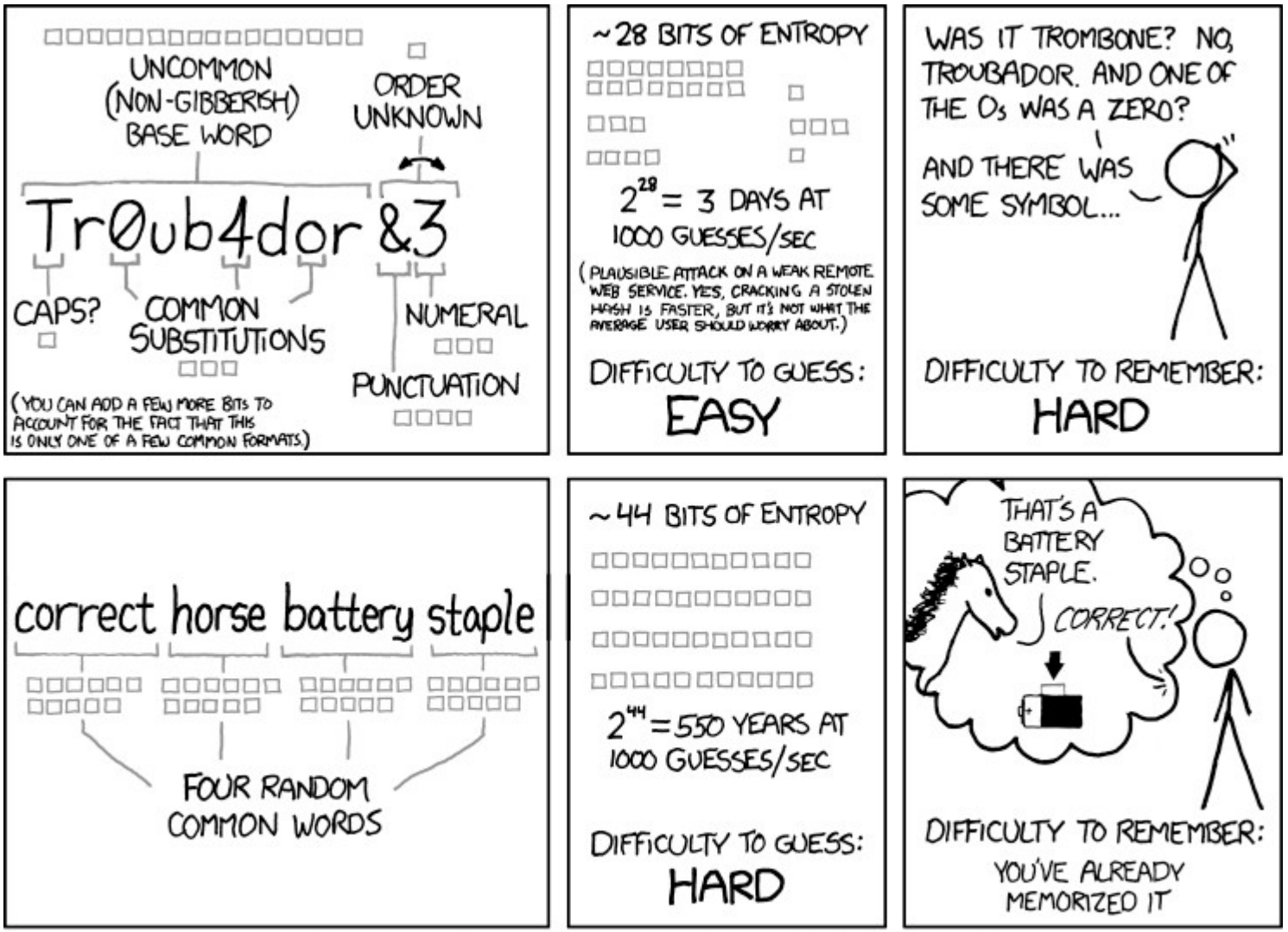
Un bon mot de passe



https://xkcd.com/936/

Google : Garanties et clauses de non responsabilité

9.2 Clauses de non-responsabilité.

DANS LES LIMITES AUTORISÉES PAR LA LOI EN VIGUEUR ET SOUS RÉSERVE DE DISPOSITIONS EXPRESSES DU PRÉSENT CONTRAT, AUCUNE PARTIE N'OFFRE D'AUTRE GARANTIE QUELLE QU'ELLE SOIT (EXPRESSE, IMPLICITE, LÉGALE OU AUTRE), Y COMPRIS, MAIS SANS S'Y LIMITER, DES