Retour d'expérience sur l'organisation d'un CTF

Rétrospective sur 6 ans de FCSC

Tristan CLAVERIE

Jérémy JEAN

Emilien COURT

Matthieu OLIVIER

Alexandre IOOSS

Adrien THUAU

5 juin 2024 @ SSTIC 2024

Plan général

> Présentation générale FCSC

> Conception des épreuves

> Deux points d'infrastructure

- MicroVM
- Système anti DDoS

> Projets annexes et évolutions

Retour d'expérience sur l'organisation d'un CTF

Rétrospective de 5 ans de FCSC

Tristan Claverie, Emilien Court, Alexandre Iooss, Jérémy Jean, Matthieu Olivier et Adrien Thuau
<Prénom>.<Nom>@ssi.gouv.fr

Résumé. Tous les ans depuis 2019, l'ANSSI organise le FCSC, une compétition CTF en ligne dont l'un des buts est de constituer une équipe nationale qui participera à l'ECSC organisé par l'ENISA. Depuis sa création il y a cinq ans, le FCSC a évolué, s'est structuré et quelques projets connexes comme Hackropole ont vu le jour. En plus d'être apprécié par les joueurs de CTFs, le FCSC permet également de répondre à des objectifs de l'ANSSI et mobilise chaque année une trentaine de personnes. Dans cet article, nous revenons sur cet événement, la sélection de l'équipe nationale et sur la mise en place d'archives des épreuves passées.

Présentation FCSC et ECSC

> FCSC (France Cybersecurity Challenge)

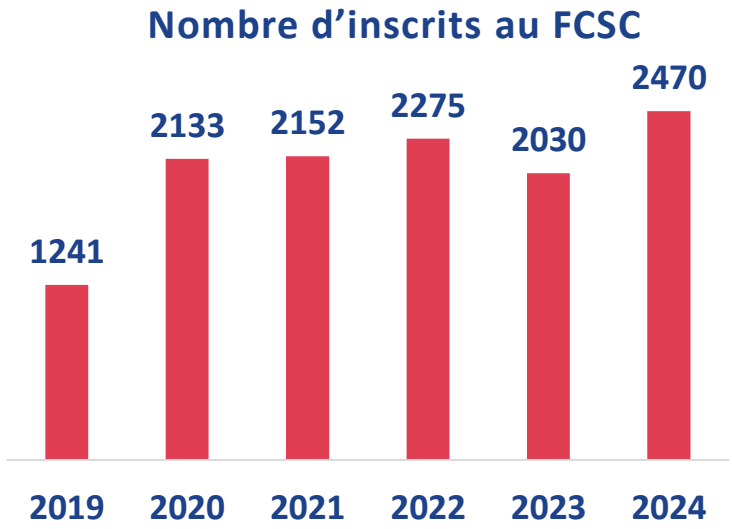
- CTF individuel
- Organisé par l'ANSSI
- En ligne tous les ans depuis 2019

> Public cible

- **Prioritaire :** jeunes, étudiants, futurs actifs
- **Autre :** professionnels, passionnés, curieux, …

> CTF ou « Capture The Flag »

- Evénement de cybersécurité
- Individuel ou en équipe
- Exercices techniques à résoudre
- Récupération de flags/points



Présentation FCSC et ECSC

> FCSC (France Cybersecurity Challenge)

- CTF individuel
- Organisé par l'ANSSI
- En ligne tous les ans depuis 2019
- **Sélection d'une équipe pour l'ECSC**

> Public cible

- **Prioritaire :** jeunes, étudiants, futurs actifs
- **Autre :** professionnels, passionnés, curieux, …

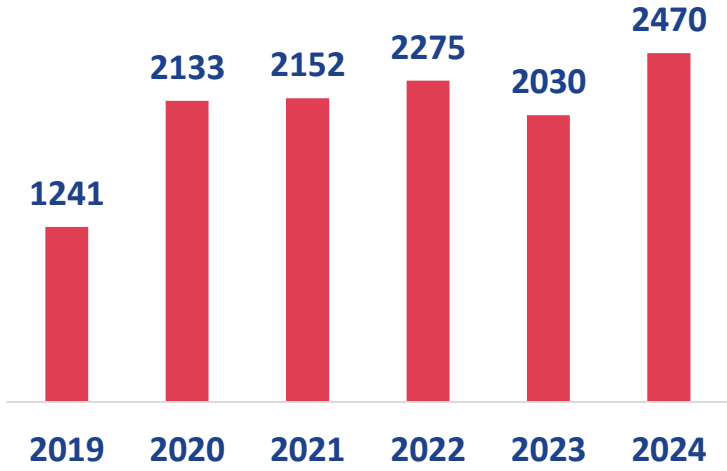
> ECSC (European Cybersecurity Challenge)

- CTF en **équipe nationale** en présentiel
- Organisé par l'ENISA tous les ans depuis 2014
- Participation de la France depuis 2018
- Equipes de 10 jeunes (moins de 25 ans)
- 30+ pays représentés en 2023

> CTF ou « Capture The Flag »

- Evénement de cybersécurité
- Individuel ou en équipe
- Exercices techniques à résoudre
- Récupération de flags/points

Nombre d'inscrits au FCSC



France Cybersecurity Challenge (FCSC)

> Utilisation de CTFd avec un thème/plugin personnalisé

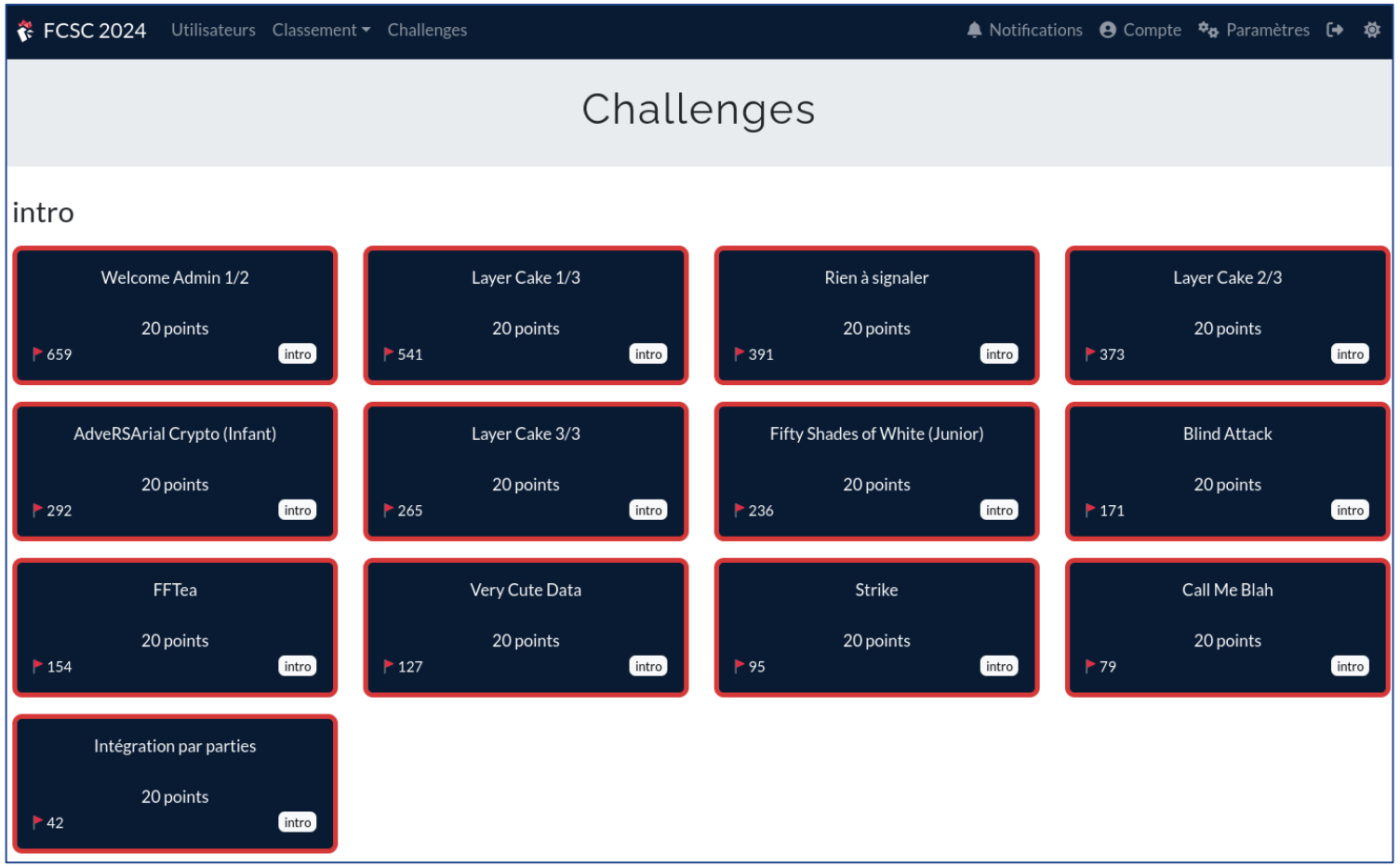
- Affichage de la liste des épreuves
- Classement des utilisateurs selon le score (liés au nombre de « flags » capturés)

> Epreuves « intro »

- Pédagogique
- Pour les débutants
- Découverte des CTF

> Catégories

- Cryptographie
- Exploitation web
- Exploitation binaire
- Rétro-conception
- Hardware
- Forensics
- Radio
- Algorithmique
- Side Channel
- Injection de fautes



Exemples d'épreuves (FCSC 2024)

- **Winternitz is coming** *(cryptographie)*
- **Call Me Blah** (pwn, introduction)

Challenge | 79 résolutions

Call Me Blah

20 points

intro pwn

On vous place dans le cas typique d'une fin d'exploitation. Pouvez-vous obtenir un shell ?

`nc challenges.france-cybersecurity-challenge.fr 2103`

call-me-blah | call-me-blah.c | ld-2.36.so | libc-2.36.so

Flag | Soumettre

Challenge | 18 résolutions

Winternitz is coming

456 points

Je vous présente une signature à usage unique inédite et à la pointe de l'innovation ! En plus j'ai bien fait attention à ne signer qu'un seul message. Il ne peut donc rien m'arriver de fâcheux, n'est ce pas ?

`nc challenges.france-cybersecurity-challenge.fr 2153`

winternitz-is-coming.py

Flag | Soumettre

Conception des épreuves

> Toute l'année

- Veille et partage d'idées

> Décembre - Mars

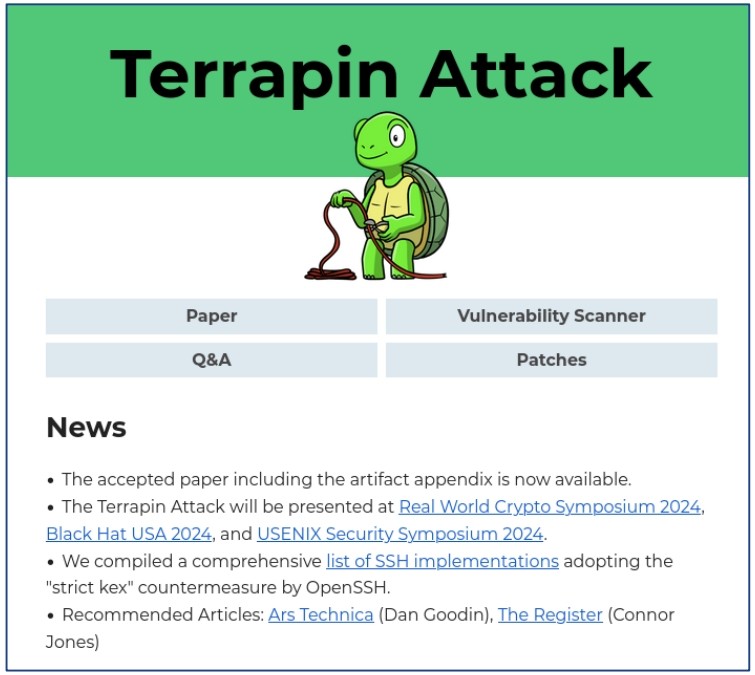
- Conception des épreuves
  - Si besoin, conteneurisation Docker
- Seul ou en binôme

> Février - Mars

- Tests des épreuves
  - Par une autre personne que le concepteur
  - En boîte noire (ou à défaut, grise)
- Déploiement/test des épreuves en « preprod »
  - Création de la VM, durcissement, CI/CD

> Mars - Avril

- Mise en production (Grafana, *rate limiting*, …)
- Derniers tests en production



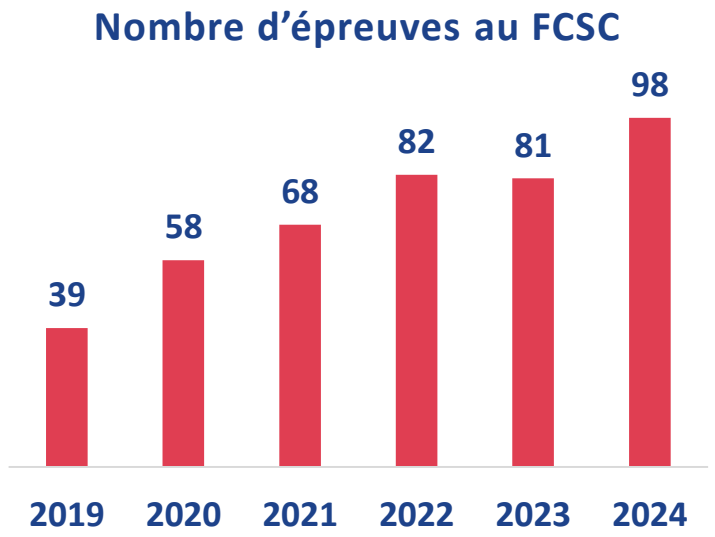
https://terrapin-attack.com

Epreuve « Secret Shenanigans » (FCSC 2024)

Conception des épreuves

> Objectifs dans la phase de conception

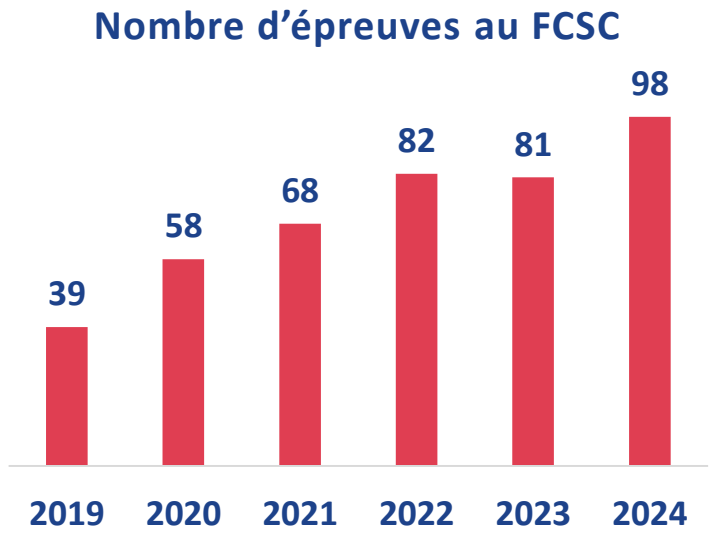
- **Apprendre quelque chose lors de la résolution**
- Eviter la présence de solutions inattendues
- Eviter le « guessing » au maximum
- Originalités des sujets (hors « intro »)
- Catégories originales représentatives des métiers de l'ANSSI (SCA/FI, Radio)
- Concepteurs externes ANSSI pour certaines épreuves



Conception des épreuves

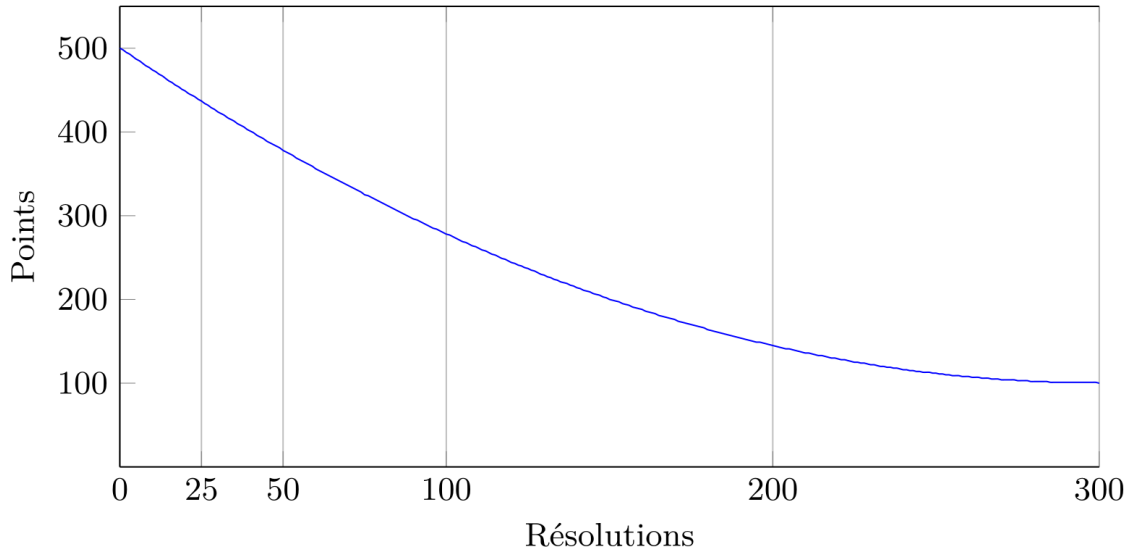
> Objectifs dans la phase de conception

- **Apprendre quelque chose lors de la résolution**
- Eviter la présence de solutions inattendues
- Eviter le « guessing » au maximum
- Originalités des sujets (hors « intro »)
- Catégories originales représentatives des métiers de l'ANSSI (SCA/FI, Radio)
- Concepteurs externes ANSSI pour certaines épreuves



> Evaluation de la difficulté

- Evaluation lors de la conception/test
  - Difficultés affichées : ★, ★★ ou ★★★
- Score dynamique
  - Le score décroît avec les résolutions
  - Supprime le biais des concepteurs



