DDoS Protection

How Cisco IT Protects Against Distributed Denial of Service Attacks

A Cisco on Cisco Case Study: Inside Cisco IT

Overview

- Challenge:

  Prevent low-bandwidth DDoS attacks coming from a broad range of spoofed addresses

- Solution:

  Deploy Cisco Guard at Cisco's Internet points of presence (POPs) and in the Internet cloud

- Results

  Successfully mitigate DDoS and other attacks

- Next Steps

  Work with service providers to offer "Clean Pipes" solution—Cisco Guard at the service provider location—to other enterprise customers

Challenge: Prevent DDoS Attacks

- Cisco IT uses multiple techniques to prevent network attacks

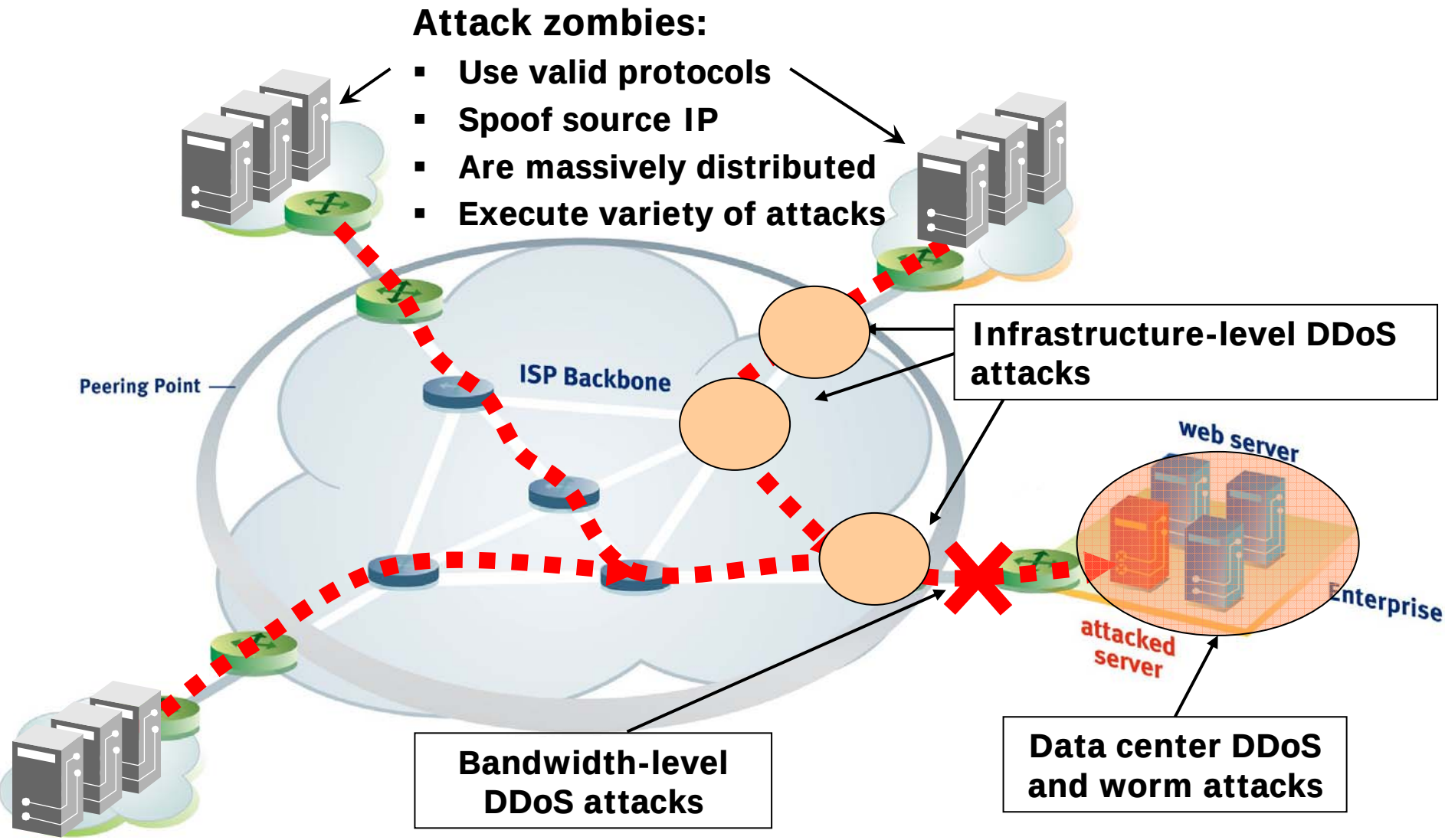
  Access control lists (ACLs) at network edge—also called black holes—coarsely filter traffic from servers spoofing Cisco addresses, or traffic to Windows control ports

  More granular ACLs protect Cisco Connection Online

Challenge: Prevent DDoS Attacks

- Cisco IT needed new techniques to prevent a new type of threat: low-bandwidth DoS attacks coming from a broad range of spoofed addresses
  - ACLs would block legitimate traffic as well as malicious traffic
  - With ACLs, IT would need to constantly shift the block as the apparent origin of the attack shifted
  - ACLs lack the sophistication to deal with DoS attacks from sites using network address translation (NAT)

