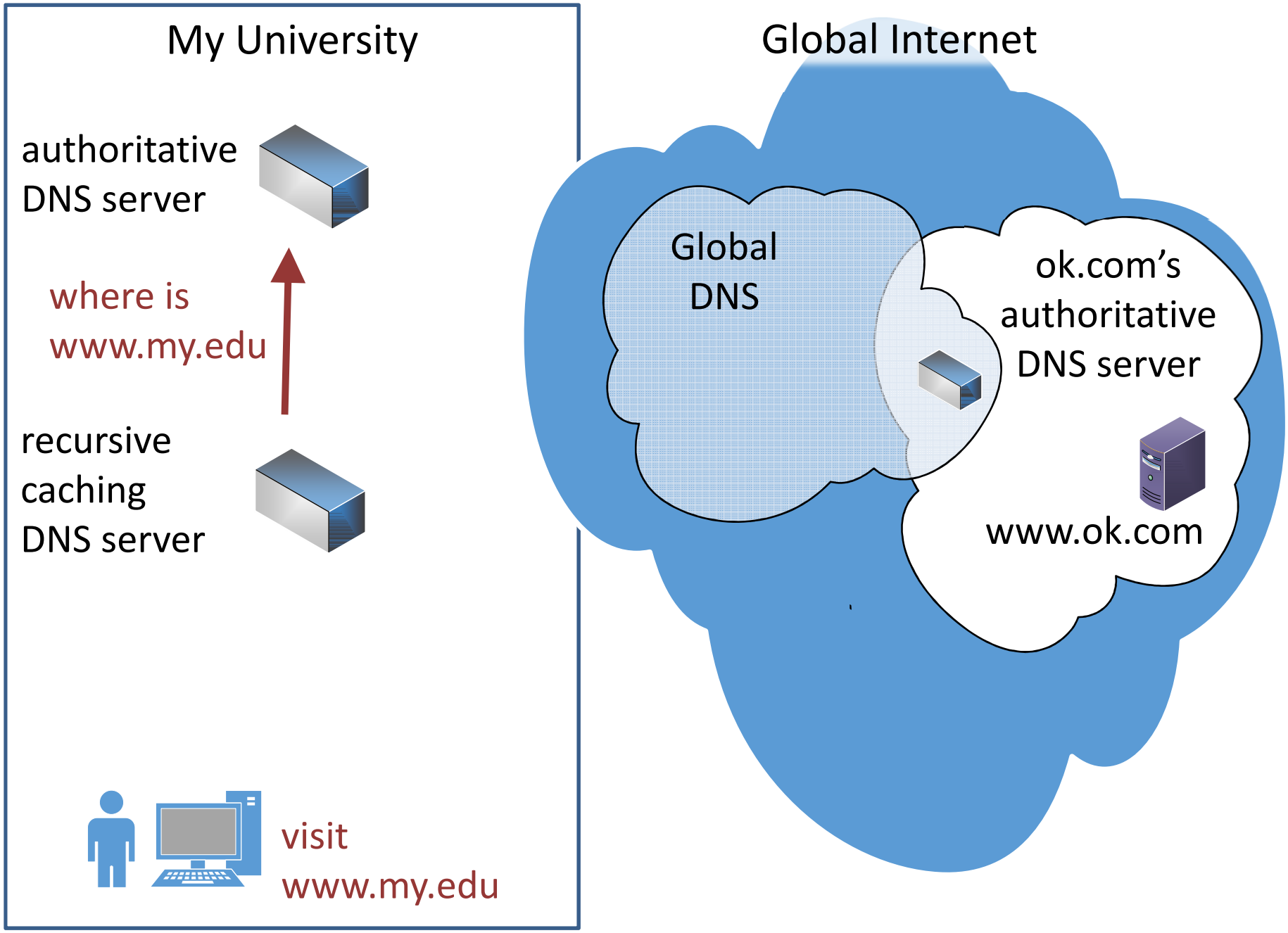

My University
authoritative
DNS server
recursive
caching
DNS server
Global Internet
ok.com's
authoritative
DNS server
www.ok.com

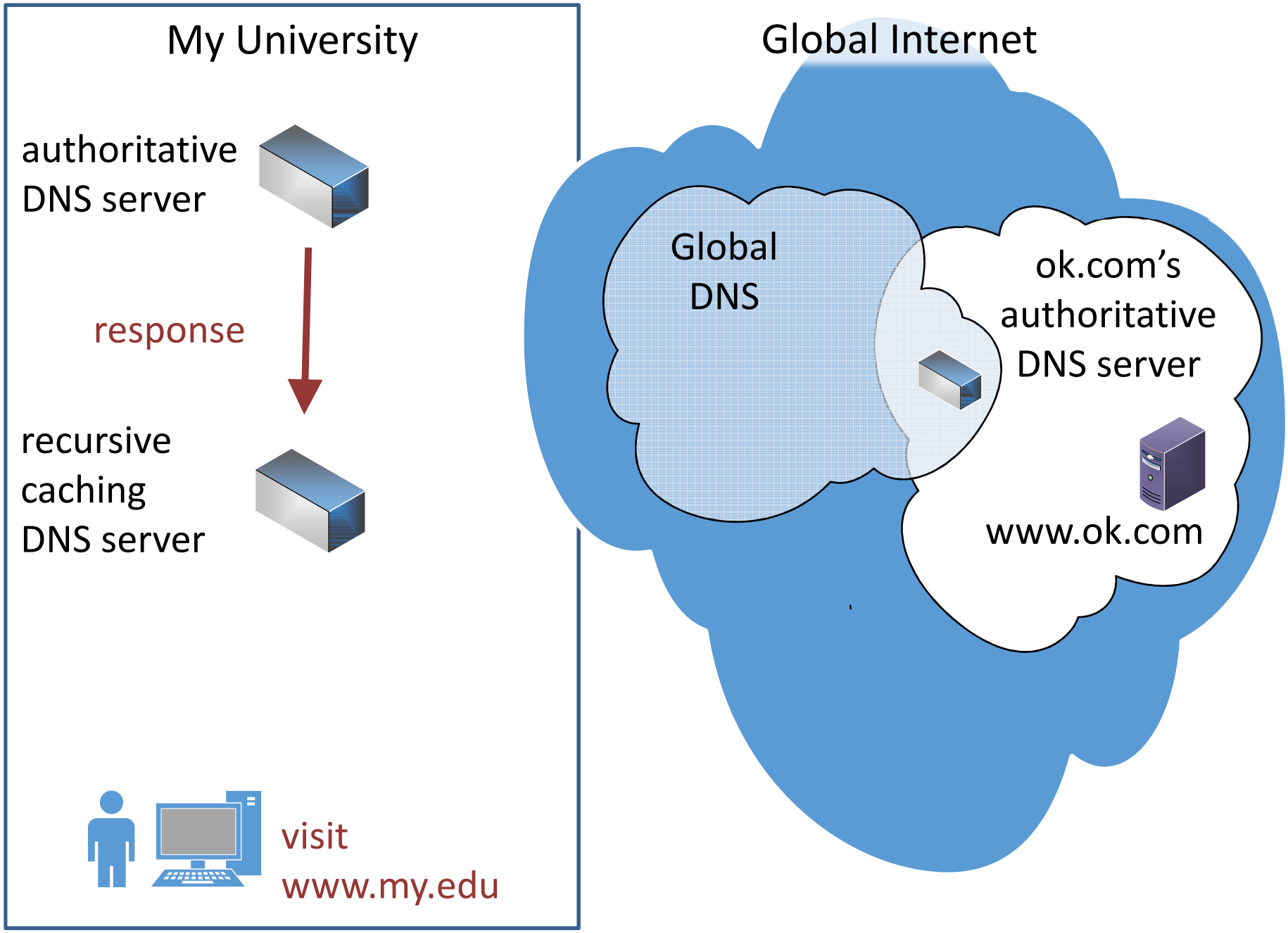

My University
authoritative
DNS server
recursive
caching
DNS server
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

