Security Incidents and Education

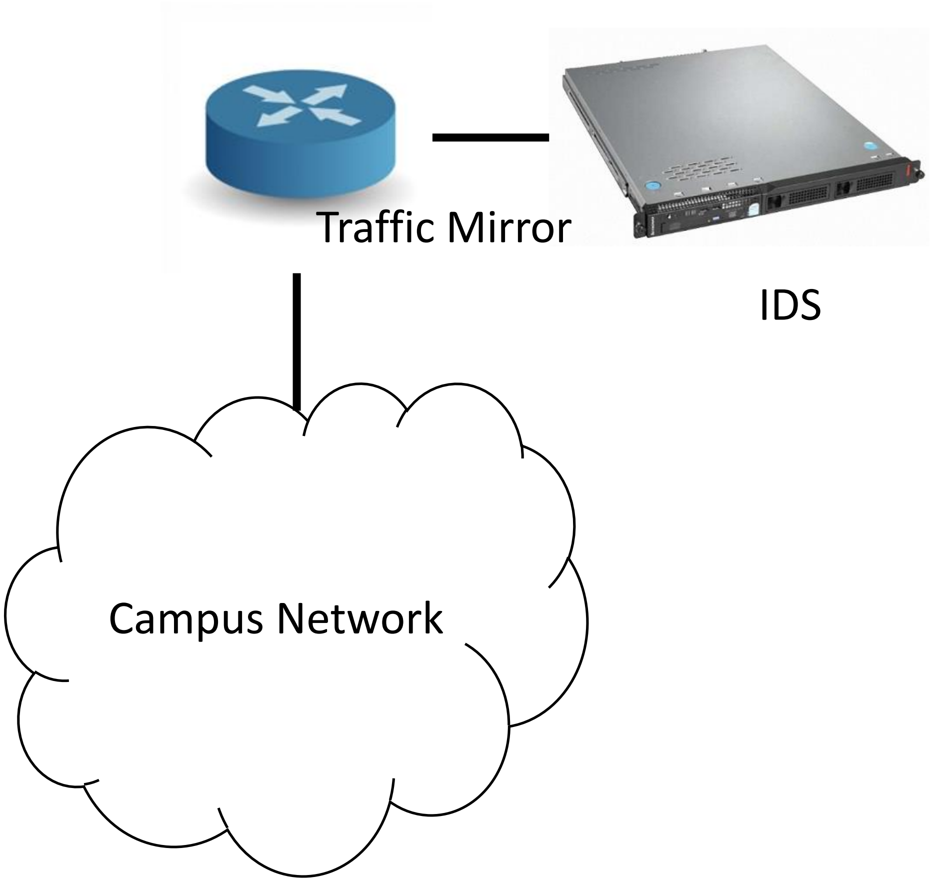
Koji OKAMURA
Cyber Security Center
Research Institute for Information Technology

History of Security Gadgets in Kyushu Univ. and Incidents(since 2000~)

- IDS (Intrusion Detection System)
- P2P finder
- IDS + Syslog analyze Out Source
- Firewall (IPS, Intrusion Prevention System), Paloalto
- APT check (Trial)
- Paloalto + Wildfire

- Bot
- Copyright Problem
  - Winny
  - BitTrrent
  - 迅雷（Xunlei、Thunder）
  - HTTP
- DDoS
  - DNS
  - NTP
  - SMTP
- Bot, Trojan

IDS vs Bot (2001-2010)



