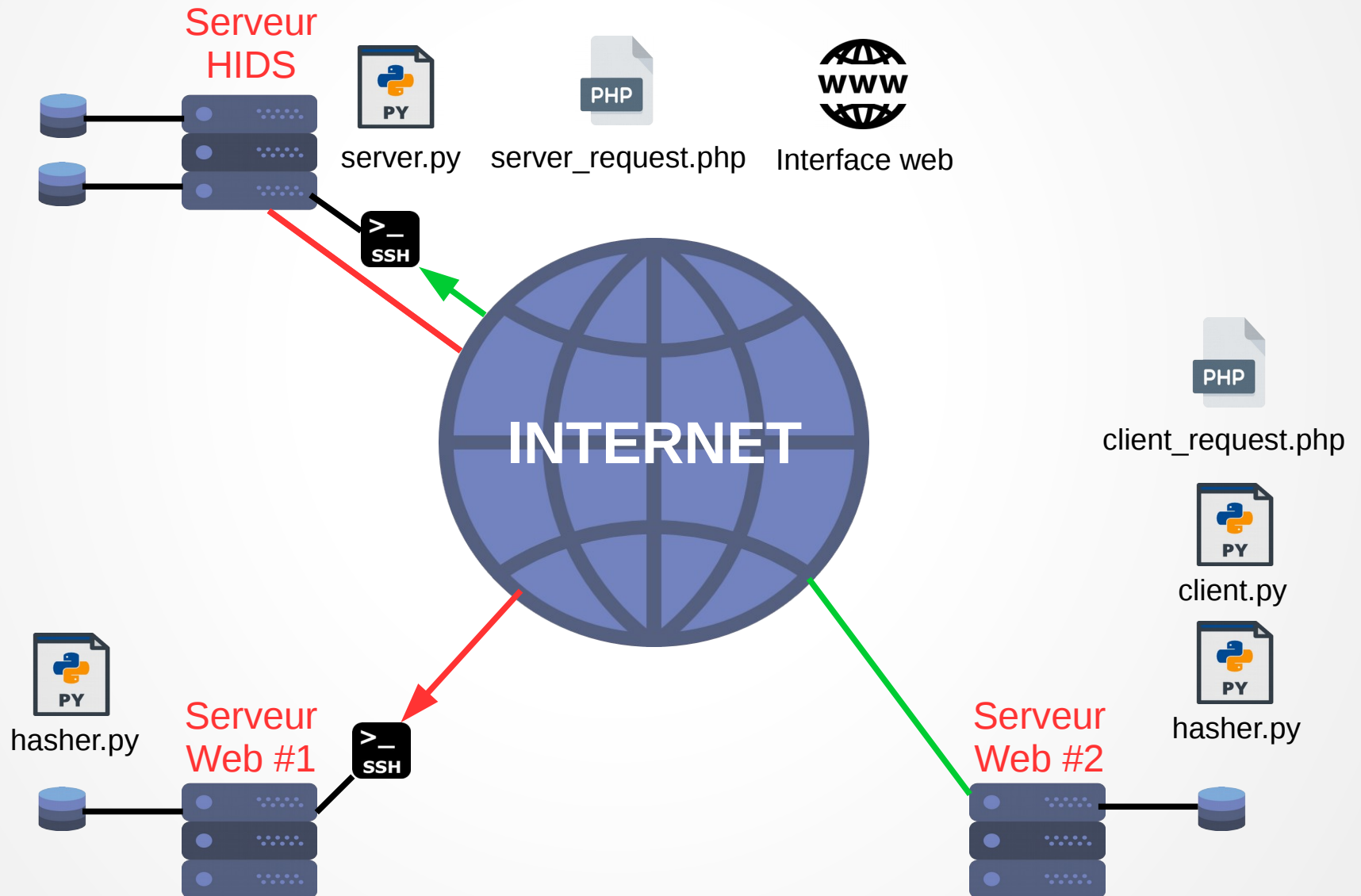


INFRASTRUCTURE



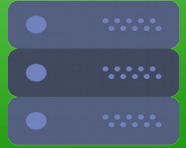
SERVEUR HIDS



- 2 Bases de données :
 - BDD des requêtes et sites
 - BDD des empreintes
- Script python server.py
- Script php server_request.php
- Interface web d'administration



SERVEUR WEB (SSH)



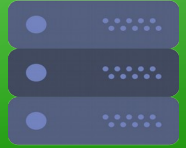
Site web (ex :
wordpress, bootstrap)

- Serveur apache
- BDD du site

Client HIDS

- Serveur ssh
- Script hasher.py

SERVEUR WEB (no SSH)



Site web (ex :
wordpress, bootstrap)

- Serveur apache
- BDD du site

Client HIDS

- Script Client.py
- Script hasher.py

BDD HIDS



BDD requêtes

- Requêtes d'états et données des serveurs web
- Ecriture par le script `server_request.php`
- Lecture et ecriture par le script `server.py`
- Lecture et ecriture par interface web

BDD sites

- Empreintes des sites
- Lecture et ecriture par script `server.py`

SERVER.PY



- Se lance au démarrage du serveur
- Fonctionne en arrière plan
- Consulte et analyse la BDD requêtes et sites
- Consulte et modifie la BDD des empreintes
- Se connecte en ssh aux serveurs web distants et copies des fichiers
- Envois des requêtes via le script `client_request.php`

SERVER_REQUEST.PHP



- Récupère les requêtes des serveurs web
- Ajout les requêtes à la BDD requêtes

INTERFACE WEB



- Se connecte via des identifiants
- Accès aux sites analysés
- Accès aux logs des analyses
- Accès aux empreintes des fichiers des sites
- Ajout/Modification des sites
- Bouton de lancement manuel des analyses

HASHER.PY



- Analyse le fichier csv permettant de générer les empreintes
- Génères un fichier csv d'empreintes
- Envois son état au serveur HIDS via le script `request_server.php`

CLIENT.PY



- Envoie via scp le fichier d'empreintes
- Définie des taches cron

CLIENT_REQUEST.PHP



- Analyse les demandes HIDS
- Lance le script client.py
- Lance le script hasher.py