GARANTIES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET DE CONFORMITÉ. GOOGLE NE FAIT AUCUNE DÉCLARATION QUANT AU CONTENU OU AUX INFORMATIONS ACCESSIBLES PAR OU VIA LES SERVICES.

Décembre 2014 http://www.google.fr/apps/intl/fr/terms/premier_terms.html

Chiffrer les données

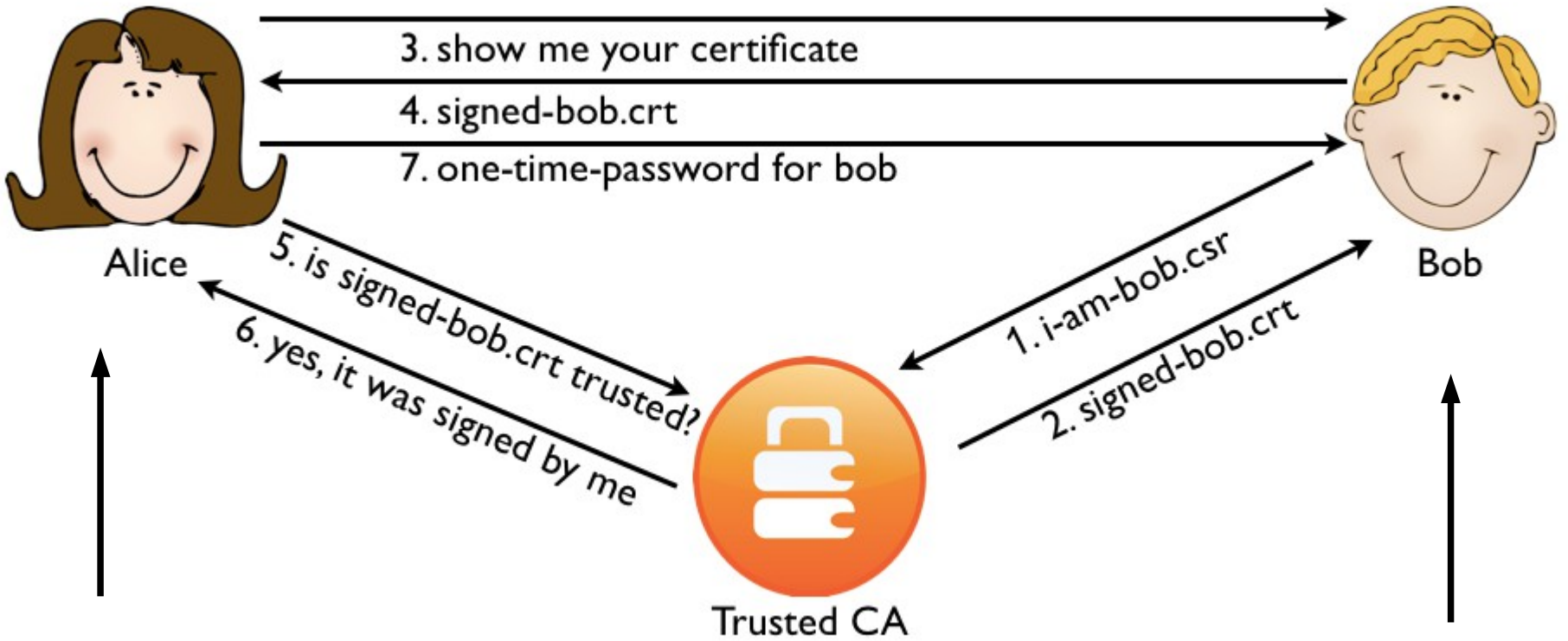
- Sur le réseau
  - Protocoles SSL, SSH, IPsec
- Sur les fichiers
- Sur les systèmes de fichiers

