DDoS and Mitigation Solutions

Stas Khirman
CTO
KHIRMAN & SON
stas@khirman.com

CoolTech Club Meeting, June 30,2004

Agenda

- Intrduction
  - DDoS definition
- DDoS classification
- DDoS Examples
  - SMURF
  - SYN Flood
  - SQL Slammer
- Mitigation

Introduction

DDoS Definition

Denial of Service (DoS) attack is a malicious use of the Internet/Intranet connectivity to cripple the online service offered by victim site, network or institution.

DDoS Definition

- Denial of Service attacks attempt to negate service by
  - exhausting the resources at the victim side (such as network bandwidth, CPU, memory, etc.) ,
  - forcing victim equipment into non operational state
  - hijacking victim equipment/resources for malicious goals.
- Distributed Denial of Service (DDoS) attack is a special case of the DoS when multiple distributed network nodes (zombies) are used to multiply DoS effect.

DDoS classification

DDoS Classification

Classification by exploited vulnerability

1. **Resource exhausting (Flooding)**
    1. Bandwidth flooding
    2. TCP Resources exhausting (example: SYN Flood)
    3. Application Flood –malicious overuse of the application services (example:web “spider” script)
    4. System/Business Resources exhausting - overuse of the system back-end resources such as transaction server, data based, fileserver (example:high-number of malicious login requests, incomplete purchase transactions)
    5. Algorithmic Complexity Attacks

