

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

Rétrospective sur 6 ans de FCSC

Tristan CLAVERIE

Emilien COURT

Alexandre looss

Jérémy JEAN

Matthieu OLIVIER

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

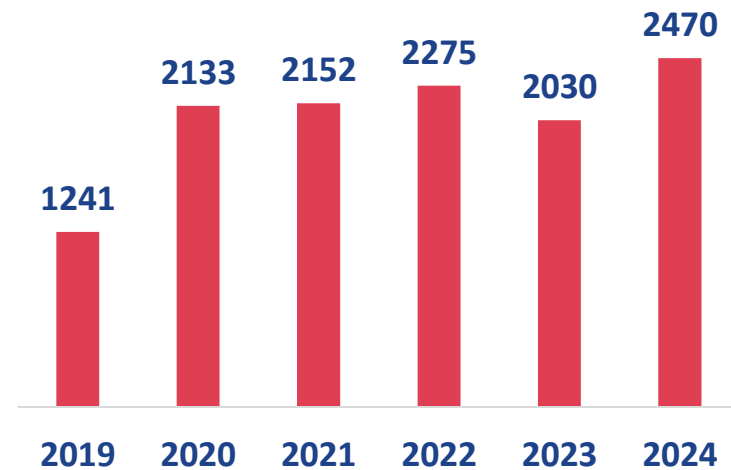
- **Prioritaire** : jeunes, étudiants, futurs actifs
- **Autre** : professionnels, passionnés, curieux, ...

> CTF ou « Capture The Flag »

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



Nombre d'inscrits au FCSC



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, ...

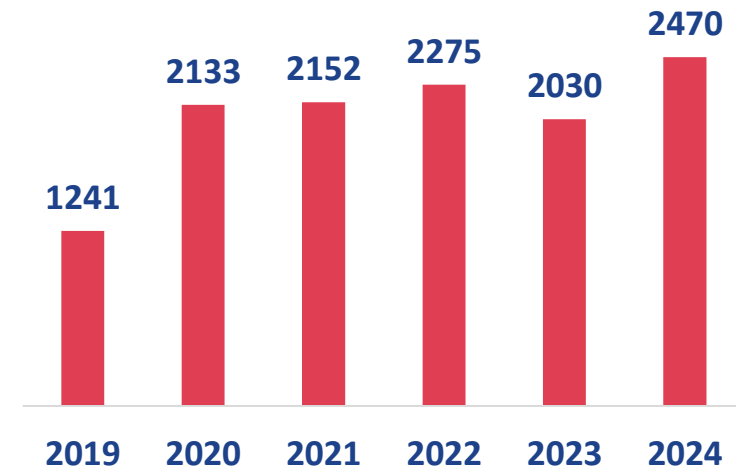
> ECSC (European Cybersecurity Challenge)

- 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

FCSC 2024 Utilisateurs Classement Challenges Notifications Compte Paramètres

Challenges

intro

Welcome Admin 1/2 20 points 659 participants	Layer Cake 1/3 20 points 541 participants	Rien à signaler 20 points 391 participants	Layer Cake 2/3 20 points 373 participants
AdveRSARial Crypto (Infant) 20 points 292 participants	Layer Cake 3/3 20 points 265 participants	Fifty Shades of White (Junior) 20 points 236 participants	Blind Attack 20 points 171 participants
FFTea 20 points 154 participants	Very Cute Data 20 points 127 participants	Strike 20 points 95 participants	Call Me Blah 20 points 79 participants
Intégration par parties 20 points 42 participants			

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

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

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

Terrapin Attack



Paper	Vulnerability Scanner
Q&A	Patches

News

- The accepted paper including the artifact appendix is now available.
- The Terrapin Attack will be presented at [Real World Crypto Symposium 2024](#), [Black Hat USA 2024](#), and [USENIX Security Symposium 2024](#).
- We compiled a comprehensive [list of SSH implementations](#) adopting the "strict kex" countermeasure by OpenSSH.
- Recommended Articles: [Ars Technica](#) (Dan Goodin), [The Register](#) (Connor Jones)

<https://terrapiin-attack.com>

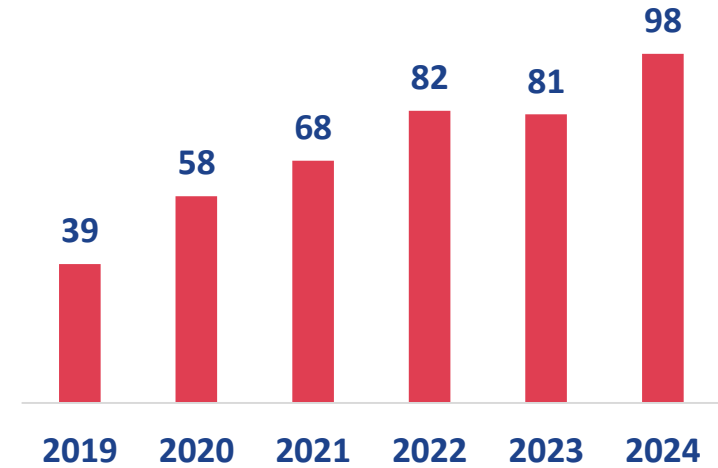
Epreuve « Secret Shenanigans » (FCSC 2024)