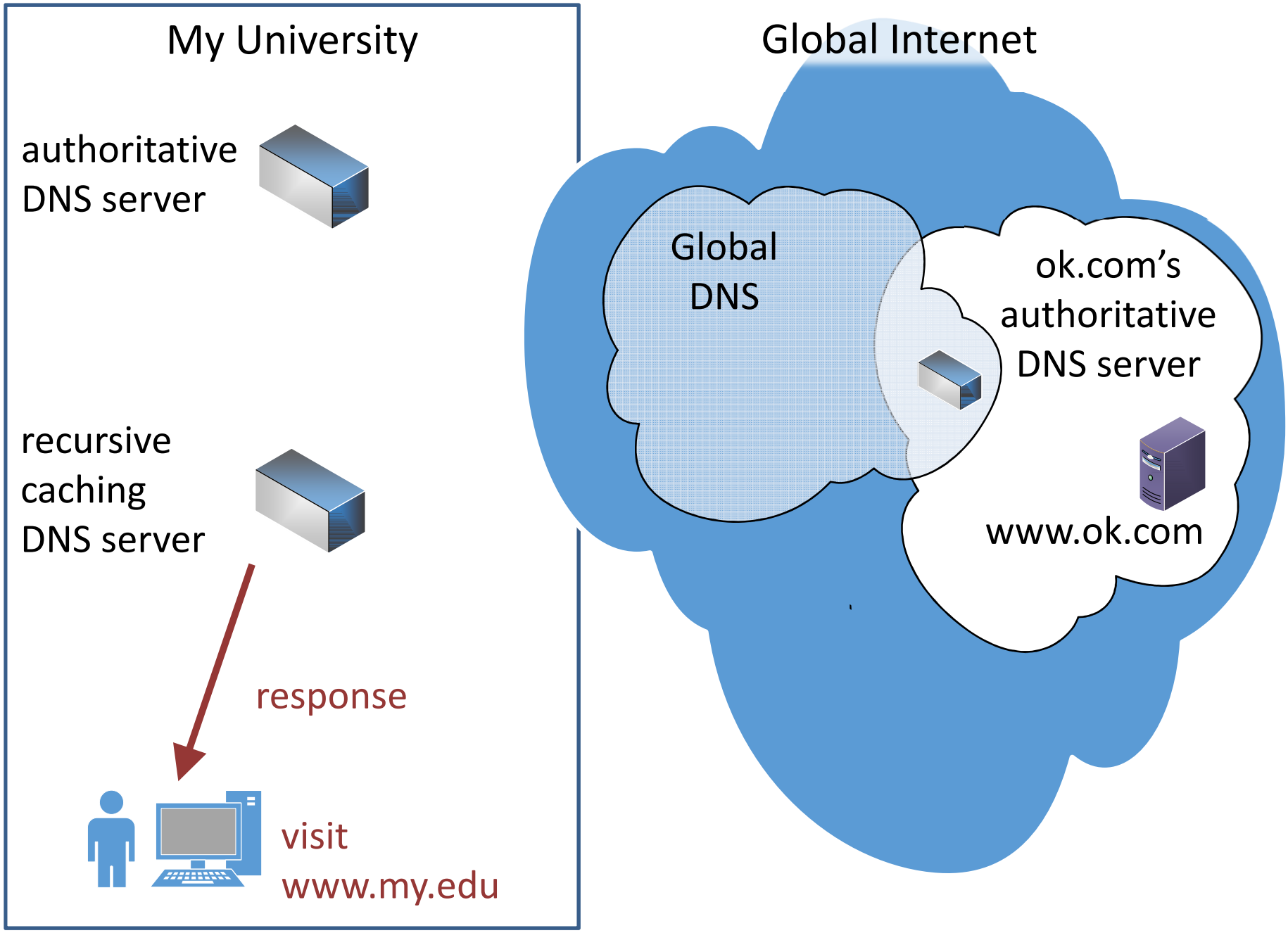

My University
Global Internet
authoritative
DNS server
recursive
caching
DNS server
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

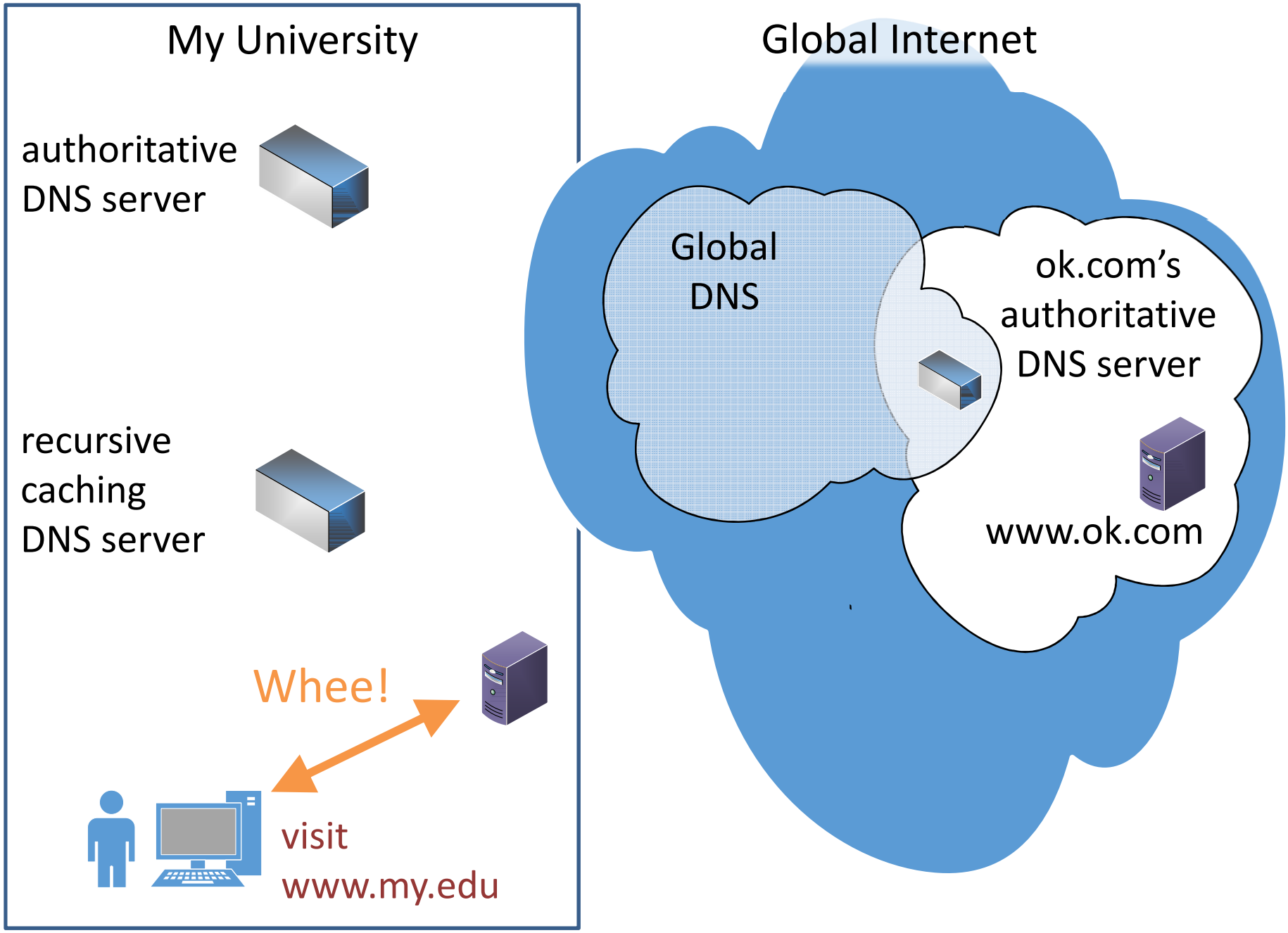

My University
authoritative
DNS server
recursive
caching
DNS server
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

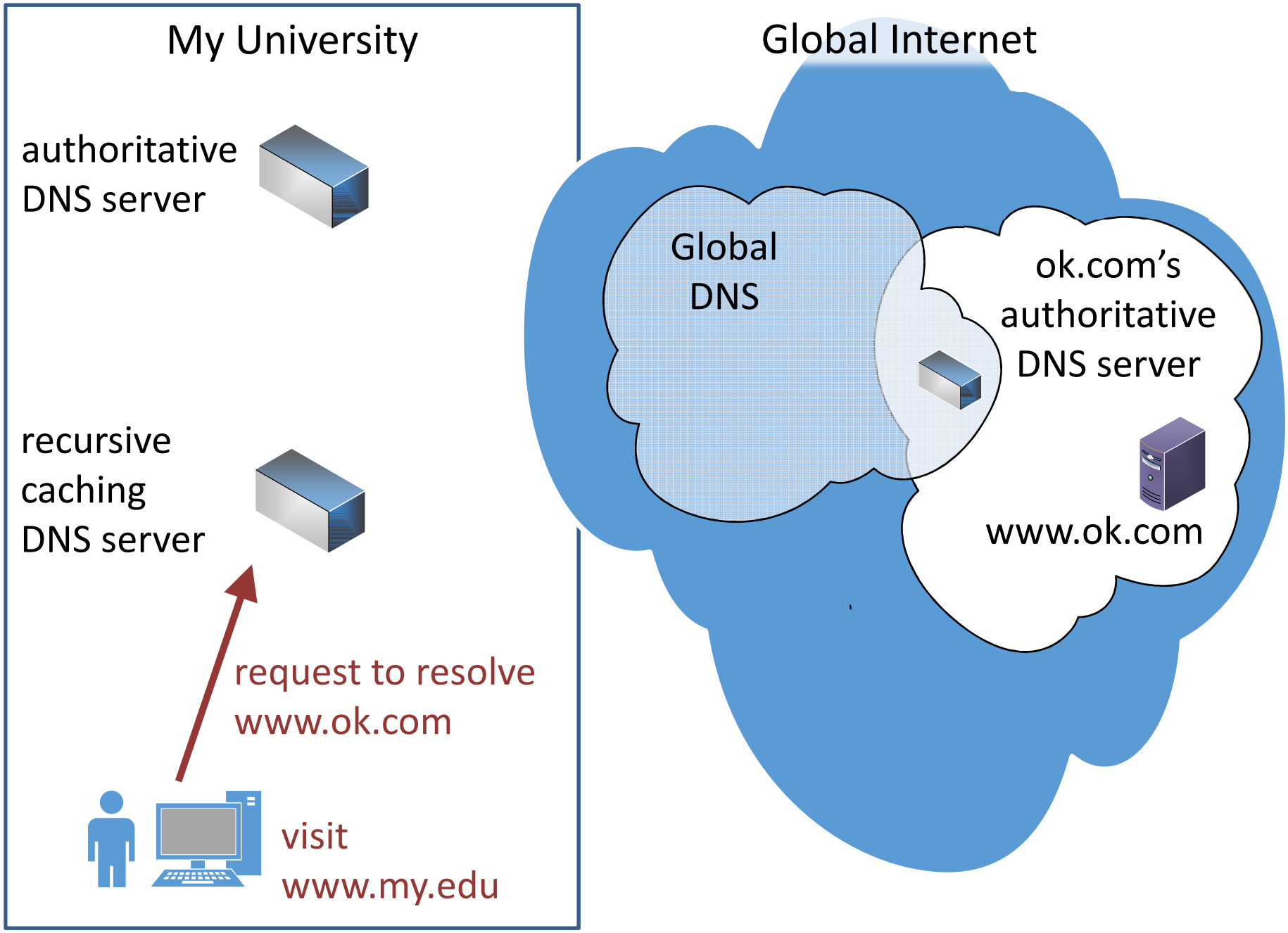

My University
authoritative
DNS server
recursive
caching
DNS server
request to resolve
www.my.edu
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