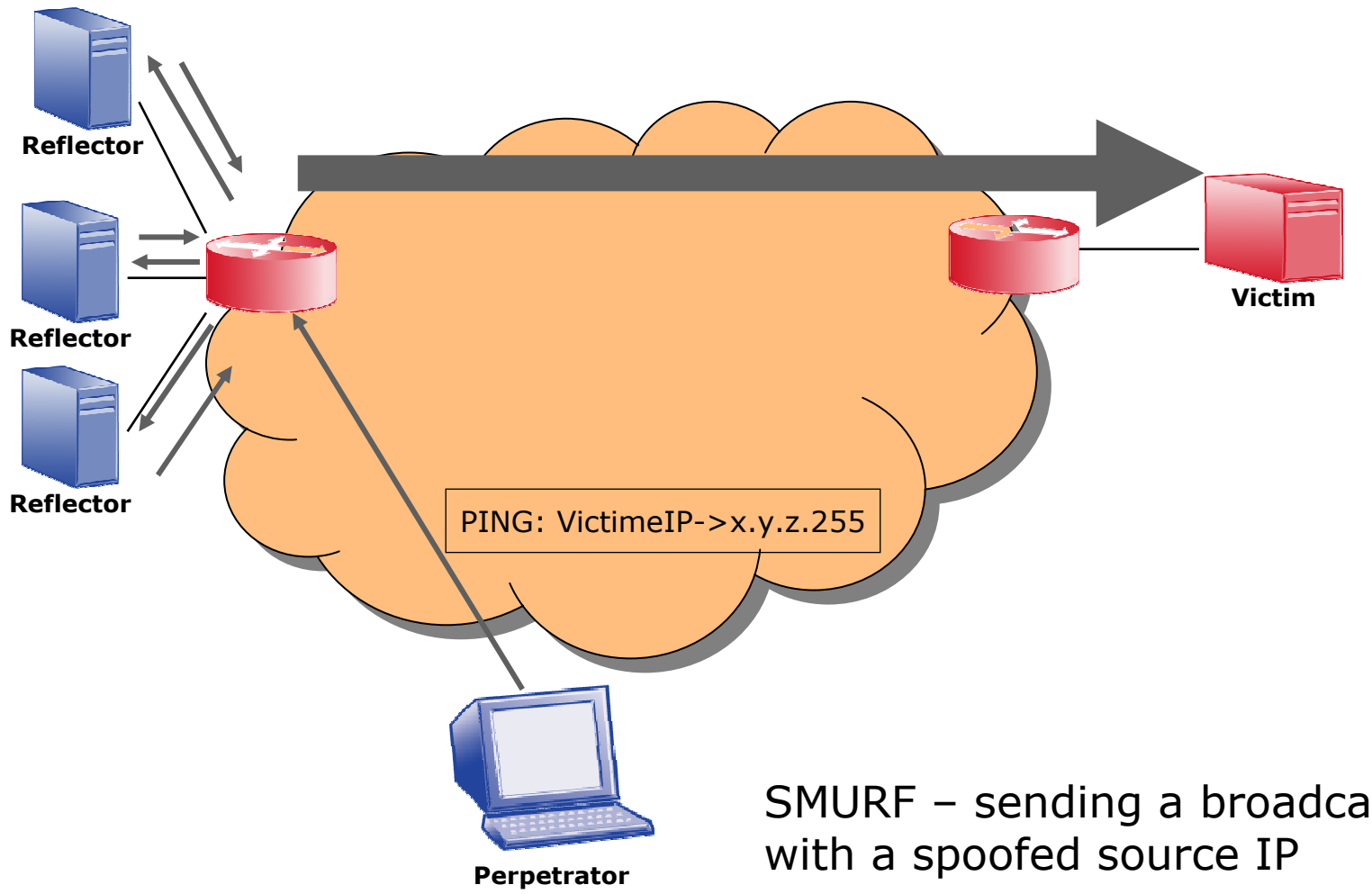
DDoS Classification

Classification by exploited vulnerability

2. Software Exploits
   1. Crash activation - sending specially crafted packet(s) to trigger of the OS kernel/software bug ("Ping of death")
   2. Stack overflow – injected code execution
   3. (intrusion) SQL Poisoning
   4. (intrusion) Cross-Site Scripting (XSS)
3. "Social Engineering"
   1. Server [miss-]configuration
   2. E-Mail Viruses ("Click to See a Nice Picture")
   3. Moderator/operator impersonation
   4. Identity theft