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

Nombre d'épreuves au FCSC



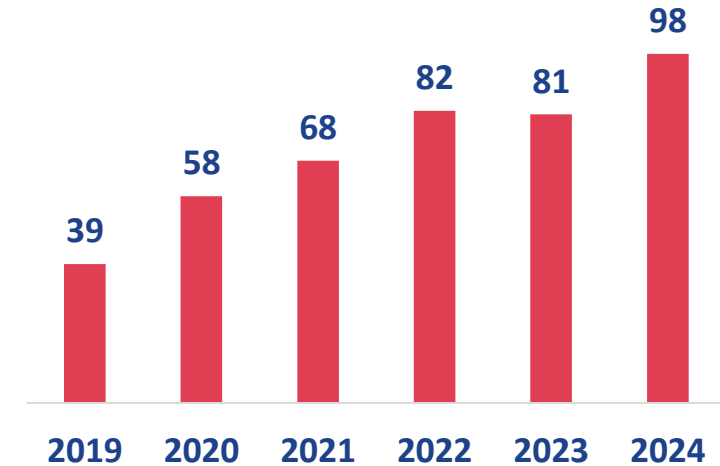
Conception des épreuves



> Objectifs dans la phase de conception

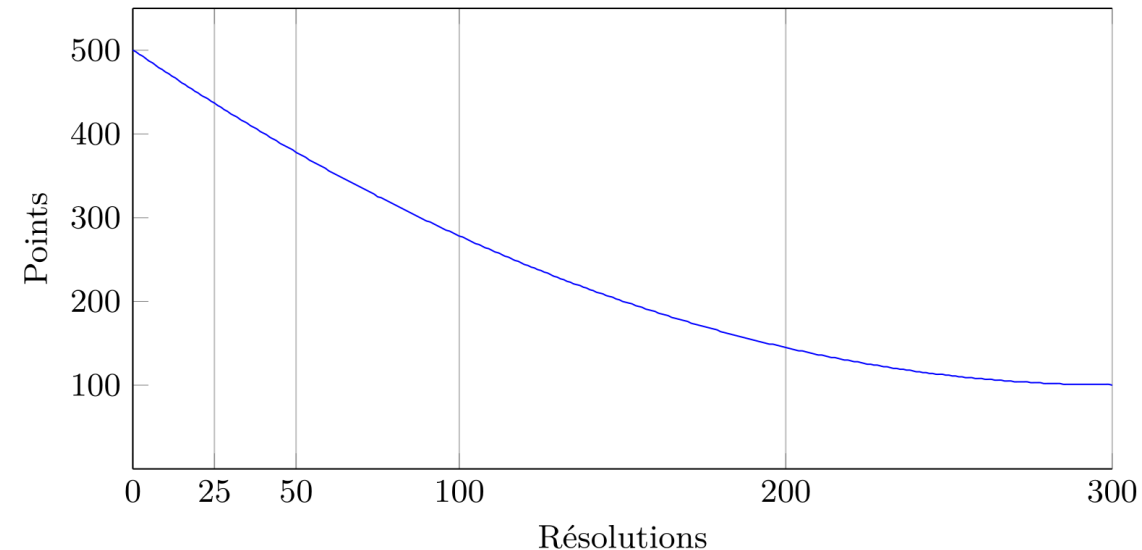
- Apprendre quelque chose lors de la résolution
- Eviter la présence de solutions inattendues
- Eviter le « guessing » au maximum
- Originalités des sujets (hors « intro »)
- Catégories originales représentatives des métiers de l'ANSSI (SCA/FI, Radio)
- Concepteurs externes ANSSI pour certaines épreuves

Nombre d'épreuves au FCSC



> 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

```
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

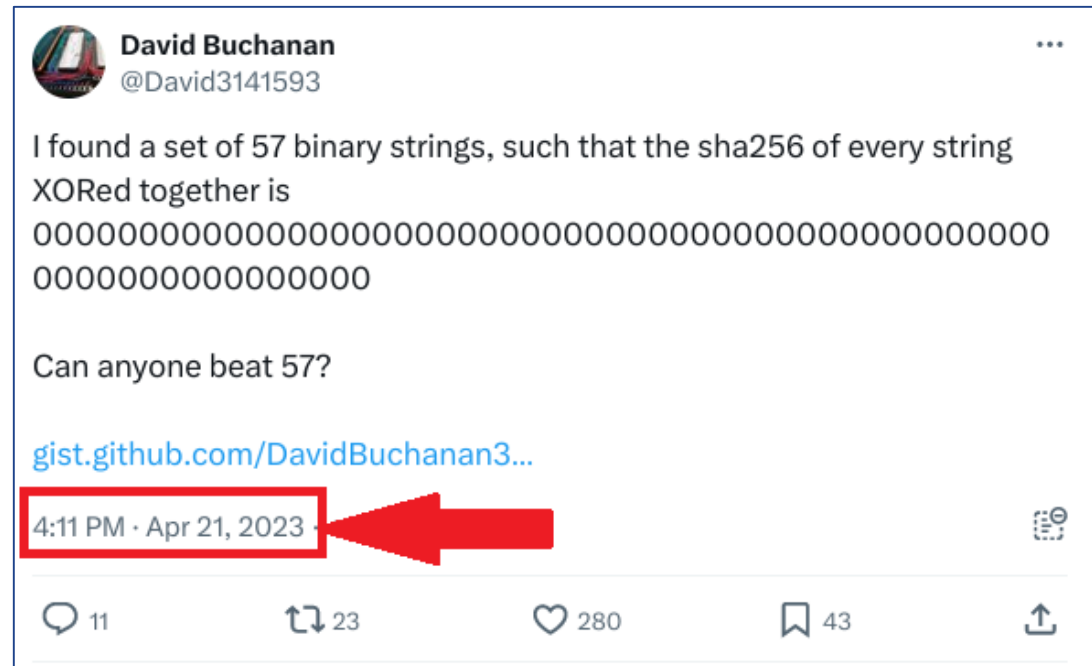


« Pain in the Hash » : épreuve crypto au FCSC 2023

- 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

```
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

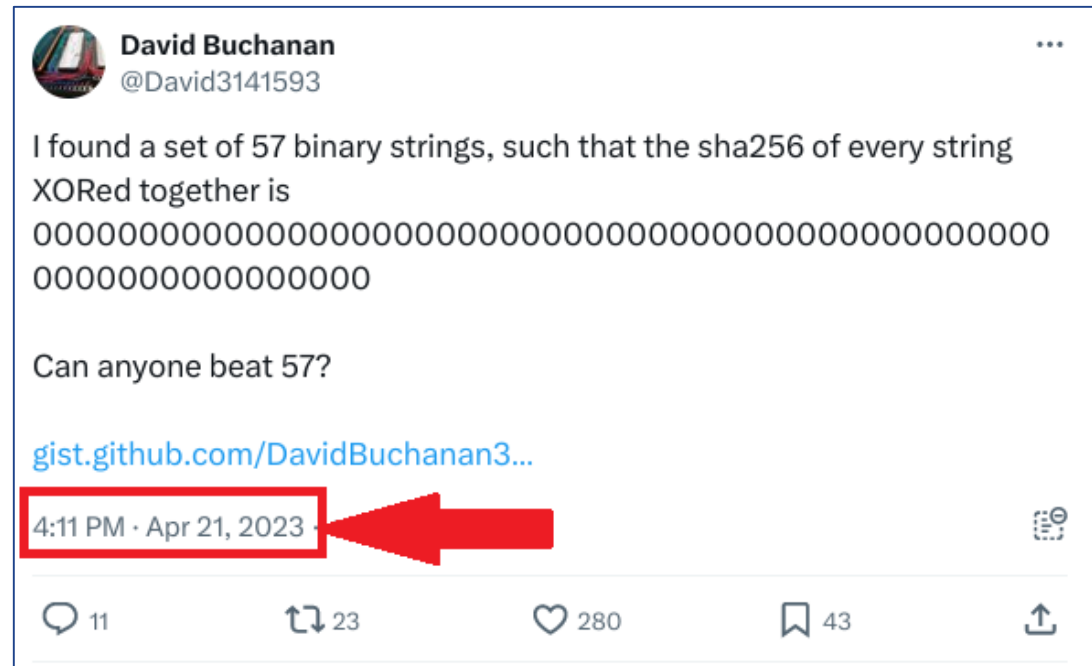


« Pain in the Hash » : épreuve crypto au FCSC 2023

- 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

```
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 overlaysfs

```
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 overlaysfs
- **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,
};
```

```
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/fs/ext4/file.c#L945>

<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



Cryptanalyse 27/04/2022 16:49

je teste rapidement de péter la crypto

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 fuient sur Discord ou sur Internet pendant le CTF
- L'utilisation de 1-day ou de 0-day
- Infra trop durcie (recompilation de noyau maison)
- ...

