DEFCON 10
August 2002

Anatomy of Denial of Service Mitigation Testing

Version 3.0

Agenda

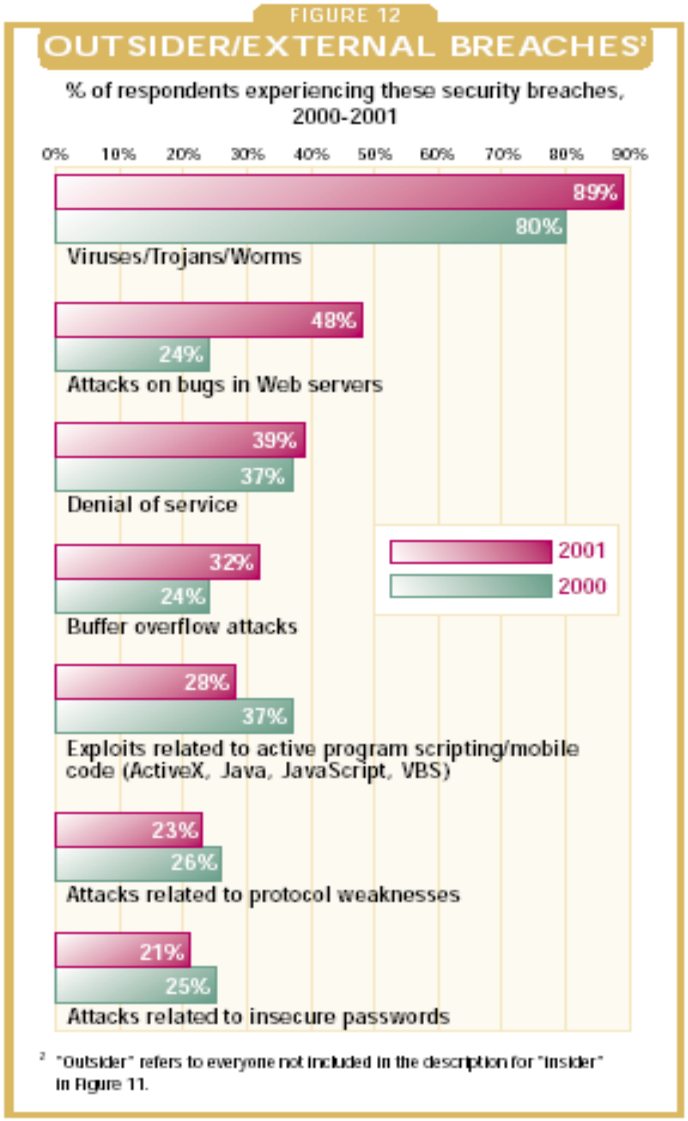
- **Why Test?**
- **Methodology**
- **Challenges and Lessons Learned**
- **Findings**

Denial of Service Mitigation Testing

WHY?

- Desire to Protect
  - Infrastructure
  - Data
  - Business Continuity
- Evaluate Emerging Technologies
- Problem is just getting worse
  - Many nasty DOS and DDOS tools in the wild