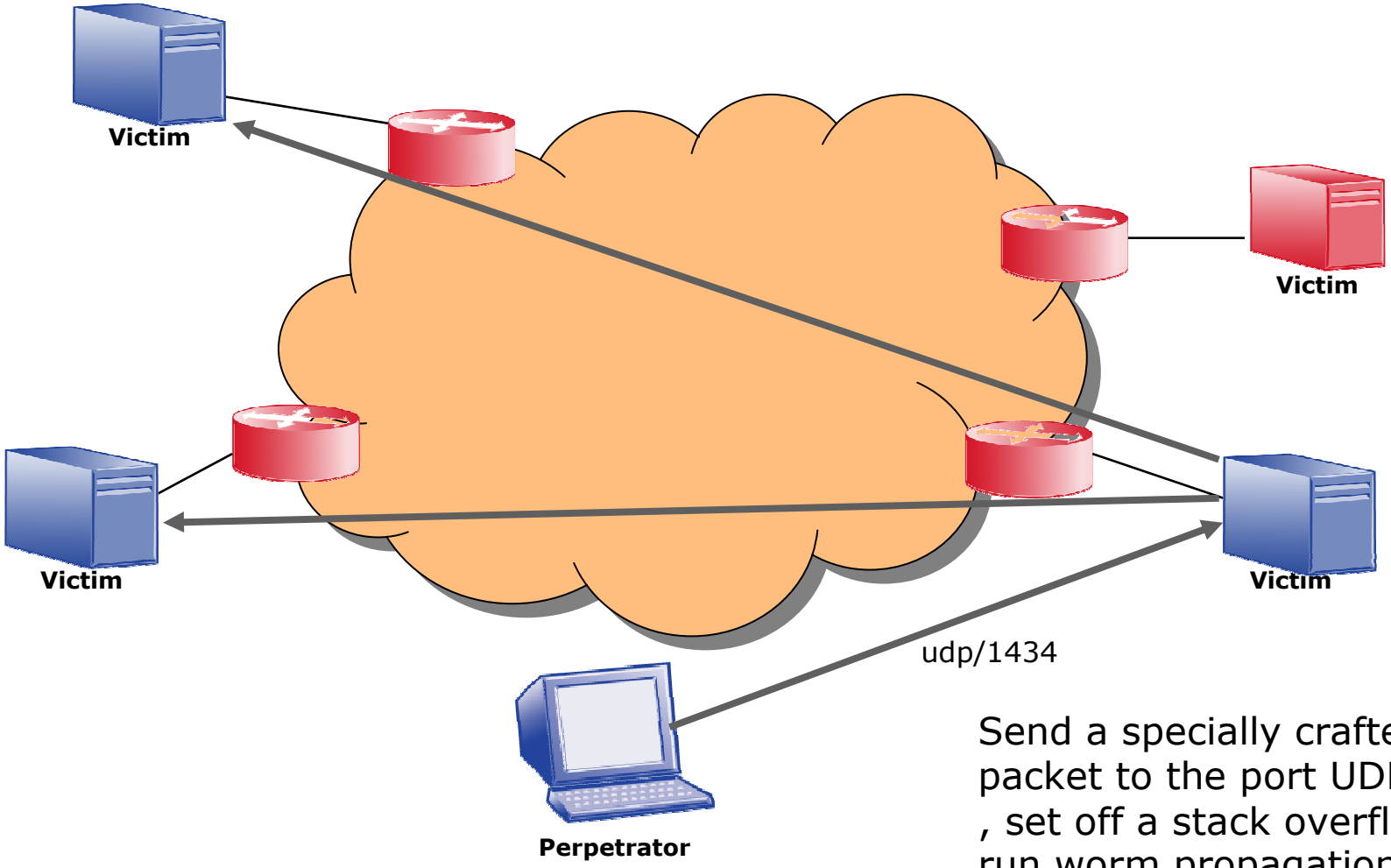
DDoS examples

DDoS Examples : SMURF



SMURF – sending a broadcast PING with a spoofed source IP

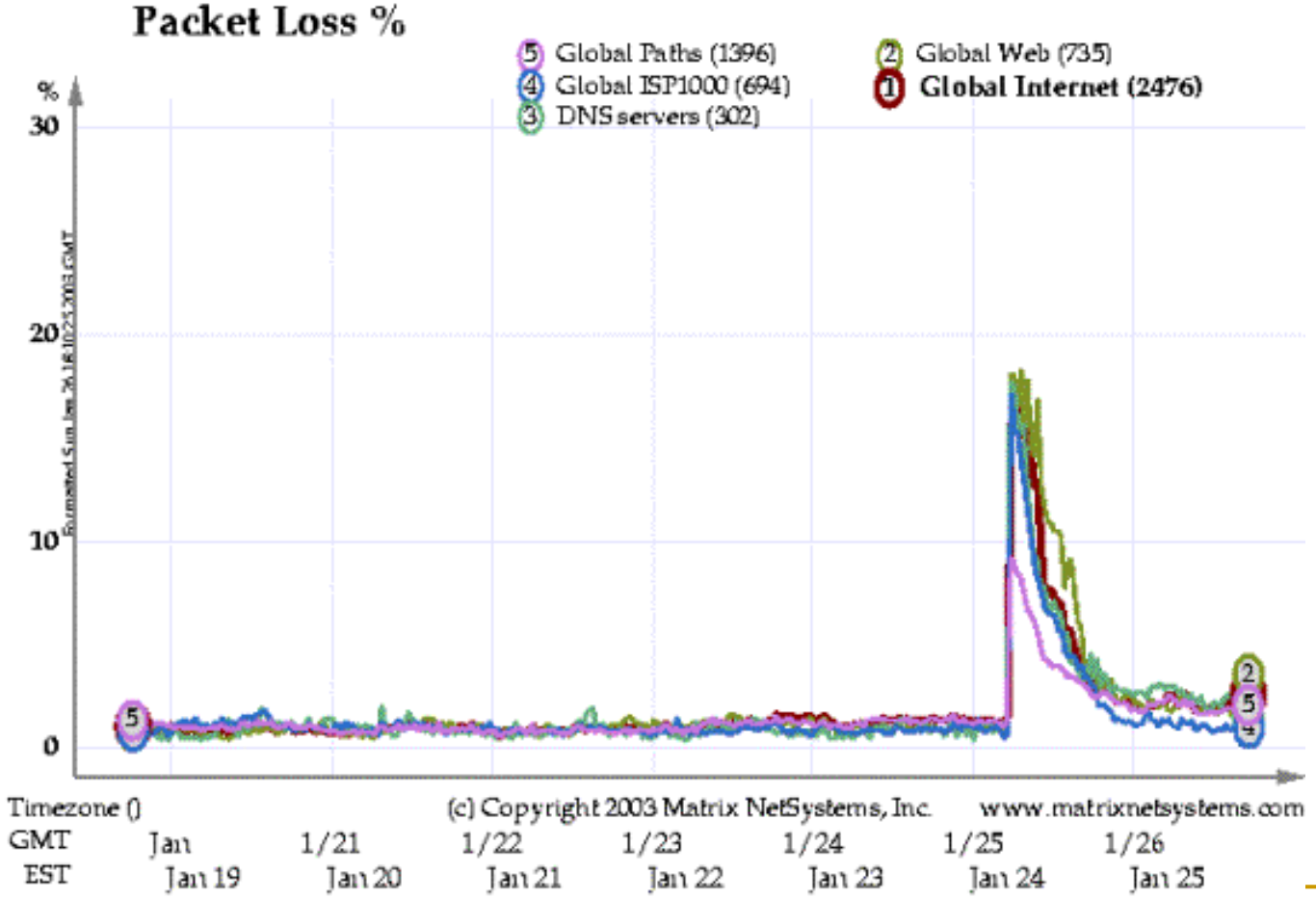
DDoS Examples : SQL Slammer



Send a specially crafted packet to the port UDP/1434 , set off a stack overflow, run worm propagation code.

SQL Slammer : Postmortem analysis

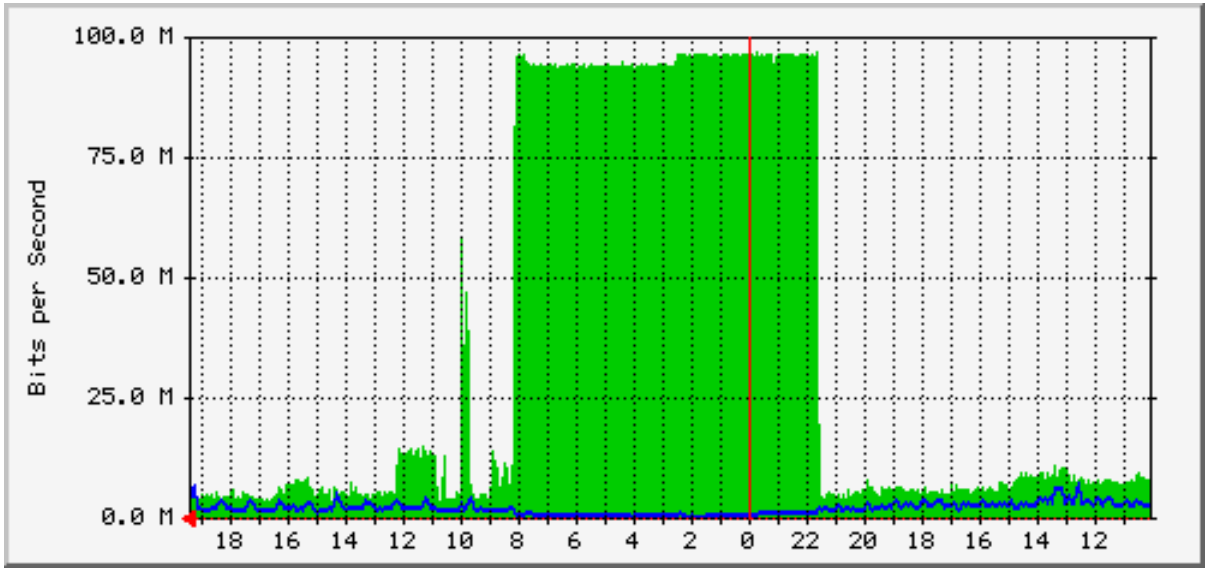
A single machine with the right Internet connection can scan the entire Internet in 12 hours for SQL Slammer vulnerabilities.



From www.robertgraham.com

SQL Slammer : Postmortem analysis

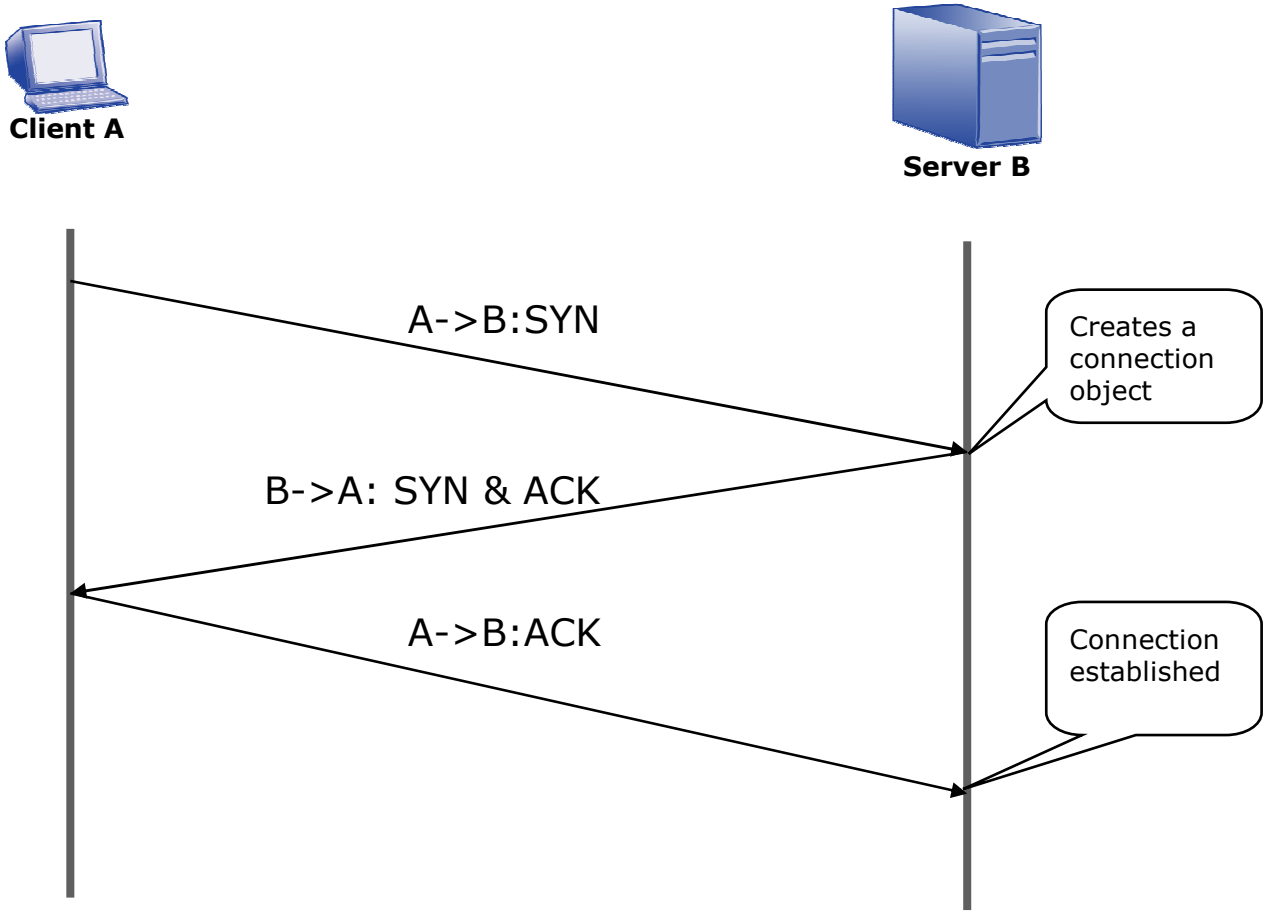
- For individuals, it was binary, a square-wave
- This graphs shows a single machine behind a 100-mbps Ethernet link.



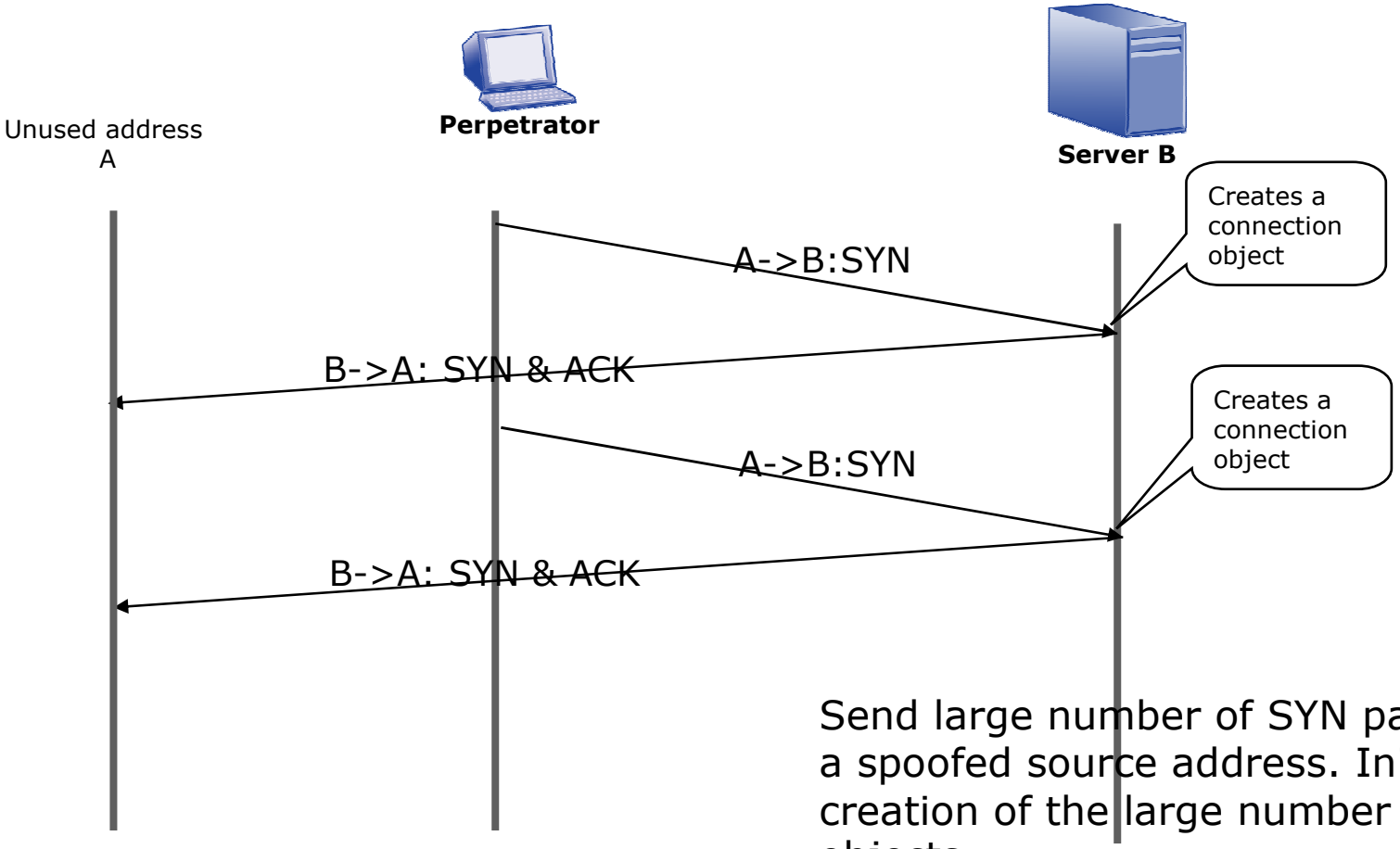
From www.robertgraham.com

DDoS Examples : SYN Flood

Normal TCP connection establishment



DDoS Examples
SYN Flood



Send large number of SYN packets with a spoofed source address. Initiate creation of the large number connection objects.