3:26 PM XeR

C'est possible de recompiler un `linux-hardened-but-not-too-much` pour les années suivantes ?
Au moins pour les épreuves de pwn



5

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

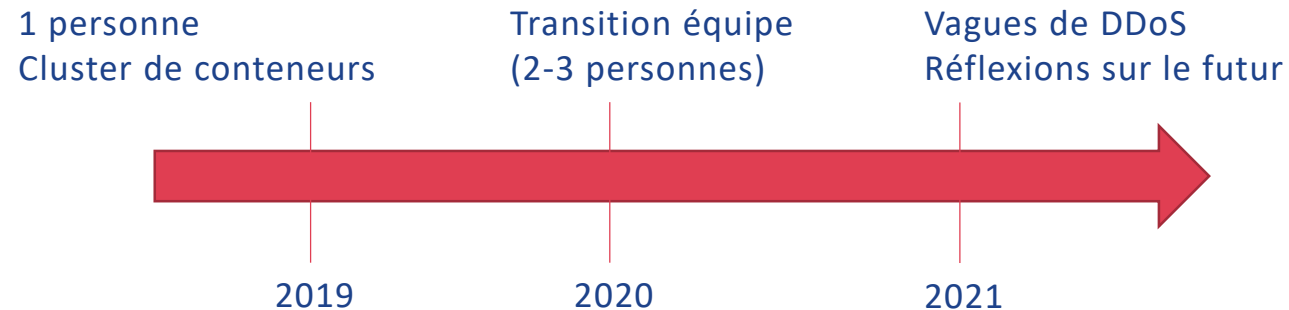
- En service 2 à 4 mois selon les éditions
- Décommissionnée après la fin du FCSC

> 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 !**



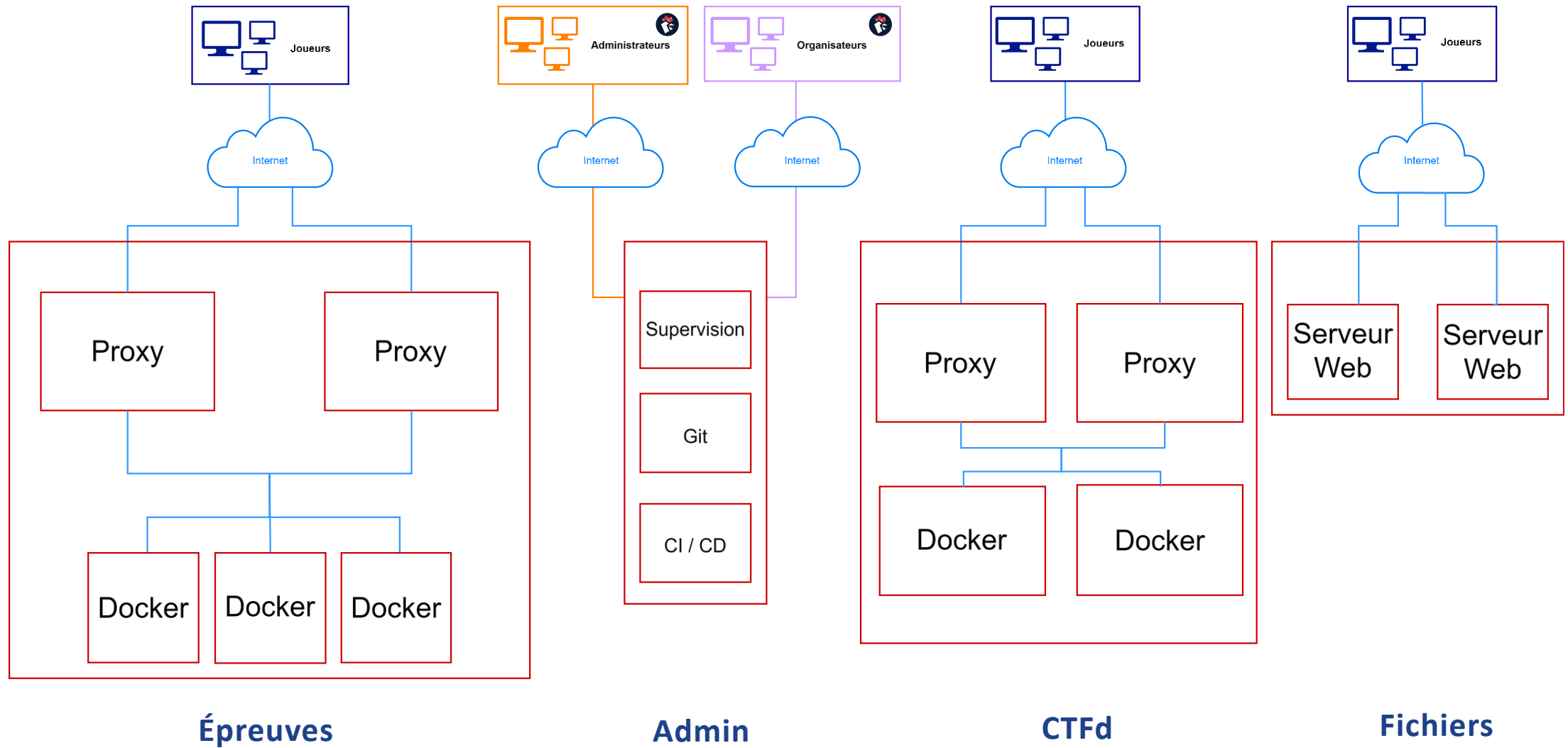
Fin 2021 : comment valoriser cette infra ?



> 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)

