

# Inter-opérabilité



# Enjeux de l'inter-opérabilité

- Objectif : avoir la possibilité de changer de fournisseur si besoin
  - Saas
  - Paas
  - Daas
  - Iaas

# Licence Affero-GPL



à destination des services types SaaS

- Dérivée de la licence GPL
- Plus l'obligation de délivrance des codes sources lors de l'usage du logiciel sur le réseau
  - Garantit la reproductibilité et l'évolutivité d'un logiciel hébergé
  - La licence porte uniquement sur le logiciel et non sur les données transmises par son biais



# Formats standards ouverts et normalisés


Qui d'entre vous est sûr d'utiliser le même [Cloud] Logiciel] dans dix ans ?

- **vCard** : données personnelles : Visit Card
- **HTML** : Hypertext Markup Language
- **ODF** : Open Document Format (norme ISO)
- **CSV** : Comma-separated values
- **JSON** : JavaScript Object Notation
- **XML** ?

<http://formats-ouverts.org/>



# Initiatives de standardisation

- Distributed Management Task Force 
  - Open Virtualisation Format OVF (Appliances virtuelles)
  - SNIA : Stockage
- Compatible One
  - Cloud management / IaaS / PaaS
  - Utilise Open Cloud Computing Interface OCCI RESTful Protocol and API

# Standardisation – le stockage

Data as a service

Service S3 de Amazon

Storage Networking Industry Association (SNIA)

Cloud Data Management Interface (CDMI)

D'abord RFC, puis validé par l'ISO (2012)

Opérations en HTTP REST et JSON

- ACL, export vers NFS, CIFS, iSCSI

<http://cdmi.sniacloud.com/>



# Standardisation – les images disques

- VMware : vmdk
- Microsoft et Citrix : vhd, vhdx
- Amazon : ami
- Xen : qcow, qcow2, vhd, raw
- QEMU : qcow, qcow2, raw, vmdk, vdi, cloop
- VirtualBox : vdi, vmdk, vhd, hdd, vdi
- Parallels : hdd

conversions de formats possibles via OVF

# Cyberattaques





# Sécurité logique

- Backups (système & données)
- Mot de passe sur screensaver,
- Anti-Virus,
- Firewalling, WAF, système anti DDOS,
- VLAN
- Détection d'intrusion IDS
- Tests d'intrusions
- Challenge

# Botnet

1) et 2) prise de contrôle : virus, faille de sécurité, cheval de Troie

3) achat

4) Attaque : spam, attaques par force brute, DDoS

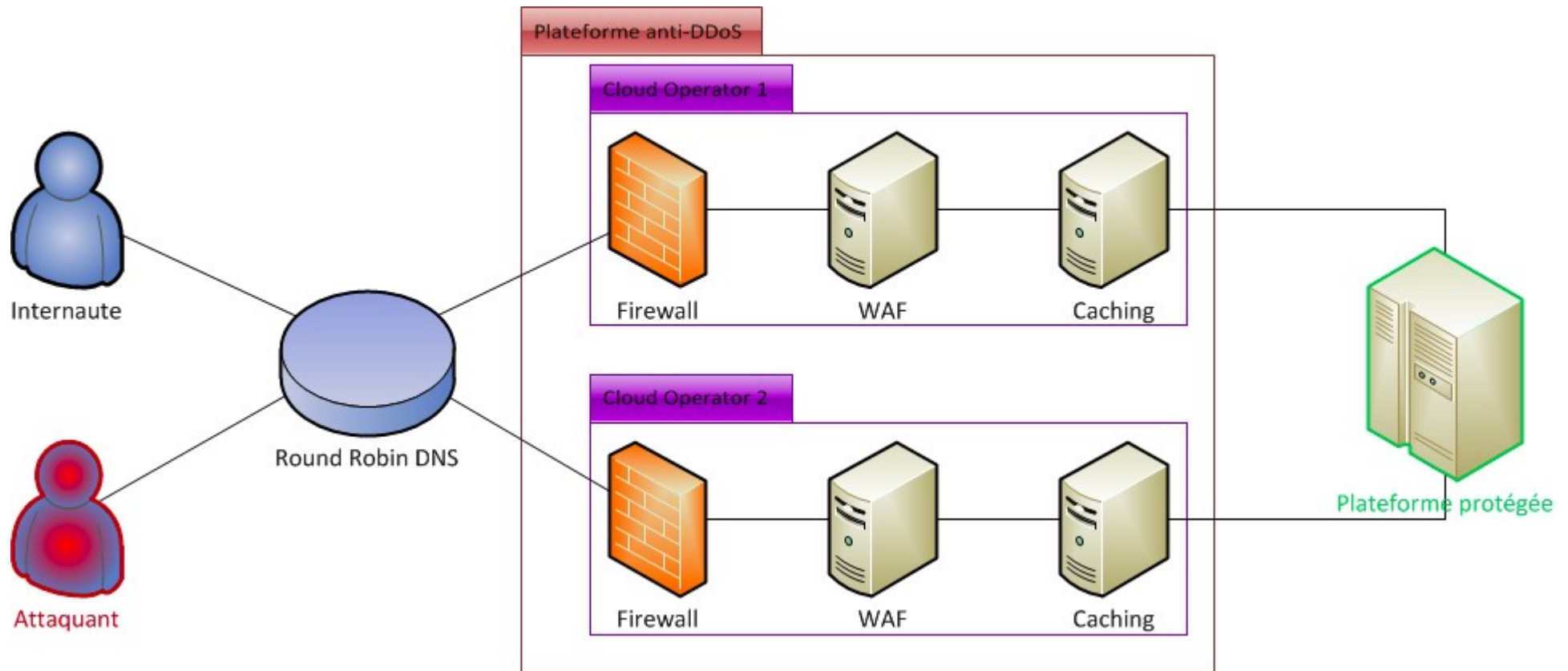


# Attaques DDoS

- Distributed Denial of Service : saturer
  - le serveur : envoyer de multiples requêtes
  - le routeur : envoyer pleins de petits paquets
  - le tuyau : envoyer pleins de gros paquets
- Requêtes lancées par des PC zombies (réseaux nommés Botnets)
- Achat (nbre machines, durée, requête à lancer)

# Plateforme anti-ddos modulaire

DROP, fail2ban, LimitReq, TARPIT



<http://francois.aichelbaum.com/creation-dune-plateforme-anti-ddos-modulaire/>  
Voir aussi <https://www.ovh.com/fr/anti-ddos/mitigation.xml>



# Attaques DDoS

## Publications Arbor Networks (3 trimestres 2013)

- Prédominance des attaques applicatives 82 %
- 37 % des attaques sont entre 2 et 10 Gbps
- Moyenne 2,64 Gbps en hausse de 78 % /2012
- Attaques >20Gbps multipliées par 3,5 /2012
- 87 % des attaques durent moins d'une heure

2015 : attaque à 500 Gbps



# Conformité



# Conformité

- ISO 27 000
- SAS 70 : conformité Sarbanes-Oxley
- Données de santé : hébergeur agréé
- Archives

# PCI DSS

## Payment Card Industry Data Security Standard

- Organisation américaine maintient une liste de société agréées pour effectuer les contrôles
- Conformité testée tous les ans (tests techniques)
- Questionnaire d'auto évaluation
- Les logs sont fournies au gestionnaire de sécurité



# Des questions

