IAB concerns against permanent deployment of edge-based filtering

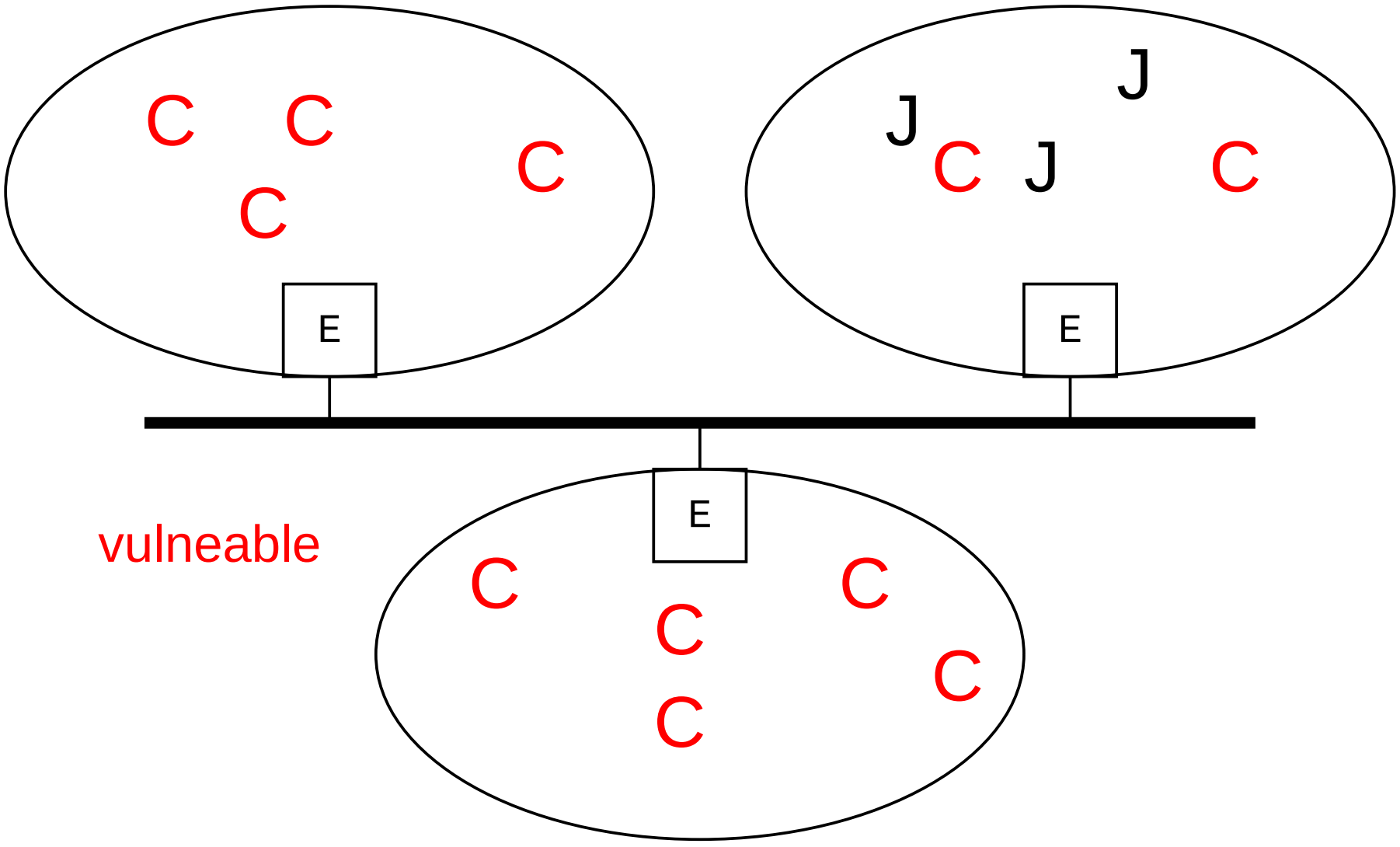
http://www.iab.org/documents/docs/2003-10-18-edge-filters.html

Jun-ichiro itojun Hagino
IAB member
Research Laboratory, Internet Initiative Japan
itojun@iijlab.net