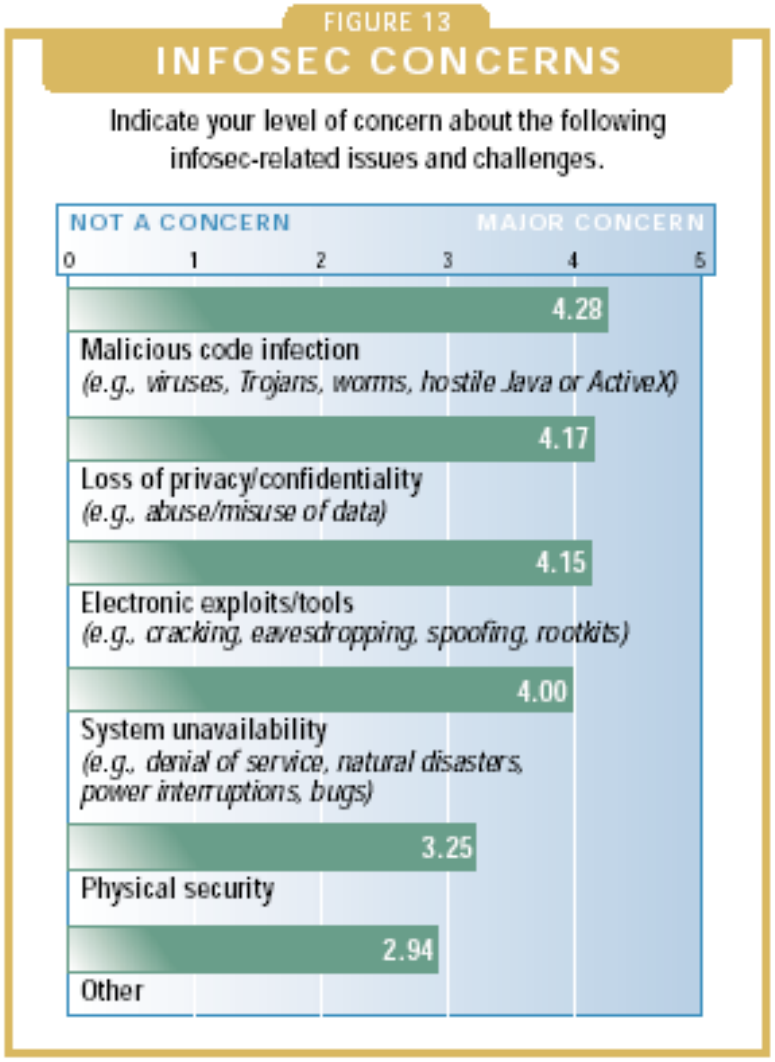
2001 Survey Results



Results of the 2001 Information Security Magazine Industry Survey shows increase in Denial of Service attacks experienced by the survey participants.

Source: Information Security Magazine, *2001 Industry Survey,* October 2001, pg 34-47.

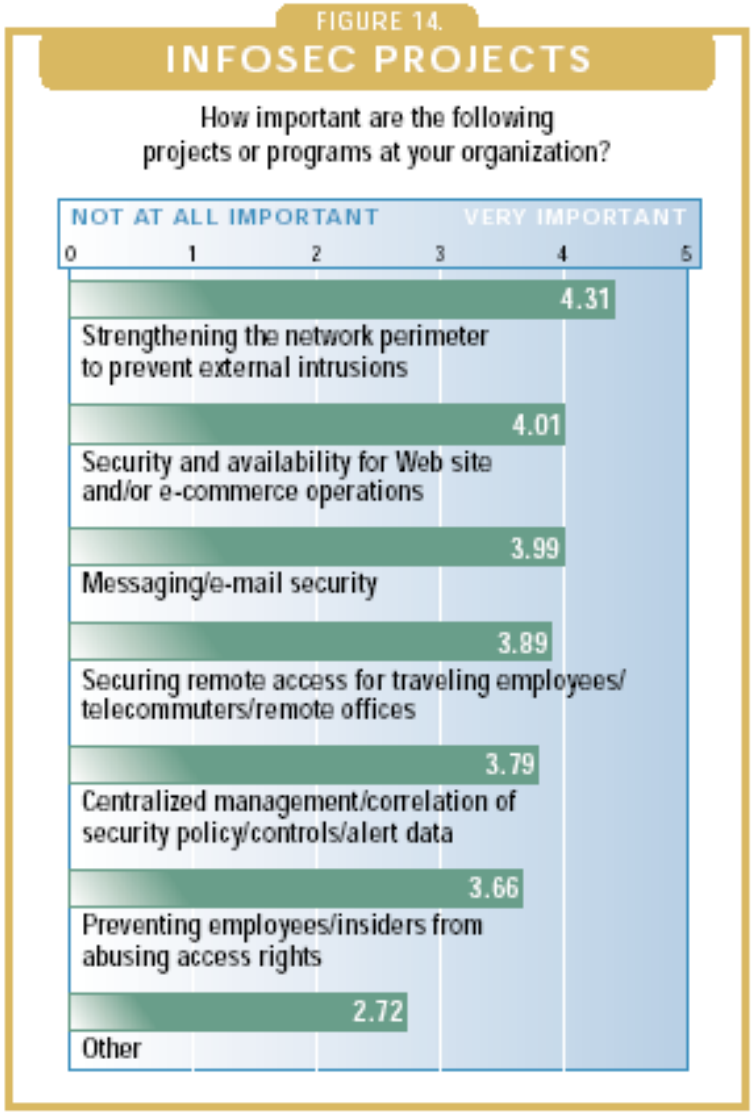
2001 Survey Results



- **System unavailability is 4th highest INFOSEC concern**

Source: Information Security Magazine, *2001 Industry Survey,* October 2001, pg 34-47.

2001 Survey Results



- **Security and Availability of Websites 2nd most important project listed**

Source: Information Security Magazine, *2001 Industry Survey,* October 2001, pg 34-47.