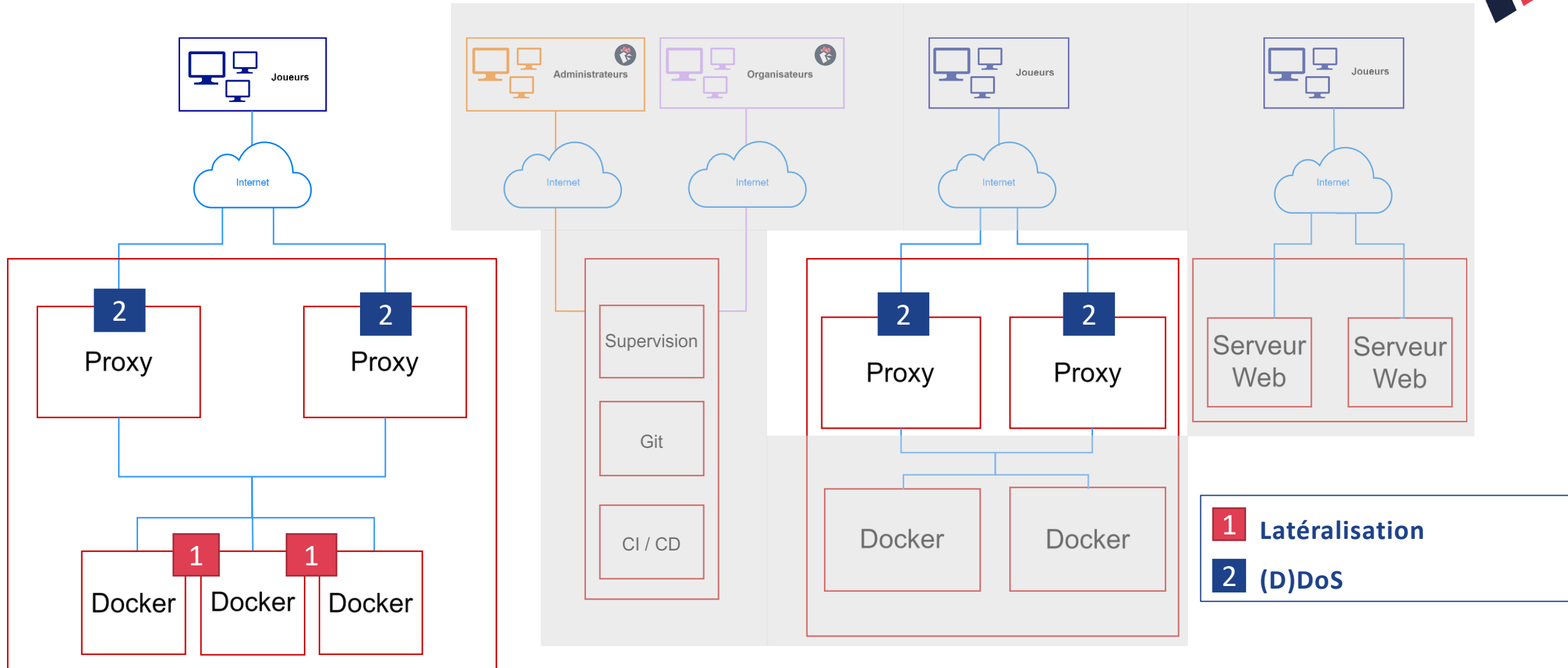
> Deux risques à adresser

- 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



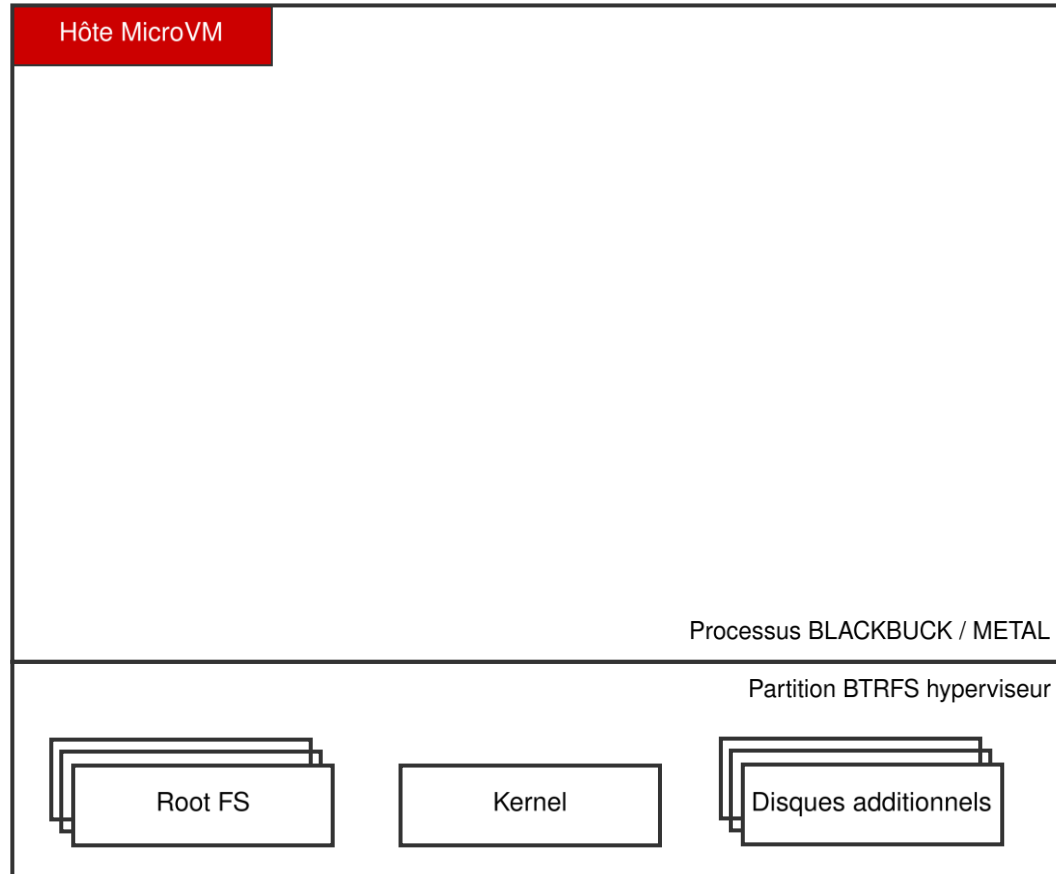
> Solution **1**

- 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 ?

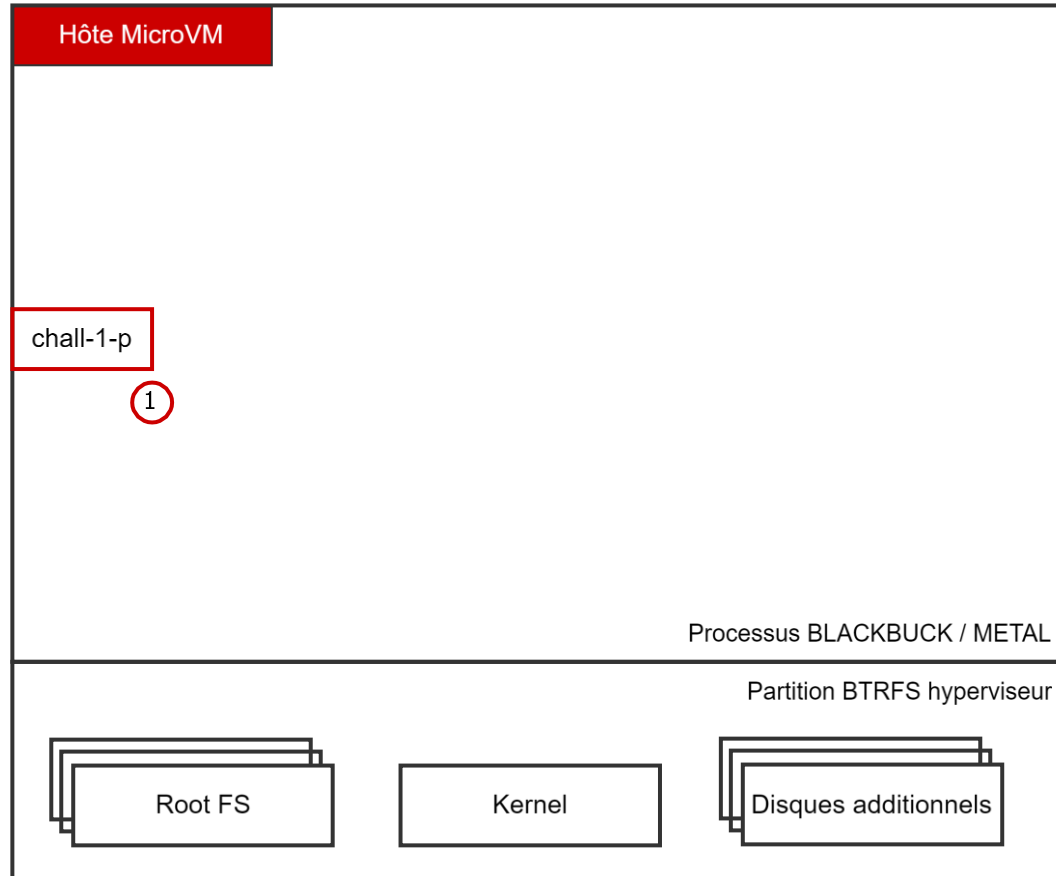
- Revue de solutions existantes
 - Non adaptées à notre situation
- Script Bash
 - Difficilement maintenable
- **Solution retenue** : développement maison
 - API pour la création de microVM et de leurs ressources
 - Deux versions interchangeables
 - Rust (Blackbuck) et Golang (Metal)
- Conteneurisation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