More DoS attacks

Ping of death	ICMP	ICMP packet with a size over 65536
ARP redirect	ARP	Local IP address highjack , middleman attack
Land	TCP SYN	Source and destination IP addresses are the same causing the response to loop.
SQL/application server attack	HTTP	Continuous requests for a heavy computational dynamic page

Mitigation Techniques

ACL – Access Control List

Layer 4 filtration rules:
<protocol,srcIP,dstIP,srcPort,dstPort>

SQL Slammer prevention ACL:

access-list 101 deny udp any any eq 1434

access-list 101 permit ip any any

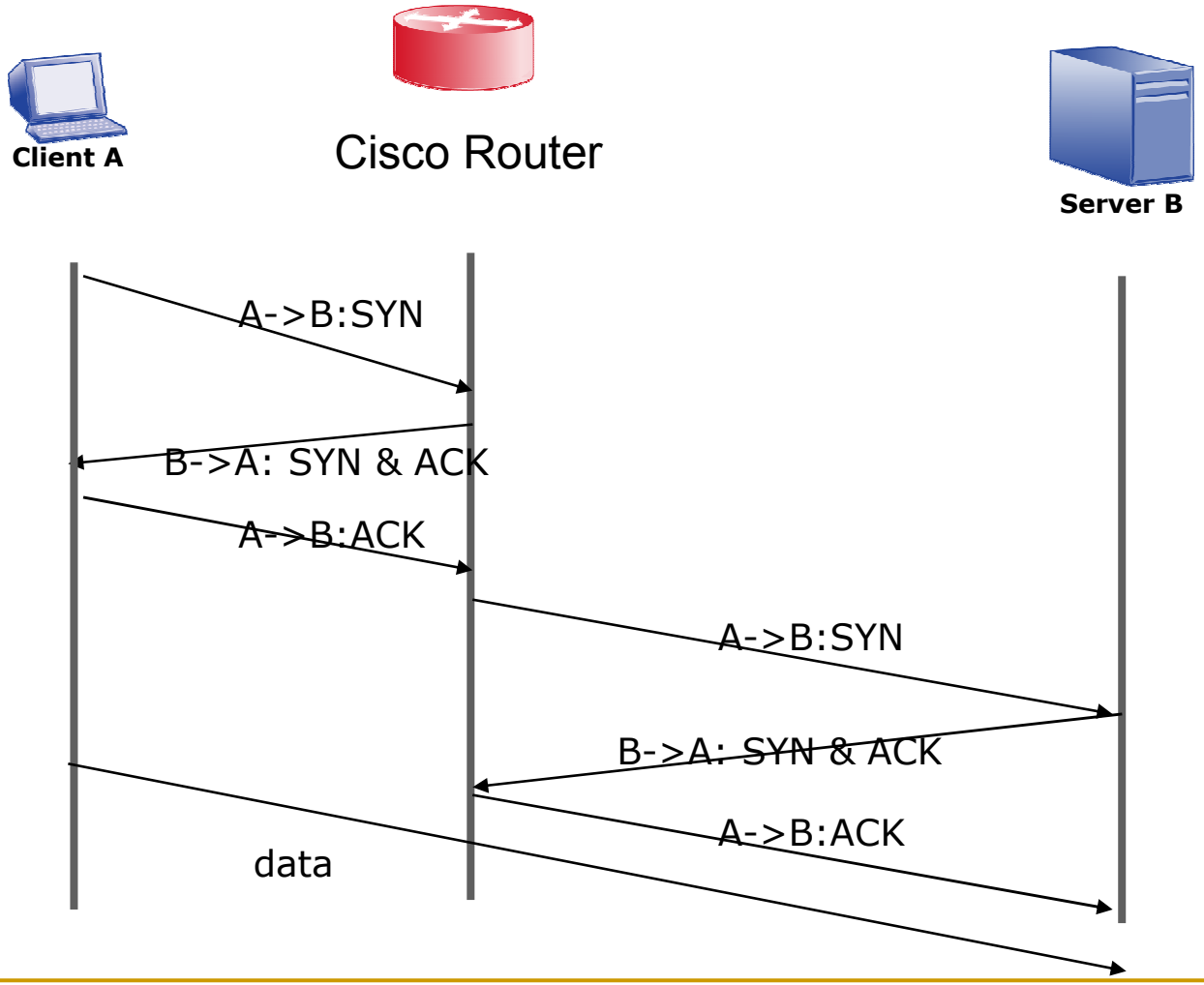
Rate Limitation

- Traffic Shaping :
  - X B/sec for udp: 1434
  - Y packets/sec fro ICMP PING
- Layer 4 rules
- Cisco CAR (Committed Access Rate)

TCP Intercept

- Cisco specific
- Intercept Mode
- Monitor Mode

Cisco TCP Intercept – Intercept mode

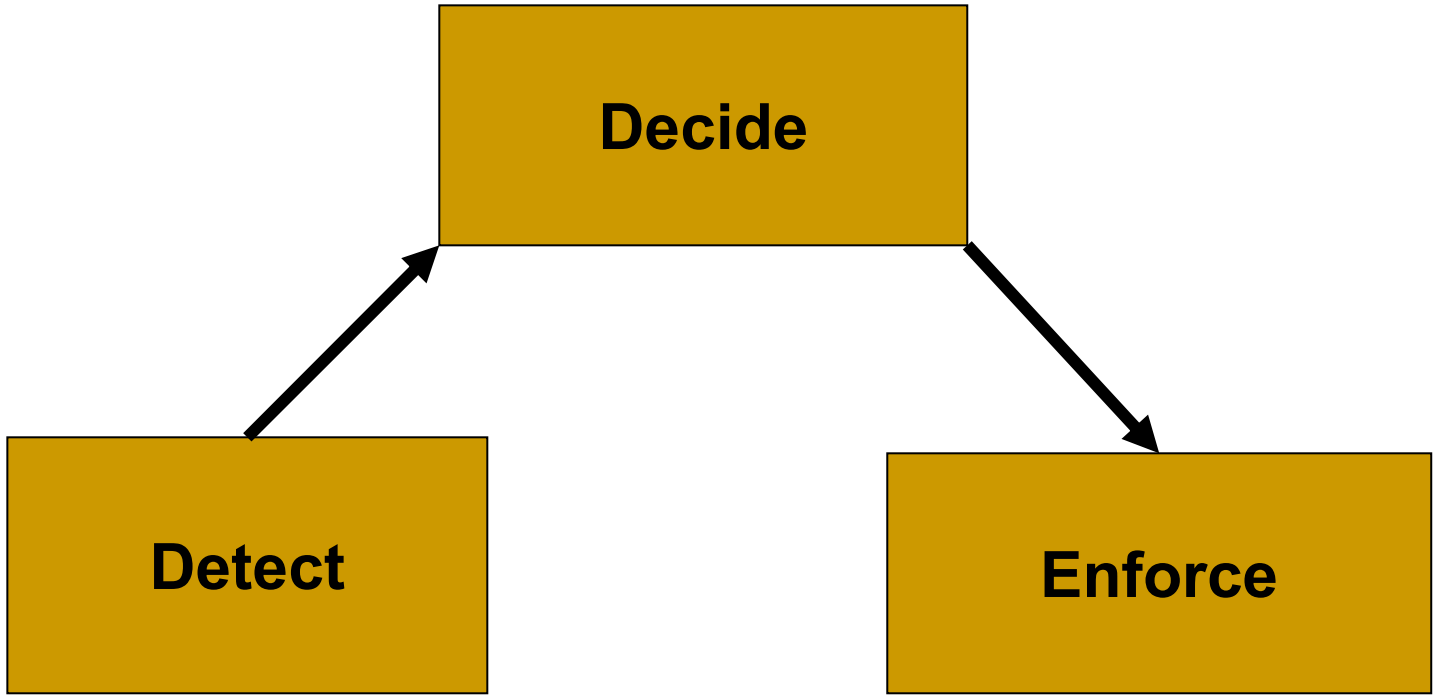


Price of Mitigation

- Excessive ACL – self inflicted DoS
- Excessive Rate Limitation:
  - Self inflicted DoS
  - CPU utilization
- TCP Intercept
  - Memory utilization
  - CPU utilization

Dynamic Mitigation

Solution ??



Conclusions

- Q & A