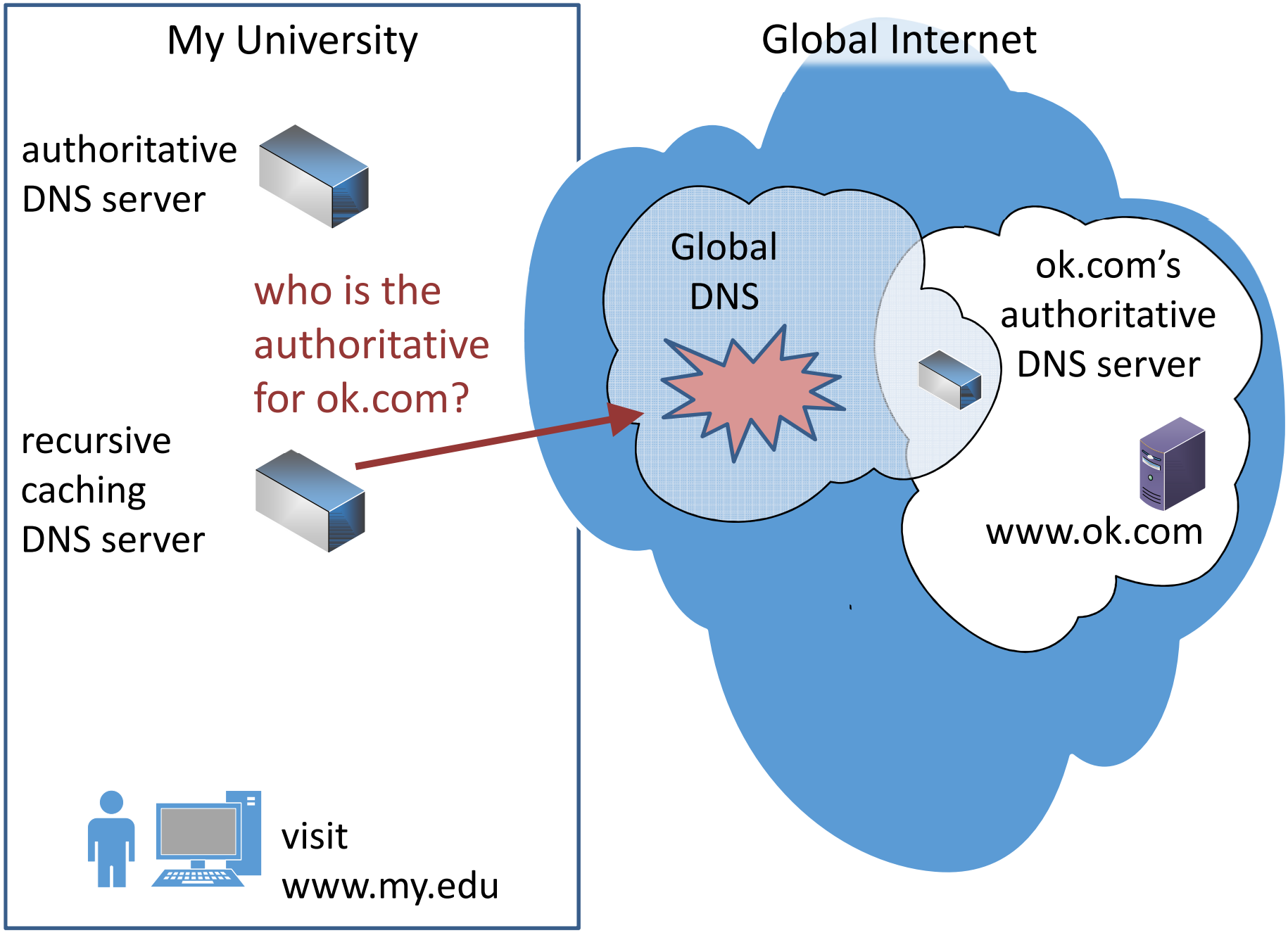

My University
authoritative
DNS server
where is
www.my.edu
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

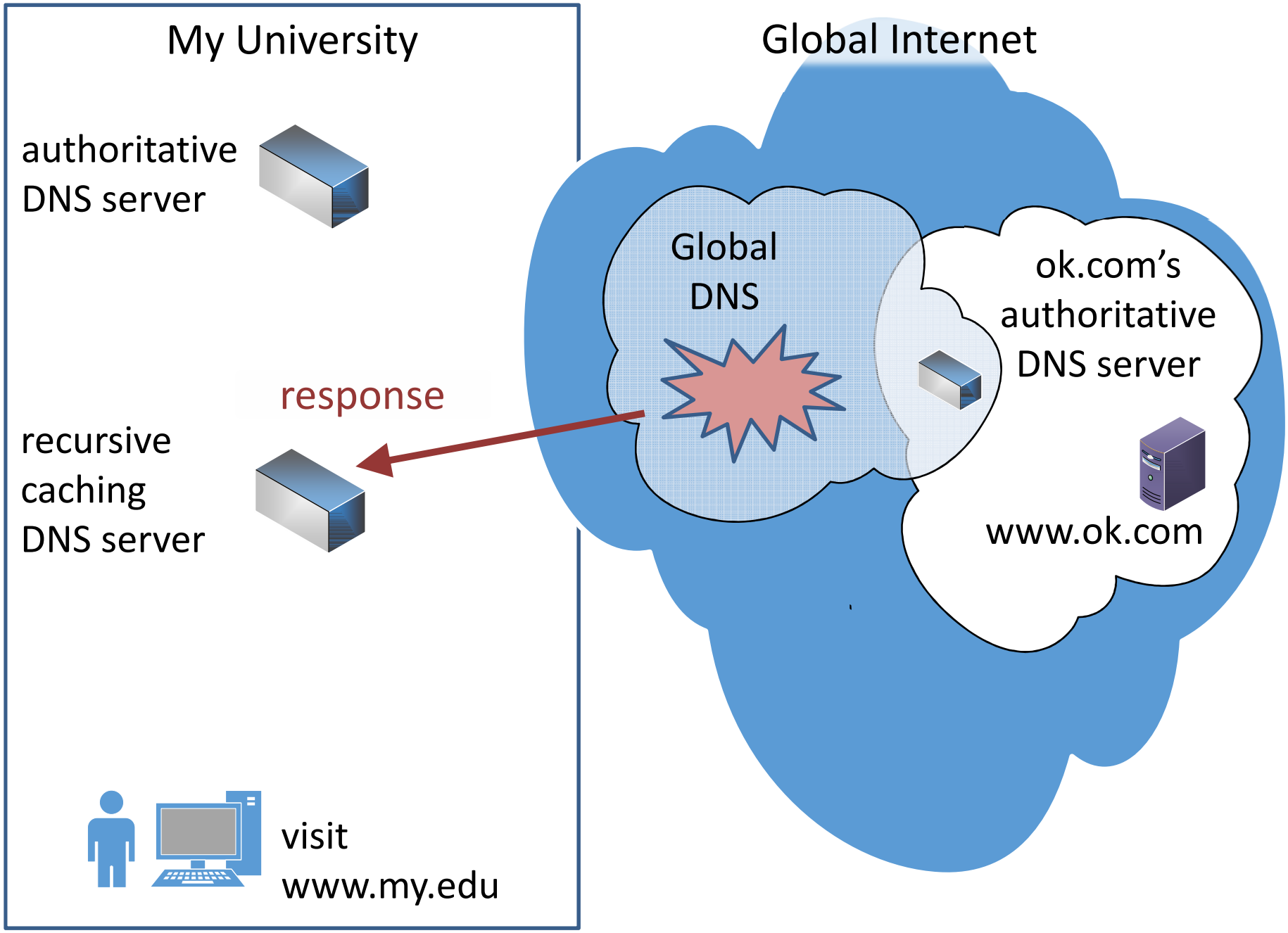

My University
authoritative
DNS server
response
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

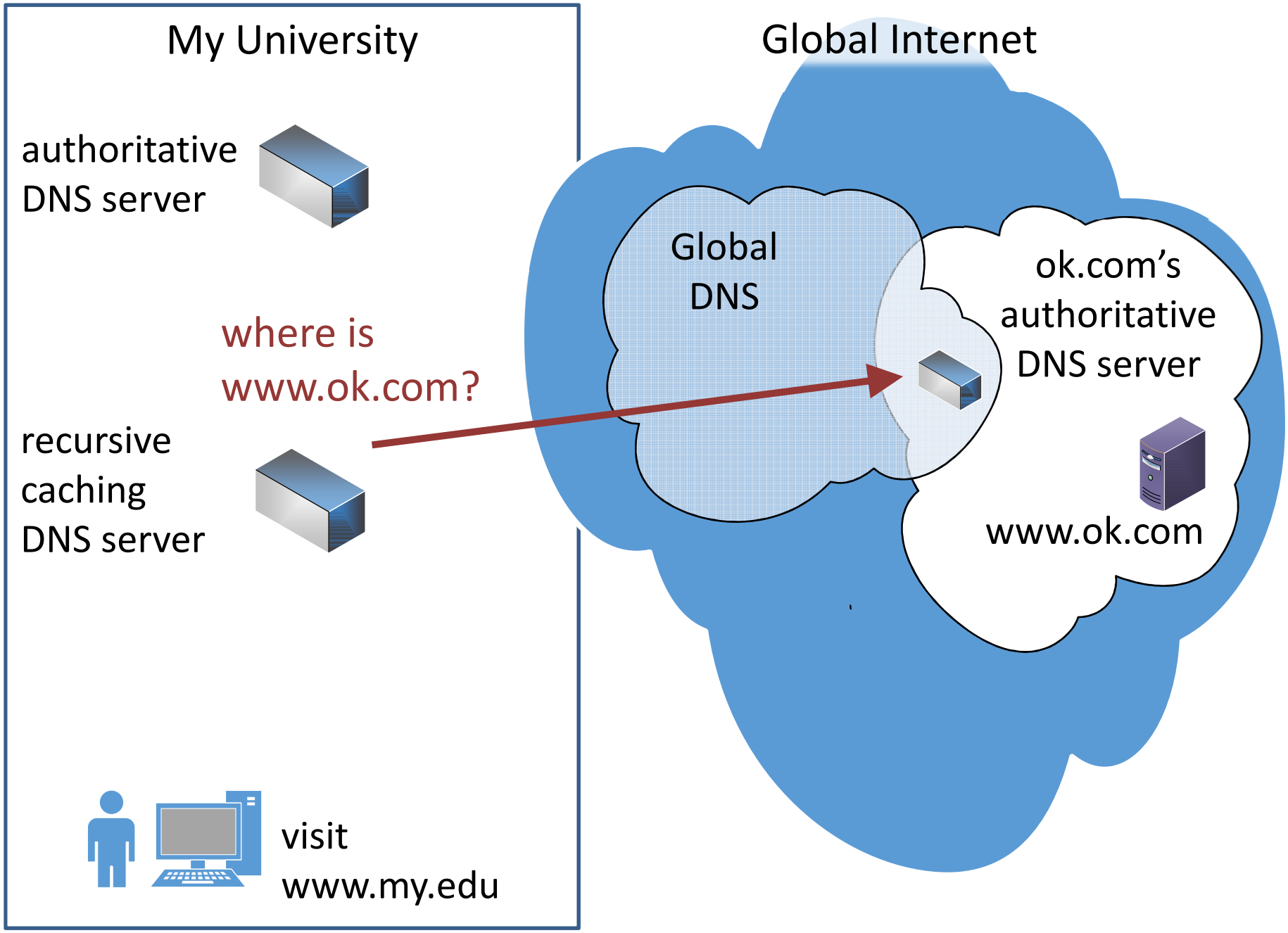

My University
authoritative
DNS server
recursive
caching
DNS server
response
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

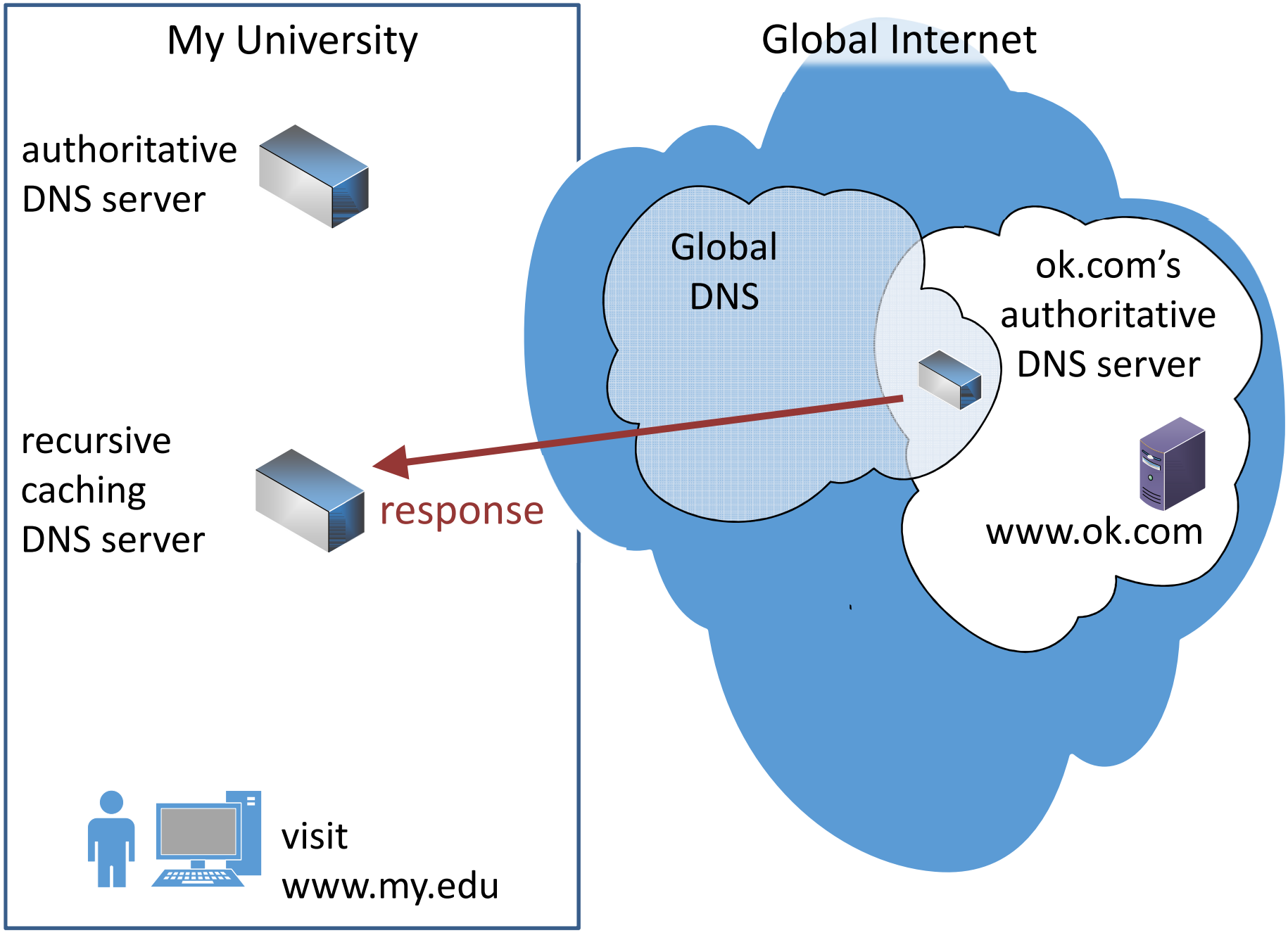

My University
authoritative
DNS server
recursive
caching
DNS server
Whee!
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

