Cisco IP Source Guard

draft-baker-sava-cisco-ip-source-guard

Fred Baker

 © 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Background of IP Source Guard

- IPv4-only
- Premise:

  BCP 38 recommends that to prevent datagrams with spoofed addresses from being in the network, one should check traffic from one's predecessor for reasonableness and discard illogical datagrams.

  Logic says that the best place to do this is at the system directly in front of the misbehaving host.

  Duh.

- Who implements this:

  Cisco Catalyst Switches can be configured to do this.

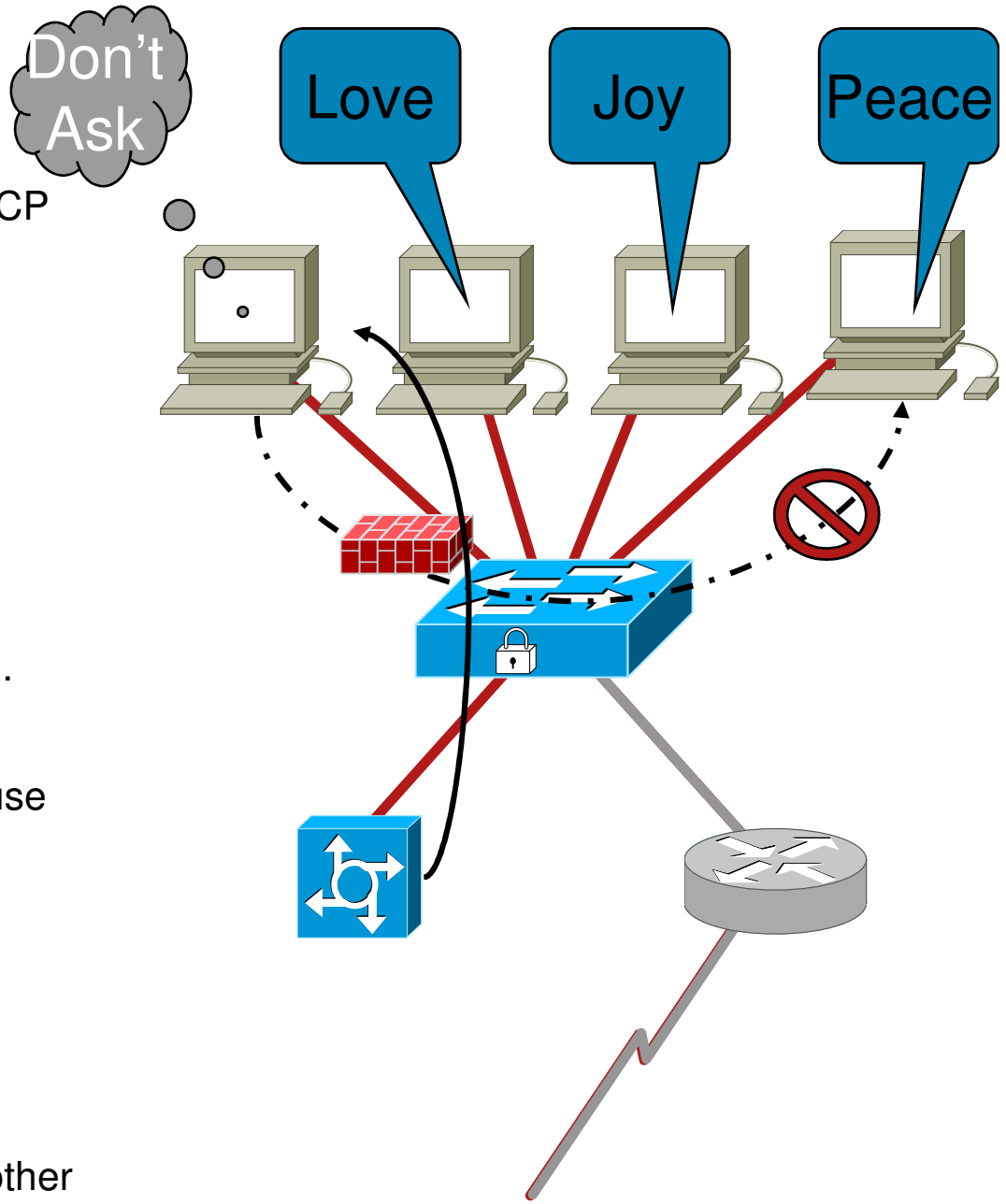
  Foundry has a similar feature by the same name