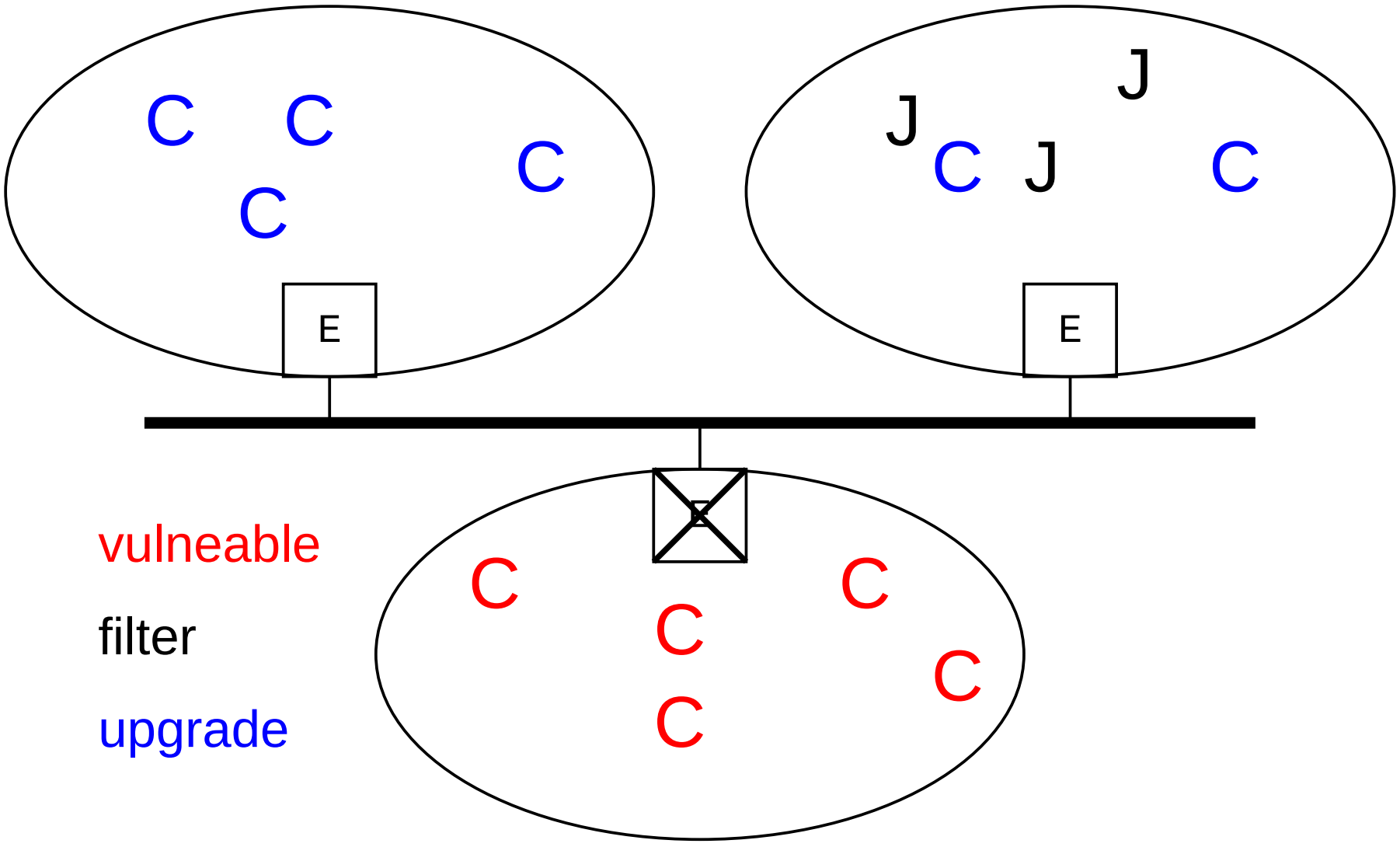
Outline

- IAB posted a note in Oct 2003 to NANOG
- ISPs' responses to CISCO vulnerability(CA-2003-015)
  - Filter based on protocol number at EBGP routers - PIM, mobile-ip4
- As a short-term workaround (while upgrading CISCO) it is okay
- IAB noted that multiple ISPs plan to leave the filter configured forever
- Filters at EBGP router does not really solve the problem
  - Attackers could be your customer
- It is a threat to the Internet itself
  - To the extensibility/adaptability of the Internet
- So, please upgrade CISCO and remove filters at EBGP routers