What We Were Looking For

- Infrastructure Protection
  - Minimum Gigabit Solutions (GigE and Fiber)
  - OC48 and OC192 capability desired
- Customer Protection
  - Gigabit MM Fiber
  - GigE
  - 10/100 Ethernet
  - Eventually OC48 and OC192

Products Tested

Passive "tapped" Solutions

- **Arbor Networks**
- **Reactive Networks**
- **Mazu Networks**
- **Asta Networks**

In-line Solutions

- **Captus Networks**
- **Mazu Networks**

- Basis of selection due to September 2001 Information Security Magazine Article, *Denying Denial-of-Service*.

Methodology

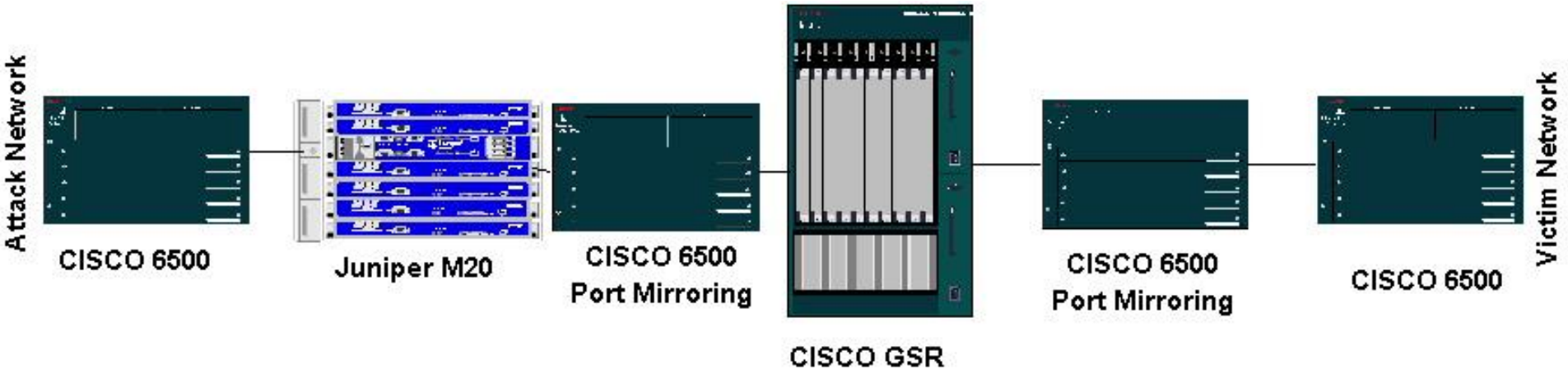
Today's DOS Prevention

- Reverse Path Filtering (deny invalid IPs)
- Allow only good traffic into your network (ingress filtering)
- Allow only good traffic out of your network (egress filtering)
- Stop directed broadcast traffic (to avoid being an amplifier)

Methodology

- Imitate a customer hosting center
- Run real tests across the infrastructure
- Test both network functionality and the management interfaces
- Find solutions that will work upstream instead of downstream