  I believe other switch vendors do as well

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Overview

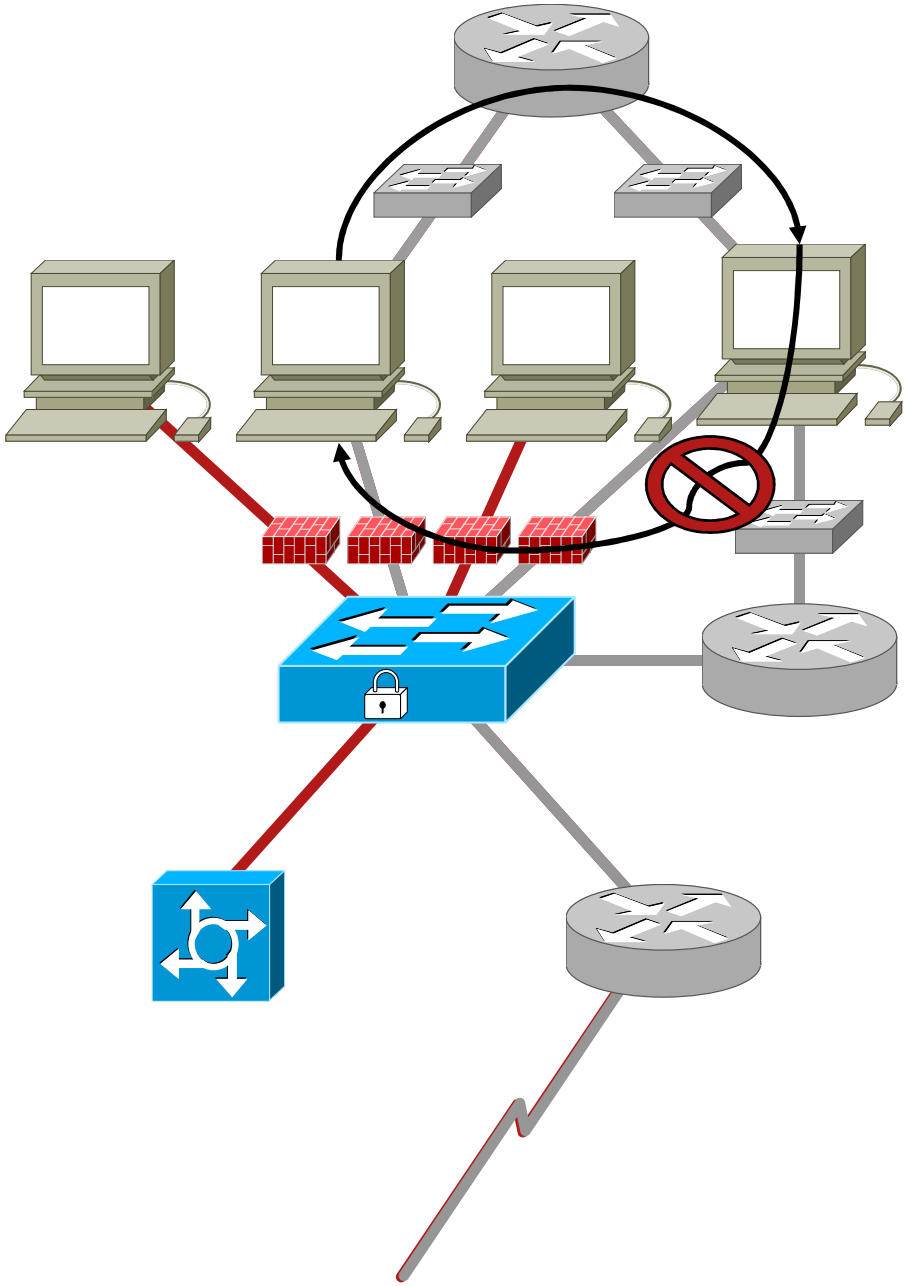
- Premise:
  - Addresses assigned using DHCP
  - One address per interface
  - One host per port
  - At most one VLAN per port
  - Host has one interface
- Algorithm:
  - Snoop DHCP assignment
    - Yes, that's a layer violation.
  - Autoconfigure port filter
  - Discard IP traffic that doesn't use that address
- Port types:
  - Protected and Unprotected
- Net effect
  - No pun intended
  - Hosts can't even attack each other



