



# ALLOT jako kostka stavebnice

bandwidth  
on demand

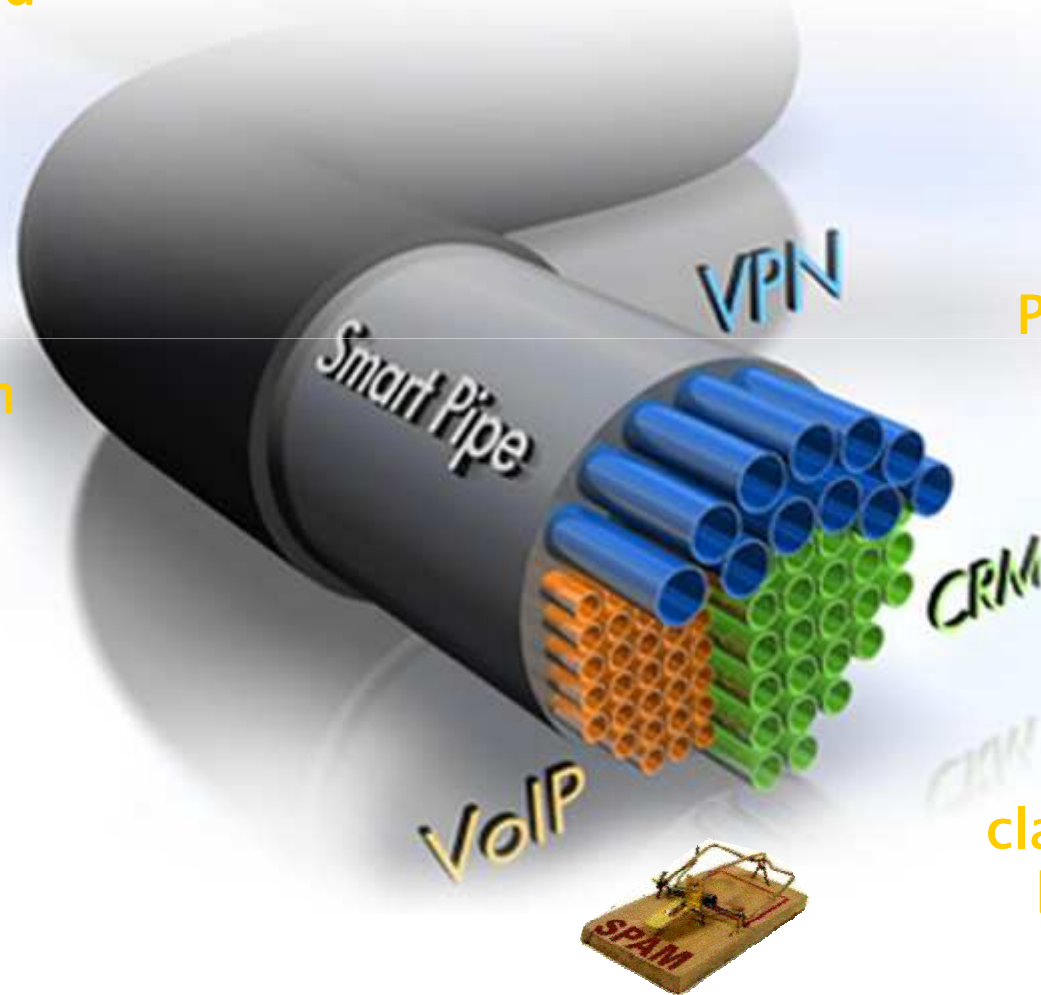
Android  
iOS

HTTP  
redirection

PlayStation  
Xbox

mobile  
trends

classification  
based on  
XFF field





# ALLOT 2011

## □ ***Nové modely postavené na AOS s DART***

- AC500
  - až 20k „vnitřních“ uživatelů
  - propustnost 200Mbps FD
- AC1400 resp. AC3000
  - až 160k „vnitřních“ uživatelů
  - propustnost 1Gbps resp. 4Gbps FD
- další blade systémy s propustností až 1Tbps

## □ ***DART (Dynamic Actionable Recognition Technology)***

- vždy 3vrstvá hierarchie s 256 lines a více než 40k pipes a 80k VCs
- podpora asynchronního provozu
- možnost vytváření vlastních signatur
- dynamické externí host files
- standardní schopnosti - priority, shaping, limiting, blocking
- ...



# A když máte ALLOT

## ❑ *otevřený systém*

- možnost vytváření vlastních signatur
- dynamické externí host files
- ...

## ❑ *vysoký realtime výkon*

- neptejte se jen na propustnost v bps, ptejte se na počet spojení
  - AC500 > 256k spojení
  - AC1400 i AC3000 > 2M spojení

## ❑ *chytré zpracování*

- HW využívající vlastní ASICy
- nízká spotřeba HW
- výrobce orientovaný na daný segment