Secure Socket Layer SSL

HTTPS, SMTPS, LDAPS, POP3S, IMAPS,
VPN OpenVPN

- Authentification avec certificat numérique
  {clé publique, noms, localisation, …, signature}
- Confidentialité
  → il faut chiffrer les données
- Intégrité
  → utilisation de fonction de hachage

Secure Socket Layer SSL



Client

Serveur

Tiers de confiance

Secure Socket Layer SSL

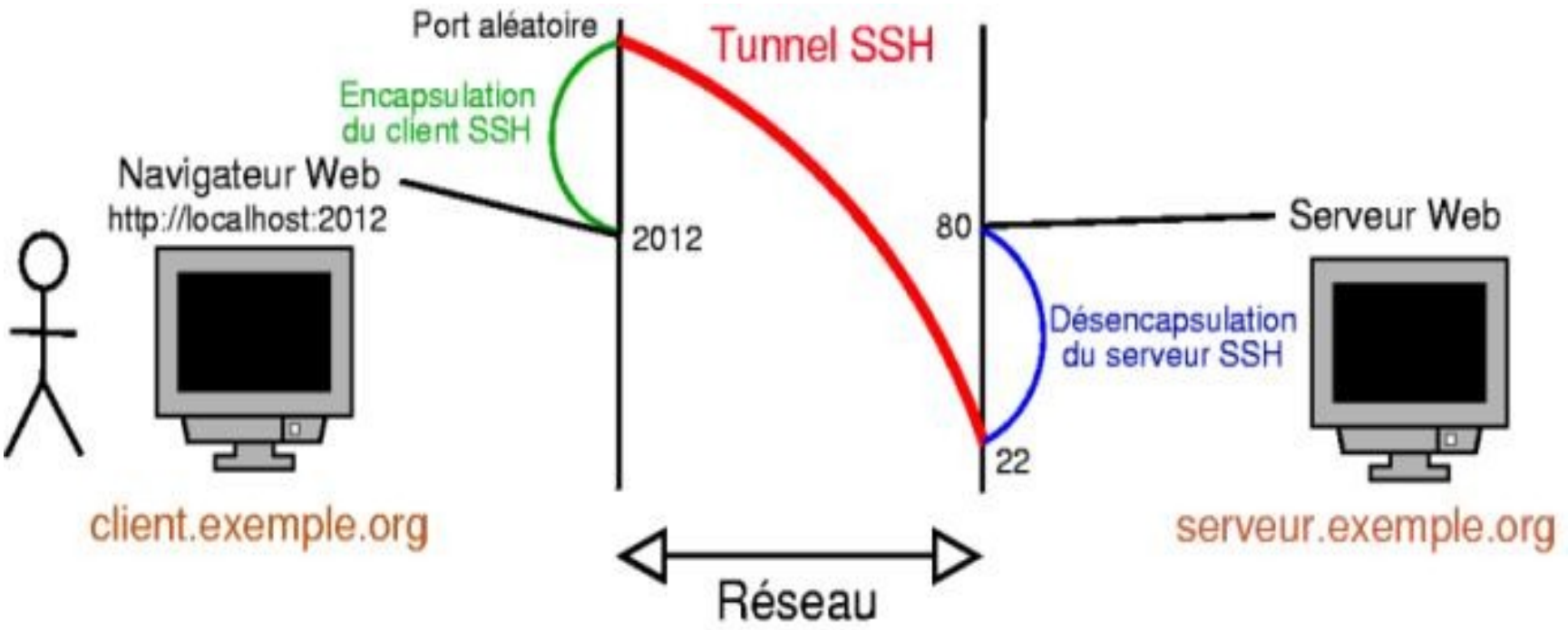
Protocole simplifié

1) Le client fait une demande de transaction sécurisée au serveur.
2) Le serveur envoie son certificat.
3) Le client vérifie que le certificat délivré est valide. Si la vérification est correcte alors le client envoie au serveur une clé symétrique chiffrée à l'aide de la clé publique du serveur qui sera donc le seul à pouvoir déchiffrer.
4) Cette clé sera utilisée pour échanger les données en toute sécurité.

Secure Shell : SSH

- Protocole de communication (utilise SSL)
- Programme qui utilise le protocole
- Cryptographie asymétrique puis symétrique
- Utilisations
  - Shell
  - Copie (scp), synchronisation (rsync) de fichiers
  - Tunnels
  - Monter un répertoire distant

Secure Shell : SSH



http://formation-debian.via.ecp.fr/ssh.html

IPsec

Internet Protocol Security

Niveau 3 du modèle OSI (couche réseau)

Utilisation de certificat

Traversée des NAT avec encapsulation

Sphère de sécurité : Safe Harbor

Un cadre juridique définit par le Département du commerce des États-Unis qui permet aux entreprises américaine de se conformer à la directive européenne sur la protection des données personnelles (2001).

- Informe sur la collecte des données
- Donne la possibilité de refuser le transfert des données à des tiers
- S'il y a transfert, les mêmes niveaux de garanties sont conservés
- Prend des mesures de protections (suppression, divulgation ...)
- Utilisation des données avec accord de l'utilisateur
- Accès aux modifications sur les données
- Obligation de tout mettre en œuvre pour le respect de ces règles

Google, Amazon, Facebook, Apple, (GAFA), Microsoft, ...

USA PATRIOT Act