MicroVM : hôte des VM



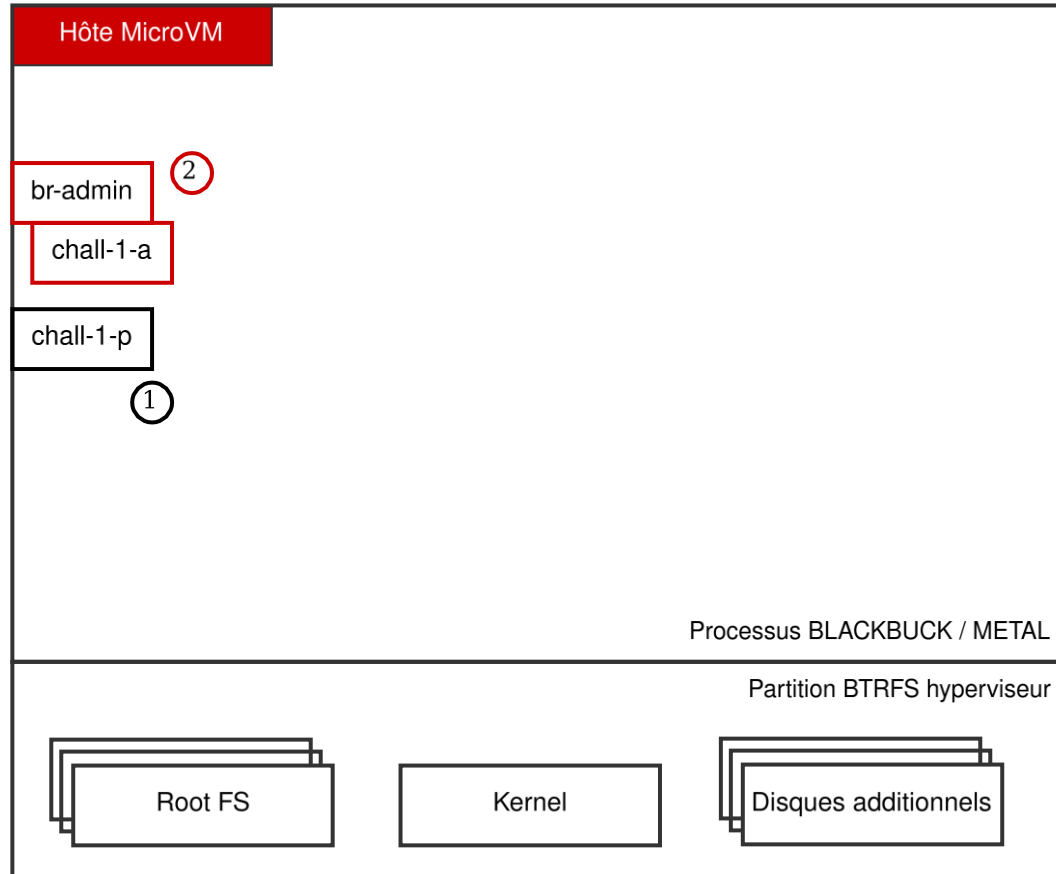
```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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



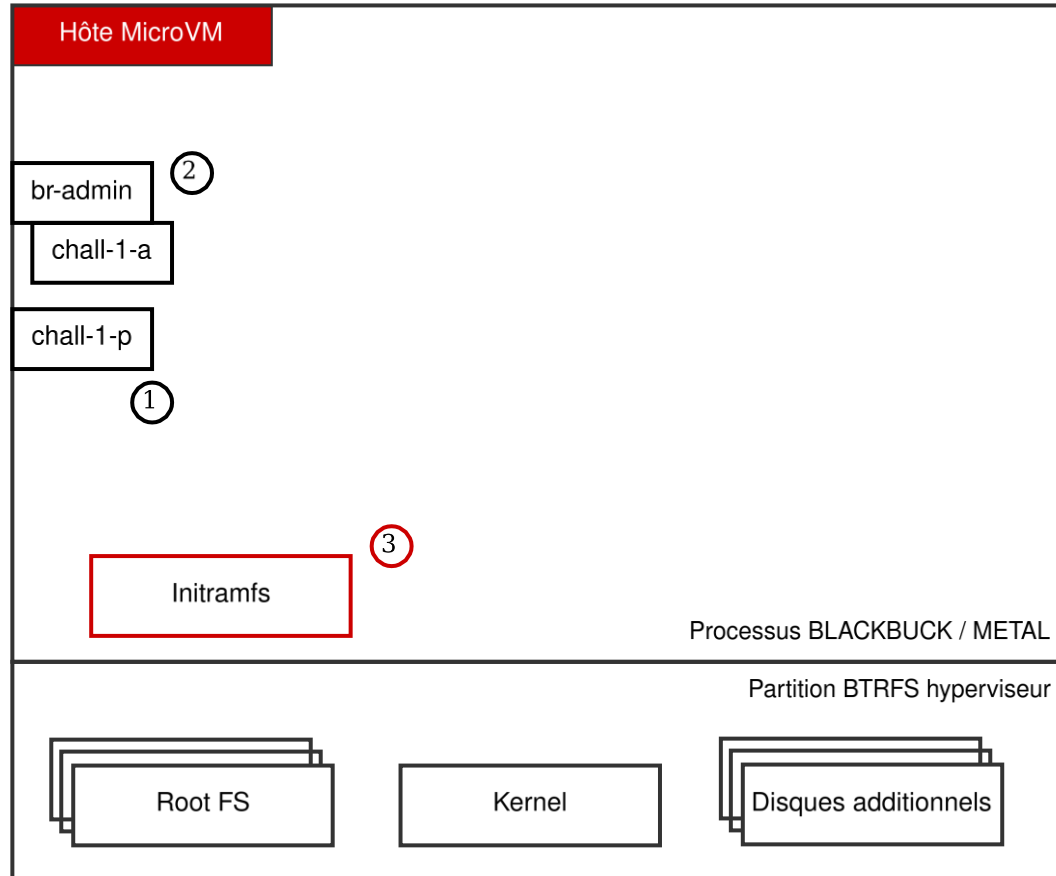
```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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