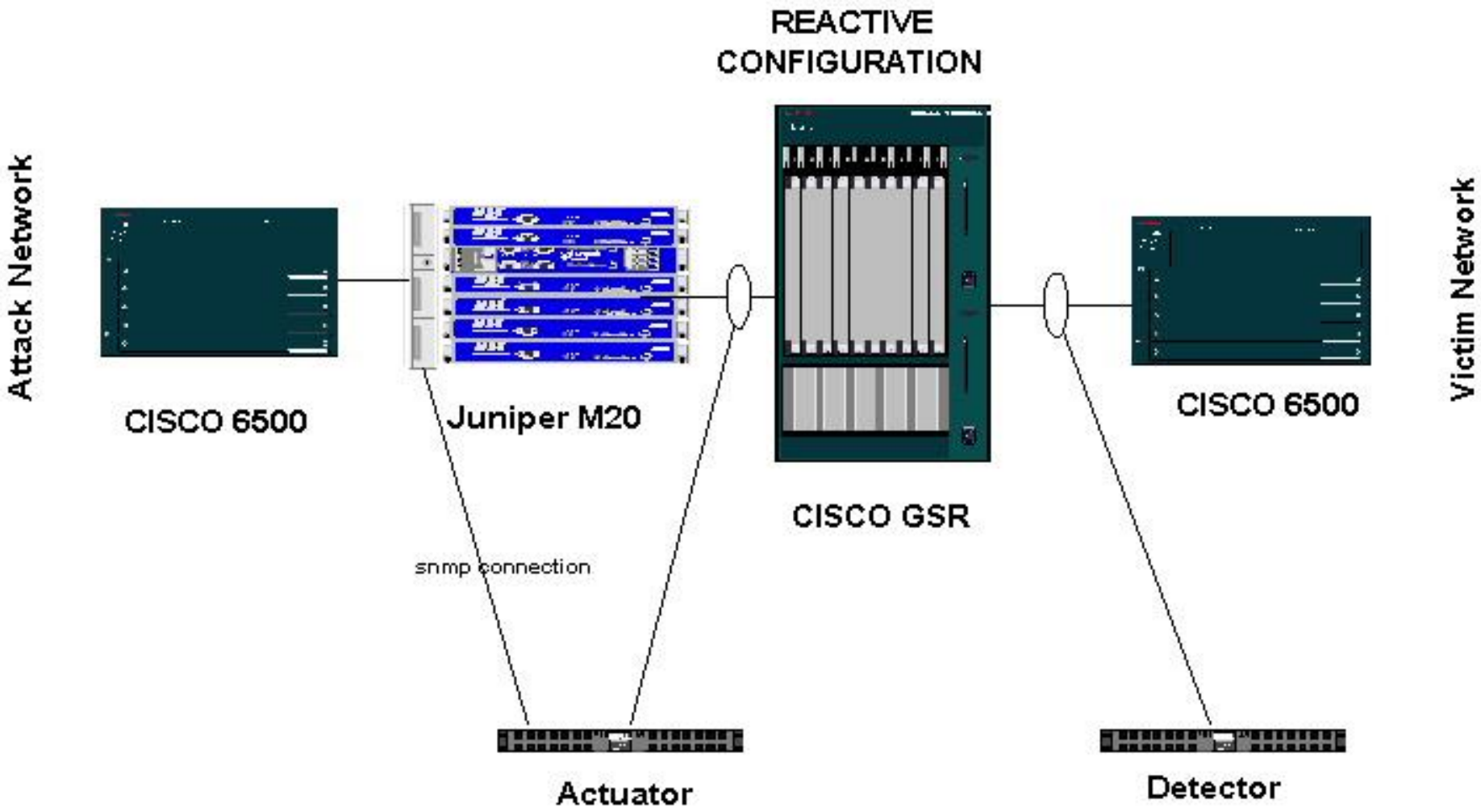
Test Environment Architecture



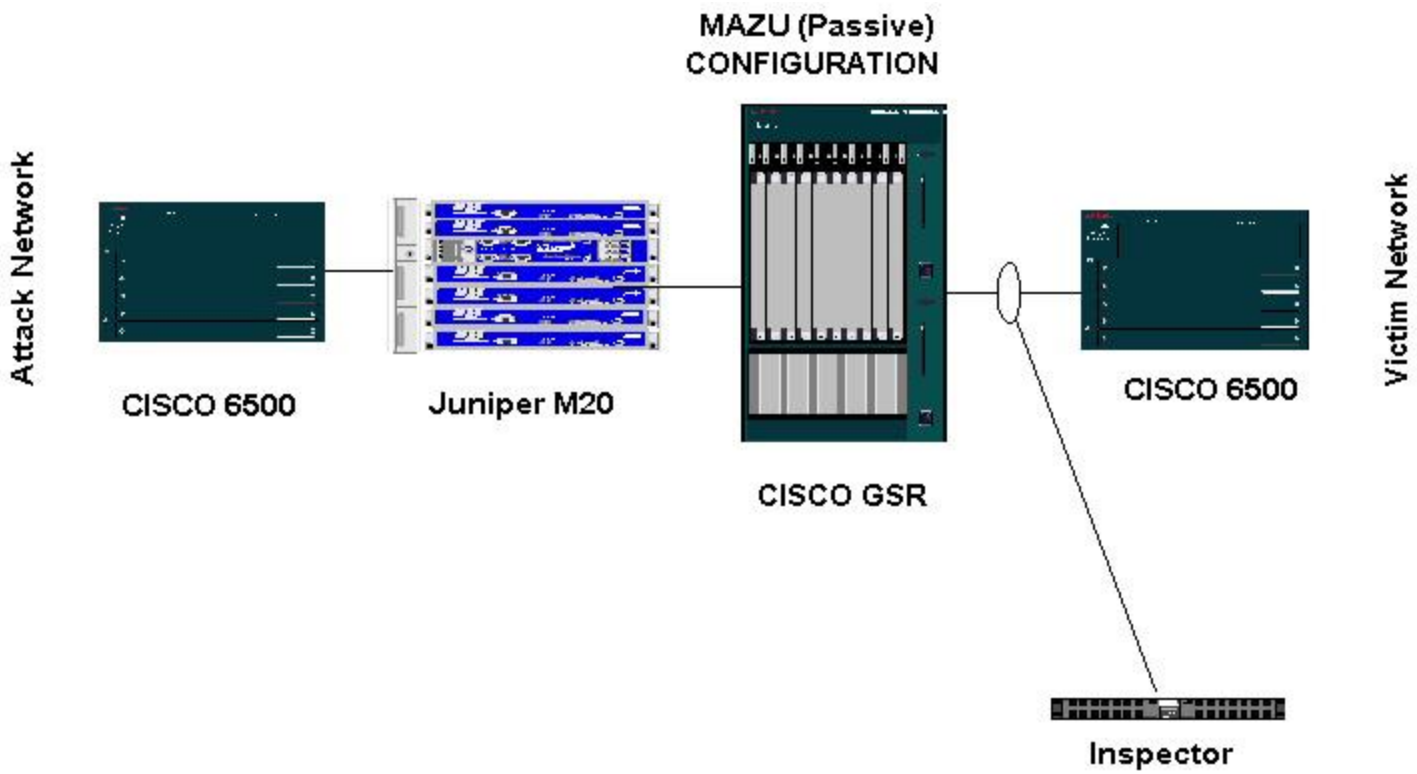
Passive “Tapped” Testing

- No network side IP address
- Data mirroring
- Not a single point of failure on the network
- Products recommend ACLs for the routers
  - Automatic
  - Semi-Automatic
  - Report only