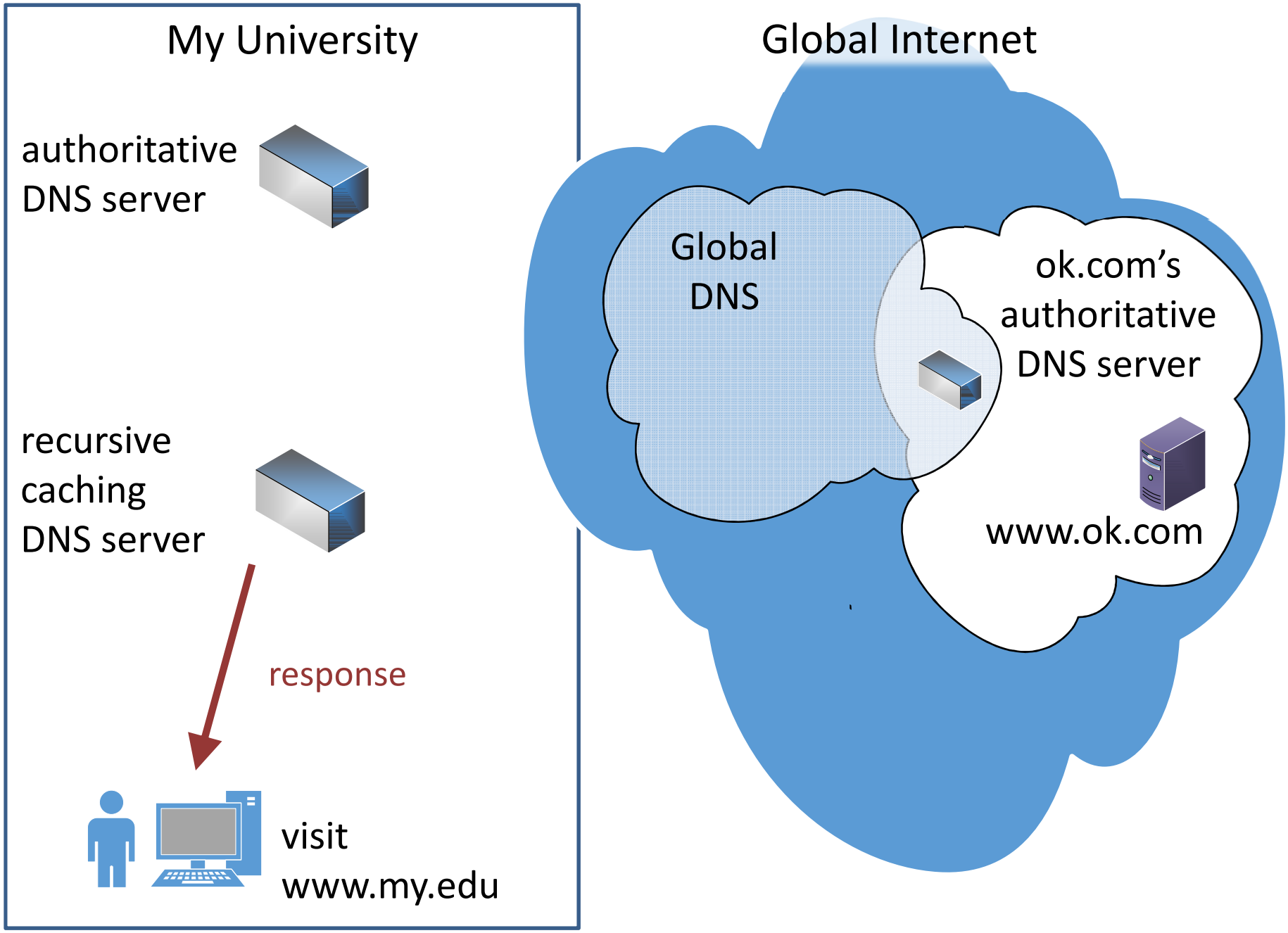

My University
authoritative
DNS server
recursive
caching
DNS server
request to resolve
www.ok.com
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

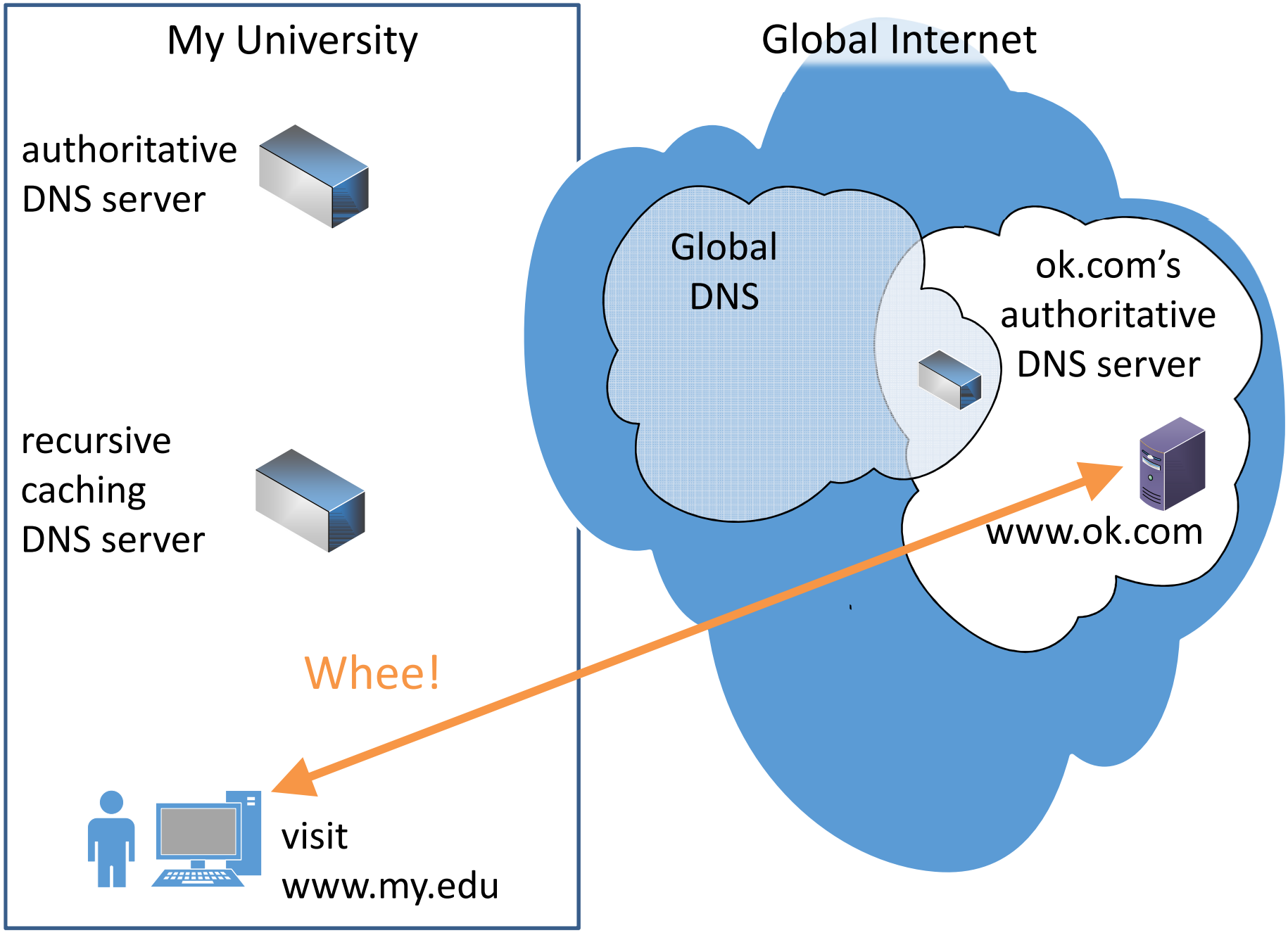

My University
authoritative
DNS server
who is the
authoritative
for ok.com?
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