Challenge: Prevent DDoS Attacks



Solution: Cisco Guard

- Provides an added layer of protection for mission-critical servers, including e-commerce
- Deployed in Cisco's major ISP points of presence (POPs) around the world, as well as in the Internet cloud
- Sits on traffic path
- During ordinary operations, traffic follows its usual path through the network

Solution: Cisco Guard Process

But when an attack begins…

- Cisco IT learns of potential attacks in numerous ways, including notification by Arbor PeakFlow DoS system which analyzes Cisco NetFlow data
- Cisco IT decides which DDoS mitigation method to use:

  For small attacks from few IP addresses: black hole technology or shutting down specific devices

  For large attacks from many IP addresses: Cisco Guard or other methods

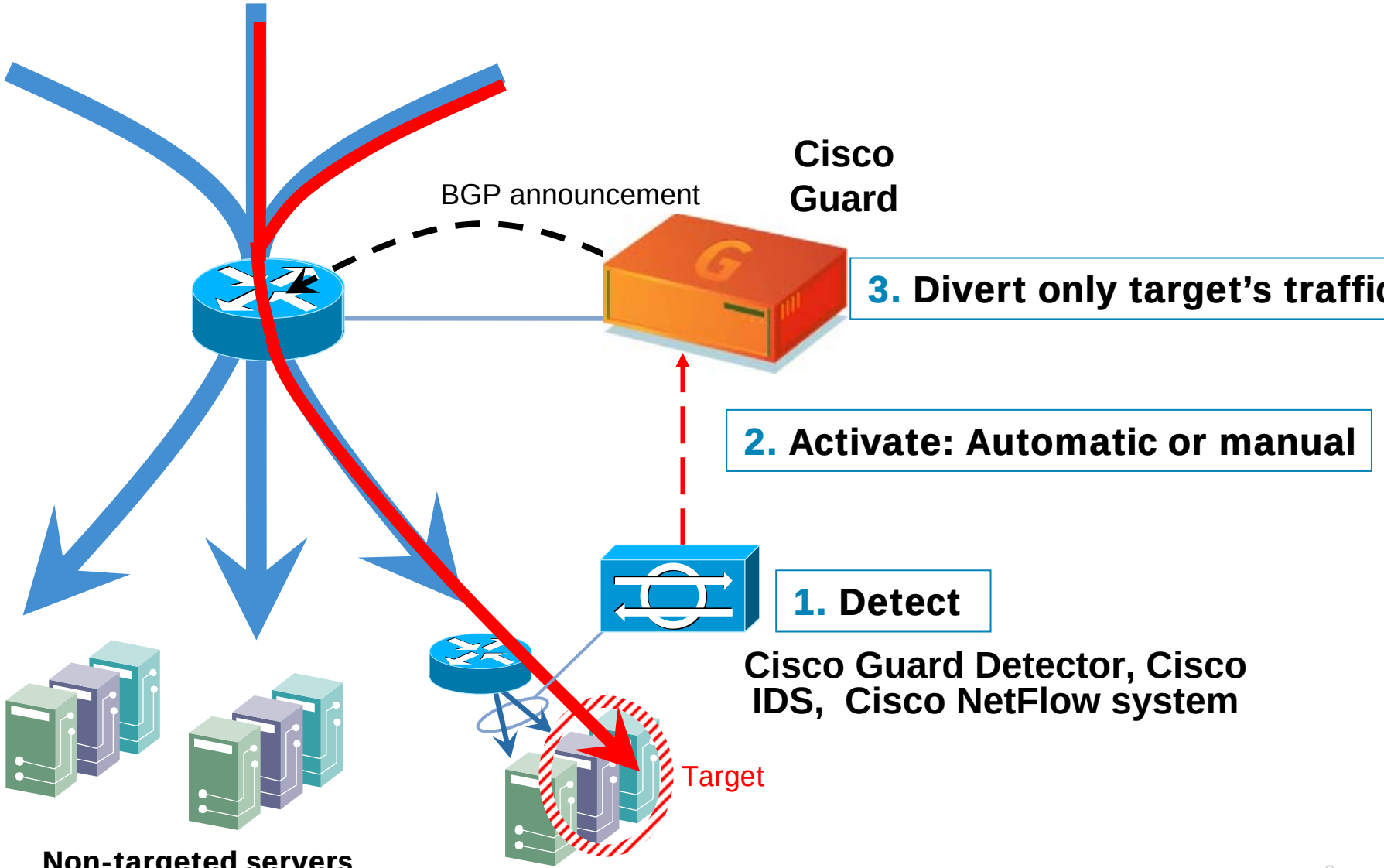
Solution: Cisco Guard Process

- Cisco Guard uses dynamic routing to divert traffic headed for protected properties
- It differentiates normal from malicious traffic by comparing it to normal traffic profile for the server