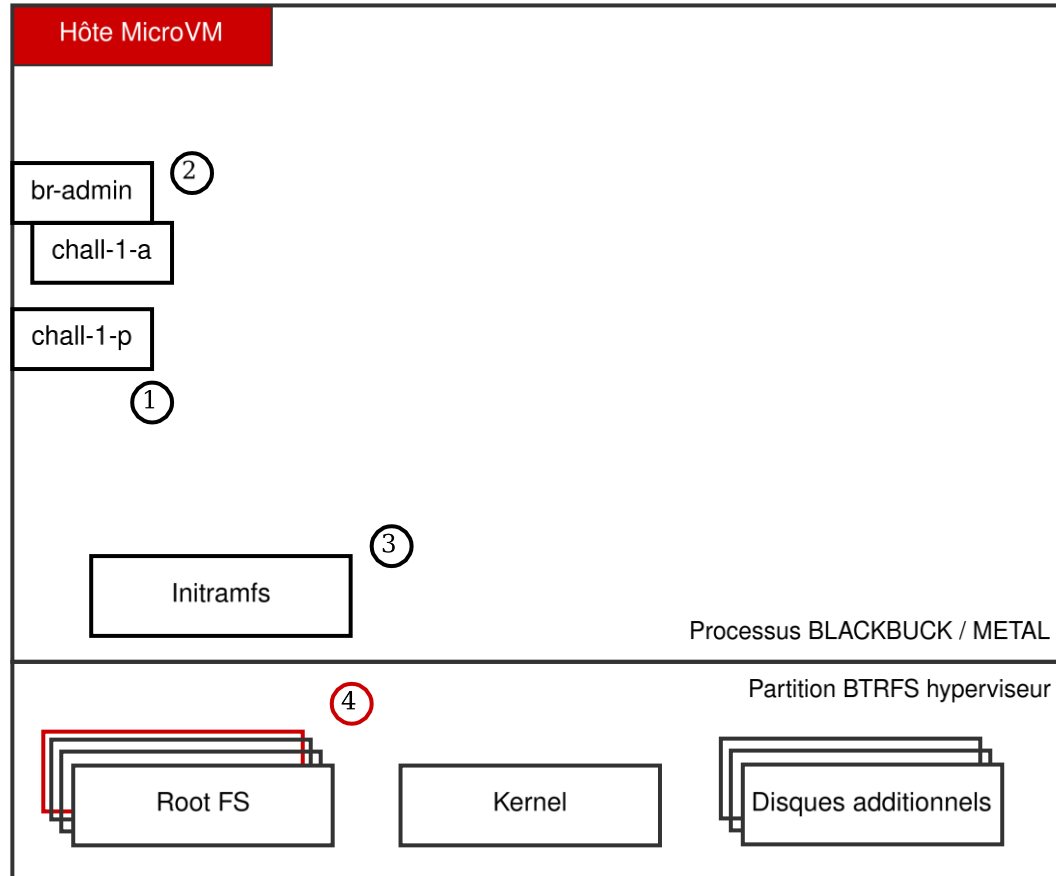
```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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



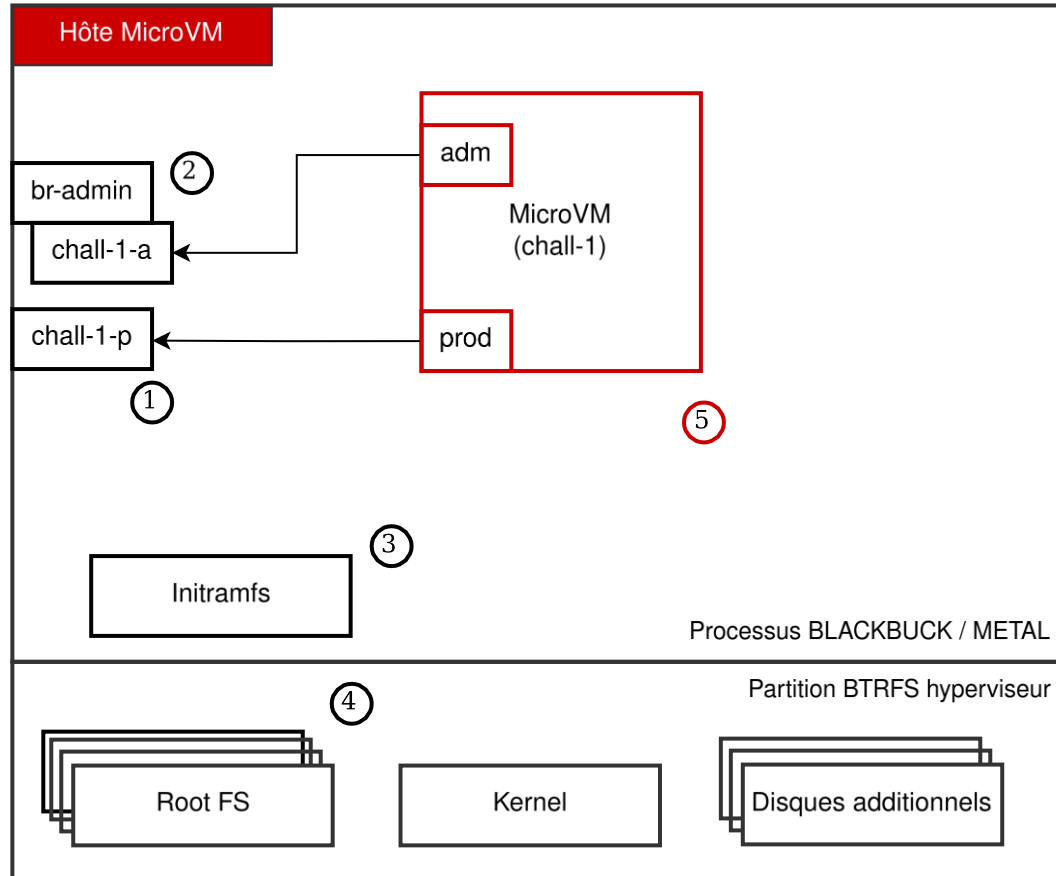
```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