# splňte si své tužby a potřeby – vol.1

## □ ***nakonfigurujeme HSS (Hybrid Security Shaping)***

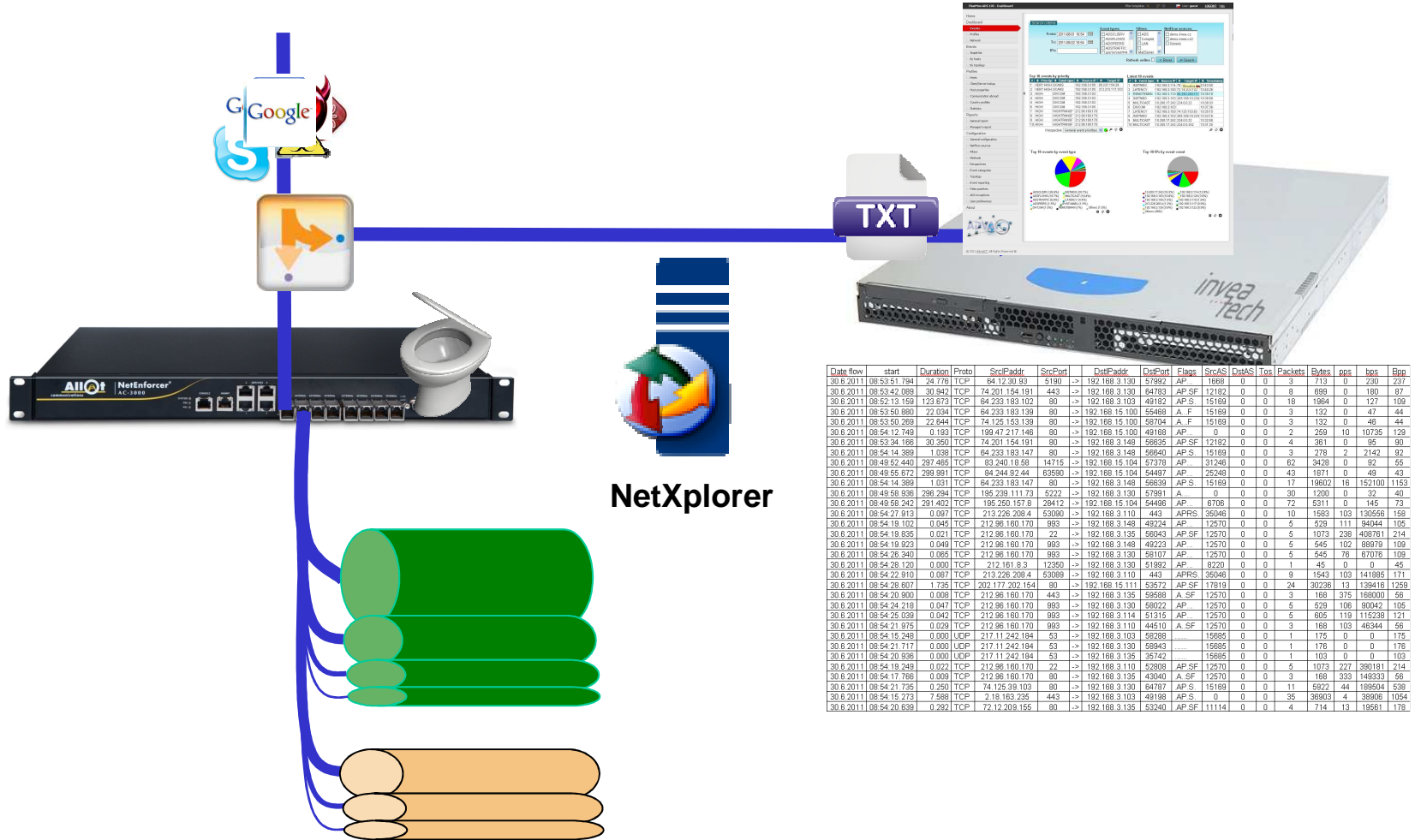
- najdeme bezpečnostní díry před útokem
  - reverzní záznamy DNS
  - scany portů nebo adres
  - nestandardní komunikace
  - ...
- poznáme možné zdroje poškození dobré reputace
  - odchozí SPAM
- ...

## □ ***HSS je sloučením***

- systému ALLOT
- systému FlowMon
- FlowMon pluginu ADS nebo C1



# splňte si své tužby a potřeby – vol.1 cont.





## splňte si své tužby a potřeby – vol.2

### □ *snížíme zátěž produkčních aplikací*

- letecká společnost bojovala s vysokou zátěží serveru pro bookování letenek
- zátěž vznikla při marketingových kampaních
  - nebylo možné se orientovat podle zdrojové adresy
  - nešlo ani dedikovat dostatečný výkon serverů resp celé sítě
  - správný marketing tak generoval provoz podobný DoS útokům
  - aplikační load balancing byl drahý a nepřinášel dostatečný užitek
- na ALLOTu začaly být vytvářené pro jednotlivé marketingové kampaně vlastní signatury
  - provoz byl prioritován podle části textu http (uvedené v kampani)
  - náklady na marketing neskončily na hranici IPS, timeoutem nebo velmi pomalou odezvou serverů/aplikací



# **splňte si své tužby a potřeby – vol.3**

## ***Pálí vás nějaký problém v síti?***

**Uživatelé mají pořád nějaké problémy.**

**Management stále touží po lepších řešeních.**

**Bezpečnost , to je nekončící boj.**

...

## ***Nenašli jste řešení na standardních aktivních prvcích?***

**Velmi často jde o systémy s omezenou sadou schopností a minimální otevřeností.**

***Pojďme to zkusit s ALLOTem.***

Je dobré mít vyřešenou end point security (osobní FW, AV, ...). Je dobré mít řešení na hranici sítě (stavový FW, IPS se signaturami, ...).

Je třeba mít kompletní přehled o provozu v celé síti. Pak se můžeme hrát se stavebnicí.



**Děkuji za pozornost**

# Otázky Odpovědi

VUMS DataCom, spol. s r.o.

U Ladronky 2331 / 7

169 00 Praha 6 – Břevnov

[www.datacom.cz](http://www.datacom.cz)

Ivo Kubíček

[ivo.kubicek@datacom.cz](mailto:ivo.kubicek@datacom.cz)

721 129 068