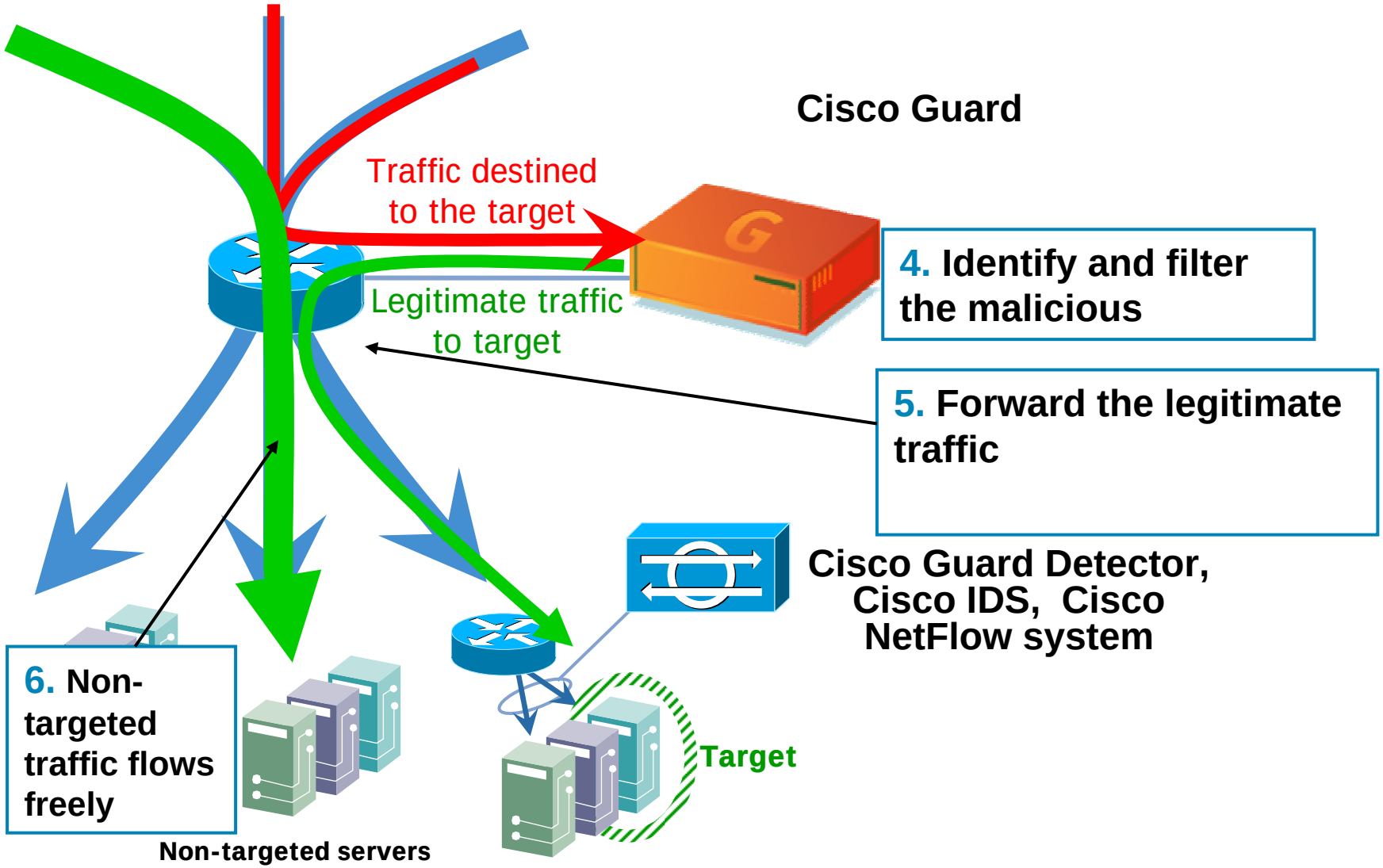
  Good traffic passed through

  Bad traffic dropped

Solution: Cisco Guard (steps 1-3)



Solution: Cisco Guard (steps 4-6)



Solution: Cisco Guard at ISP

Cisco Guard is also deployed at Cisco ISPs around the world

Cisco Guard in Cisco POPs	Cisco Guard in Internet Cloud
Protects Cisco servers from DDoS attacks originating from computers connected to Cisco network	Protects Cisco servers and upstream bandwidth from large-scale DDoS attacks originating from locations outside the Cisco network

Results: Effective Mitigation of DDoS Attacks

- Using Cisco Guard, Cisco IT has successfully mitigated:
  - Large-scale DDoS attacks
  - SYN flood attacks
  - ICMP attacks
- Other successes with Cisco Guard include:
  - Ruling out a SYN flood attack
  - Providing insurance that a potential attack could not disrupt quarter-end activities
  - Preventing spamming of a customer Web site
  - Preventing a DNS attack

Next Steps: Clean Pipes Solution for ISPs

- Cisco is working with service providers to offer Cisco Guard solution to other enterprise customers
- Goal: to contain DDoS attacks at the ISP site so that the attacks do not affect the target company's Internet connection

To read the entire case study, or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT
www.cisco.com/go/ciscoit

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**