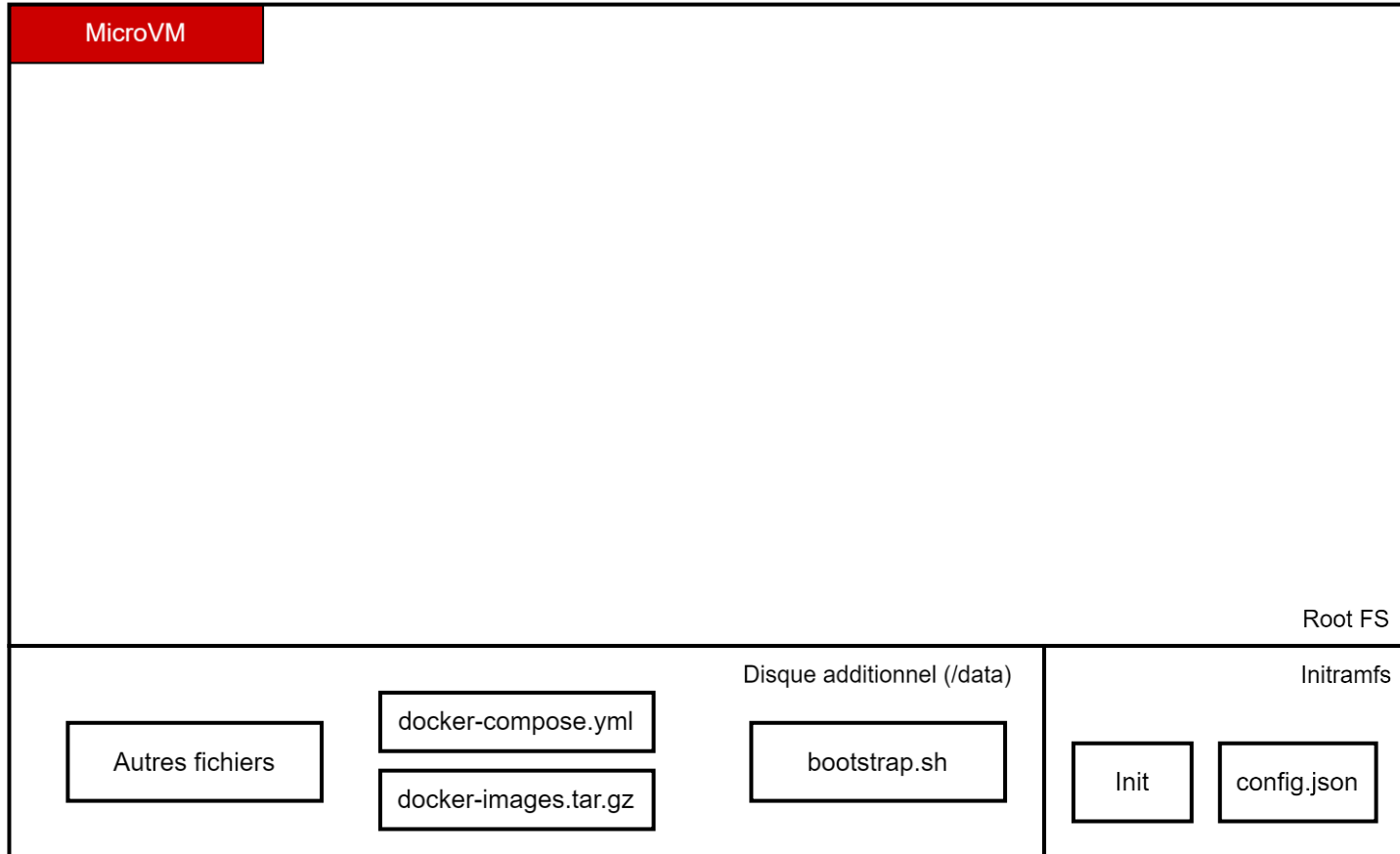


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

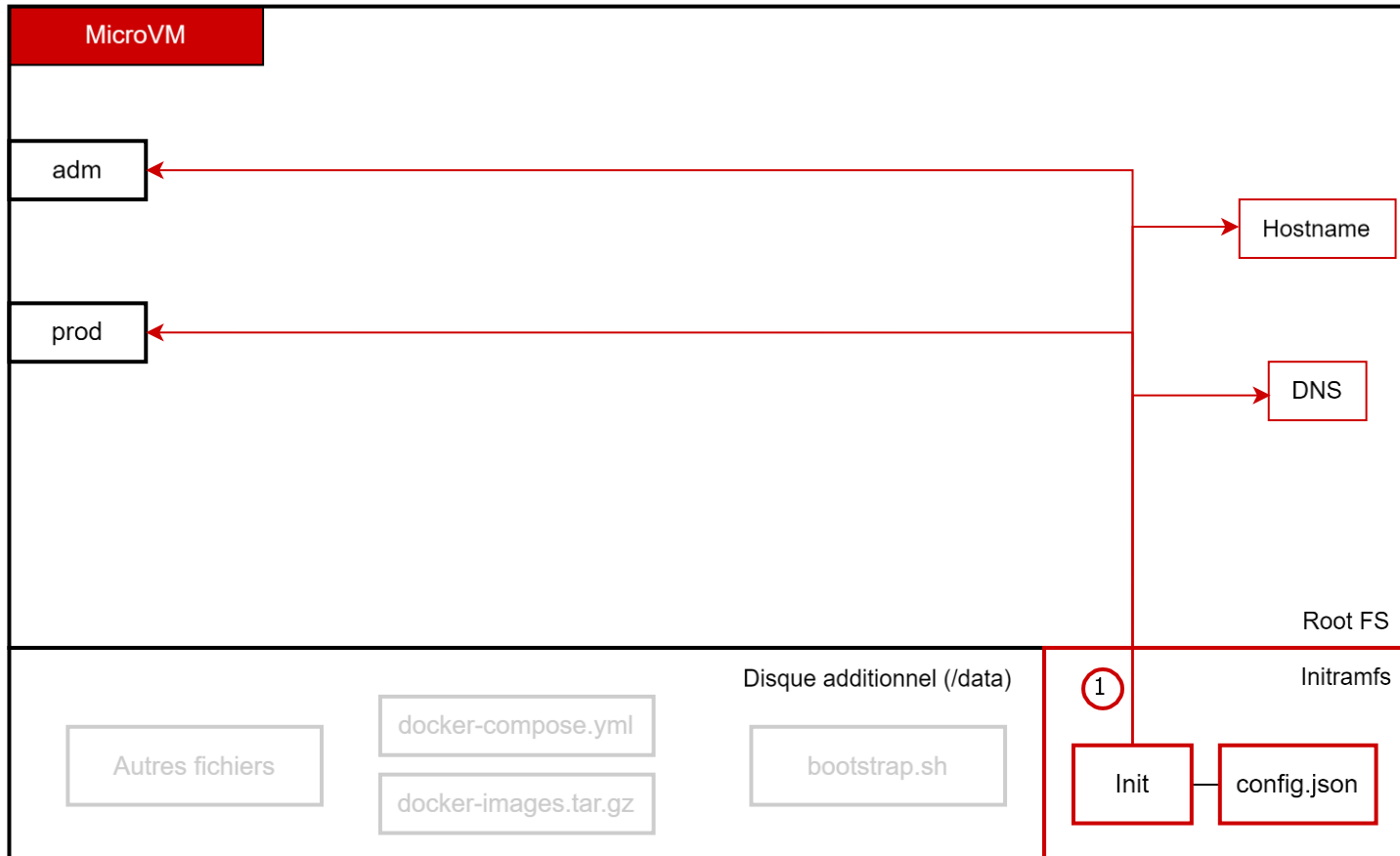


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

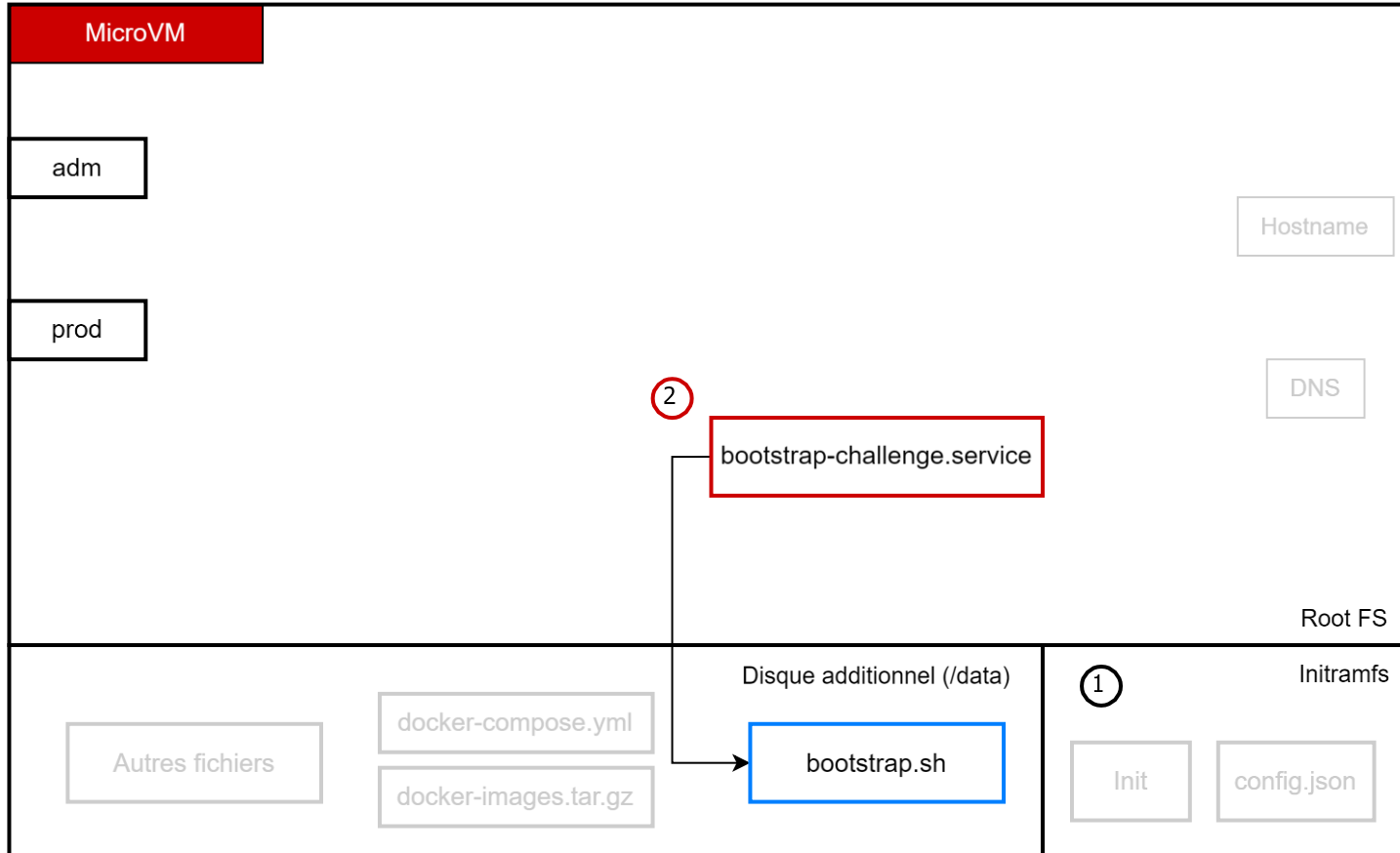