Aléas lors de la conception des épreuves

« Pain in the Hash » : épreuve crypto au FCSC 2023

- Idée initiale et conception fin 2022

```python
S = set()
for _ in range(55):
    m = input()
    if m == "": break
    S.add(bytes.fromhex(m))
r = reduce(xor, map(SHA256, S))
if r == b"\x00" * 32:
    print(open("flag.txt").read())
```

Pain in the Hash (FCSC 2023, code simplifié)

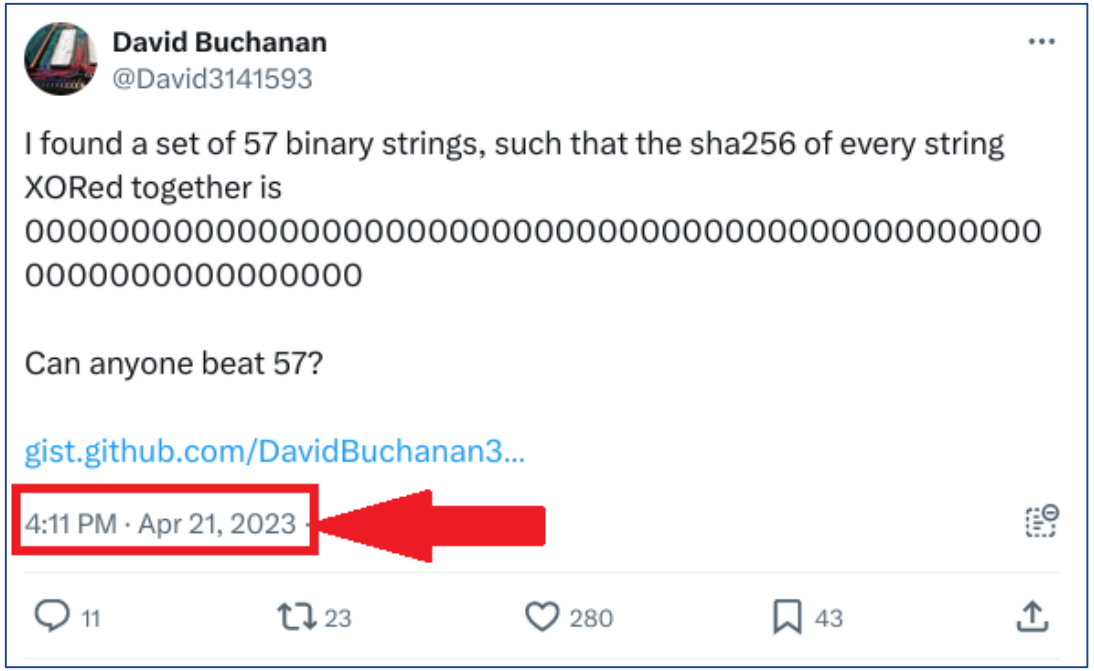
Aléas lors de la conception des épreuves

« Pain in the Hash » : épreuve crypto au FCSC 2023

- Idée initiale et conception fin 2022
- 2 heures après l'ouverture du FCSC, Retr0id tweet un problème crypto
- Exactement le sujet de cette épreuve du FCSC, 1 solution valide est publiée

```python
S = set()
for _ in range(55):
    m = input()
    if m == "": break
    S.add(bytes.fromhex(m))
r = reduce(xor, map(SHA256, S))
if r == b"\x00" * 32:
    print(open("flag.txt").read())
```

Pain in the Hash (FCSC 2023, code simplifié)



https://twitter.com/David3141593/status/1649415552463503360

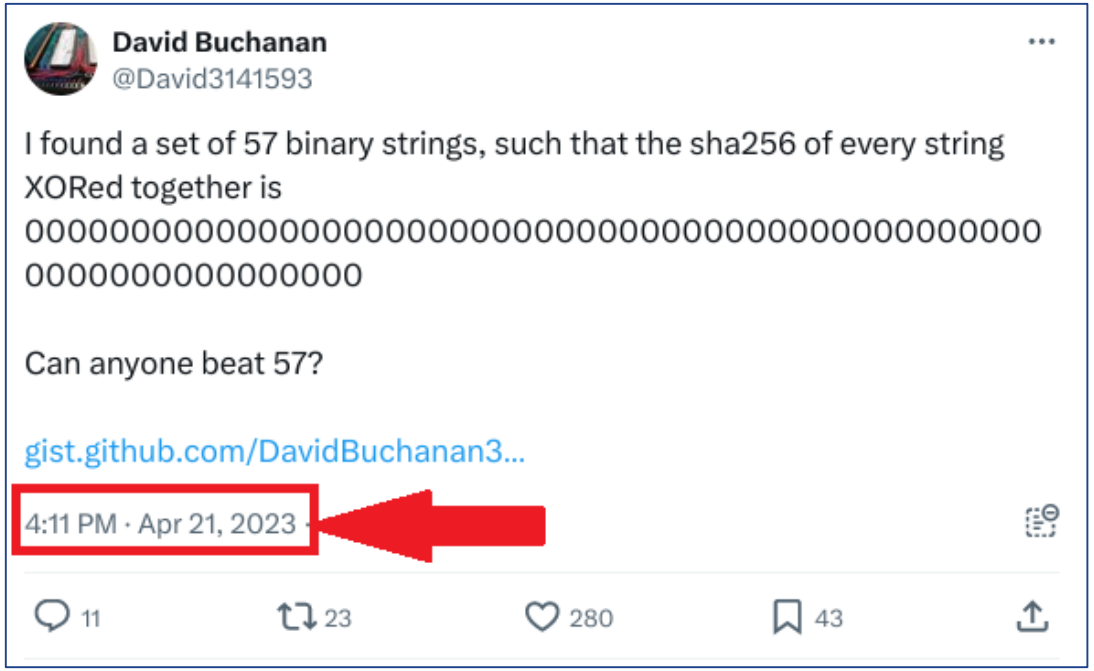
Aléas lors de la conception des épreuves

« Pain in the Hash » : épreuve crypto au FCSC 2023

- Idée initiale et conception fin 2022
- 2 heures après l'ouverture du FCSC, Retr0id tweet un problème crypto
- Exactement le sujet de cette épreuve du FCSC, 1 solution valide est publiée
- **Décision :** *blacklist* de la solution publique
- **Contact avec Retr0id :** il accepte de ne pas publier d'autres solutions au problème

```python
S = set()
for _ in range(55):
    m = input()
    if m == "": break
    S.add(bytes.fromhex(m))
r = reduce(xor, map(SHA256, S))
if r == b"\x00" * 32:
    print(open("flag.txt").read())
```

Pain in the Hash (FCSC 2023, code simplifié)



https://twitter.com/David3141593/status/1649415552463503360

Aléas lors de la conception des épreuves

« File Checker » : épreuve pwn au FCSC 2024

- Epreuve difficile de corruption mémoire
- Dockerisation du challenge : changement du *layout* mémoire

Aléas lors de la conception des épreuves

« File Checker » : épreuve pwn au FCSC 2024

- Epreuve difficile de corruption mémoire
- Dockerisation du challenge : changement du *layout* mémoire
- **Bug :** *mmap* n'appelle pas la même fonction *get_unmapped_area* selon que la libc est montée sur un système de fichiers ext4 ou un overlayfs

```
const struct file_operations ext4_file_operations = {
        .llseek         = ext4_llseek,
        .read_iter      = ext4_file_read_iter,
        .write_iter     = ext4_file_write_iter,
        .iopoll         = iocb_bio_iopoll,
        .unlocked_ioctl = ext4_ioctl,
#ifdef CONFIG_COMPAT
        .compat_ioctl   = ext4_compat_ioctl,
#endif
        .mmap           = ext4_file_mmap,
        .mmap_supported_flags = MAP_SYNC,
        .open           = ext4_file_open,
        .release        = ext4_release_file,
        .fsync          = ext4_sync_file,
        .get_unmapped_area = thp_get_unmapped_area,
        .splice_read    = ext4_file_splice_read,
        .splice_write   = iter_file_splice_write,
        .fallocate      = ext4_fallocate,
};
```

https://elixir.bootlin.com/linux/latest/source/fs/ext4/file.c#L945

```
static const struct file_operations shmem_file_operations = {
        .mmap           = shmem_mmap,
        .open           = shmem_file_open,
        .get_unmapped_area = shmem_get_unmapped_area,
#ifdef CONFIG_TMPFS
        .llseek         = shmem_file_llseek,
        .read_iter      = shmem_file_read_iter,
        .write_iter     = shmem_file_write_iter,
        .fsync          = noop_fsync,
        .splice_read    = shmem_file_splice_read,
        .splice_write   = iter_file_splice_write,
        .fallocate      = shmem_fallocate,
#endif
};
```

https://elixir.bootlin.com/linux/latest/source/mm/shmem.c#L4532

Aléas lors de la conception des épreuves

« File Checker » : épreuve pwn au FCSC 2024

- Epreuve difficile de corruption mémoire
- Dockerisation du challenge : changement du *layout* mémoire
- **Bug :** *mmap* n'appelle pas la même fonction *get_unmapped_area* selon que la libc est montée sur un système de fichiers ext4 ou un overlayfs
- **Fix :** stockage de la libc en ext4 dans la microVM puis montage d'un volume en read-only dans le conteneur

```
const struct file_operations ext4_file_operations = {
        .llseek         = ext4_llseek,
        .read_iter      = ext4_file_read_iter,
        .write_iter     = ext4_file_write_iter,
        .iopoll         = iocb_bio_iopoll,
        .unlocked_ioctl = ext4_ioctl,
#ifdef CONFIG_COMPAT
        .compat_ioctl   = ext4_compat_ioctl,
#endif
        .mmap           = ext4_file_mmap,
        .mmap_supported_flags = MAP_SYNC,
        .open           = ext4_file_open,
        .release        = ext4_release_file,
        .fsync          = ext4_sync_file,
        .get_unmapped_area = thp_get_unmapped_area,
        .splice_read    = ext4_file_splice_read,
        .splice_write   = iter_file_splice_write,
        .fallocate      = ext4_fallocate,
};
```

https://elixir.bootlin.com/linux/latest/source/fs/ext4/file.c#L945

```
static const struct file_operations shmem_file_operations = {
        .mmap           = shmem_mmap,
        .open           = shmem_file_open,
        .get_unmapped_area = shmem_get_unmapped_area,
#ifdef CONFIG_TMPFS
        .llseek         = shmem_file_llseek,
        .read_iter      = shmem_file_read_iter,
        .write_iter     = shmem_file_write_iter,
        .fsync          = noop_fsync,
        .splice_read    = shmem_file_splice_read,
        .splice_write   = iter_file_splice_write,
        .fallocate      = shmem_fallocate,
#endif
};
```

https://elixir.bootlin.com/linux/latest/source/mm/shmem.c#L4532

Aléas lors de la conception des épreuves

« C-3PO, R2-D2, R5-D4 » : épreuves forensics au FCSC 2022

- Epreuves forensics Android facile, moyenne et difficile, avec émulateur
- Développement d'un module noyau malveillant, qui **chiffre** les frappes au clavier
- Revue finale de l'épreuve par les pairs, deux jours avant le FCSC

Aléas lors de la conception des épreuves

« C-3PO, R2-D2, R5-D4 » : épreuves forensics au FCSC 2022

- Epreuves forensics Android facile, moyenne et difficile, avec émulateur
- Développement d'un module noyau malveillant, qui **chiffre** les frappes au clavier
- Revue finale de l'épreuve par les pairs, deux jours avant le FCSC

Aléas lors de la conception des épreuves

« C-3PO, R2-D2, R5-D4 » : revue par les pairs

Aléas lors de la conception des épreuves

« C-3PO, R2-D2, R5-D4 » : revue par les pairs

Cryptanalyse 27/04/2022 16:49

je teste rapidement de péter la crypto

Cryptanalyse 27/04/2022 16:53

```
from pwn import *
for x in open("/tmp/output", "rb").readlines():
    y = xor(b"F", xor(b64d("Gvzn1Ig="), b64d(x)))
    print(y[4:])
```

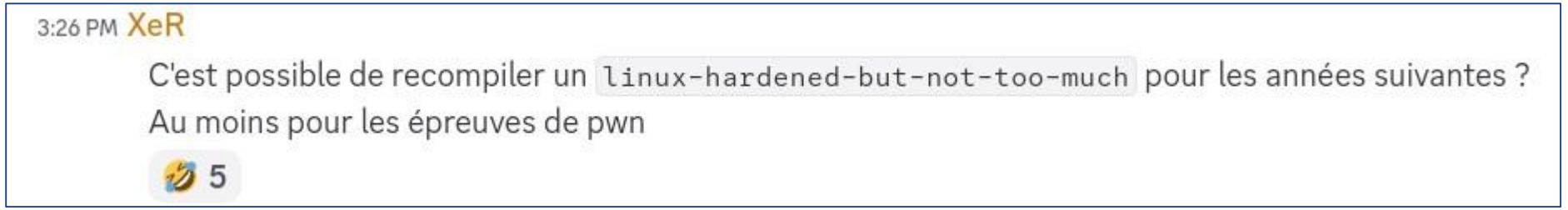
```
b'F'
b'C'
b'2\xc7'
b'S'
b'C'
```

Aléas lors de la conception des épreuves

« C-3PO, R2-D2, R5-D4 »

Sans oublier...

- Les épreuves que personne ne résout durant le FCSC :-(
- Les flags qui fuitent sur Discord ou sur Internet pendant le CTF
- L'utilisation de 1-day ou de 0-day
- Infra trop durcie (recompilation de noyau maison)
- ...



Infrastructure du FCSC

> **Infrastructure temporaire**

- En service 2 à 4 mois selon les éditions
- Décommissionnée après la fin du FCSC

> **Équipe restreinte**

- 1 à 3 personnes selon les éditions

Infrastructure du FCSC

> **Infrastructure temporaire**

- En service 2 à 4 mois selon les éditions
- Décommissionnée après la fin du FCSC

> **Équipe restreinte**

- 1 à 3 personnes selon les éditions

> **Cahier des charges classique**

- Haute disponibilité
- Sécurisée
- Facile à comprendre et administrer
- Déploiement automatisé

Infrastructure du FCSC

> **Infrastructure temporaire**

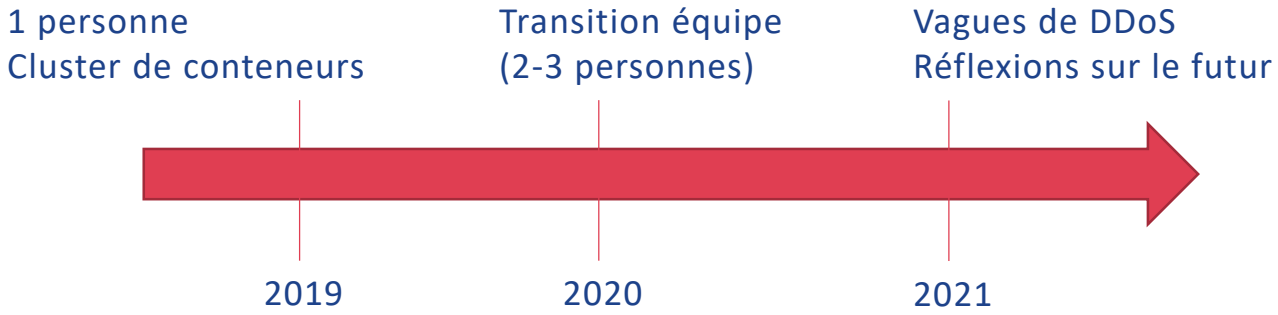
- En service 2 à 4 mois selon les éditions
- Décommissionnée après la fin du FCSC

> **Équipe restreinte**

- 1 à 3 personnes selon les éditions

> **Cahier des charges classique**

- Haute disponibilité
- Sécurisée
- Facile à comprendre et administrer
- Déploiement automatisé



En quoi cette infra est spéciale ?

> **Points communs**

- Hébergement d’applications vulnérables :’-)

- On se fait attaquer

En quoi cette infra est spéciale ?

> **Différences**

- Hébergement d'applications vulnérables :'-)
  - **On choisit (une partie de) nos vulnérabilités**
- On se fait attaquer
  - **On connaît (un partie) des attaquants**
    - Quand
    - Comment
    - Pourquoi

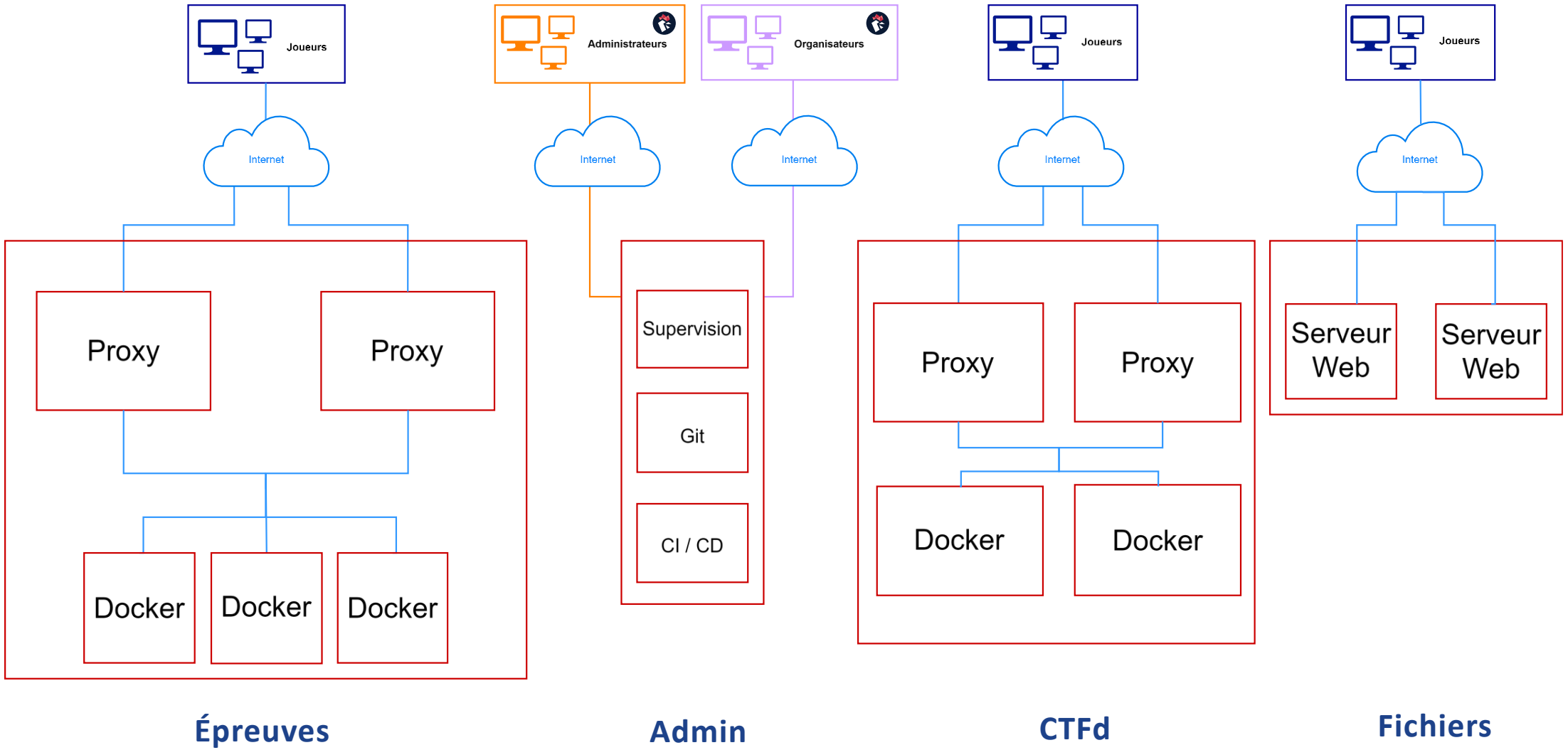
Super défi pour un sysadmin, il faut en profiter !

Fin 2021 : comment valoriser cette infra ?

> **Objectifs**

- Utiliser le FCSC comme un **laboratoire**, pour tester des idées en production
- Limiter l'impact des attaques **DoS/DDoS** sur les services (cf. 2021)
- **Simplifier** l'administration et l'investigation en production
- Priorité : la **sécurité**
  - Au détriment de la haute disponibilité si nécessaire (quelques secondes)

Architecture 2022



Fin 2022, on réfléchit à la suite

> **Constats**

- Les joueurs s'améliorent
  - La conteneurisation ne suffit plus
  - +70% temps : durcissement des épreuves
- Les (D)DoS rendent l'expérience frustrante
- Les admins veulent
  - Dormir plus tranquillement
  - Tester de nouvelles architectures (s'amuser)

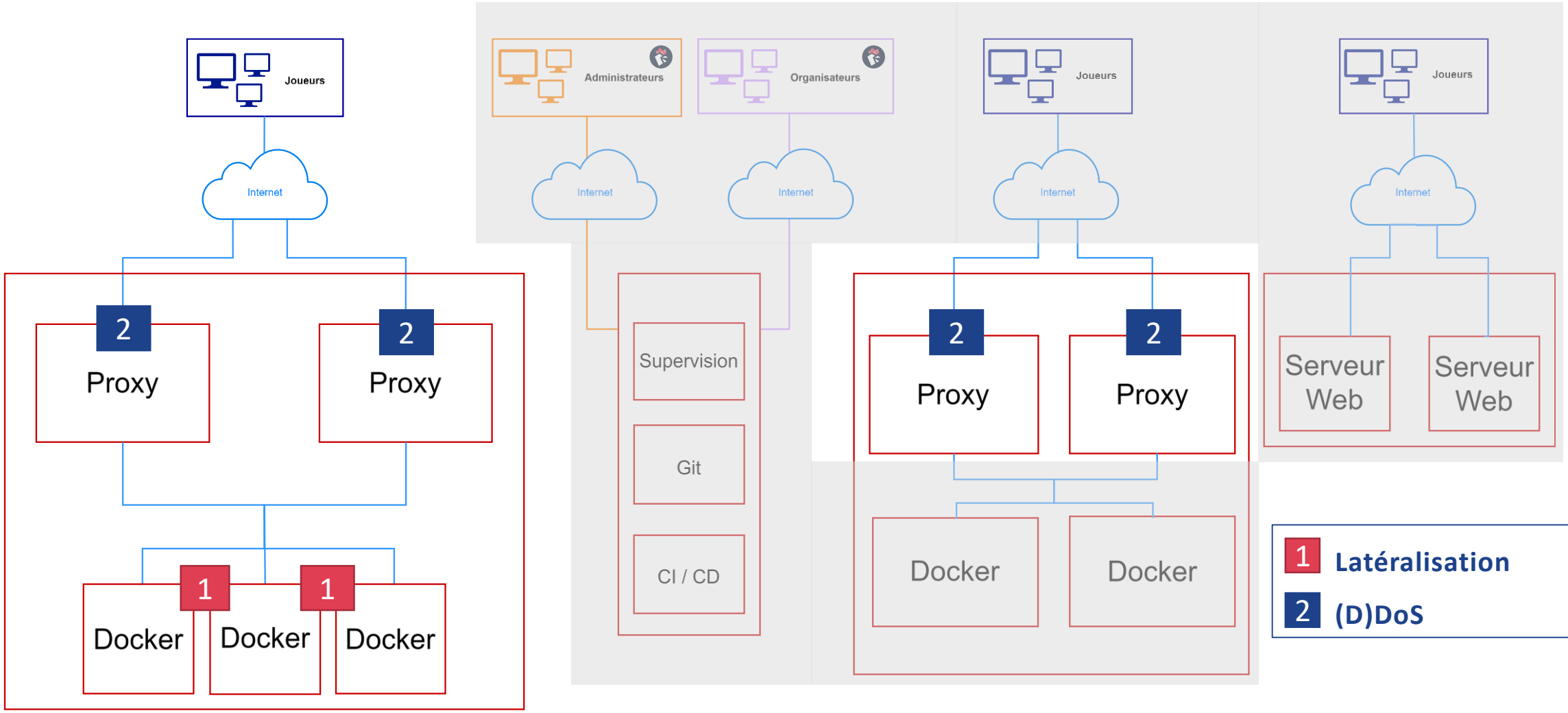
> **Deux risques** à adresser

1. **Latéralisation entre les épreuves**
2. **(D)DoS**

> **Fil rouge**

- Limiter l'augmentation des ressources nécessaires

Parties de l'infrastructure abordées



Architecture 2023 : latéralisation entre les épreuves

> **Solution** 1

- Utilisation de **microVM** (QEMU allégé)
  - Amélioration du cloisonnement
  - Faible consommation de ressources
- Implémentation retenue : **Firecracker** (AWS)
- Solution brute, nécessite une intégration
  - création interfaces réseau, kernel, rootfs

Architecture 2023 : latéralisation entre les épreuves

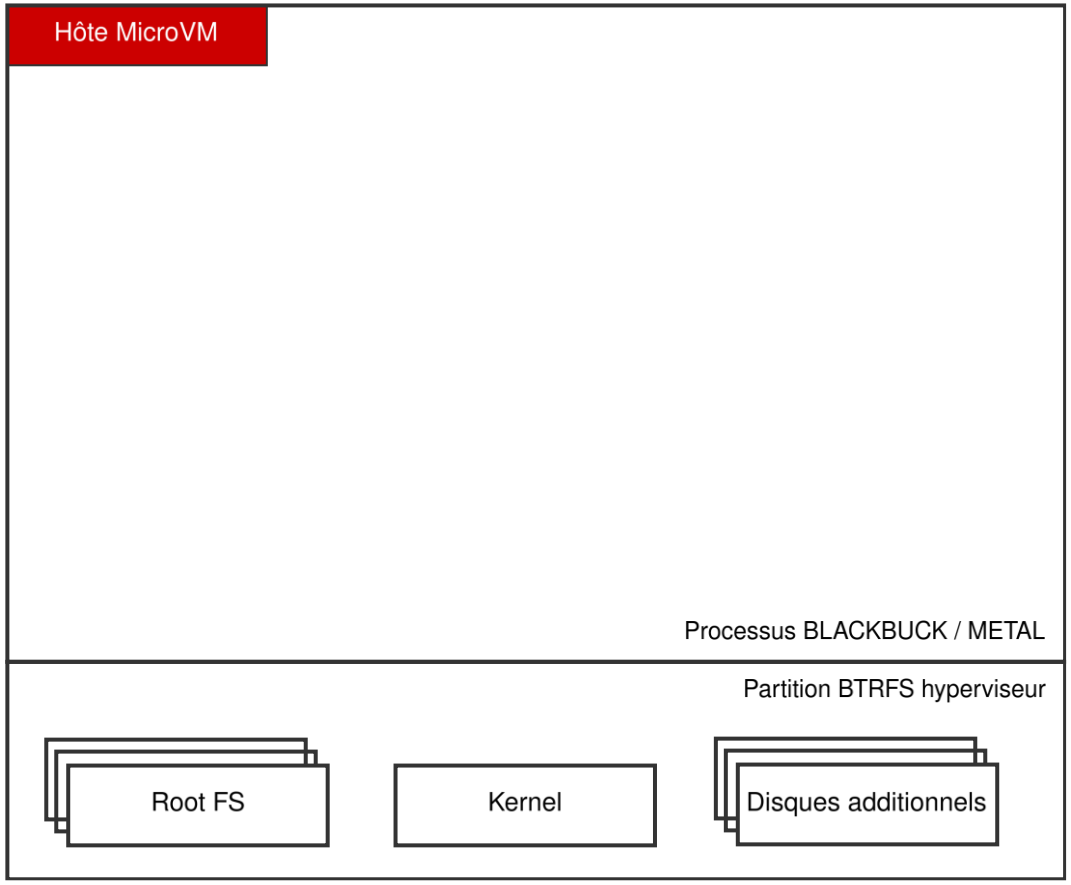
> **Solution** 1

- Utilisation de **microVM** (QEMU allégé)
  - Amélioration du cloisonnement
  - Faible consommation de ressources
- Implémentation retenue : **Firecracker** (AWS)
- Solution brute, nécessite une intégration
  - création interfaces réseau, kernel, rootfs

> **Comment intégrer des microVM à l'infra ?**

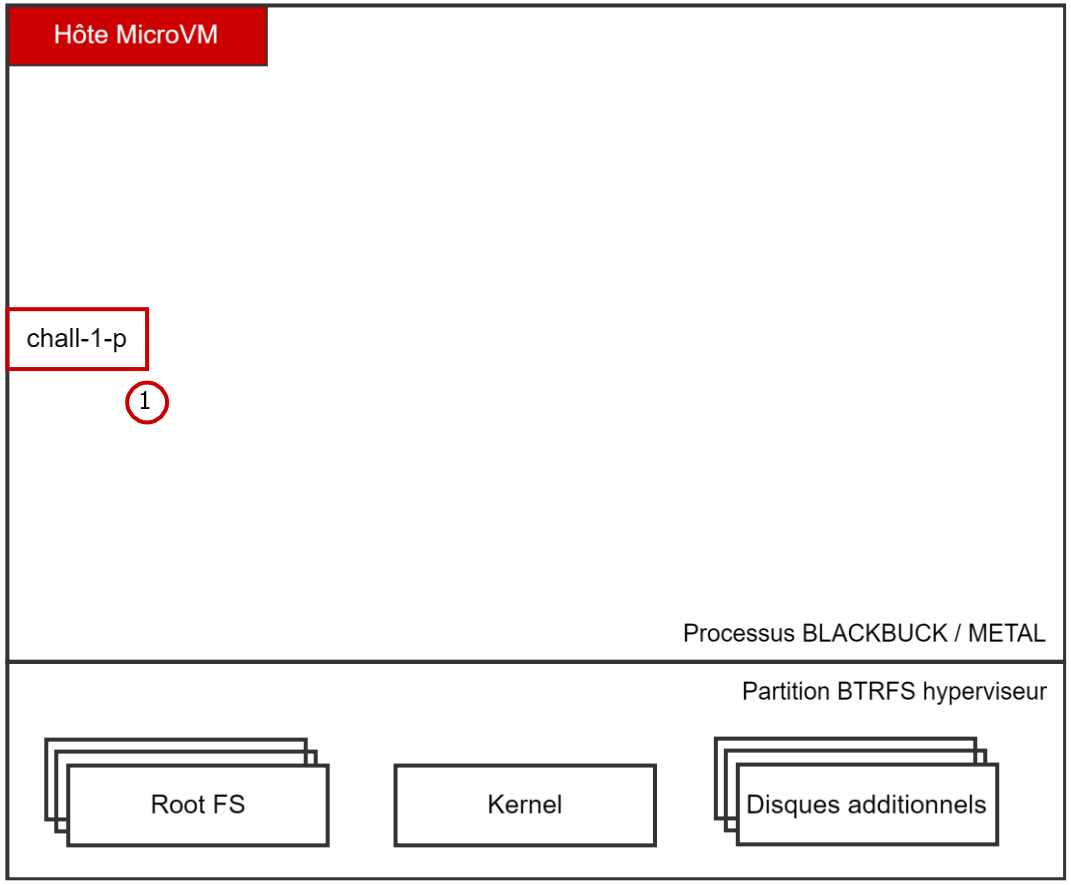
- Revue de solutions existantes
  - Non adaptées à notre situation
- Script Bash
  - Difficilement maintenable
- **Solution retenue :** développement maison
  - API pour la création de microVM et de leurs ressources
  - Deux versions interchangeables
    - Rust (Blackbuck) et Golang (Metal)
- Conteneurisation : moins une frontière de sécurité qu'un outil de développement

MicroVM : hôte des VM



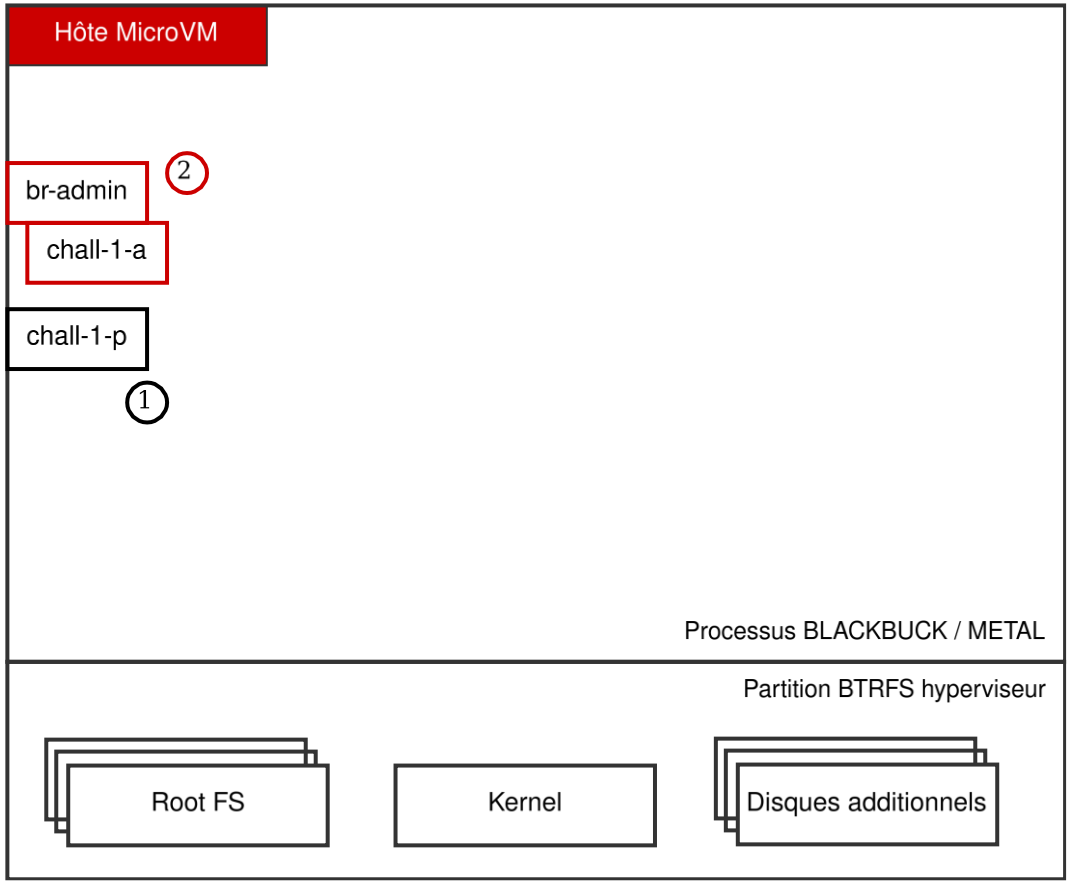

```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : hôte des VM



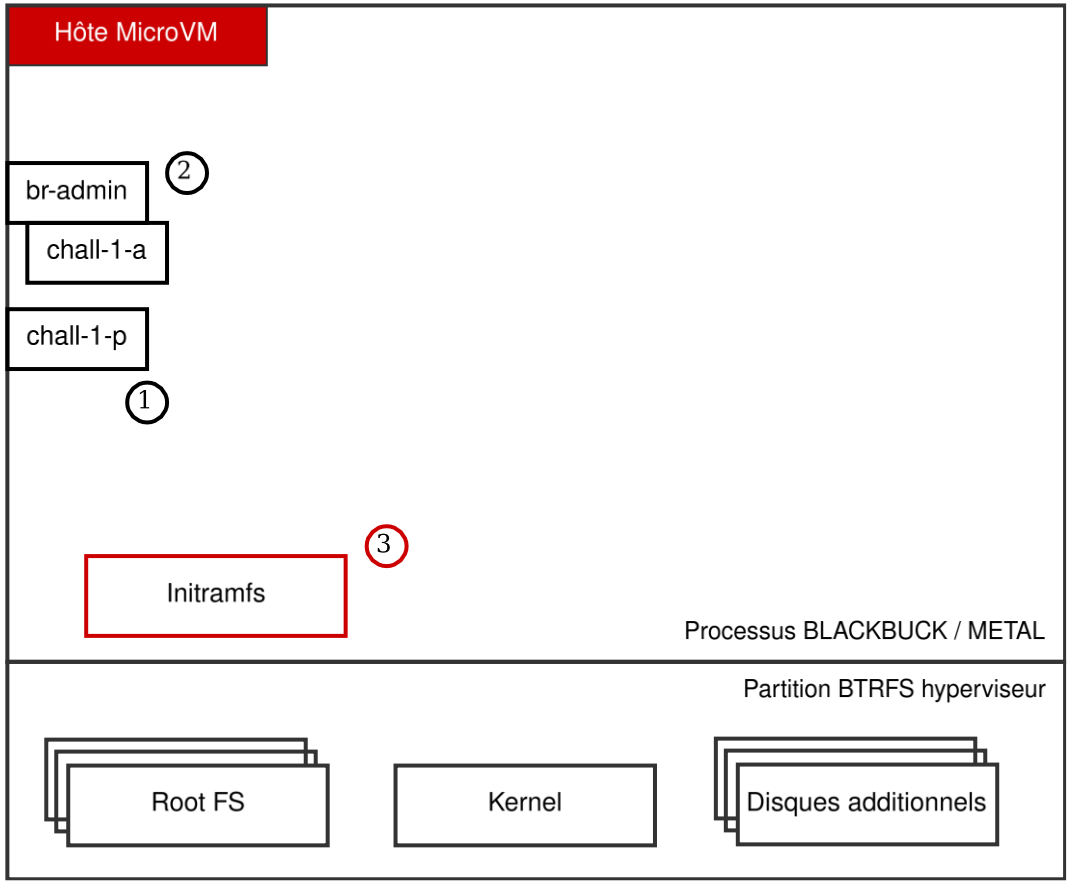

```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : hôte des VM



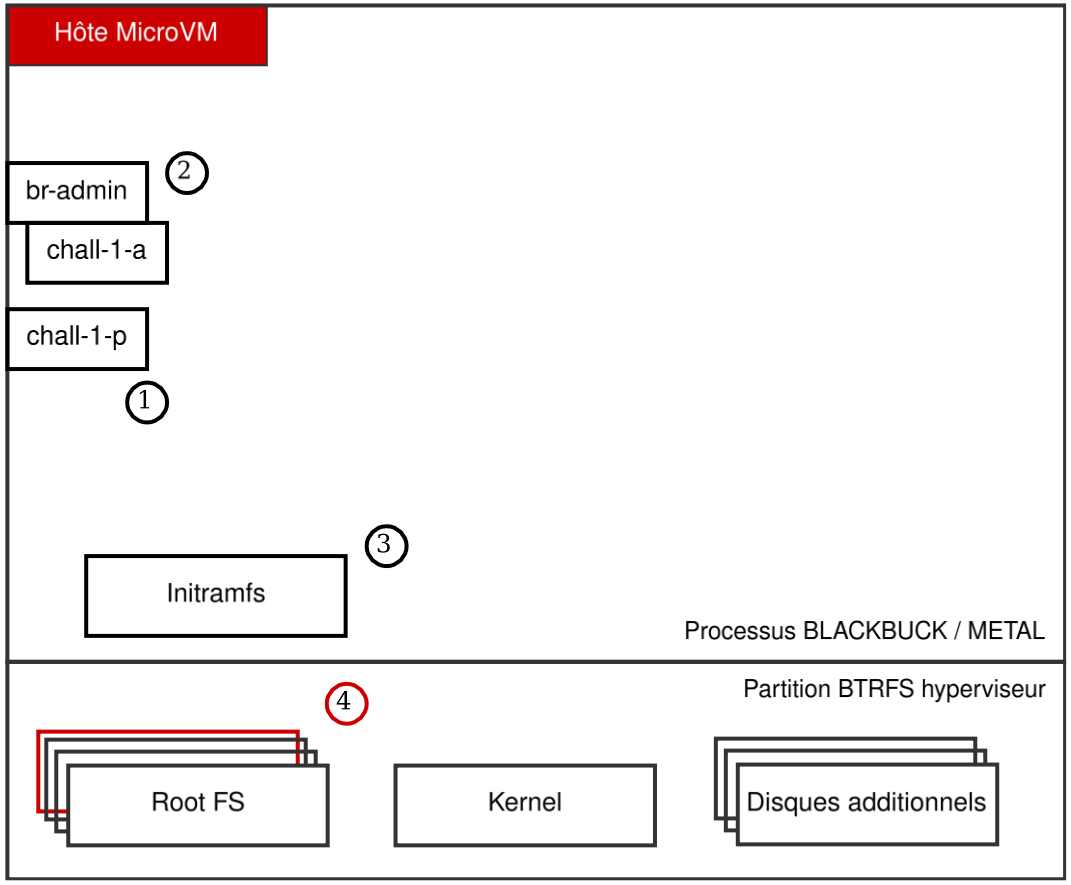

```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : hôte des VM



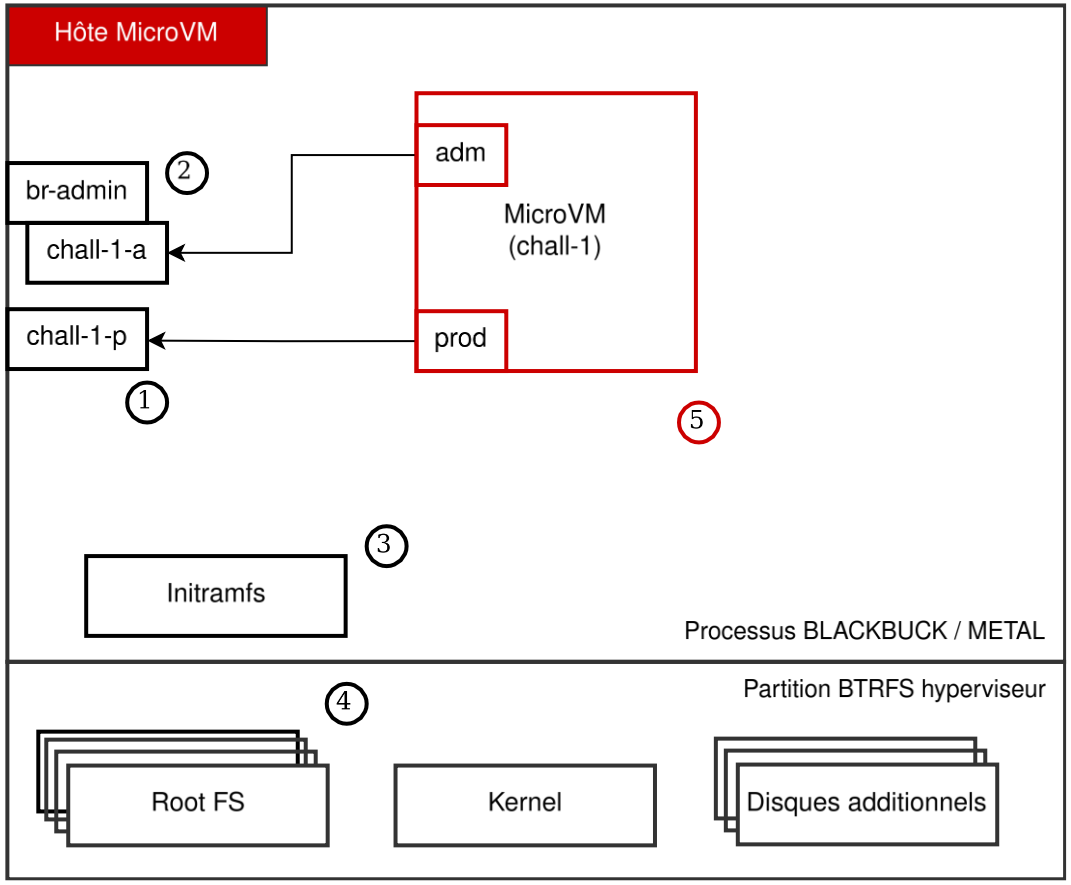

```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : hôte des VM




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

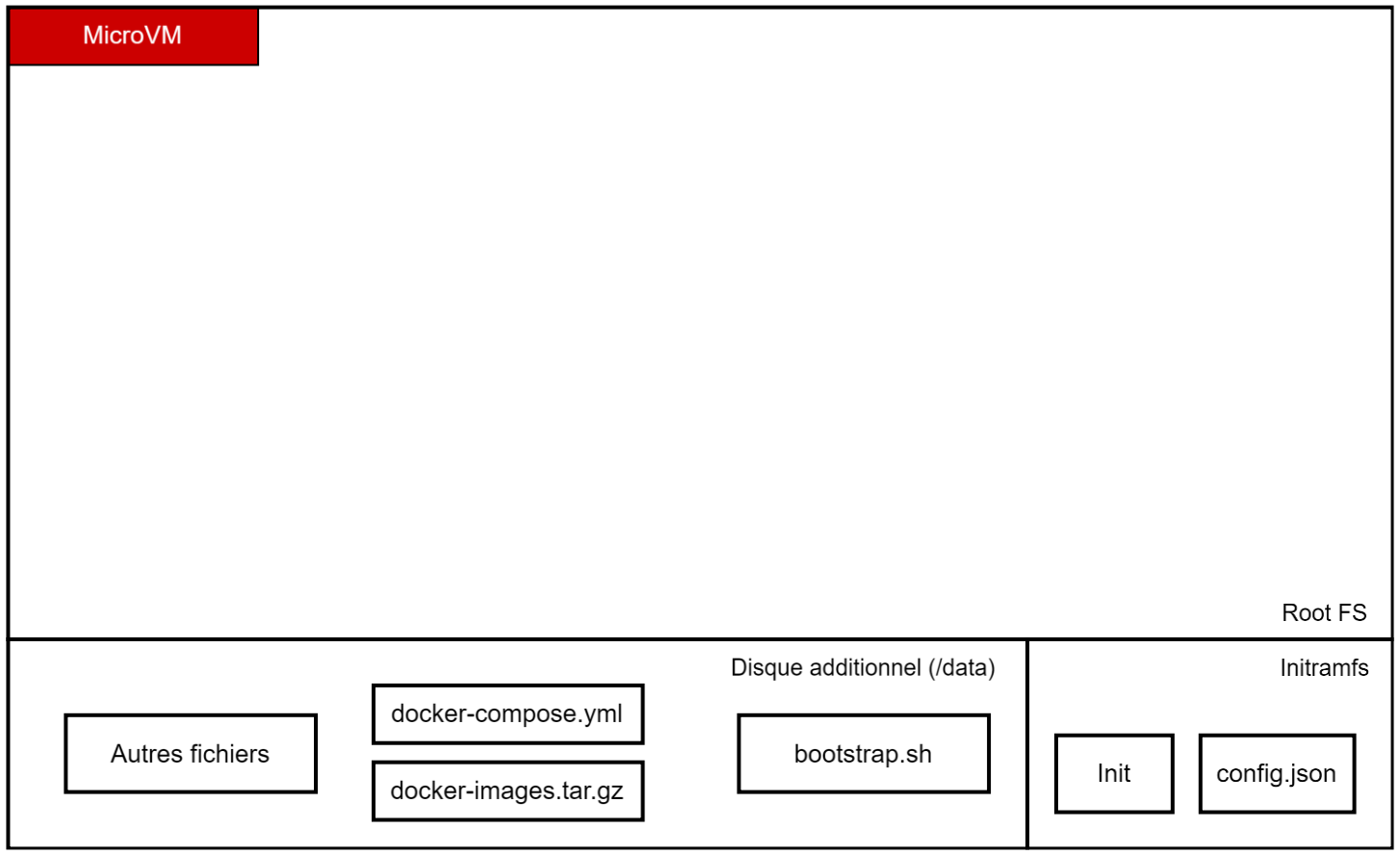
MicroVM : hôte des VM




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

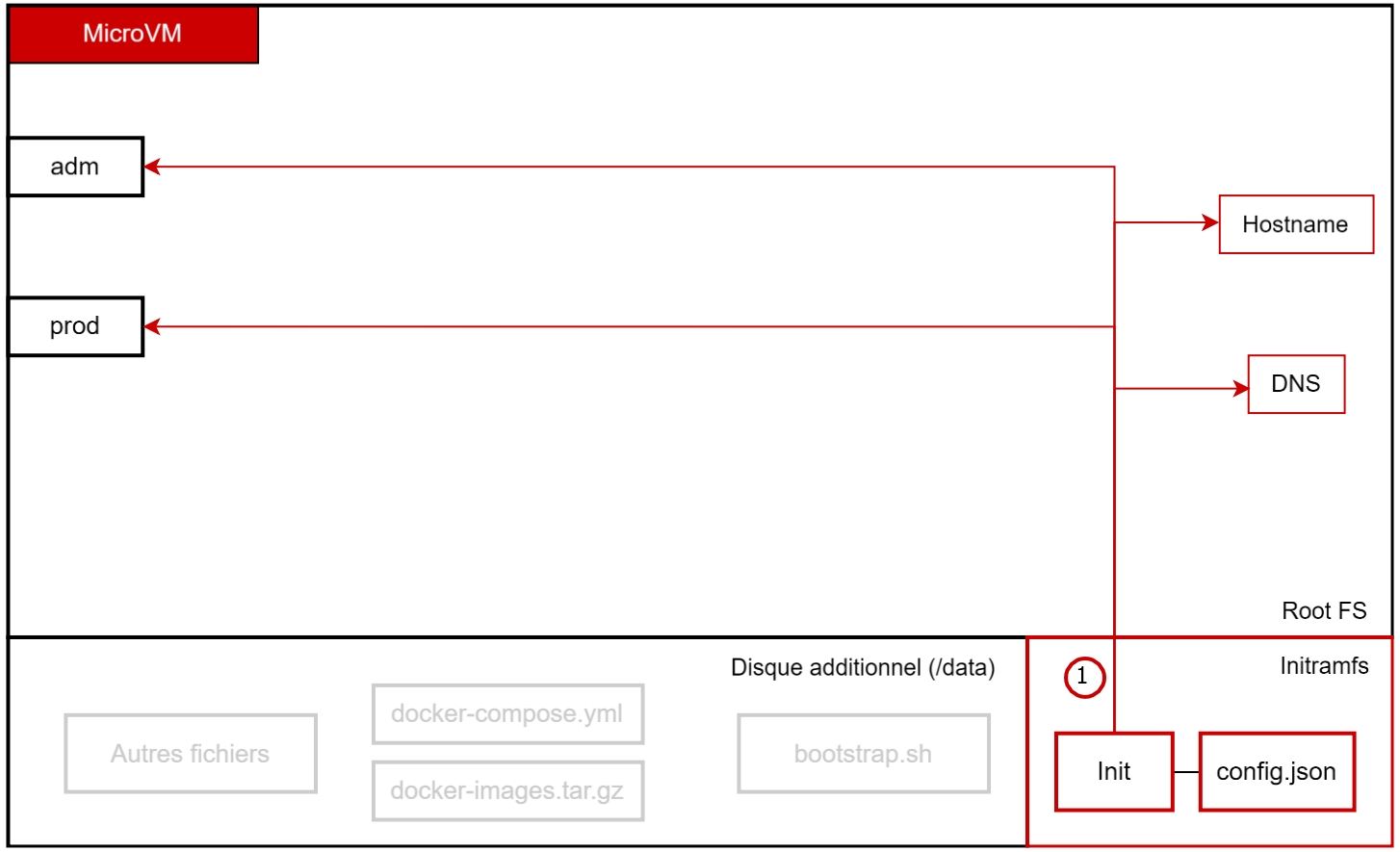
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

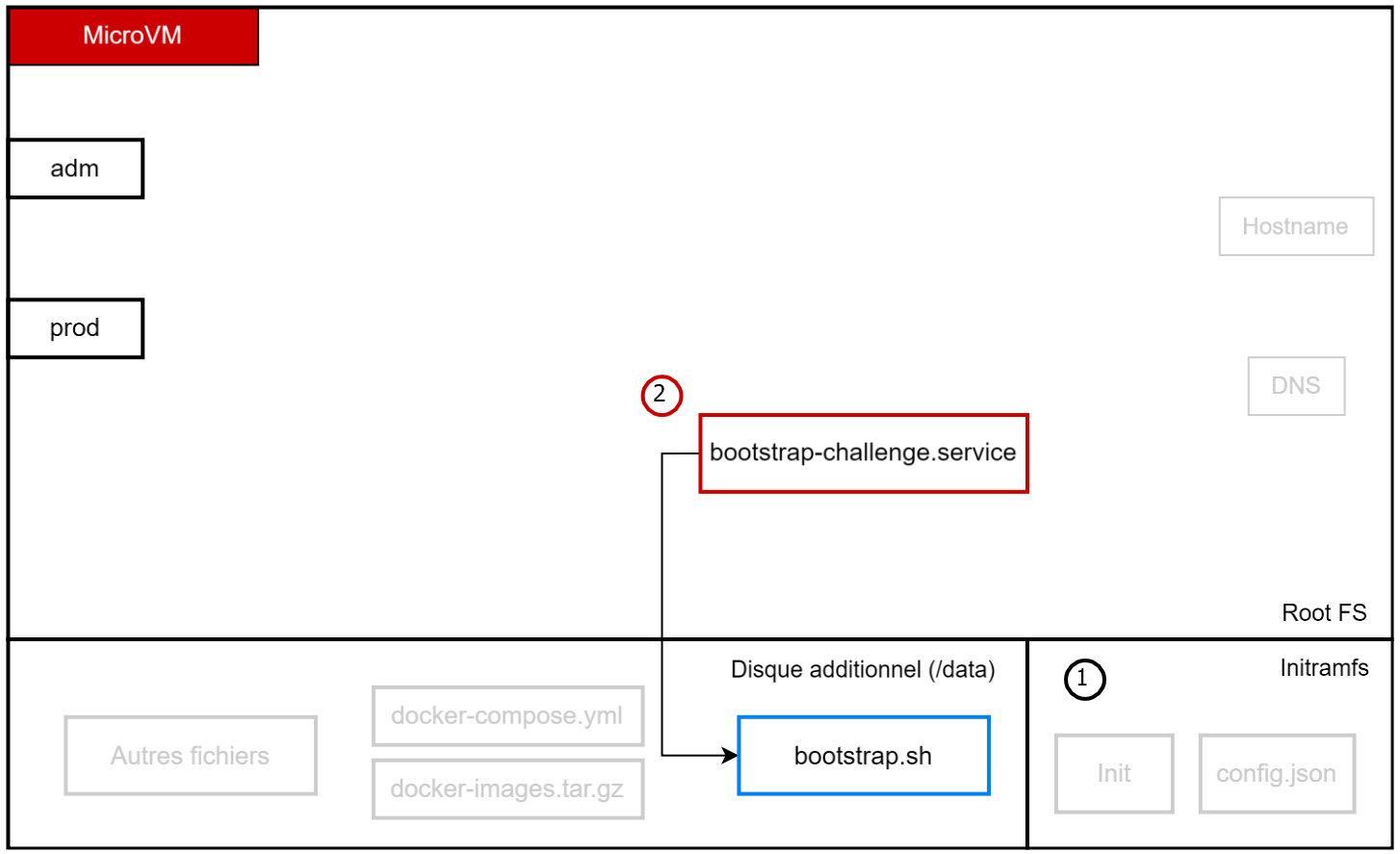
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

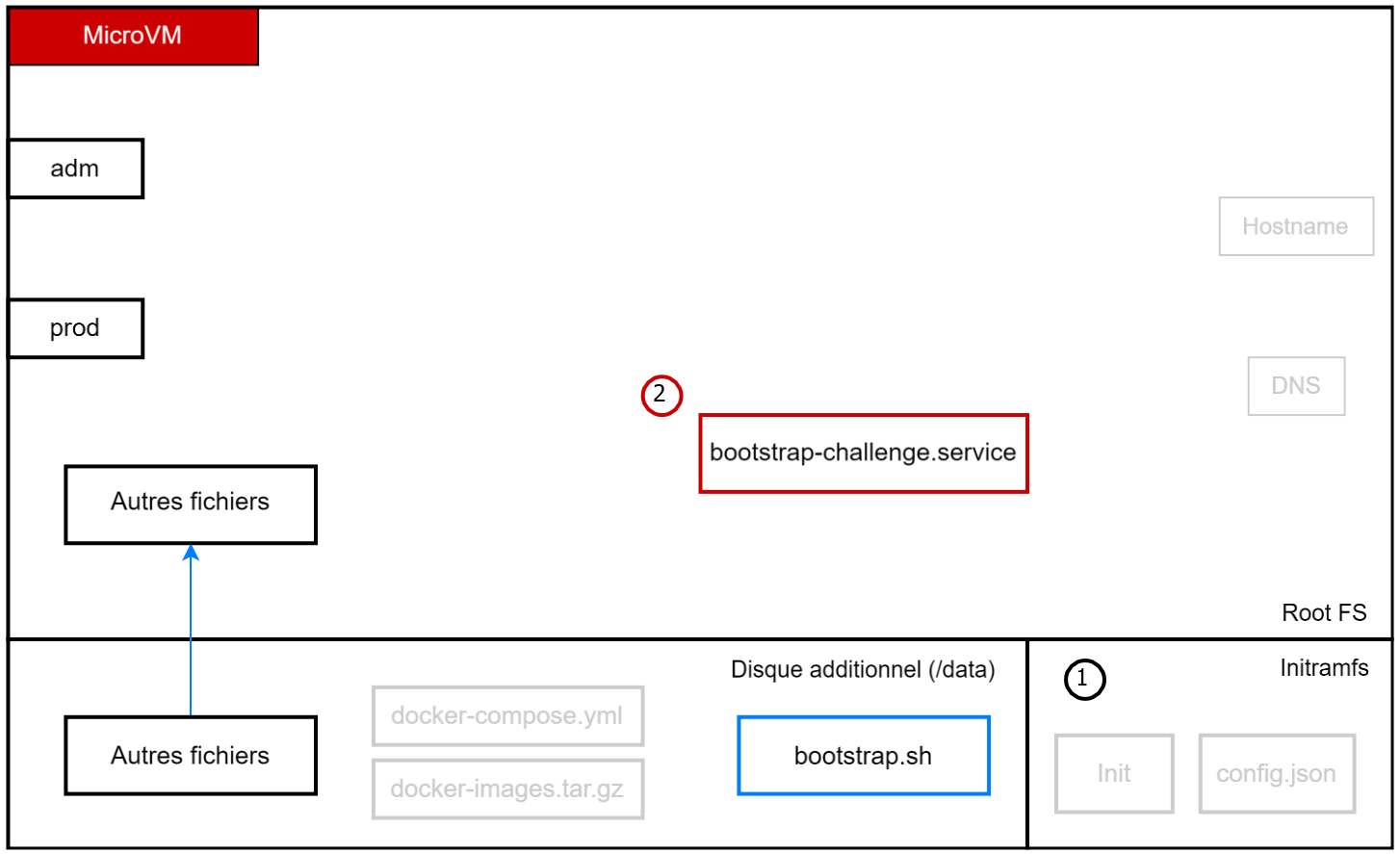
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

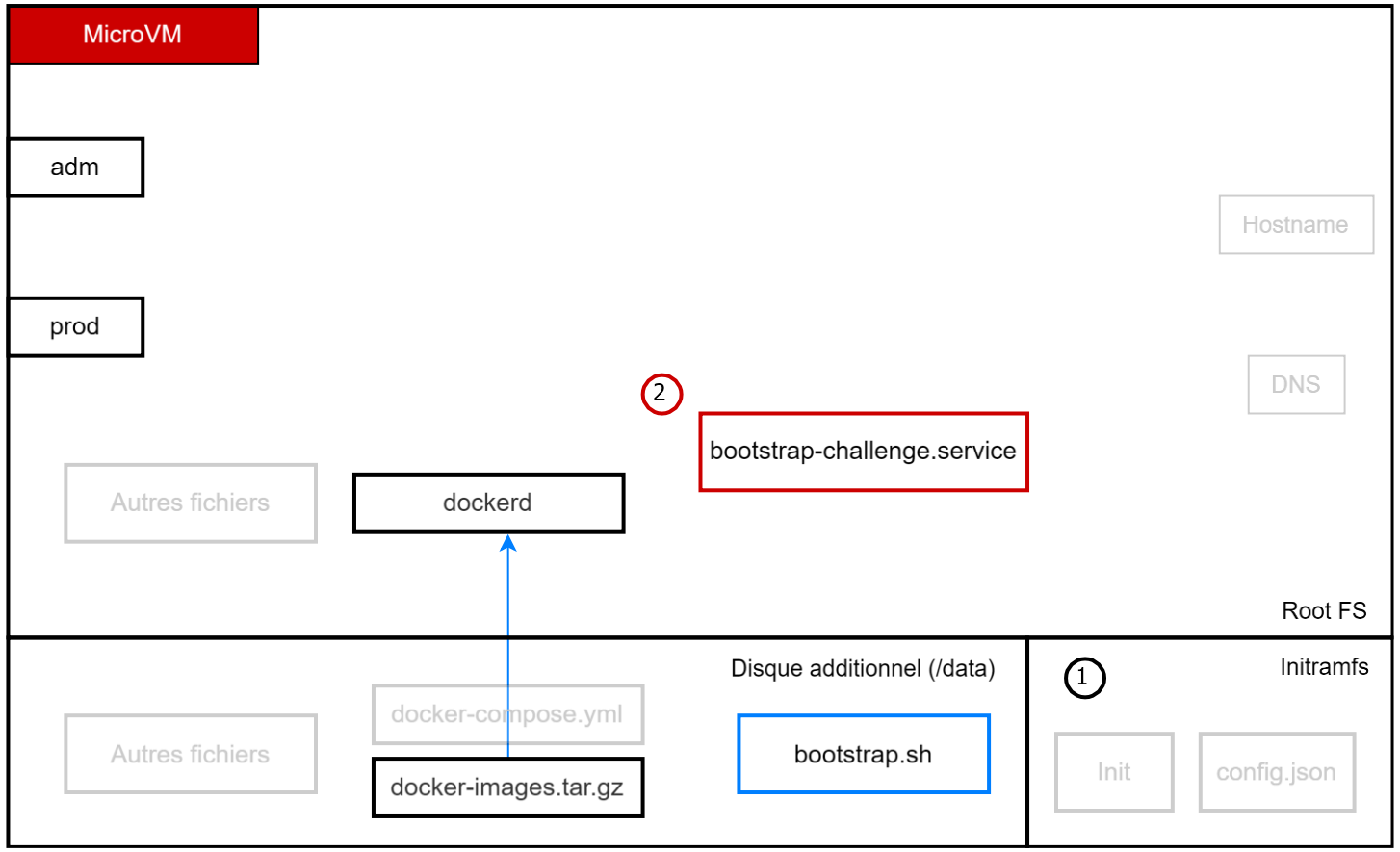
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

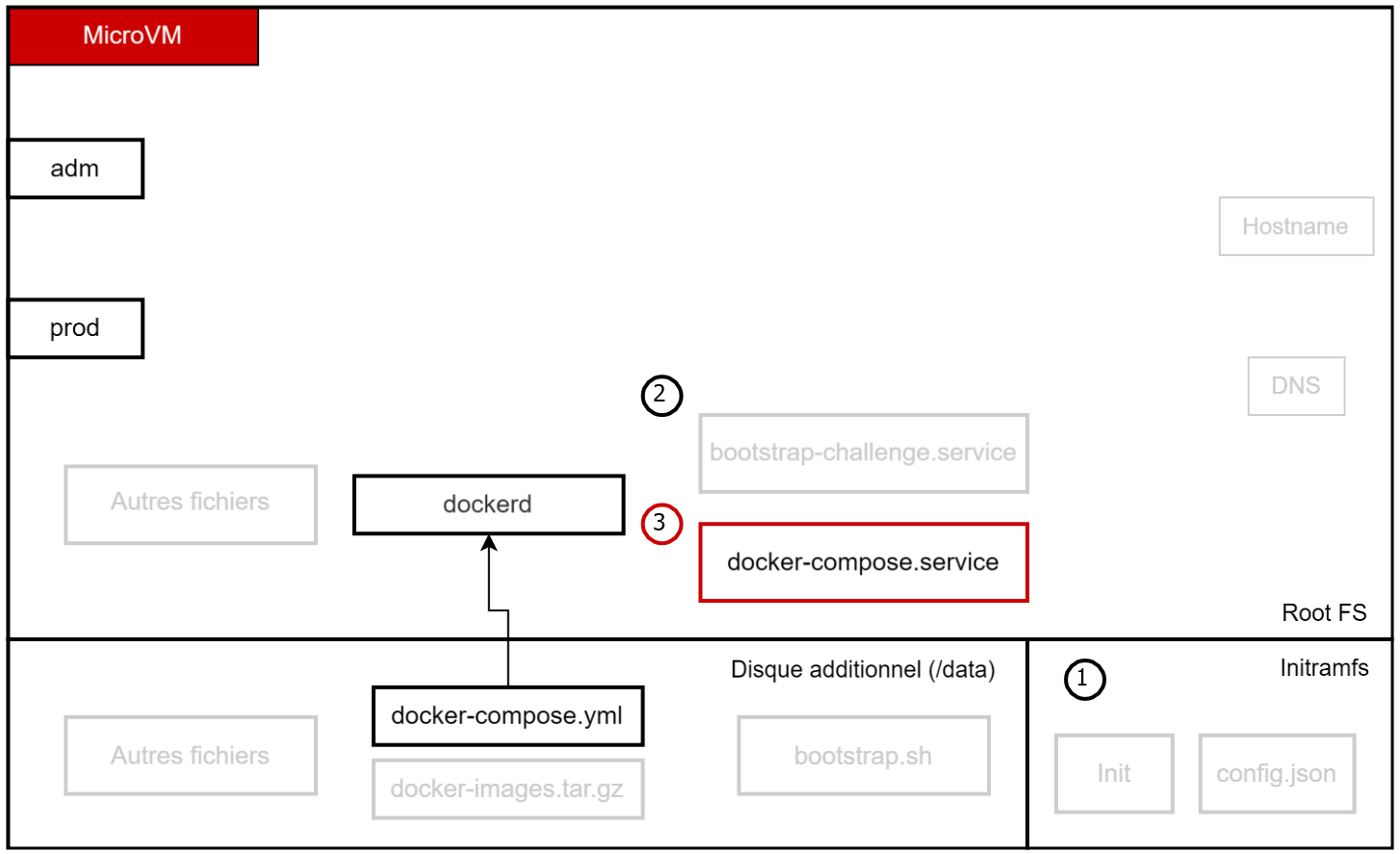
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

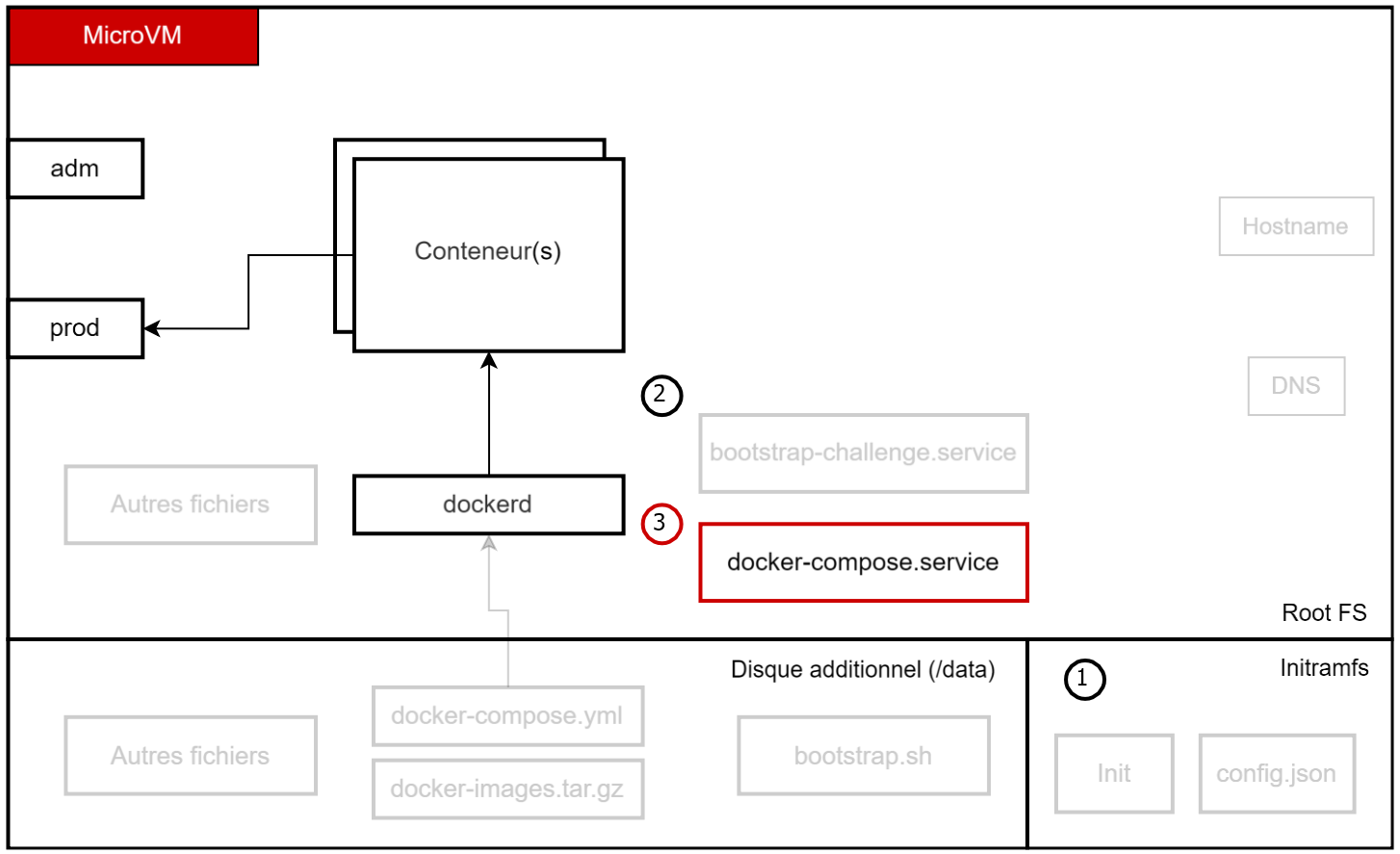
> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

MicroVM : démarrage de la VM

> Aucun accès à Internet




```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "guest_dev": "eth1",
      "host_dev": "file-chk-a",
      "ip_configs": [
        {
          "host_net": "172.16.98.12/24",
          "guest_net": "192.168.98.12/24",
          "network": "chall-adm"
        }
      ]
    }
  ],
  "additional_drives": [
    {
      "id": "docker",
      "read_only": true,
      "device_path": "/data/disks/file-checker/docker.ext4",
      "mount_point": "/data/bootstrap"
    }
  ],
  "kernel": "hardened/6.7/vmlinux.bin",
  "rootfs": "debian.ext4",
  "rootfs_overlay": false,
  "disk_size": "5 GiB",
  "resources": {
    "ram_size": "1 GiB",
    "vcpu": 1
  },
  "dns": [
    "8.8.8.8",
    "1.1.1.1"
  ]
}
```

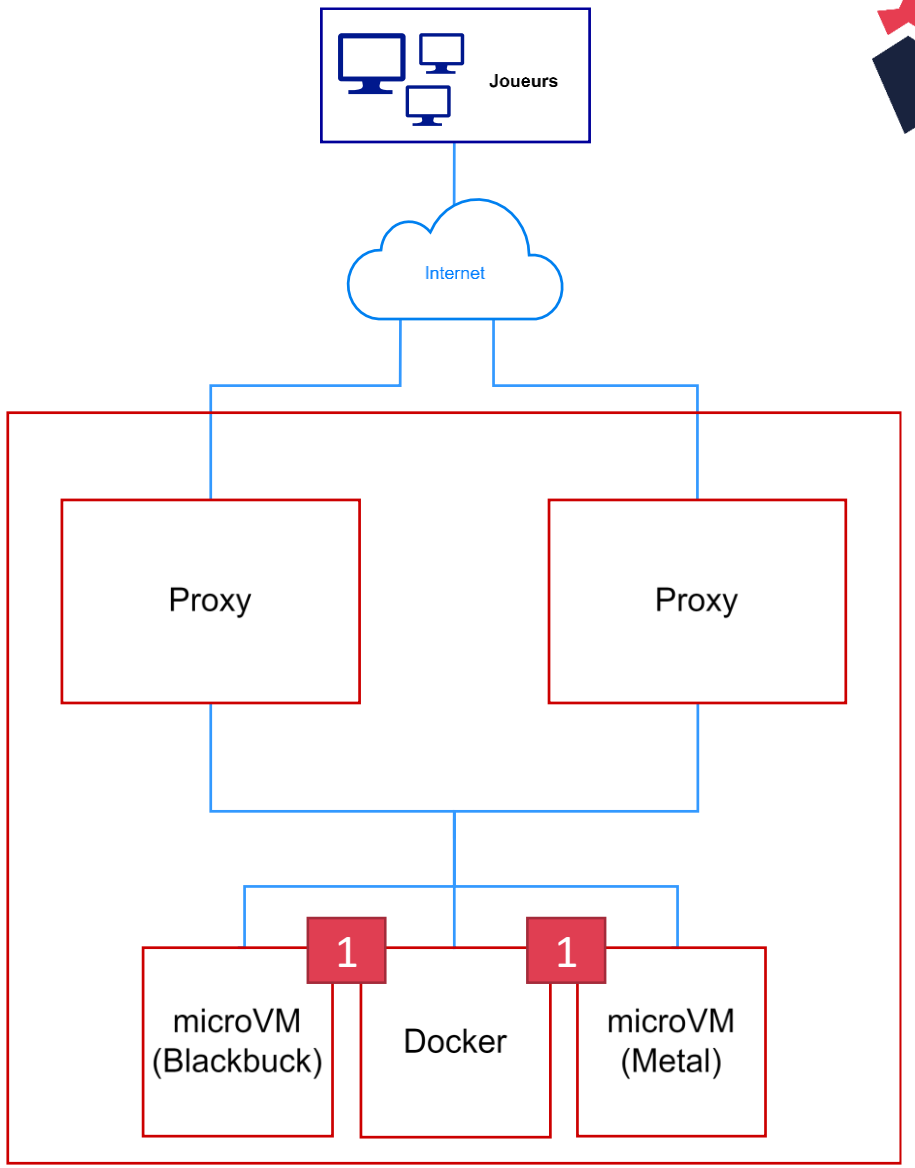
Architecture 2023

> **Édition 2023**

- Hybride conteneurs / microVM
- Solutions de microVM interchangeables

> **Retour d'expérience**

- Fonctionne bien
- Complètement transparent
- Aucune intervention en phase de production



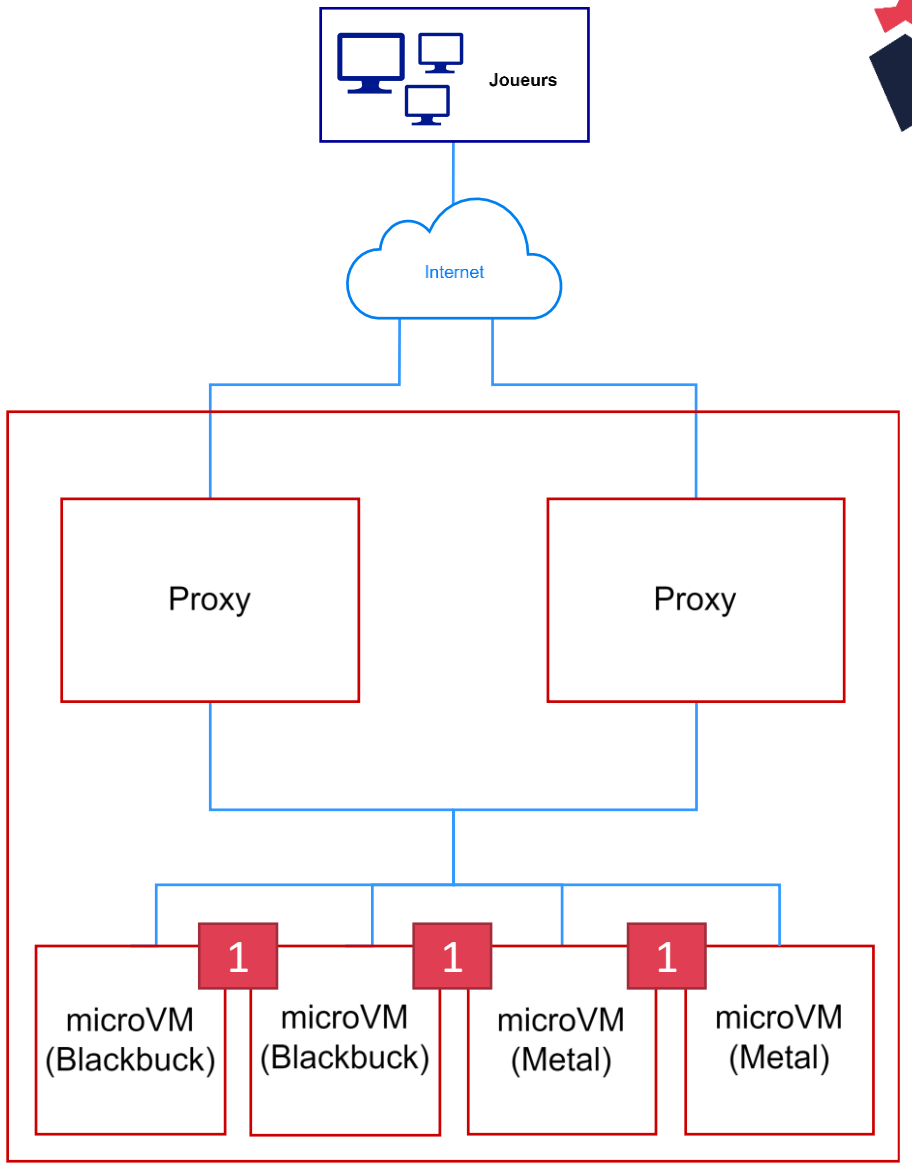
Architecture 2024

> **2024**

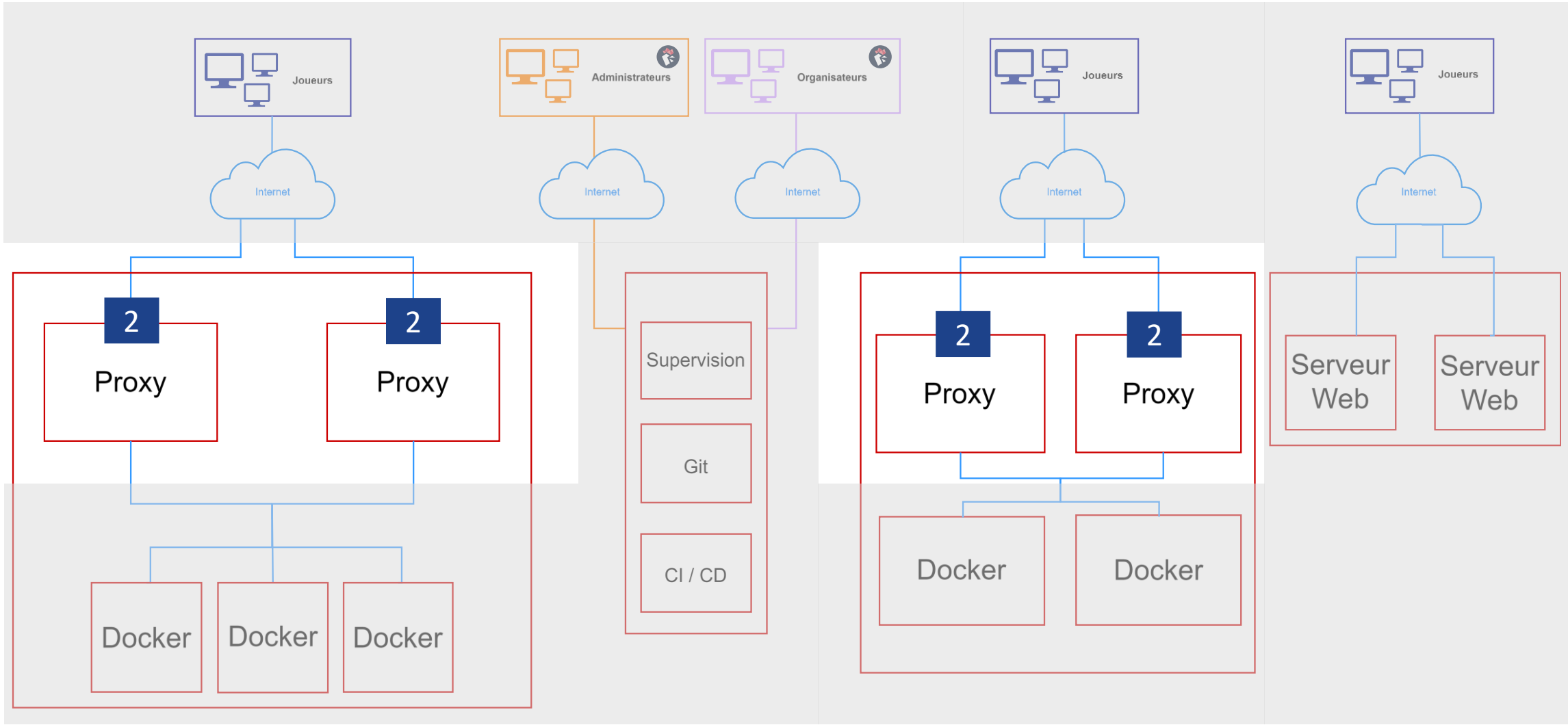
- Épreuves hébergées exclusivement dans des microVM
- Environ 50 épreuves en ligne (~200 VM avec la redondance)
- +1000 microVM déployées (tests, corrections, …)

> **Par serveur physique**

- 36 GB de disque (+200 GB en données brutes)
  - Au minimum 5 GB de disque par VM
  - Merci le *copy-on-write*
- Environ 50 GB de RAM (souvent 1 GB/VM)



Protection DDoS 2



Protection DDoS - 2021

> **Problématique**

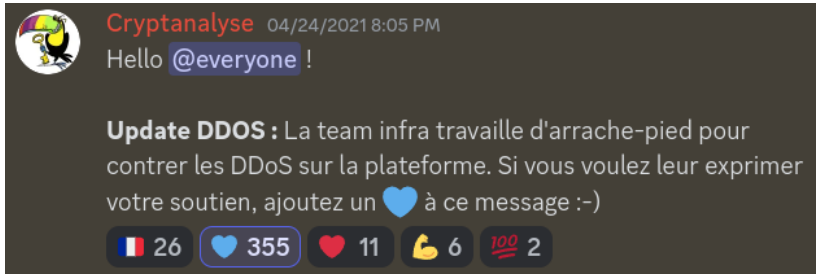
- Plusieurs DDoS dans les premières 48 heures
- Instabilités voire indisponibilités

> **Constat**

- Ciblage du CTFd
- Pas de protection applicative (serveurs physiques)
- La protection réseau de l'hébergeur ne suffit pas

> **Solution de secours**

- Modification en production sur l'infra
- Isolation du CTFd
- Renforcement du *rate-limiting* + *fail2ban*



Protection DDoS - 2021

> **Résultat**

- Nouvelles vagues de DDoS largement atténuées
- Limitations des outils
  - Performances limitées de *fail2ban*

Protection DDoS - 2021

> **Résultat**

- Nouvelles vagues de DDoS largement atténuées
- Limitations des outils
  - Performances limitées de *fail2ban*

> **Besoin d'un outil de protection au niveau applicatif**

- Actif **avant** la protection réseau hébergeur

Protection DDoS - 2021

> **Résultat**

- Nouvelles vagues de DDoS largement atténuées
- Limitations des outils
  - Performances limitées de *fail2ban*

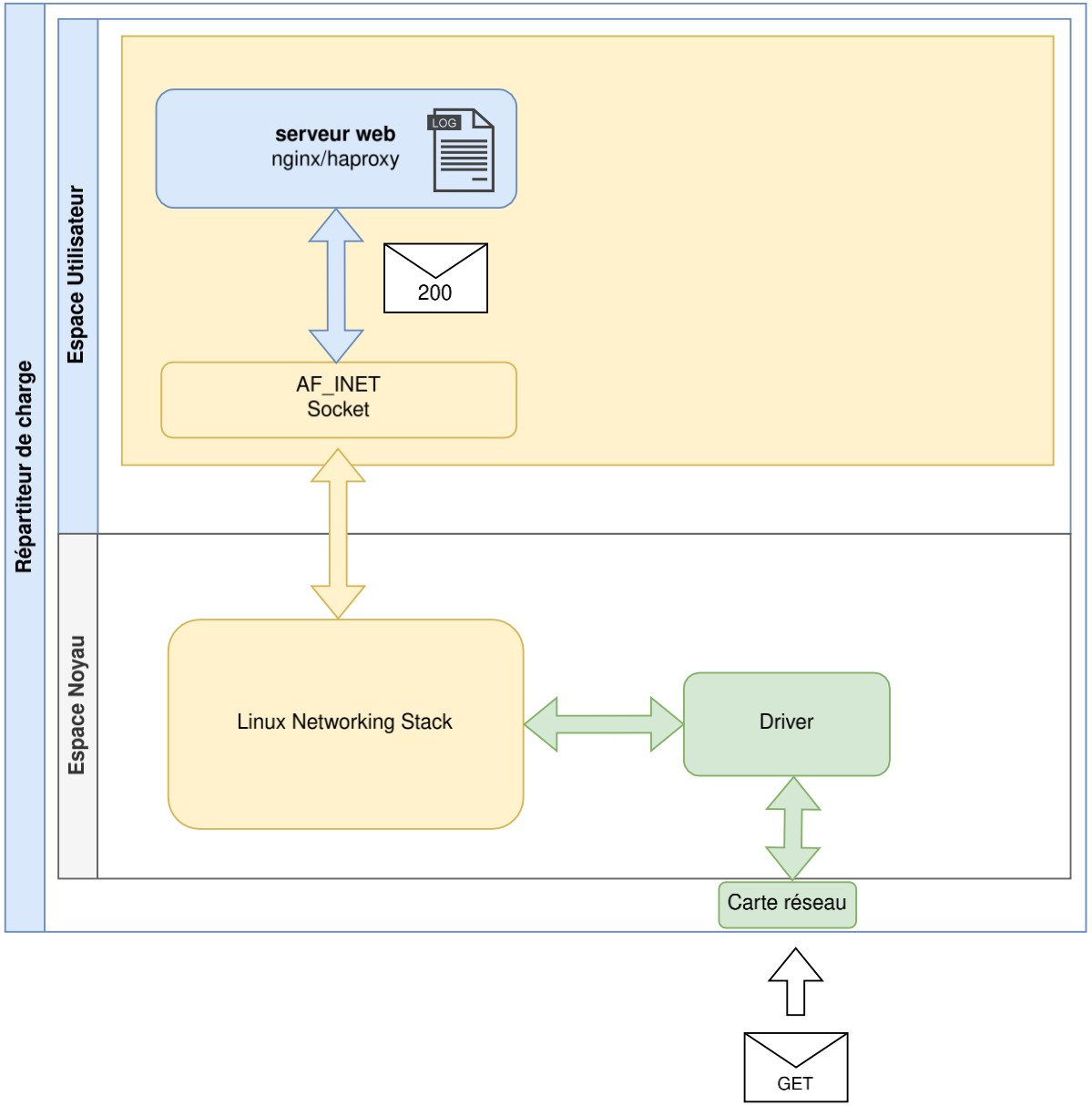
> **Besoin d'un outil de protection au niveau applicatif**

- Actif **avant** la protection réseau hébergeur

Hodor est né !

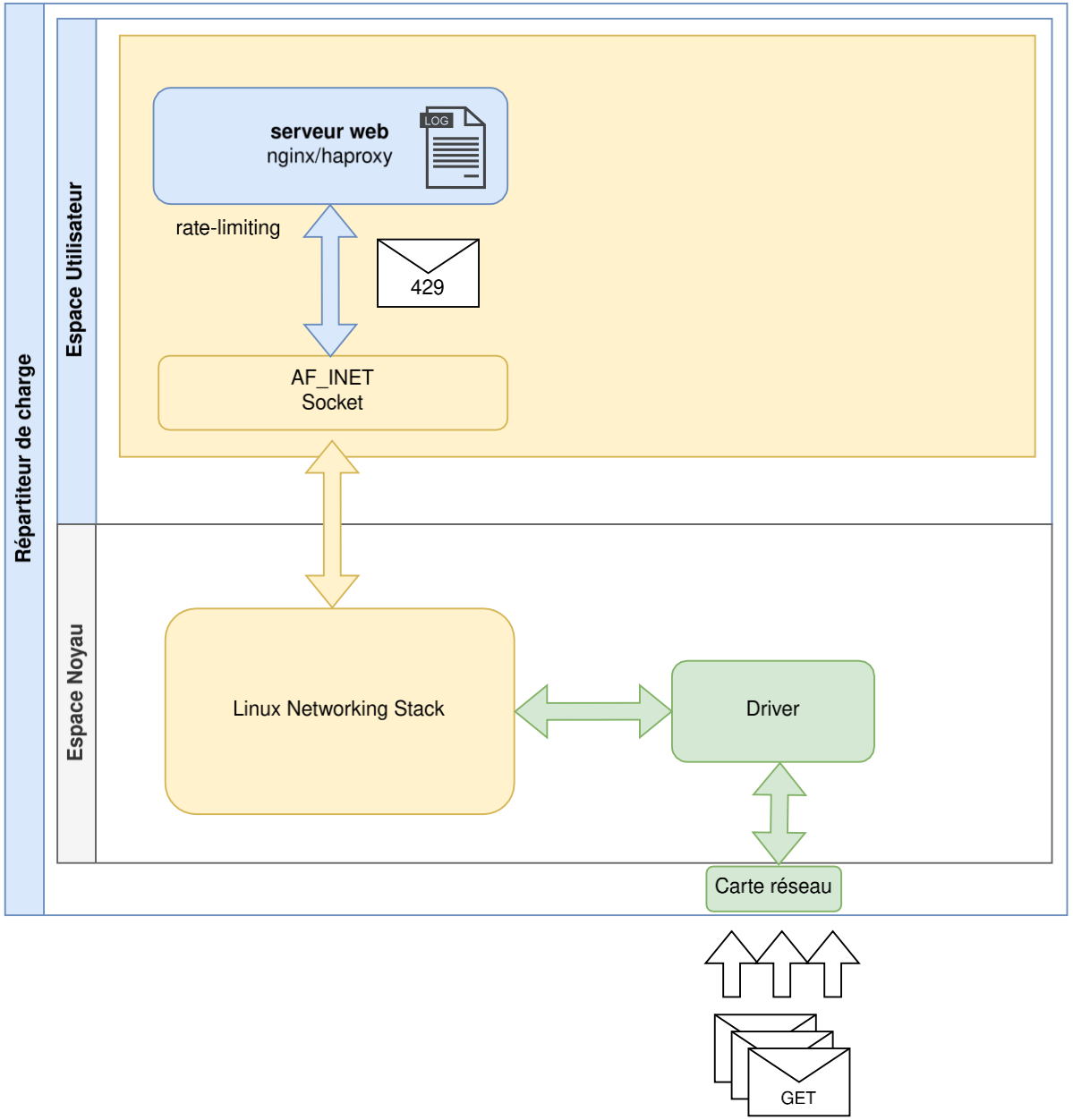
Protection DDoS - Hodor

> Trafic légitime, sans Hodor



Protection DDoS - Hodor

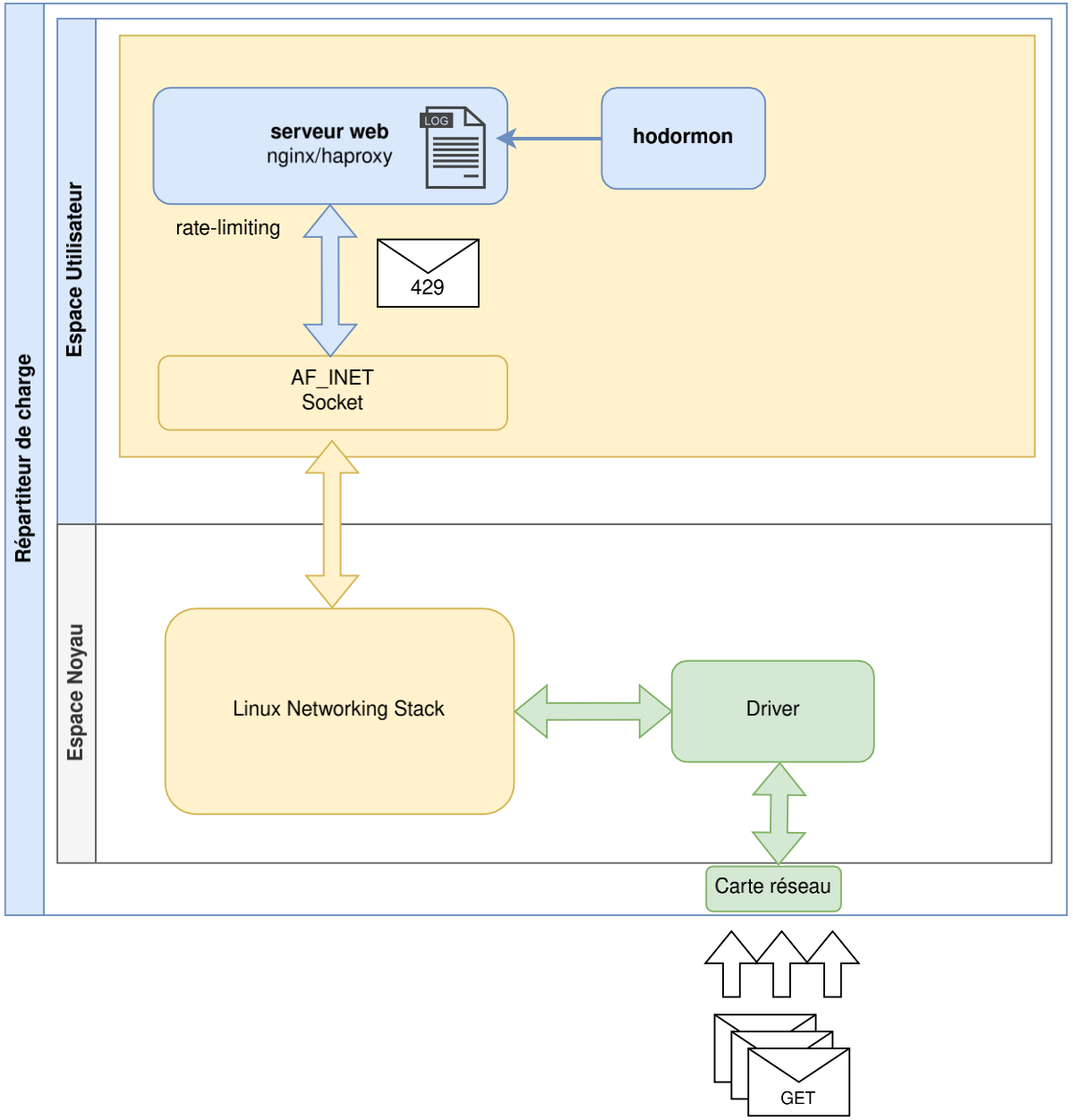
> Pic de trafic, sans Hodor



Protection DDoS - Hodor

> **Hodormon**

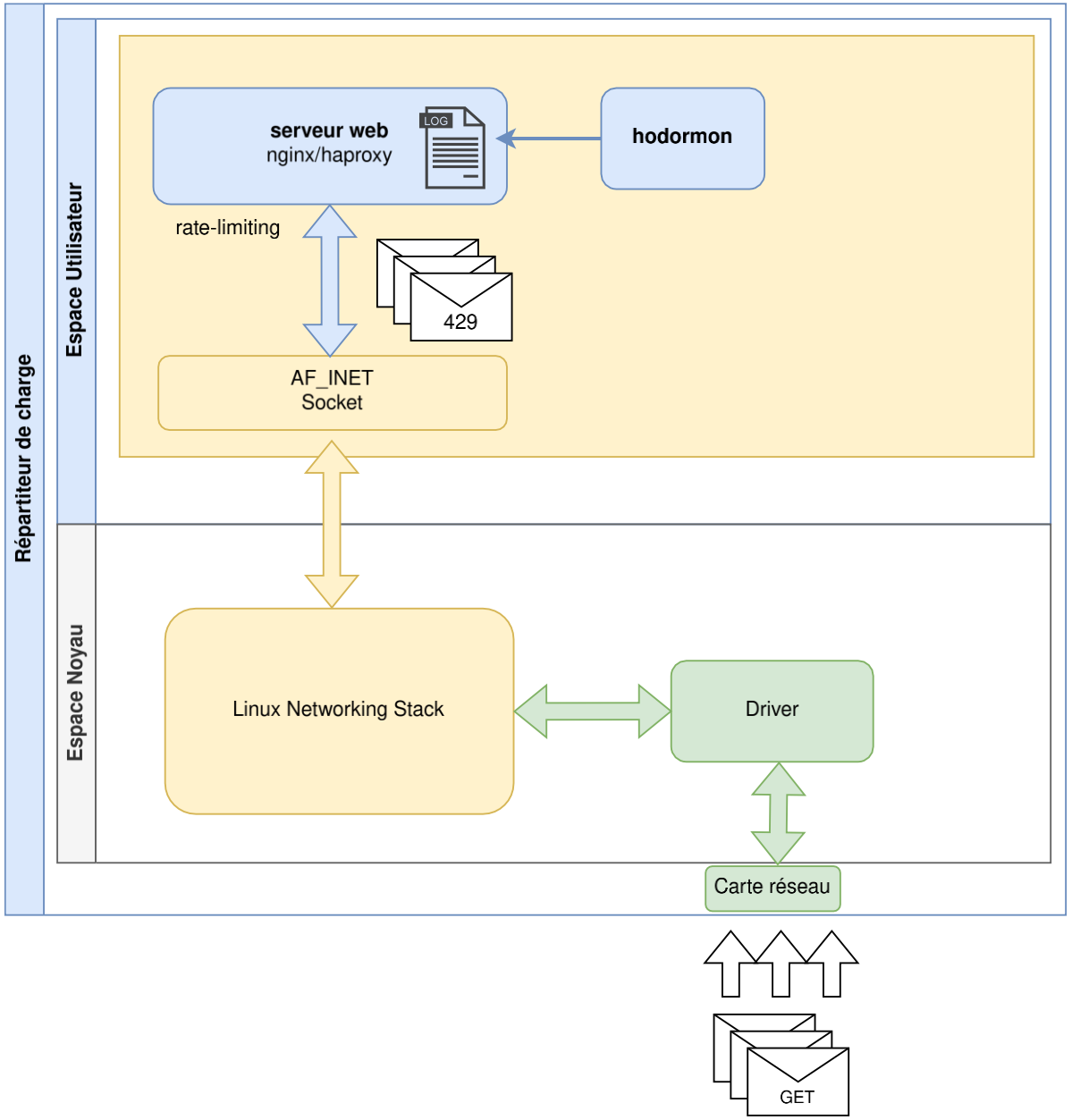
- Surveillance logs web
- Capacité : +300k logs/s



Protection DDoS - Hodor

> **Hodormon**

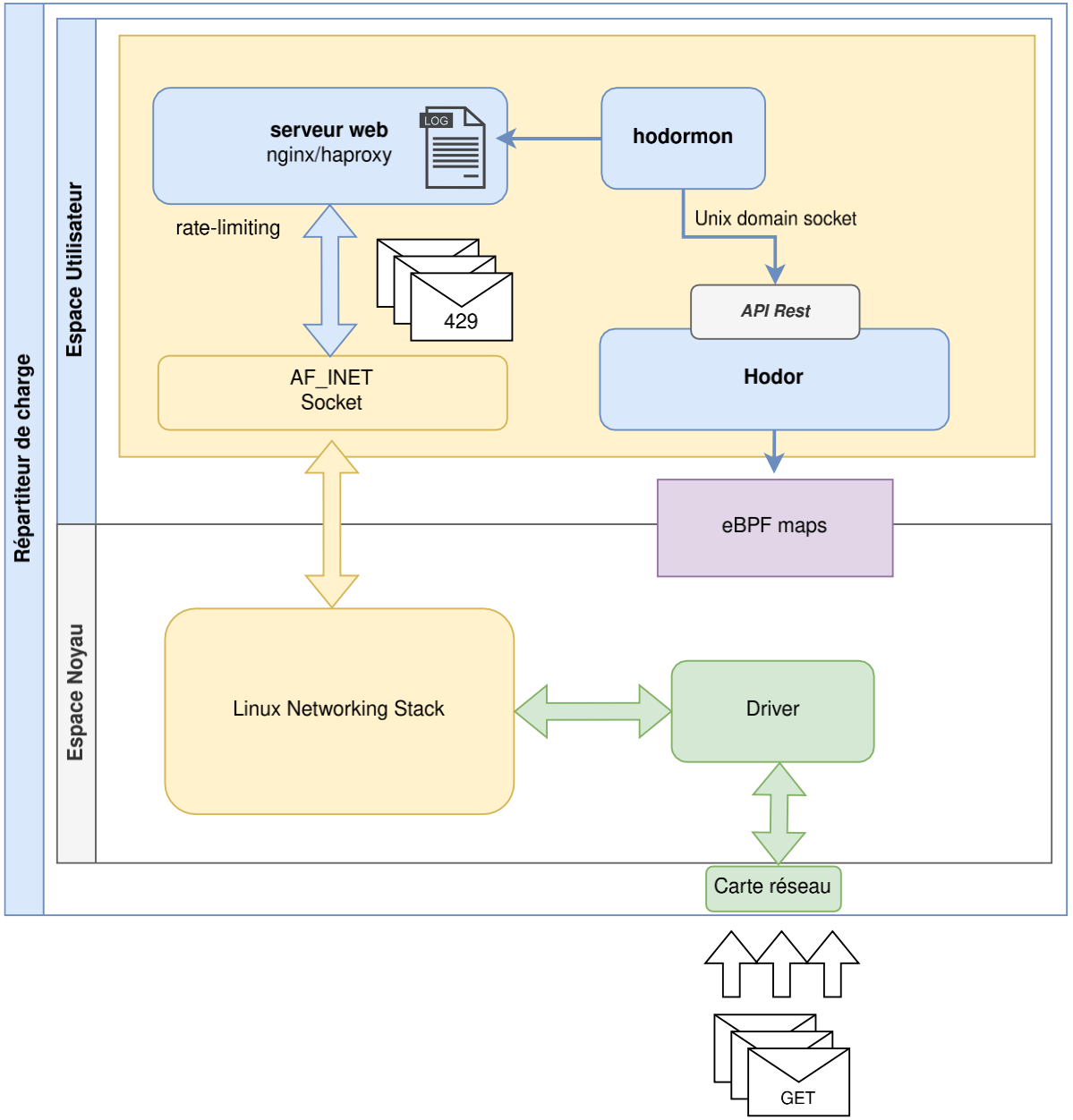
- Détection de nombreux dépassements du *rate-limiting* (429)



Protection DDoS - Hodor

> **Hodormon**

- Détection de nombreux dépassements du *rate-limiting* (429)
- Insertion (via API) dans une structure kernel (map eBPF)



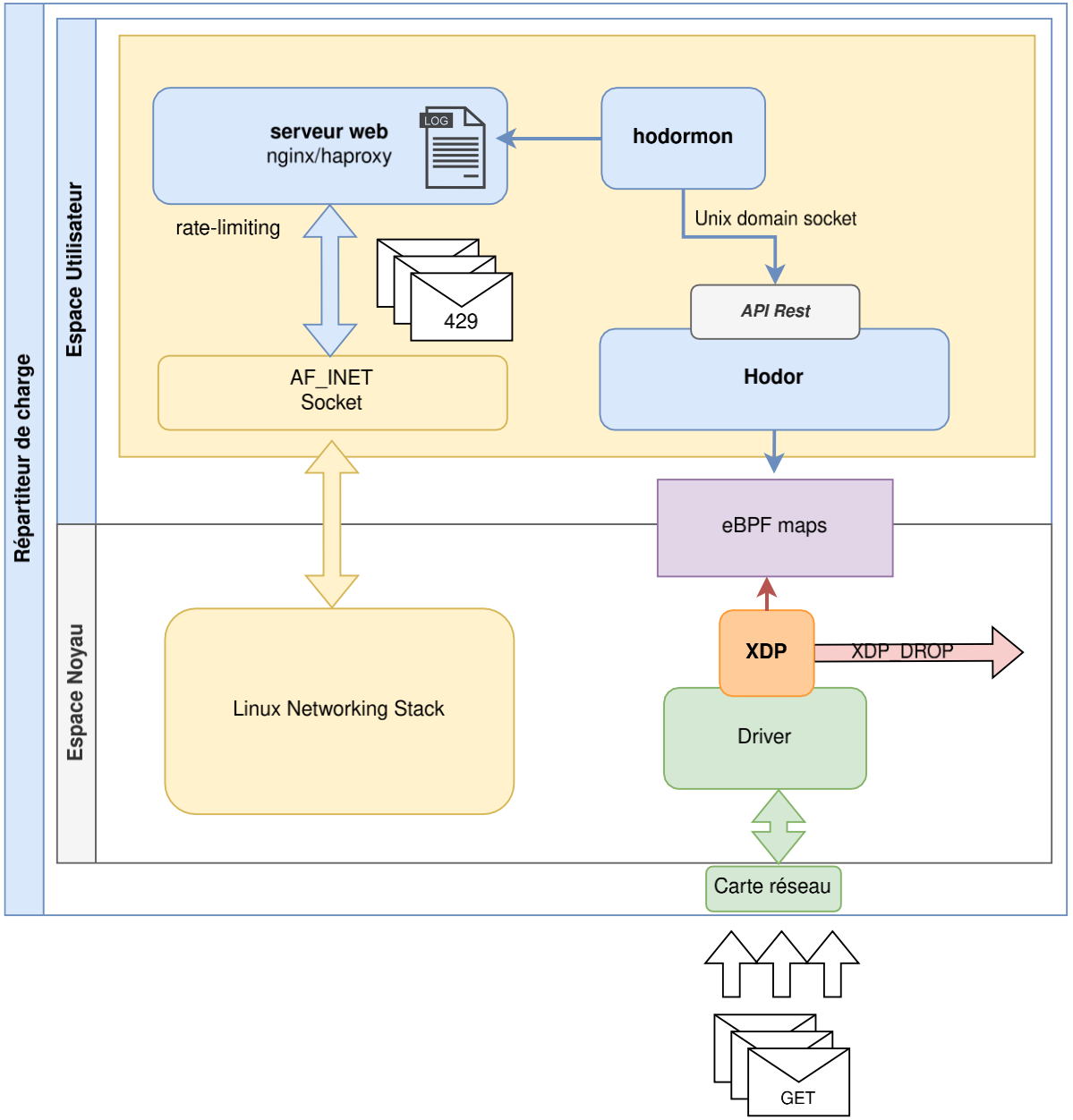
Protection DDoS - Hodor

> Hodormon

- Blocage bas niveau (XDP)
  - Driver carte réseau
  - *Offloading* matériel possible
  - Capacité : ~1M paquets/s
- RAM < 100MB

> Temps de ban aléatoire

- Borné (1-2 min)
- Bornes exponentielles

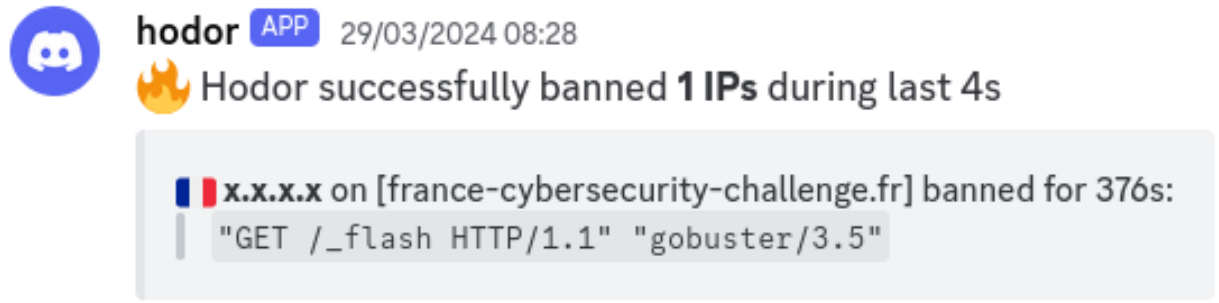


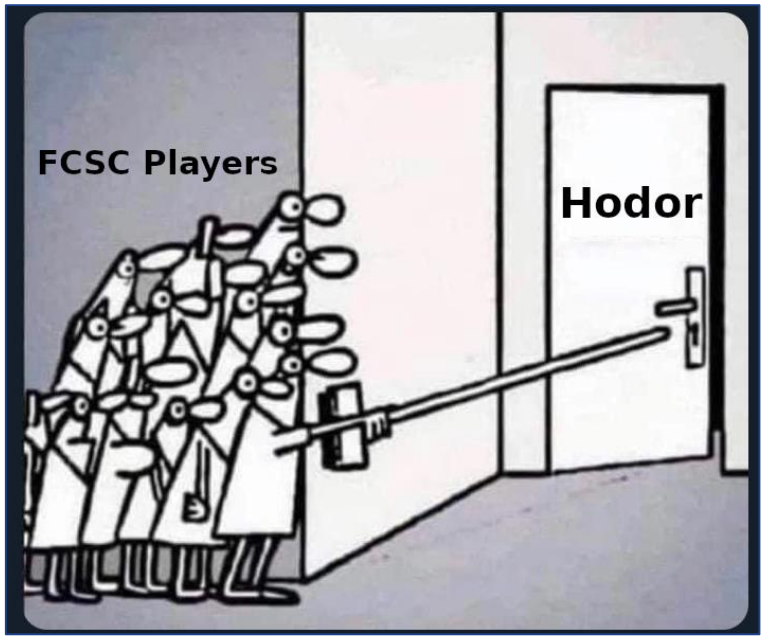
Protection DoS – Blocage de joueurs

> But

- Protéger les épreuves des outils automatisés
- Le faire de façon pédagogique (ban temporaire)

> Notification rapide (quelques secondes maximum)

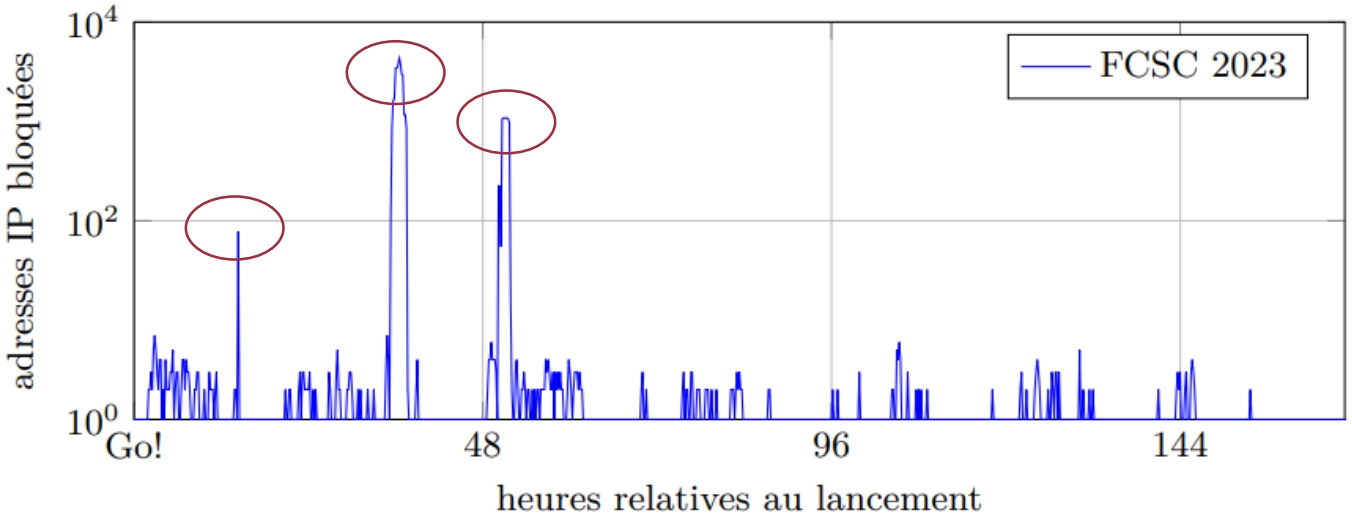


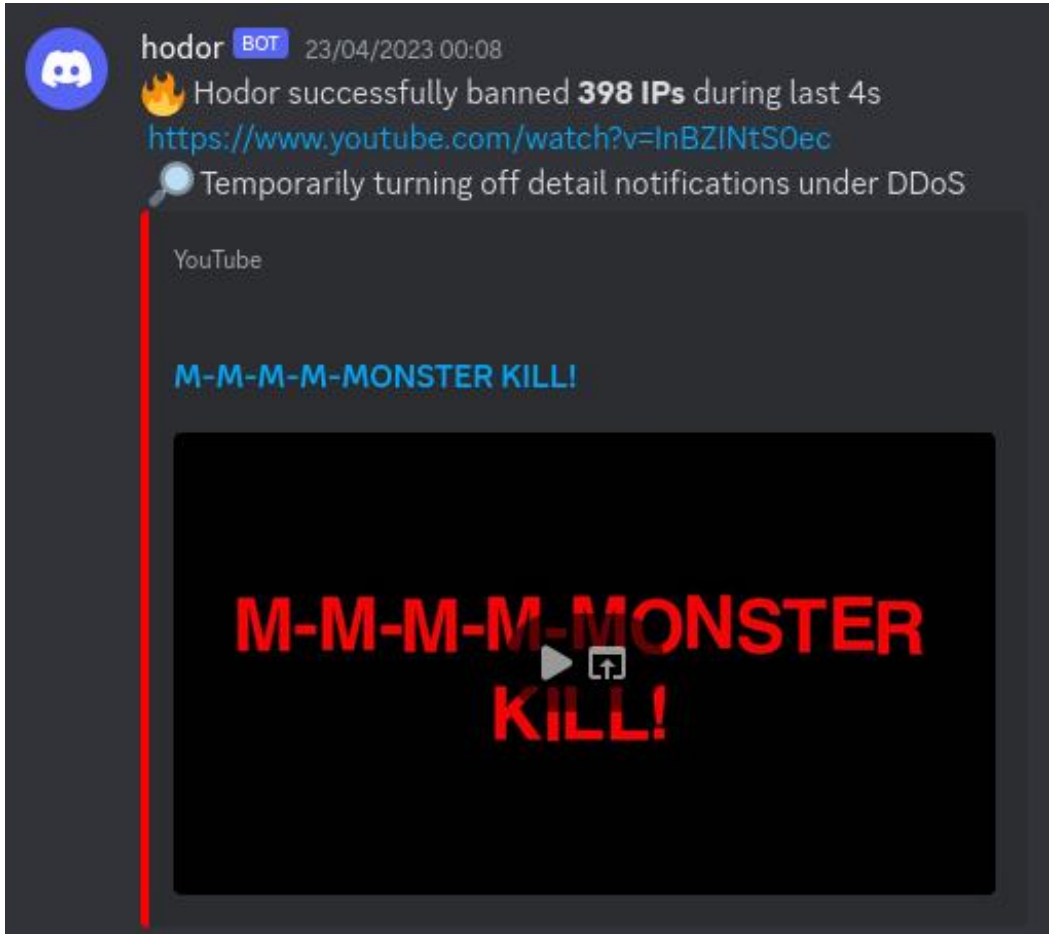


Protection DDoS – Blocage de vrais DDoS

> 2023 : vagues de DDoS successives

- 3 vagues
- Plusieurs milliers d'IP
- CTFd et épreuves ciblés
- Pas d'impact visible pour les joueurs



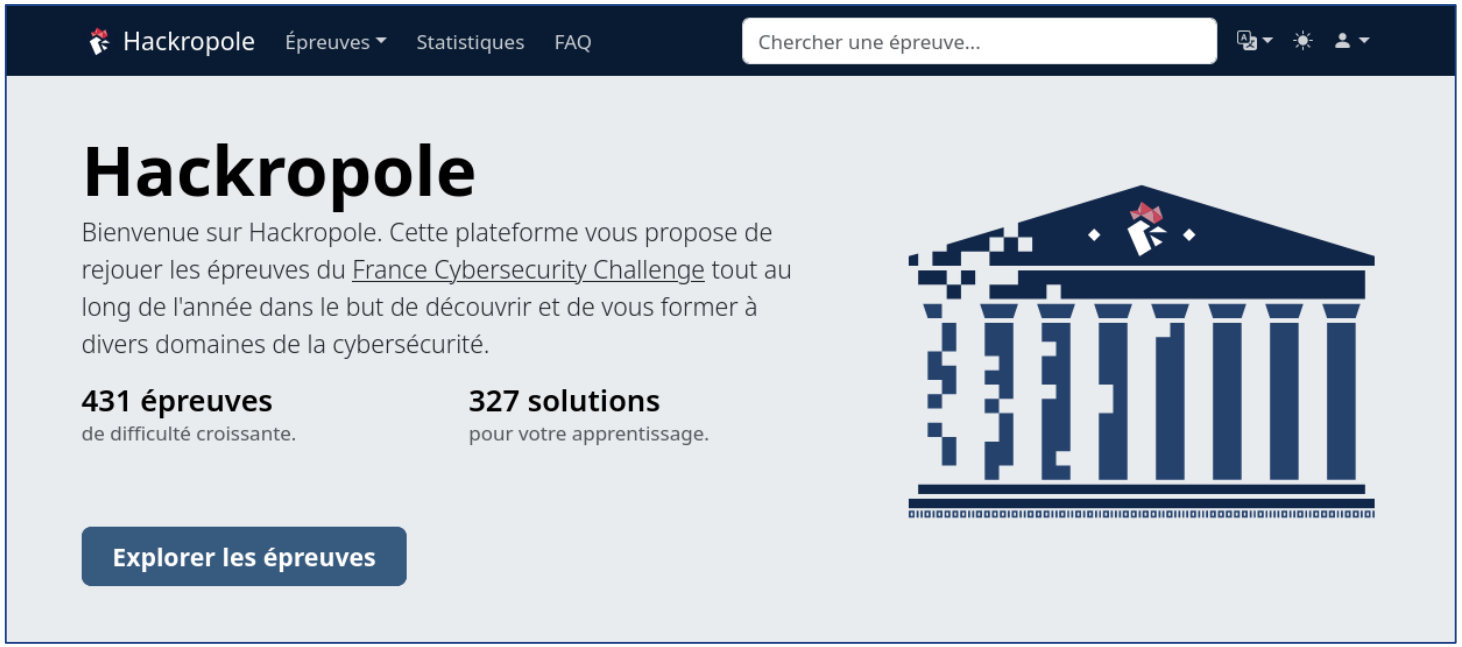


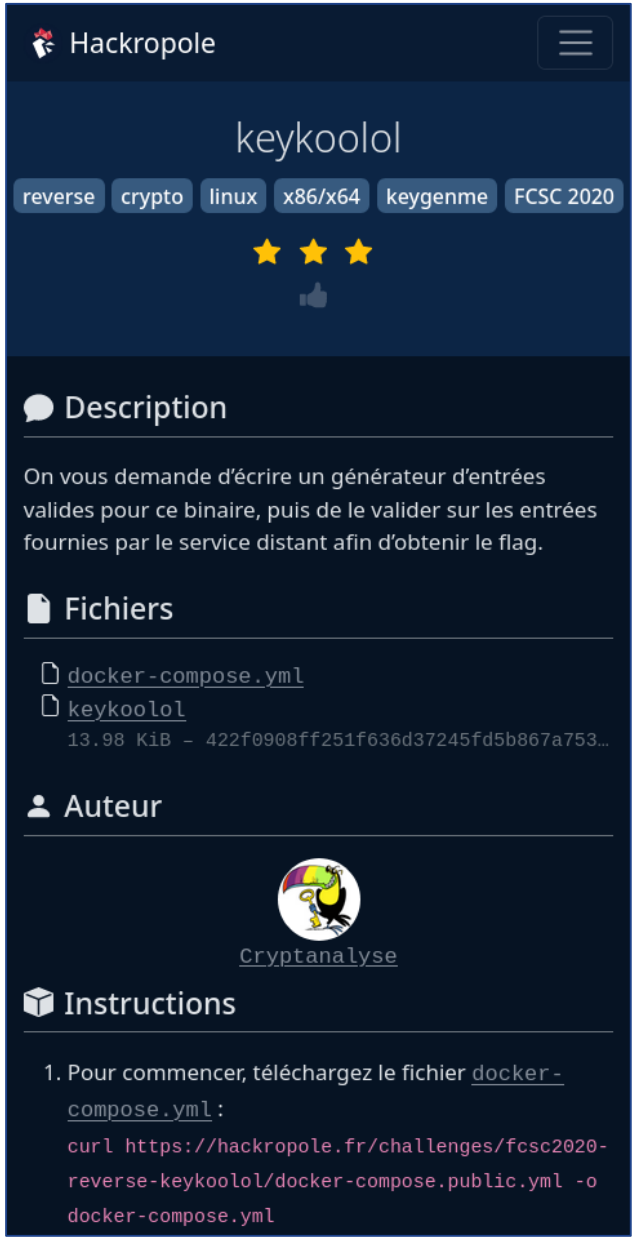
Disclaimer

- Les solutions présentées ne constituent pas des recommandations de l'ANSSI
- Possible car c'est une infra temporaire (infra de CTF)
- Le but est de présenter des solutions possibles de cloisonnement d'applicatifs et d'anti-DDoS pour du CTF

Projets annexes : Hackropole

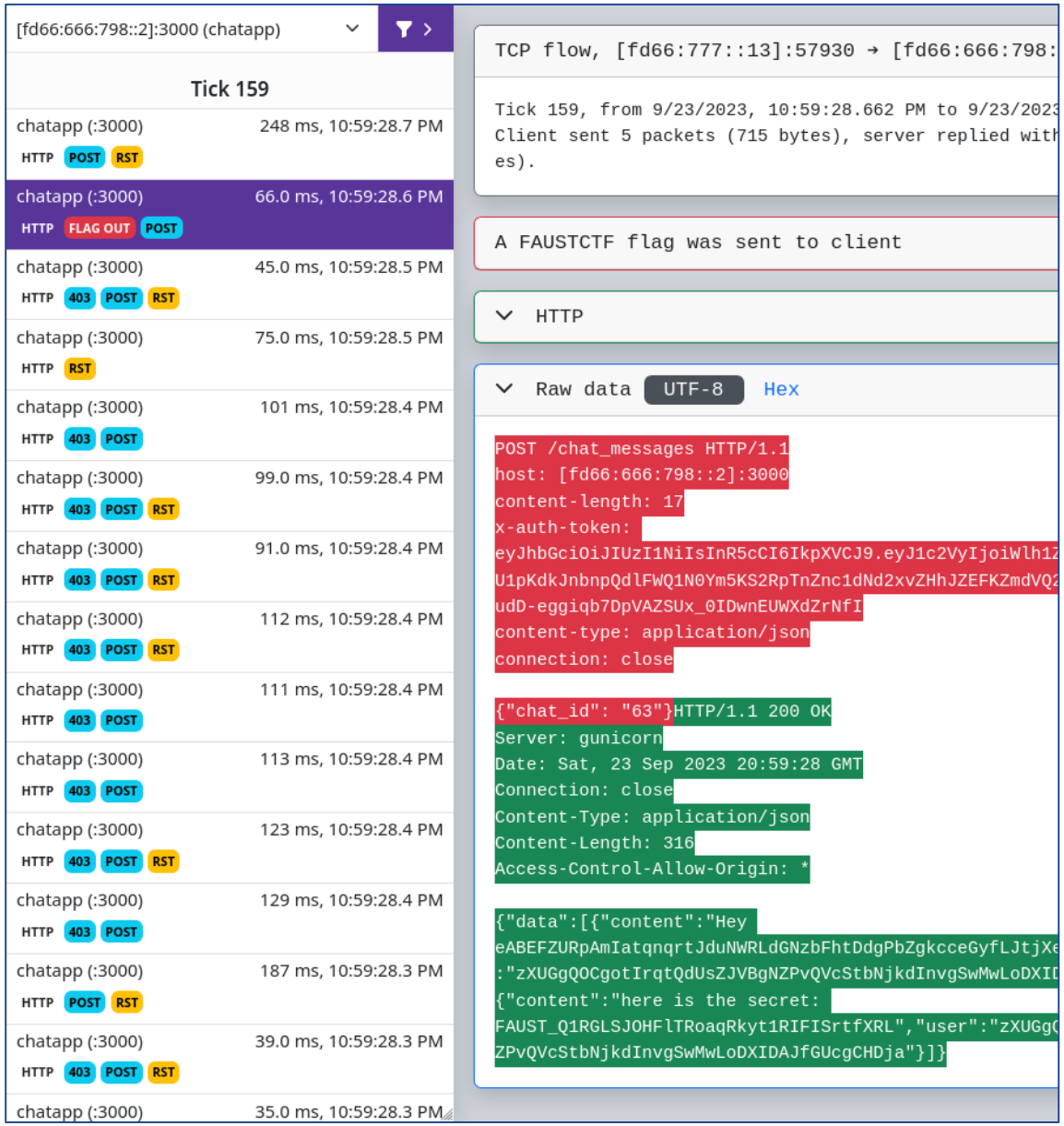
- Archives du FCSC depuis 2019
- Plus de 400 épreuves (images Docker fournies)
- Plus de 300 solutions ouvertes proposées par la communauté
- Français et anglais





Projets annexes : Shovel

- Outil développé pour la Team France
  - Exemple : « chatapp », FAUST CTF 2022
- Utilisé pour l'aspect défense de l'A/D
- Traitement de pcaps avec suricata
- Interface web efficace et minimaliste
- Quelques fonctionnalités
  - Tri par services et tag de paquets
  - Exports de flots TCP vers pwntools



Conclusion et évolutions

> Conclusions

- FCSC : CTF français en ligne depuis 2019
- Infrastructure moderne mais minimaliste
- Epreuves techniques de tous les niveaux
- Contributions à CTFd
  - Upstream de quelques fonctionnalités et correctifs de bugs
  - Upstream de tous nos patchs du thème de base

> Evolutions envisagées (selon temps)

- **Kernel :** publication de la configuration durcie
- **Hodor :** publication de l'outil sur GitHub
- **Hackropole :** ajout de contenu pour aider les débutants

Merci à tous pour votre attention

et en particulier merci à

toutes les personnes ayant déjà participé au FCSC
tous les concepteurs d'épreuves
tous les membres actuels et passés de l'orga
tous les alumnis de la Team France