Uniting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act** of 2001 (26 octobre)

Les services de sécurité américains peuvent accéder aux données à caractère personnel

Cela concerne les données hébergées

- sur le continent américain par n'importe quelle société
- par des sociétés de droit américain n'importe où

http://www.fincen.gov/statutes_regs/patriot/

Lanceur d'alerte

- Wikileaks
  - Julian Assange
  - Chelsea Manning – vidéo Collateral Murder
- Edward Snowden

PRISM

- Cible : des personnes vivant hors des États-Unis
- la NSA dispose d'un accès direct aux données hébergées par Google, Facebook, Apple, Microsoft, Yahoo, Skype, AOL…
- captation des métadonnées des appels téléphoniques aux États-Unis
- la NSA a développé de multiples méthodes de contournements des cryptages SSL

XKeyscore

- collecte quasi-systématique des activités de tout utilisateur
- 700 serveurs localisés dans des dizaines de pays
- 20 To / jours
- Données : 3 à 5 jours
- Metadonnées : 30 jours
- Données intéressantes : 5 ans

Bullrun

- casser les systèmes de chiffrement
- Intervention sur les normes
- Intégration de portes dérobées
- Collaboration avec fournisseur de services
- Utilisation de superordinateur (force brute)
- Cyberattaques / espionnage (vol de clés)
- => le NIST : ~~Special Publication 800-90A~~
- => RSA Security : ~~B-SAFE~~

Loi de programmation militaire LPM

pour les années 2014 à 2019

- Promulguée le 19/12/2013
- Article 20 : Pour les finalités énumérées à l'article L. 241-2, peut être autorisé **le recueil**, auprès des opérateurs de communications électroniques [...], des **informations** ou **documents** traités ou conservés par leurs réseaux ou services de communications électroniques, [...] au recensement de l'ensemble des **numéros d'abonnement** ou de **connexion** d'une personne désignée, à la **localisation** des équipements terminaux utilisés ainsi qu'aux communications d'un abonné [...]
- Décret d'application signé le 24 décembre 2014

Confidentialité

Expliquer en quoi la réunion des trois conditions suivantes permet un bon niveau de confidentialité.