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The snaky case

- Hosts may have multiple interfaces without routing between them.
  - Hosts send “from” the IP address of the interface they request on.
  - Hosts respond “from” the IP address the request was sent to
  - Host routing may not send data back the way it came
- Implication:
  - Hosts with multiple interfaces cannot be protected under these assumptions

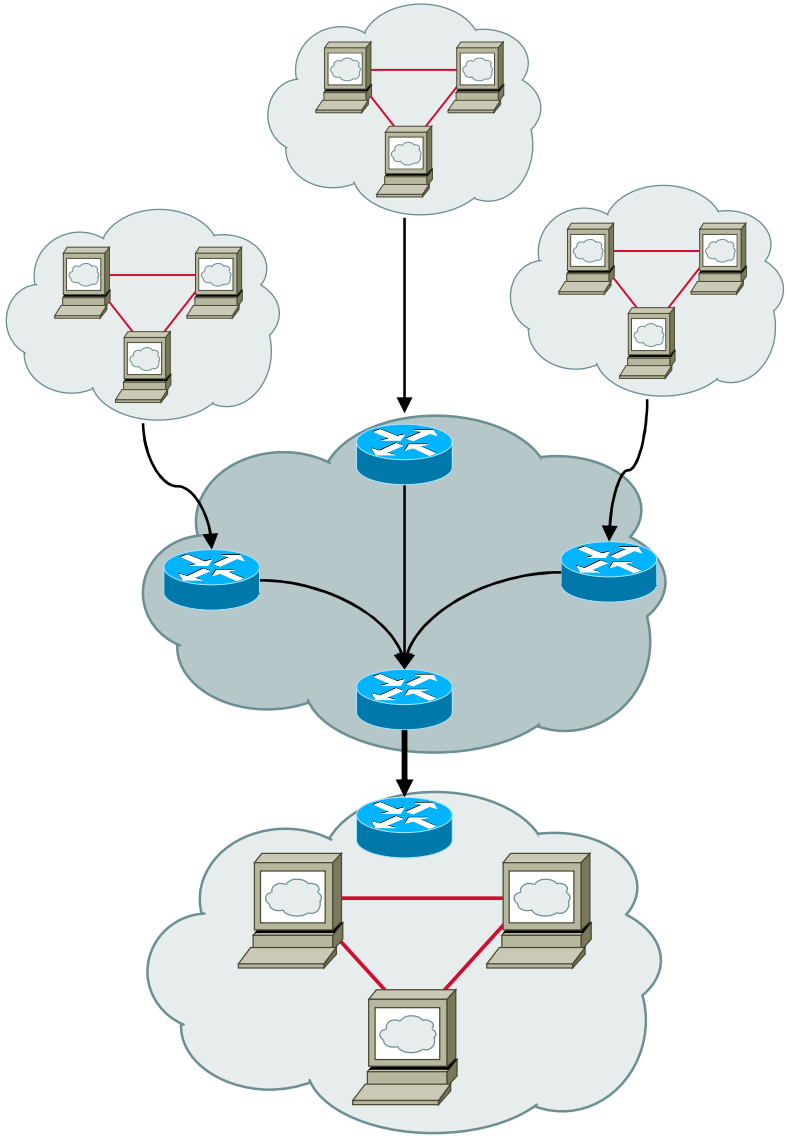


© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Value of source address verification

- Removes attacks that use spoofed addresses
- If I have eliminated spoofed addresses, I know that remaining attackers are using their real ones
- If I then eliminate traffic from/to bots, I free bandwidth for useful traffic
- My customers are happier.

  I may also gain customers if I build a reputation for having few successful attacks.



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential