IPS test

Author: Aco Dmitrović

Hrvatski geološki institut – Croatian Geological Survey
Aco.Dmitrovic@hgi-cgs.hr

Protective devices

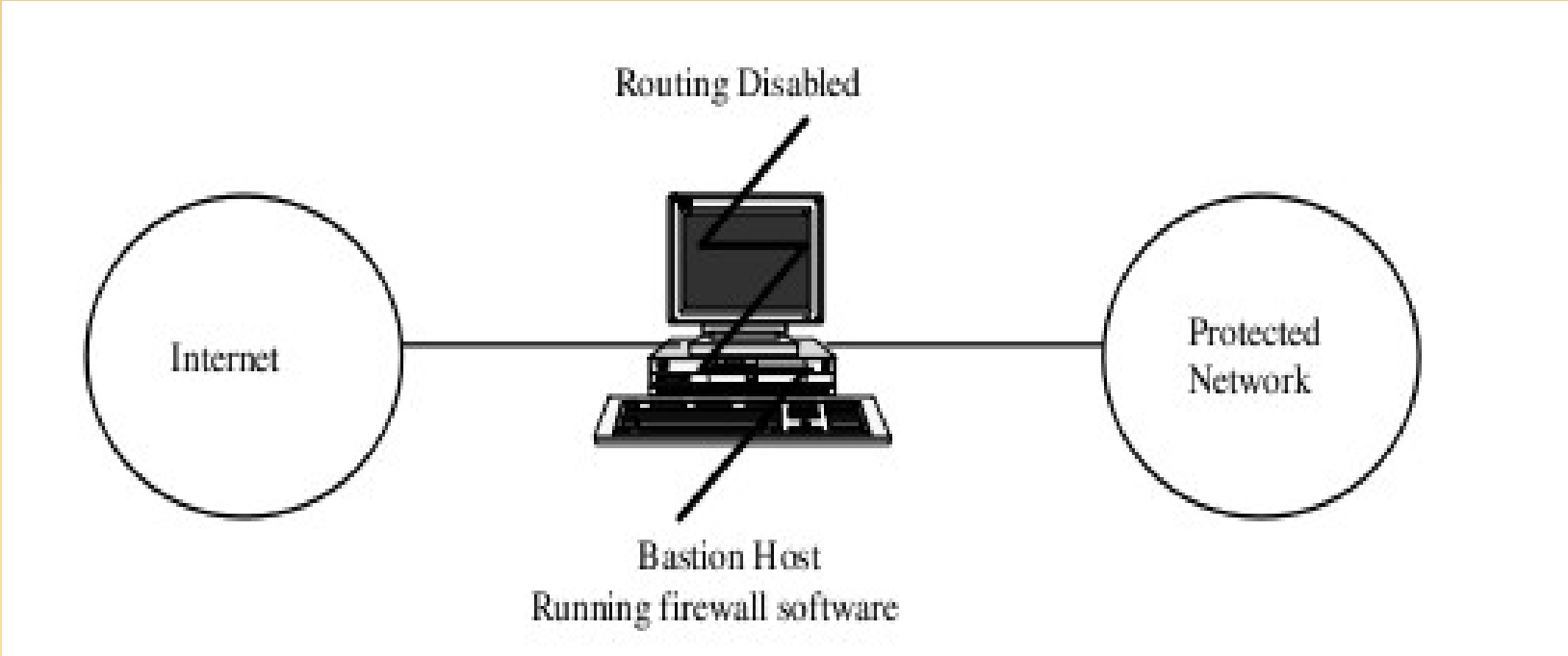
- Firewall
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System
- VPN – Virtual Private Network
- Mail gateway – AV & antispam filter
- Web filtering, Content filtering
- New buzzwords: UTM, Next generation firewall

History of firewalls

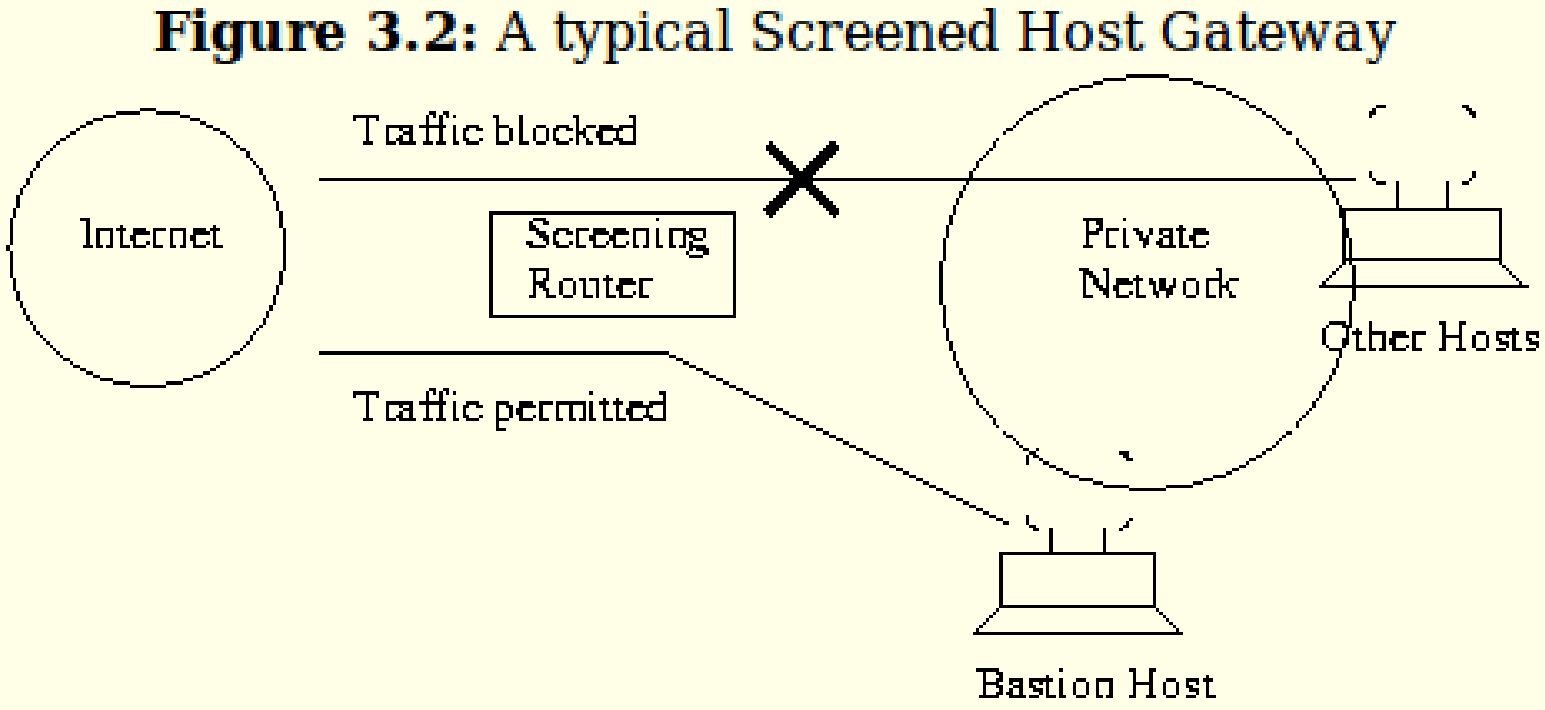
- Dual homed gateway
- Screened host gateway
- Screened subnet gateway

- Bastion host
  - Application forwarder
  - Traffic loger
  - Service provider

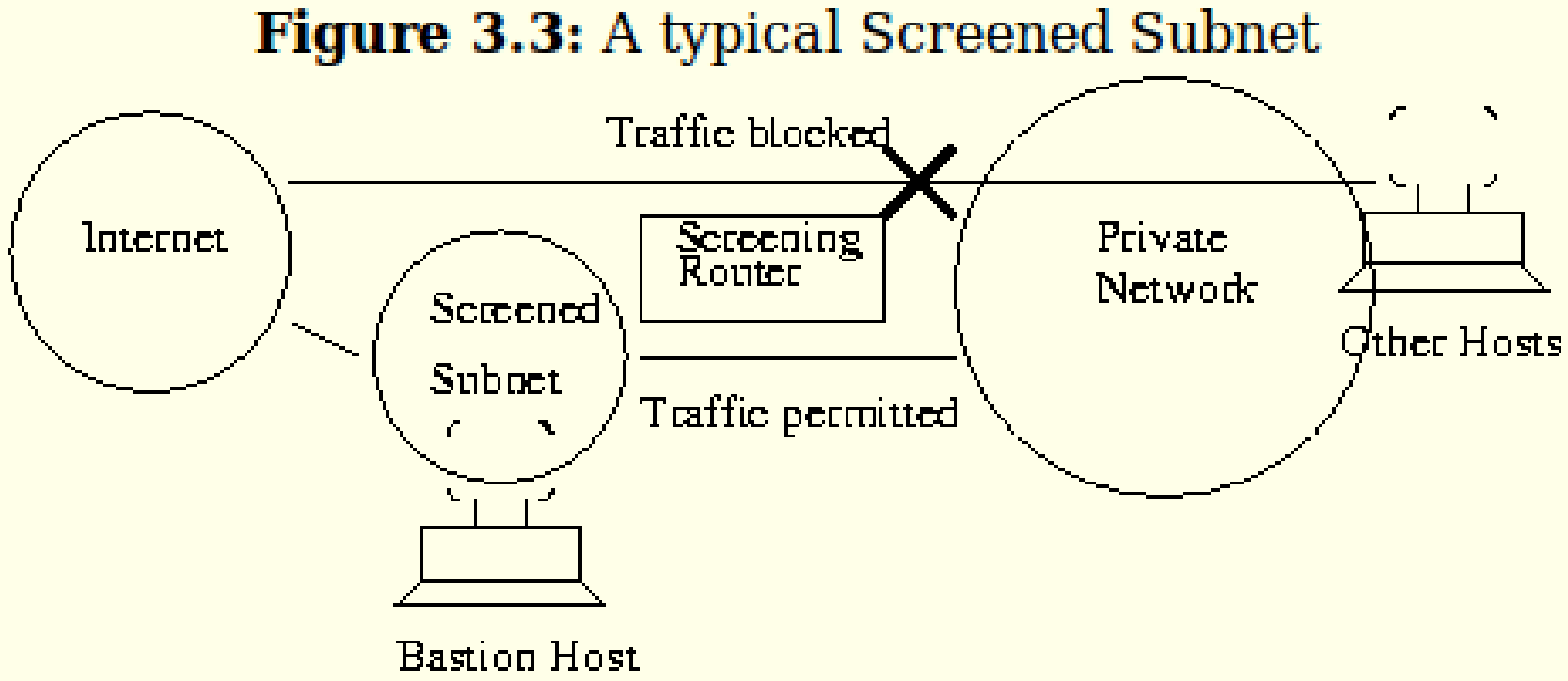
Dual-homed gateway



Screened Host Gateway



Screened subnet



IDS

- NIDS & HIDS
- Signature recognition
- Statistical anomalies
- SNORT – open source IDS
  - Martin Roesch, Source Fire
- Seminar: Otkrivanje upada, 2004.
  - IDS, not IPS, but you can activate automatic reply

Signature

- Header inspection
- Pattern-matching
  - Atomic – single packet
  - Stateful – stream
- Protocol based
- Heuristic – statistical analysis
- Searching for anomalies

Traffic

- Known ”good traffic”
  - Trusted, allowed to pass
- Known ”bad traffic”
  - Should be stopped before damage occures
- ”Ugly” traffic
  - Deep packet inspection before decision

Botnets

- 5000 – 6000 CnC (*Command & control sites*) daily on Internet
- They control army of robots, compromised computers
- Quickly replaced with new ones
- Communicate using IRC, IM, P2P, HTTP
  - Open ports on firewalls
- Dinamic algorithms for discovering CnC

Malvare depots

- ~ 50.000 computers daily spred malware
  - *Sophos Security Threat report 2010*
  - Malicious web pages using vulnerabities in browsers, flash players, PDF readers...
  - Compromised legitimate servers

Phishing

- 50.000 new phishing sites monthly
  - *Antiphishing workgroup, Trends report Q3-2009*
- Pages that look like legitimate site
- Steal usernames, passwords, accounts, personal data...

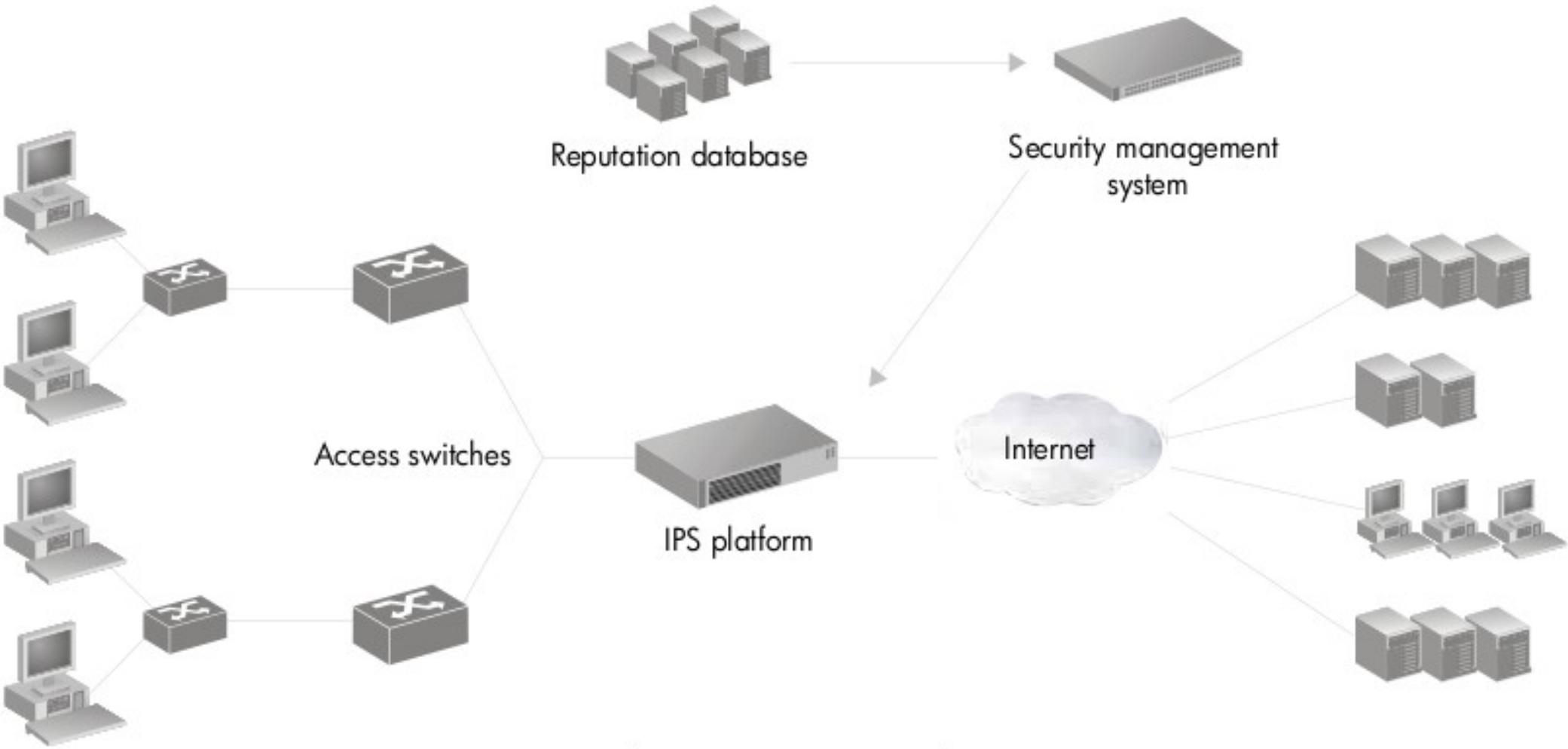
Compromised PC

- Millions of hacked computers daily
- Waiting in company networks, universities, homes
- Ruled by bot master using CnC
  - Spread malware
  - Attack other computers
  - Scan netwoks (*reconnaisance*)
  - DDoS
  - Send spam, phishing mails

Device reputation

- Dinamic database - adresses of computers with bad reputation
- Traffic analysis
- Network of IPS computers collect and share data

TippingPoint Reputation Digital Vaccine Service



Block outbound traffic to prevent

- Botnet Trojan downloads
- Malware, spyware, and worm downloads
- Access to botnet CnC sites
- Access to phishing sites

Block inbound traffic to prevent

- Spam and phishing emails
- DDoS attacks from botnet hosts
- Web application attacks from botnet hosts

8 questions

- Is your IPS in-band?
- Does your IPS support max network and application availability?
- Deep inspection of traffic without slowing down network or applications?
- Does it protect perimeter and key points?
- Broad and deep attack coverage?
- How accurate is it?
- How timely and up to date is attack coverage?
- References

1. Is IPS in-band?

- Not on mirror port
- Real time analysis of traffic
- IDS – network device with security funtionality
- High throughput and availabity
- High safety
  - Many filters
  - Precise filters
  - Quick reaction to new attacks

2. Availability

- Redundant power supply
- In case of failure device should not block traffic

3. Deep inspection

- Without slowing down traffic
  - Throughput - from 10 Mb to 10 Gb
  - Latency
- Must work like switch with added functionality

4. Perimeter protection

- Not sufficient any more
- Protect all critical resources, in public or private network, as well as clients
- Attacks come from inside too
- IPS with mulitiple ports
  - Different filtering rules for DMZ, internal servers, user computers etc.

5. Wide and deep defense

- Bloking worms, viruses, DoS/DDoS, P2P, spyware, phishing, cross site scripting, SQL injection, PHP file include, VoIP...
- Vulnerable OS-es, aplications...
- Dozens of exploits for one vulnerability
- Attackers study IPS, learn how to bypass it
- Virtual software patching

6. Accurate

- Does your IPS stops bad traffic, and lets good one pass?
- False pozitive
  - Blocking good traffic
- False negative
  - Passing bad traffic

7. 0day

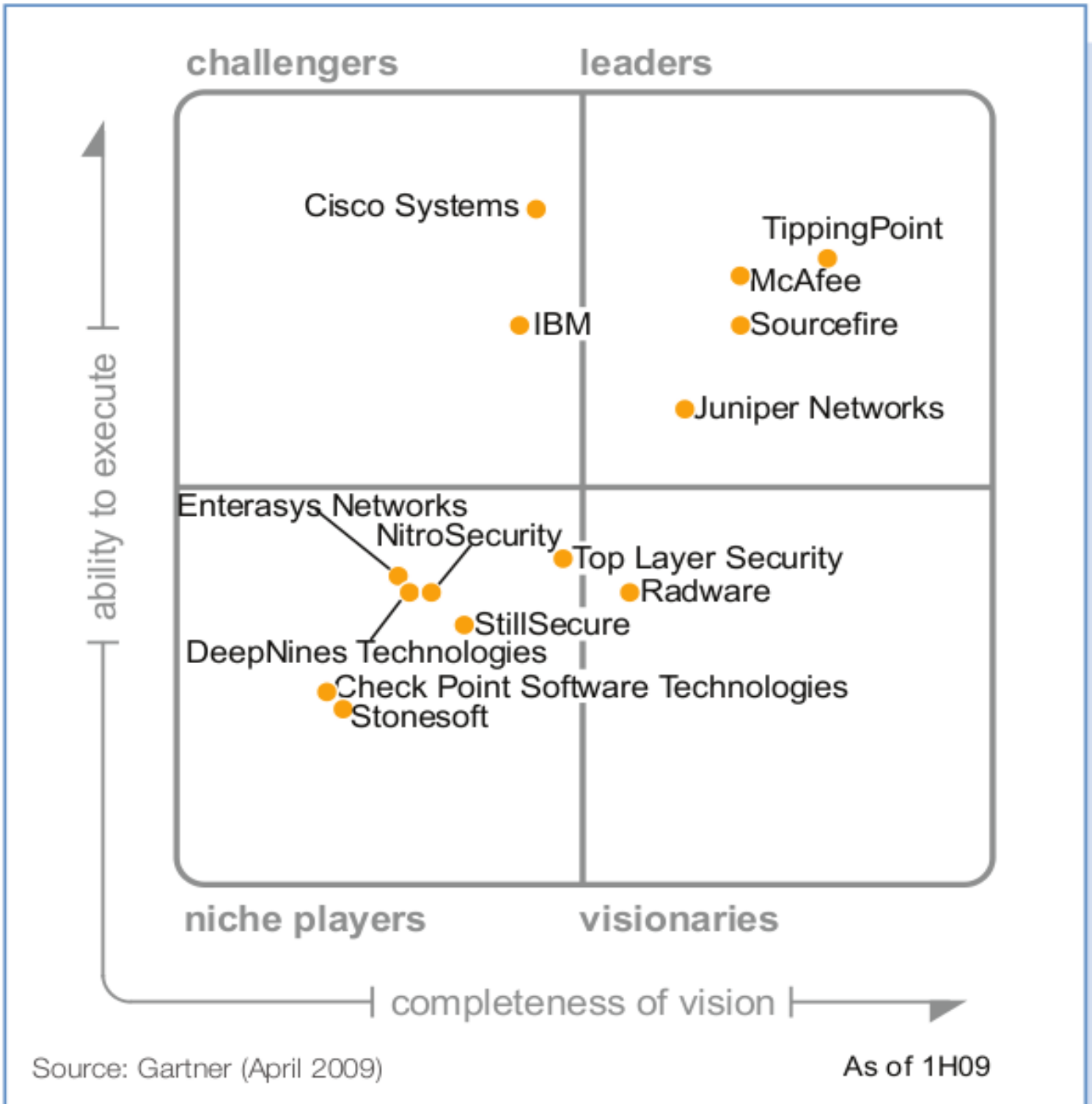
- Can IPS detect Zero day attacks?

- R&D with large team of experts?
  - DVLabs – delivers filters 52 days before Microsoft releases pathches
  - ISS – discovers allmost 50% of vulnerabilities
    - Half of them are never pathched
  - Snort – large base of volunteers

8. References

- Ask for evidence
- Consult existing users
- Check number of active filters

Figure 1. Magic Quadrant for Network Intrusion Prevention System Appliances



Source: Gartner (April 2009)

As of 1H09

Tested IPS appliances

- IBM/ISS Proventia
  - MX 1004
- HP/Tipping Point
  - 210E
- SourceFire
  - 3D2500.

Test

- Devices tested in production, not in lab
  - Inline & mirror port
- NSS Labs - real lab tests
  - http://www.nsslabs.com/research/network-security/network-ips/

IBM/ISS Proventia

- Multifunctional device
  - NAT
  - AV (Sophos)
  - Web filtering
    - p0rn, erotics, violence...
  - Firewall
  - IPS
  - VPN
- Single device connects and protects remote office

Hard start

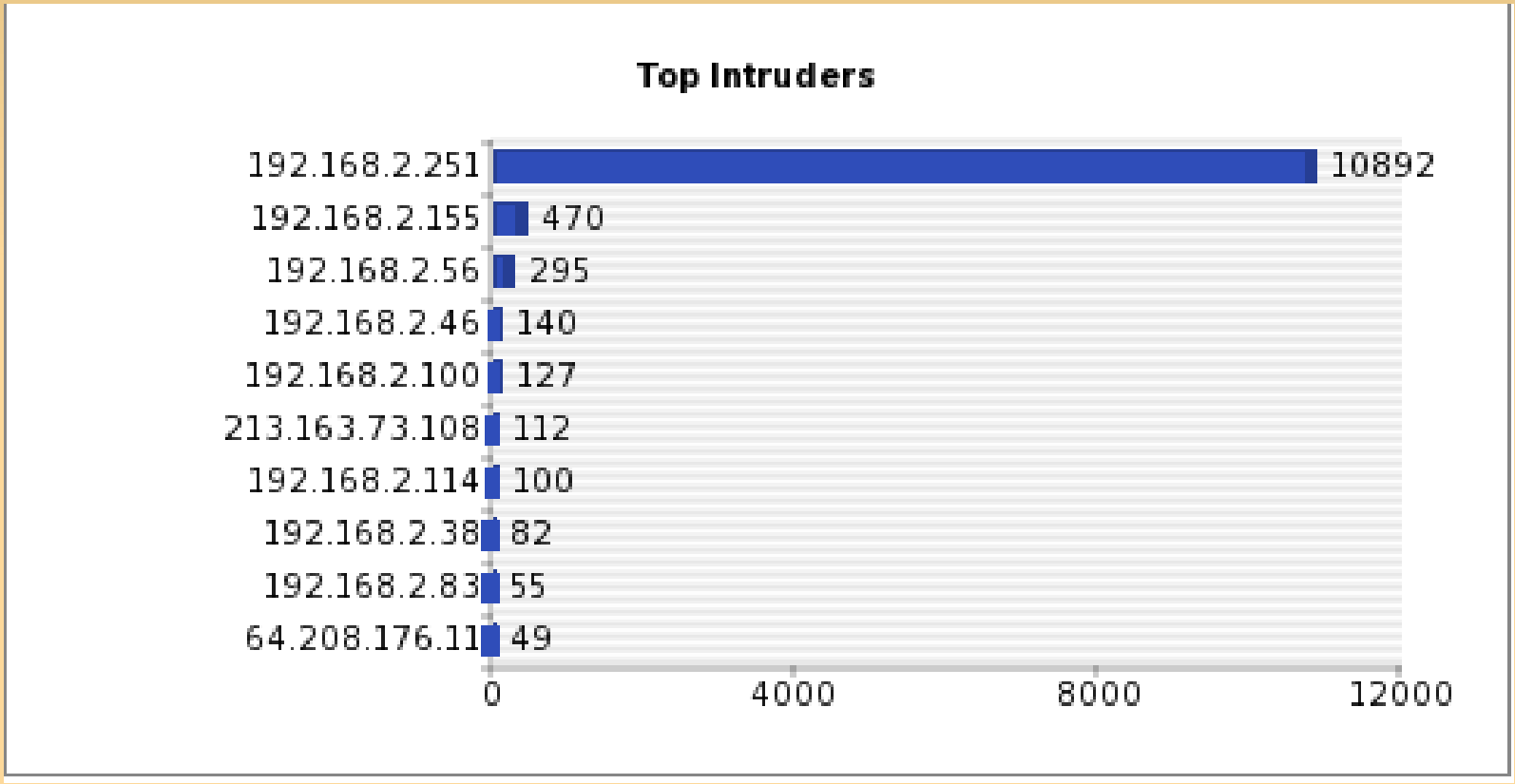
- Default policy – everything is forbiden
- Add rules to allow standard services
- Admin must have a lots of knowledge and experience

Blocked NTP, IMAP

- Must read logs:

- Dec 15 07:15:50 isa.igi.local igateway: id=firewall time="2009-12-15 07:15:39" fw=Firewall pri=4 proto=17(udp) **src=192.168.2.17:123 dst=88.159.82.127:123** mid=2076 mtp=10 msg="Access **Policy not found, dropping packet** from corp n/w" agent=Firewall
- Dec 15 10:09:48 isa.igi.local iss-ipm[962]: Packet dropped: Blocked TCP connection: time=1260868176, src-ip=192.168.2.251, dst-ip=161.53.85.3, ipprotocol=TCP(6),src-port=33349,**dst-port=143**

Dashboard


Top Intruders
192.168.2.251
10892
192.168.2.155
470
192.168.2.56
295
192.168.2.46
140
192.168.2.100
127
213.163.73.108
112
192.168.2.114
100
192.168.2.38
82
192.168.2.83
55
64.208.176.11
49
0
4000
8000
12000

Drag & drop e-mail

```
Dec 15 10:10:52 isa.igi.local iss-ipm[962]:
Event:issueid=2110082,name=IMAP_Tag_Overflow,
type=attack,protocol=imap4,user-defined=false,
count=1,priority=high,time=1260868180,blocked=true,
ether-type=IP(0x0800), src-ip=192.168.2.251,
dst-ip=161.53.85.3,intruder-ip=192.168.2.251,
victim-ip=161.53.85.3,ip-protocol=TCP(6),
src-port=50556,dst-port=143, intruder-port=50556,
victim-port=143,event-info:tag=
\xc2\xb7\xc3\x87\xc3\xbe\xc2\xb0.\x7f\xc3\xb3^\xc3\x9f
.\xc3\x9d\xc2\xa8\xc2\xbf*o.\xc2\xb3.#\xc2\x93@\xc2\xa
a\xc3\x81b.\xc2\xbd\xc3\x8b\xc3\x85\xc3\x9f\xc3\x9a.\x
c3\x9f~\xc2\x84\xc2\x86\xc3\x99\xc3\x8e\xc2\x81.T\xc2\
x85\xc2\xaayw\xc2\x84\xc3\xa0}\xc3\xb1\x7f\xc2\x8d\xc3
\xb9b\xc2\xbd\xc3\xa0\xc2\xabp\xc3\x99&\xc2\xa9d\xc2\x
ac\xc3\x97\xc2\xbdMs\xc2\x94\xc3\xba\xc3\xa8.\[...],
len=108,binarycount=71,pam.imap4.tag.limit=100,
coalescer-info=Forwarded due to age
```

- This signature detects an IMAP tag that exceeds pam.imap4.tag.limit (default 100) bytes in length.

Log

```
Dec 15 13:10:24 isa.igi.local iss-ipm[962]: Packet
dropped: Invalid protocol: time=1260879011,src-
ip=192.168.2.251,dst-ip=67.215.65.132,ip-
protocol=TCP(6),src-port=59407,dst-port=5988

Dec 15 13:10:24 isa.igi.local iss-ipm[962]: Packet
dropped: Invalid protocol: time=1260879011,src-
ip=192.168.2.251,dst-ip=67.215.65.132,ip-
protocol=TCP(6),src-port=37807,dst-port=7937

Dec 15 13:10:24 isa.igi.local iss-ipm[962]: Packet
dropped: Invalid protocol: time=1260879011,src-
ip=192.168.2.251,dst-ip=67.215.65.132,ip-
protocol=TCP(6),src-port=40759,dst-port=125
```

HP/Tipping Point

- Simple configuration
- Plug&forget
- Works well with default configuration
- You can
  - Add rules, for instance to block P2P
  - Add exceptions
- Mature, polished product, user friendly
- HW designed for IPS functionality

Source Fire

- Built around Snort engine
- Dashboard
  - Easy configuration, reporting
- Additional modules
  - Network awareness
  - User awareness
- Adaptable IPS, hides unnecessary alerts
- Greatest number of filters, large community
- OS: Linux

Why IPS?

1. Information security
2. Audit
3. Regulatory compliance
   - Personal data protection
   - Copyright protection

- The paper you have to sign before Source Fire gives you appliance for testing

Conclusion

- This is not a commercial presentation!
- Each tested appliance has value of its own
  - I would be happy with any of them!
- They all
  - Block much more traffic than traditional firewalls
  - Stop attacks from outside and inside
  - Show admin what is really going on in their network!
  - Force admin to stay alert and learn!
  - Show some degree of false positives & negatives
  - Miss particular events, at least some of them
  - Come with a price...