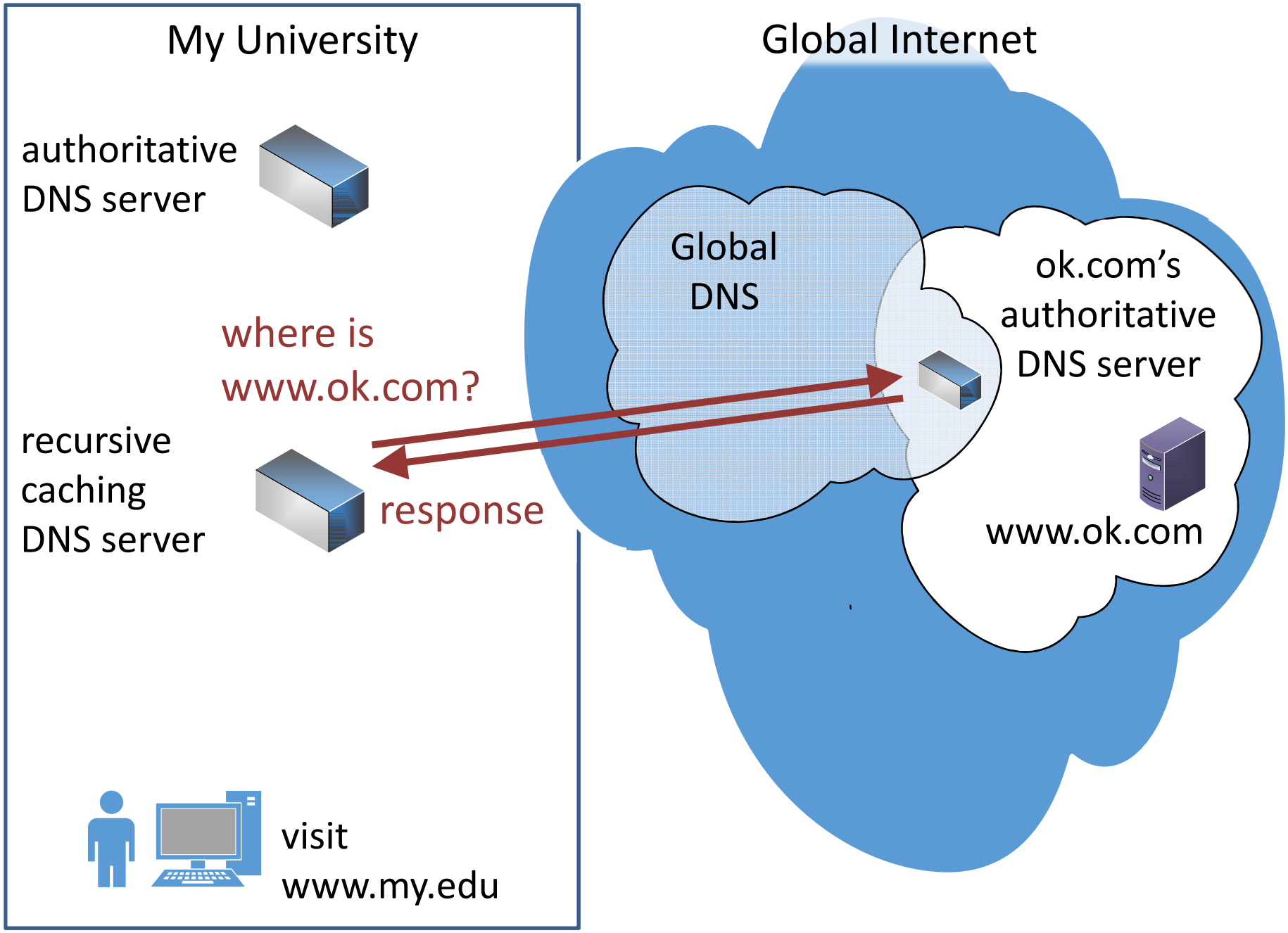

My University
authoritative
DNS server
recursive
caching
DNS server
response
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

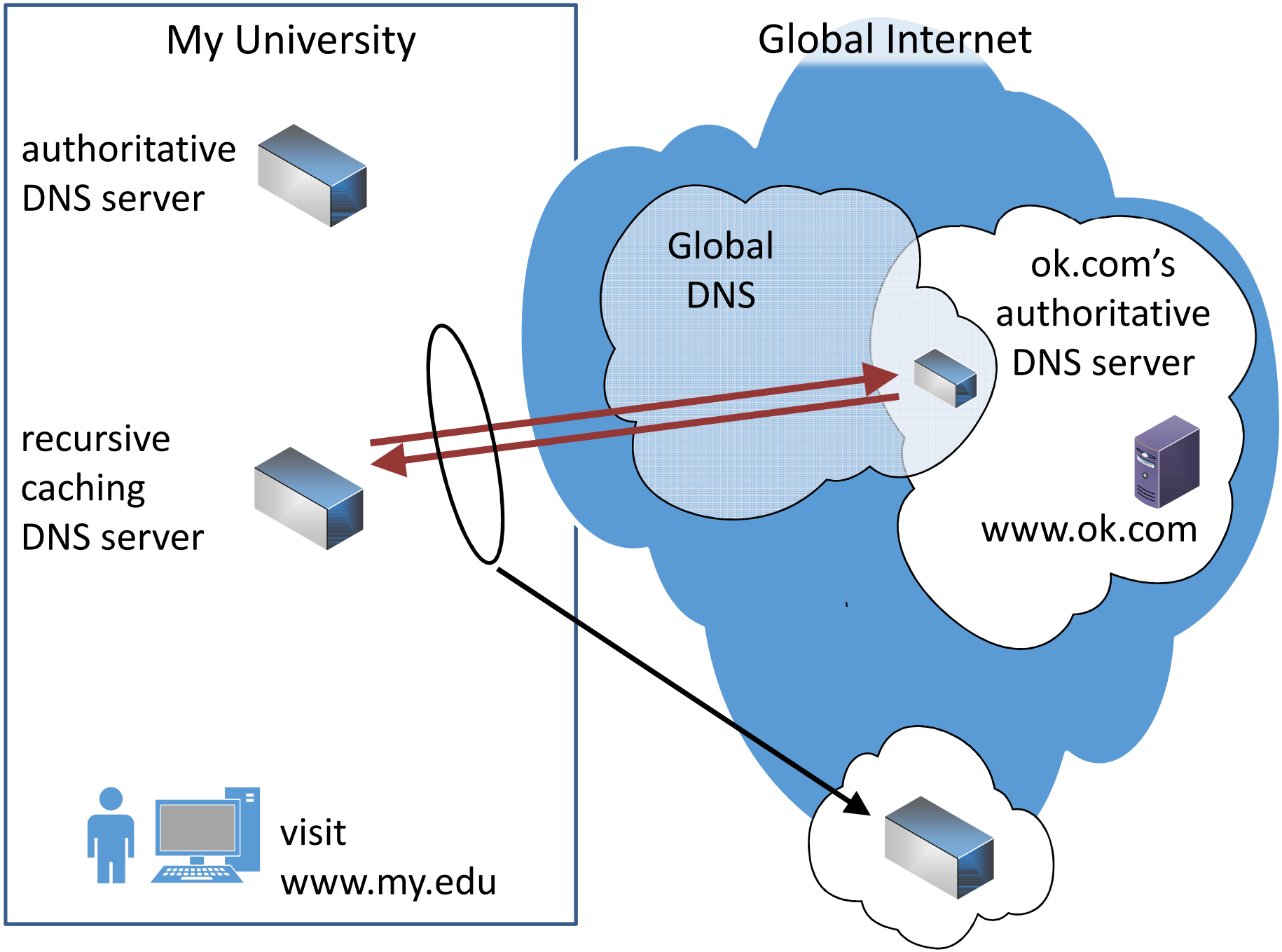

My University
authoritative
DNS server
where is
www.ok.com?
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com