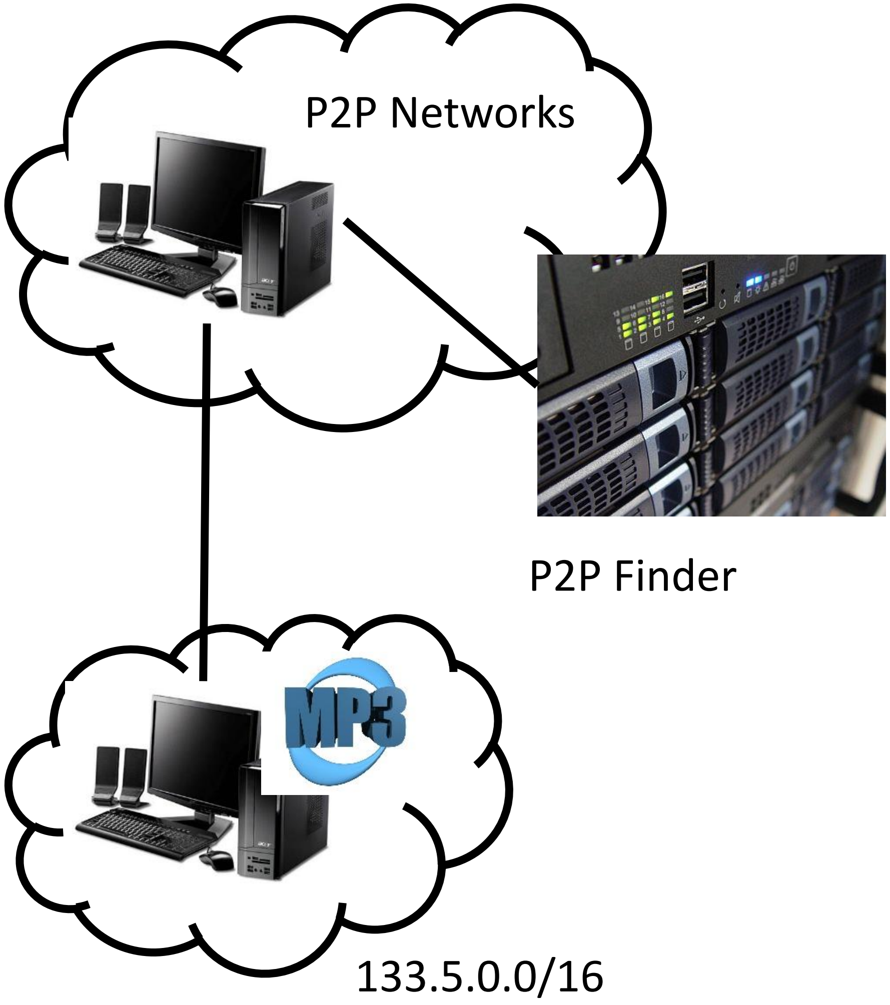
Traffic Mirror

IDS

Campus Network

- First Gadget for Security in Kyushu Univ.
- Detect so many Dot infected PCs
- Manual analyze
  - Consume much time of Faculty
  - Can not 365days 24hours
- We have used manual IDS until IDS + Rac.

P2P Finder vs Copyright Issues (2005-2013)



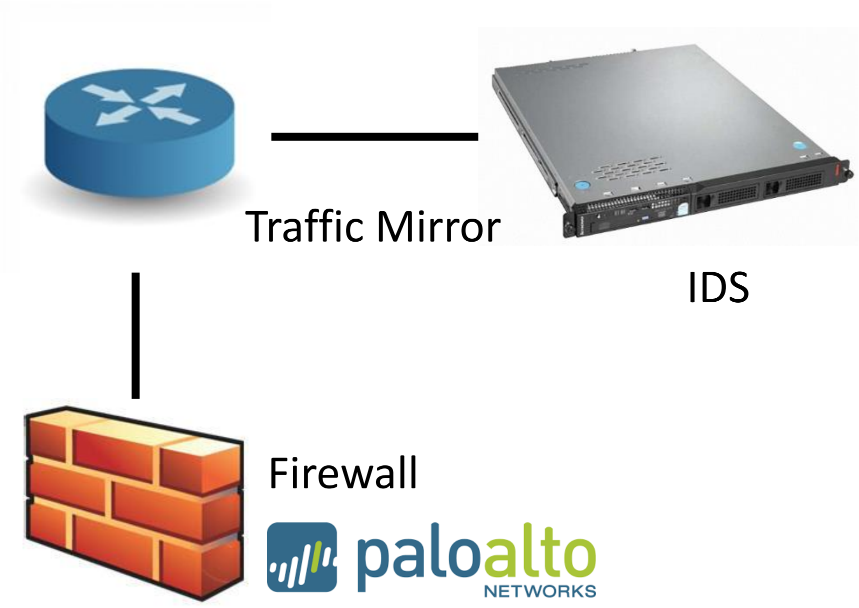
- Copyright Problem by P2P Software
- P2P Finder can detect after P2P user download and start upload Copyright Files.
- Winny, BitTrrent…
- 迅雷（Xunlei、Thunder） X
- P2P Finder can not detect file sharing by HTTP.

IDS + Lac (2010-) LAC

- We start to get so much information about Incidents.
- We detect more Bot infected PCs and have removed from the Campus.
- We just detect but can not filer automatically.
  - Incidents were solved by the users.

Cisco IPS

Firewall (2013-)



- We became to be able to filter what should be filtered.
- FW filters and we do not necessary to remove infected PCs.
  - When we tried FireEye recently, we found so many Trojan infected PCs…

FireEye
Next Generation Threat Protection

- Paloalto can filter P2P perfectly but we do not mind that students install P2P software or not.
  - 迅雷（Xunlei、Thunder）
- We have another incidents which firewall can not work well for.
  - DDoS
    - SMTP
  - Zero Day
    - Wildfire (vs Anti-Virus Soft?)
  - APT

Just FYI.

- MeeGoPad T01
- This is first time for me to buy Windows PC from China.
- There are so many Trojan infected Files…
- Windows8.1 activetools provided by seller is also infected.
- Anti-Virus Soft installed in advance never detect Trojans inside.

Security Gadgets vs Education

- *Security Gadgets* protect *University* from incidents with keeping PC infected.
- Campus network with Firewall is bored due to much limitation but becomes safety than Home Internet.

- *Education* protects *students* from incidents.
- Campus network is like Green House. But students must live in Free Cyber Space under personal responsibility in Future over the World.