- Utiliser le chiffrement point à point
- Utiliser un système décentralisé
- Utiliser les logiciels libres

Inter-opérabilité

Enjeux de l'inter-opérabilité

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

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/

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

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

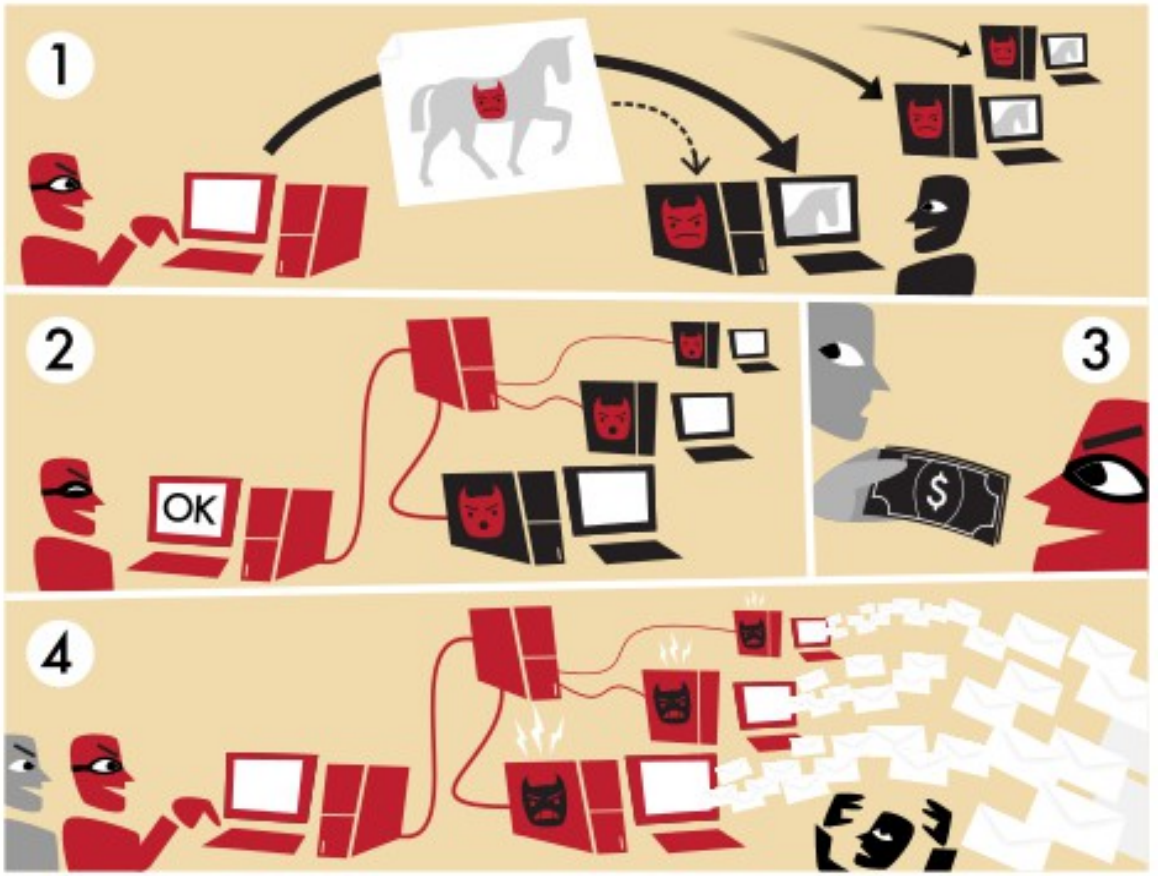
- Backups (système & données)
- Mot de passe sur screensaver,
- Anti-Virus,
- Firewalling, WAF, système anti DDOS,
- VLAN
- Détection d'intrusion IDS
- Tests d’intrusions
- Challenge