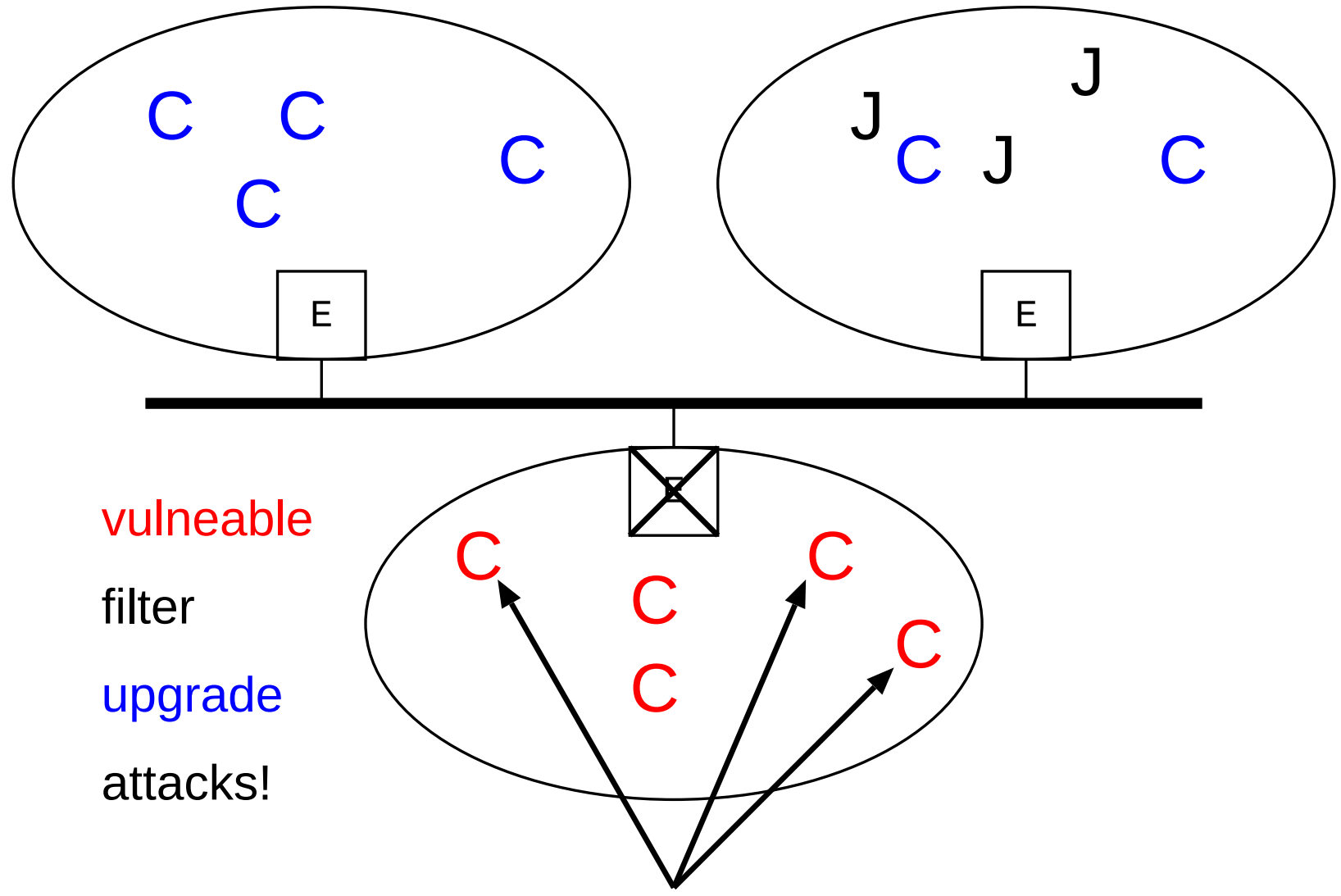
Vulnerability was found



Upgrade (good), or filter (not good)



Filters at EBGP are not good (1)



- Attackers could be your customers
  - Filters at EBGP router is useless

Filters at EBGP are not good (2)

- Filters ban some of important protocols
  - CA-2003-015: mobile-ip4, PIM
- The key architectural importance of Internet: extensibility
  - Scalability (extensibility in size)
    - Good scalability of IPv4, v6
  - Protocol extensibility
    - It is easy to introduce new protocols
    - it is not necessary to upgrade routers to introduce new protocols
- Filters at EBGP routers will damage protocol extensibility
  - Extreme example: (pseudo) Internet that pass TCP port 80 only

Filters at EBGP are not good (3)

- Customers are not notified of filters at EBGP routers
  - Even if they are notified, they have no control
- Customers have no idea why specific protocol (mobile-ip4) cannot go through
- It is okay to filter, as a service to customer, with customers' concent, at customer edge routers
  - IAB comment does not discuss this

Summary

- ISPs' responses to CISCO vulnerability(CA-2003-015)
  - Filter based on protocol number at EBGP routers - PIM, mobile-ip4
- As a short-term workaround (while upgrading CISCO) it is okay
- IAB noted that multiple ISPs plan to leave the filter configured forever
- Filters at EBGP router does not really solve the problem
  - Attackers could be your customer
- It is a threat to the Internet itself
  - To the extensibility/adaptability of the Internet
- So, please upgrade CISCO and remove filters at EBGP routers
- Comments to: iab@ietf.org