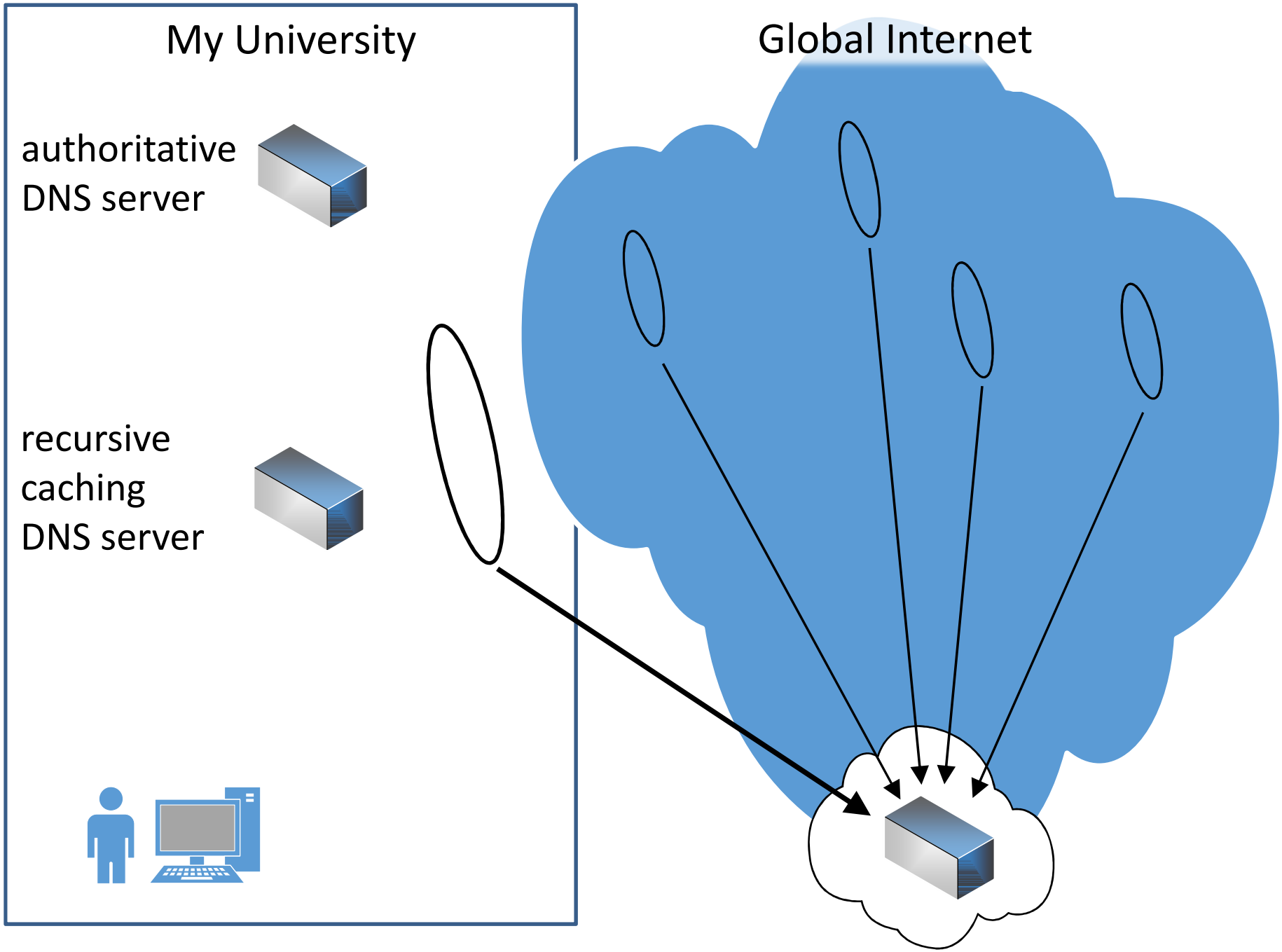

My University
authoritative
DNS server
recursive
caching
DNS server
response
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com


My University
authoritative
DNS server
recursive
caching
DNS server
response
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com


My University
authoritative
DNS server
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com
Whee!


My University
authoritative
DNS server
where is
www.ok.com?
recursive
caching
DNS server
response
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com


My University
authoritative
DNS server
recursive
caching
DNS server
visit
www.my.edu
Global Internet
Global
DNS
ok.com's
authoritative
DNS server
www.ok.com


My University
Global Internet
authoritative
DNS server
recursive
caching
DNS server

REN-ISAC

Are there privacy concerns?

- No… the “outside” data doesn’t contain information about who “inside” made the request.
- Information identifying the enterprise at which the request was made is there… but many pDNS collection efforts allow scrubbing that upon submission.

pDNS Query:
54.209.159.227

2015-07-04 lg.surveys-centre.com
2015-07-01 www.htcsurveycentre.com
2015-06-30 www.digitalappsolution.com
2015-06-26 www.worldnewstoday247.com
2015-06-24 www.samsungsurveycentre.com
2015-06-08 www.healthierlivings.com
2015-05-20 www.theavengerssurvey.com
2015-05-14 www.yourmacsecurity.com
2015-04-22 www.superdealmaker.com
2015-03-30 www.bestapp2015.com
2015-03-22 www.topcriticalerror.com
2015-02-28 www.cellphoneupdated.com
2015-01-22 www.scanmyphones.com
2015-01-09 www.cleanfileupdate.com
2015-01-03 www.easytvcodec.com
2014-12-19 www.opensoftfile.com
2014-12-19 www.scanningdesktop.com
2014-12-19 www.tvstreamcodec.com
2014-11-26 www.smarttvcodec.com
2014-11-17 www.whatsappversion.com
2014-11-12 www.videocodecnow.com
2014-11-07 www.officialrewardcentre.com
2014-10-24 www.phoneupdating.com

pDNS Query:
104.238.102.226

2015-07-27 ip-104-238-102-226.ip.secureserver.net
2015-06-10 www.systemtechies.com
2015-06-04 www.windows-crash-report.info
2015-06-03 windows-crash-report.info
2015-05-28 systemtechies.com
2015-05-26 www.networkerrorfixer.com
2015-05-21 networkerrorfixer.com
2015-05-18 system-error-fixer.com
2015-05-16 network-error.net
2015-05-08 network-issue.net

REN-ISAC

What can you do with pDNS data

- Add valuable intelligence to your IR process
- Map criminal infrastructure
  - Domain names from IP addresses
  - Domain names from “bad” name servers
- Track malware C&Cs
- Monitor your own space
  - “Is evil being hosted in my IP space?”
  - Domain hijacking
- Domain name enumeration for e.g. discovering disaster scams
- Contribute to first-seen gray listing approaches
- &c

REN-ISAC

Public Passive DNS efforts

http://www.bfk.de/bfk_dnslogger.html

http://blog.virustotal.com/2013/04/virustotal-passive-dns-replication.html

http://passivedns.mnemonic.no/search/

REN-ISAC

Passive DNS project status

- Partnership with a third-party for underlying tech
- At the beginning step of working with a pilot institution to develop:
  - information package that informs internal decision making for participation,
  - policy guidance for contributing institutions,
  - implementation documentation
- Plan to aggressively seek contributing institutions in late fall

REN-ISAC

- REN-ISAC introduction
- Expanded Participation
- SES evolution
- Passive DNS project
- Chum

REN-ISAC

Project CHUM

- Concerning phishing
- Goals:
  - Rapid turn around of protection information via SES
  - Make it difficult for phishers to use free, form hosting sites to stand up phish forms (e.g. wix, weebly, jimdo, &c).
- Develop process that allows members to submit phish to REN-ISAC (e-mail phish@ren-isac.net) to:
  - Trigger notifications to source and hoster abuse contacts
  - Extract malicious URLs, reply-to, &c for inclusion to SES for rapid application to local protections
- Status:
  - developing the capability to extract the bad parts from the phish with high confidence and reliability

REN-ISAC

Contacts

Doug Pearson, Technical Director, dodpears@ren-isac.net

http://www.ren-isac.net

24x7 Watch Desk:

soc@ren-isac.net

+1 (317) 278-6630