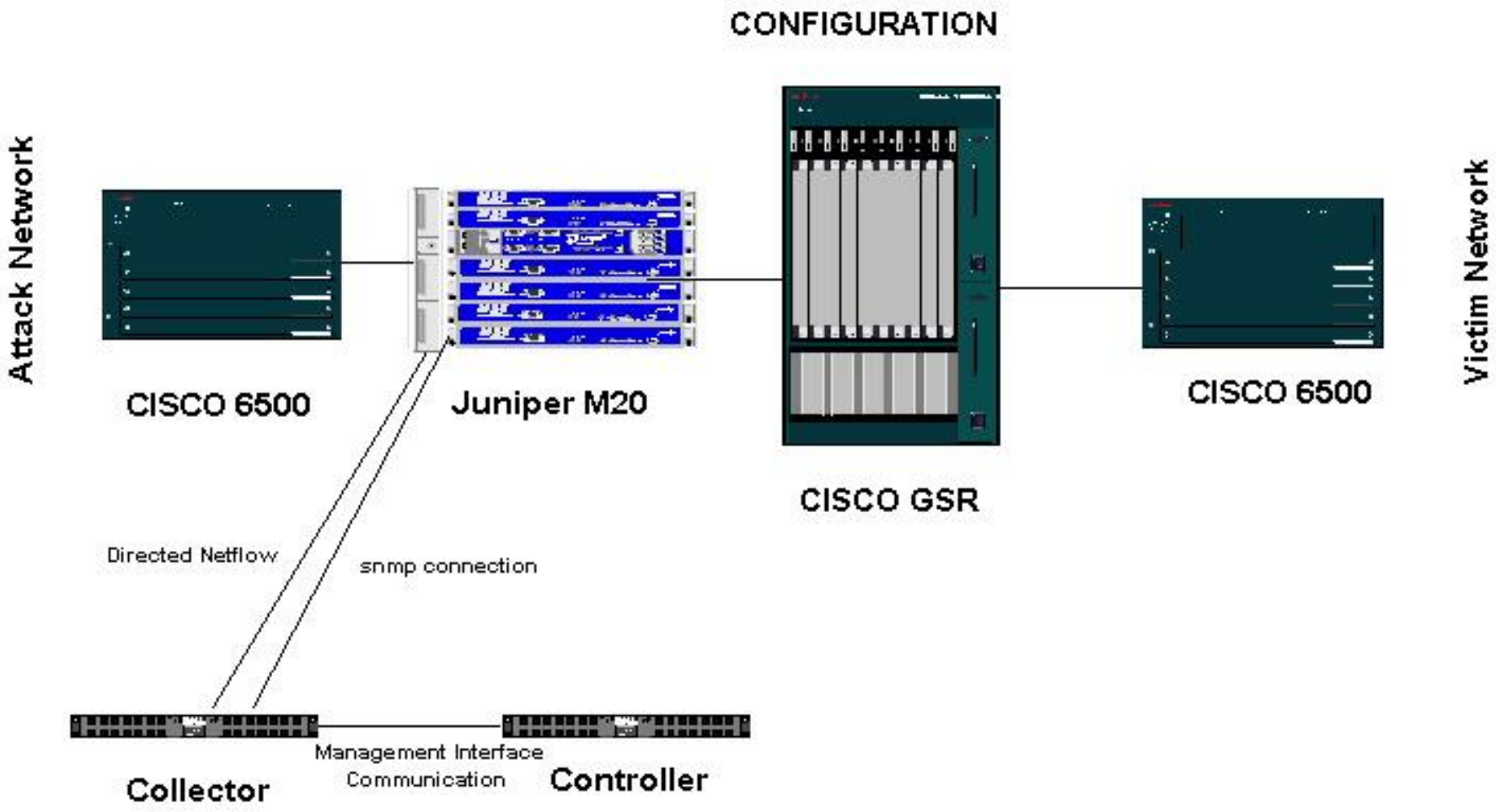
Reactive Network Solutions FloodGuard



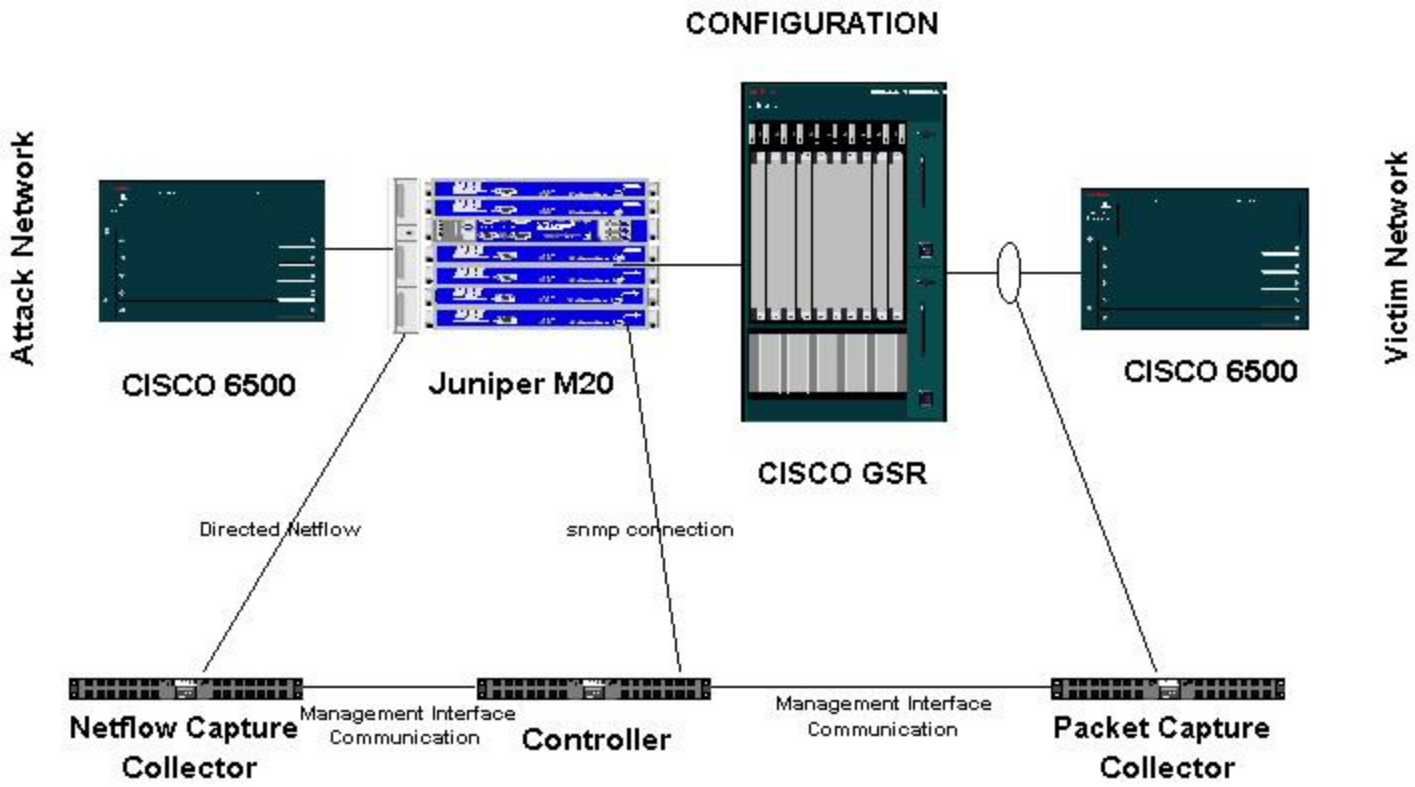
MAZU Networks TrafficMaster



Asta Networks Vantage



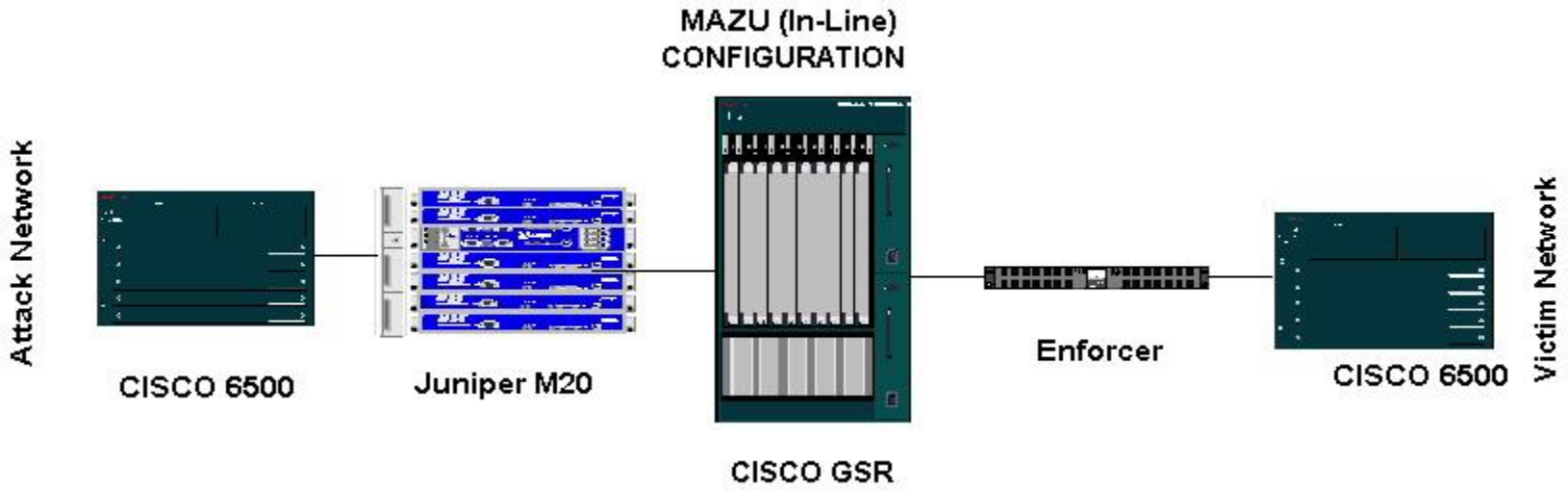
Arbor Networks PeakFlow



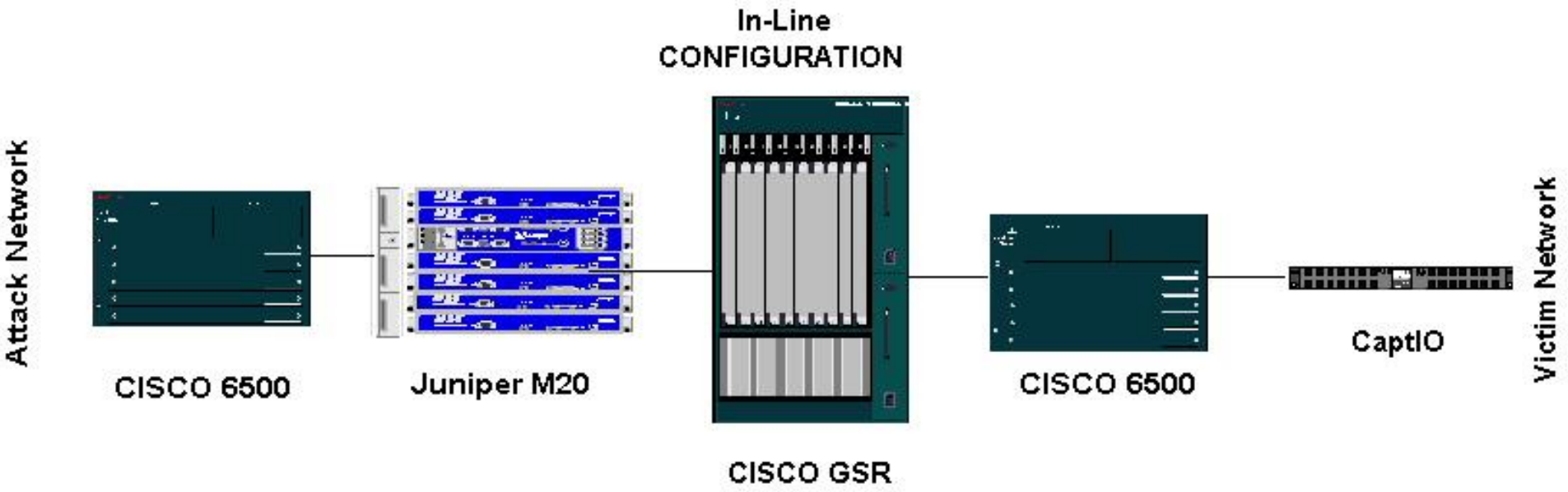
In-Line Testing

- Boxes placed in the data stream
- Quicker response to attacks based on implemented rules
- Interfaces visible on the network

Mazu Networks (inline)



Captus Networks



Types of Tests

- Baseline traffic generation to emulate a web hosting center
  - ldgen with replayed traffic
- Attack Traffic (DOS and DDOS)
  - TCP SYN
  - TCP ACK
  - UDP, ICMP, TCP floods
  - Fragmented Packets
  - IGMP flood
  - Spoofed and un-spoofed

Lesson Learned

Network

- **Baseline Traffic must be stateful (TCP 3-way handshake must be complete)**

Routes

- **Bad Routes will kill your network and make you unemployed**
  - **Thank God we were in the lab**
- **Be sure to isolate your management network from the attack network ON EVERY BOX**

Attack Network

- Different tools on different systems
  - Linux 6.2 and Linux 7.2
  - Open BSD