Botnet

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

3) achat

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

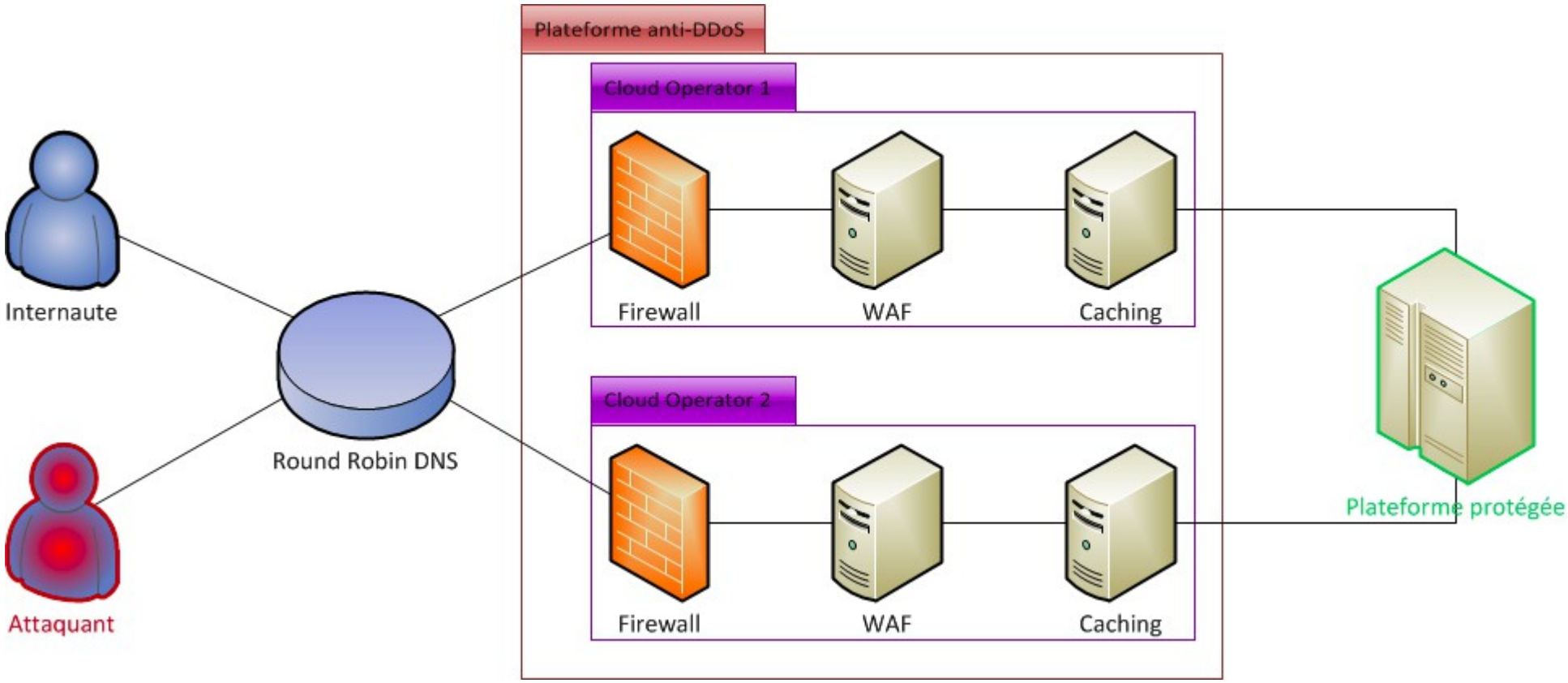


Attaques DDoS

- 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
- Attaque la plus élevée : 309 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