  - Solaris
- Mix of 10/100 and Gig Interfaces needed to push the traffic levels

Tools Utilized

- DOS/DDOS Tools
  - Vendor provided
    - Arbor TrafGen
  - Open source
    - stream
    - litestorm
    - rc8.o
    - f__kscript
    - slice3

Victim Network

- Monitoring Tools
  - Lebrea
  - Snort
- Manual Checks
  - Simple Pings
  - CPU usage monitoring

Flow Sampling

- Netflow/Cflowd from Cisco and Juniper
  - Sampling rates must match in both the router and the DDOS mitigation device
  - Juniper had more consistent flow characteristics and reported faster
  - Flow sampling has many value adds
    - Traffic characterization
    - Customer billing
    - And DOS/DDOS detection

SNMP Communications

- SNMP is used to monitor the status of the routers and providing alerts when an attack is underway.
- Connectivity is necessary for proper operation.
- SNMP community stream required for proper communications (NOT PUBLIC)

FINDINGS

What Vendors Did Well!

- Monitor baseline traffic
- Detect changes in traffic patterns away from baseline
- Alerting and Alarming when thresholds or statistics were exceeded

What wasn't so Good

- Protection of the management interfaces
- Implementing warning banners and account lockouts
- Port lockdown on the management interfaces

Solutions

Large Enterprise

- Passive Solutions best
- Mix of flow collectors and packet collectors that can visualize your entire network
- Centralize the management consoles into a security operations center of NOC
- Products:
  - Arbor
  - Asta
  - Reactive

Smaller Enterprise

- In-Line Solutions worth considering
- Combination firewall/DOS solutions
- Combination IDS/DOS solutions
  - Captus
  - Mazu
  - Recourse (not tested)

Resources

- www.sans.org/ddos_roadmap.htm
- www.sans.org/dosstep/index.htm
- www.nipc.gov
- staff.washington.edu/dittrich/misc/ddos
- www.cert.org

Conclusions

- Technology still evolving
- Integrated products likely the future (DOS combined with IDS or Firewall)
- Positive strides toward solutions

Questions ?

Greg Miles, Ph.D., CISSP

- **CIO – Security Horizon Inc.**
- **Information Technology – 15 Years**
- **Information Security – 11 Years**

- **e-mail:** gmiles@securityhorizon.com
- **Web:** www.securityhorizon.com