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

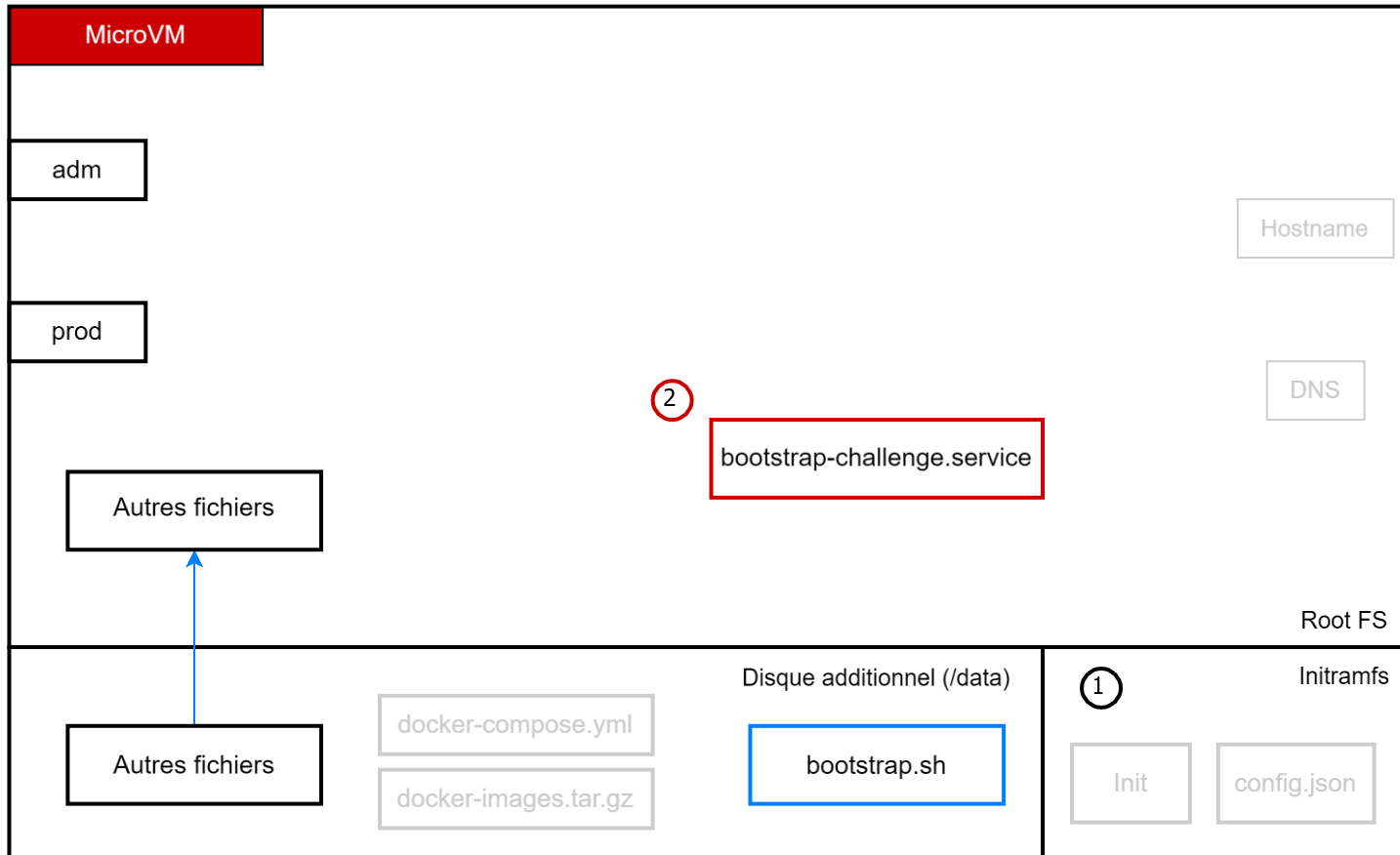


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

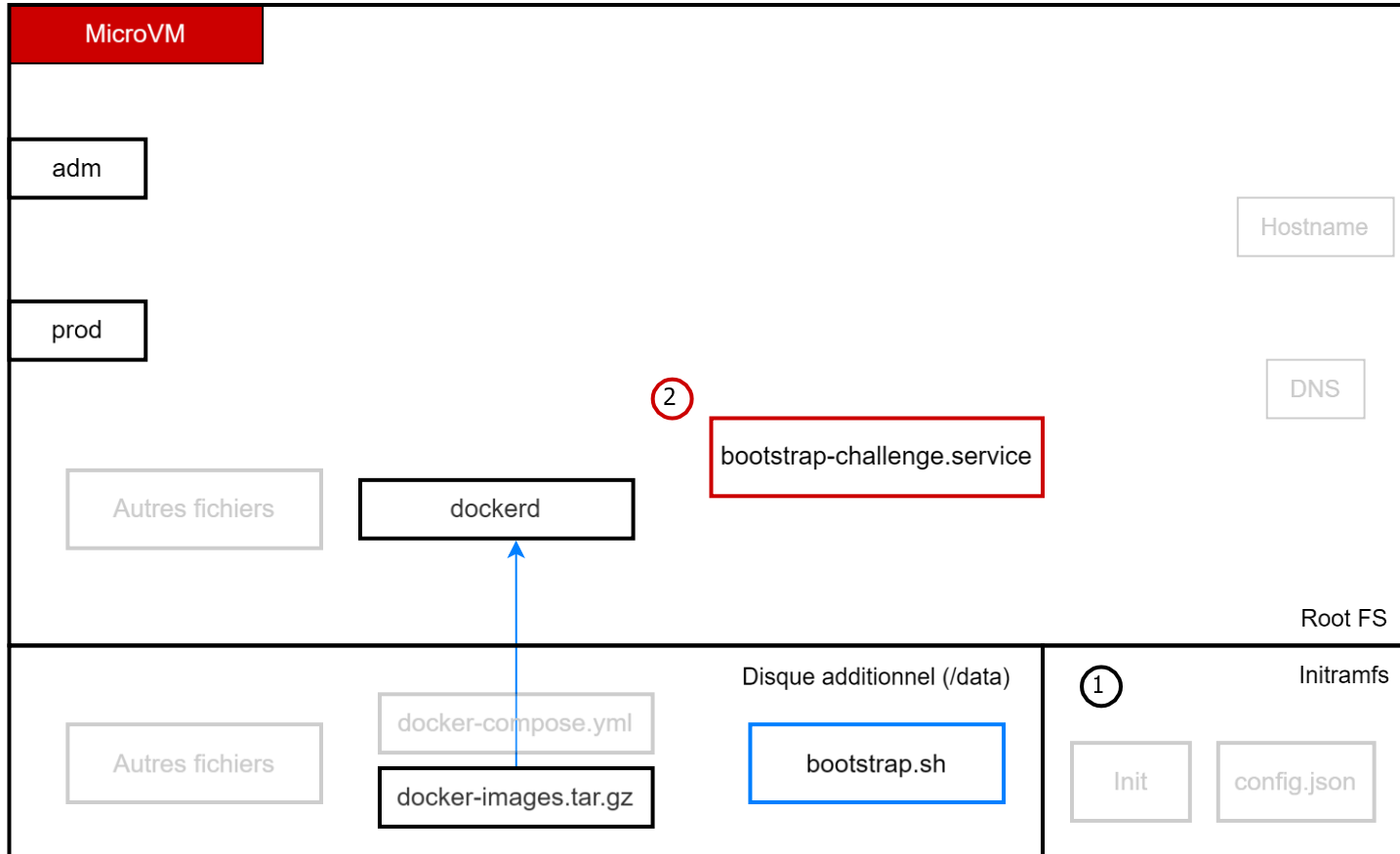


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

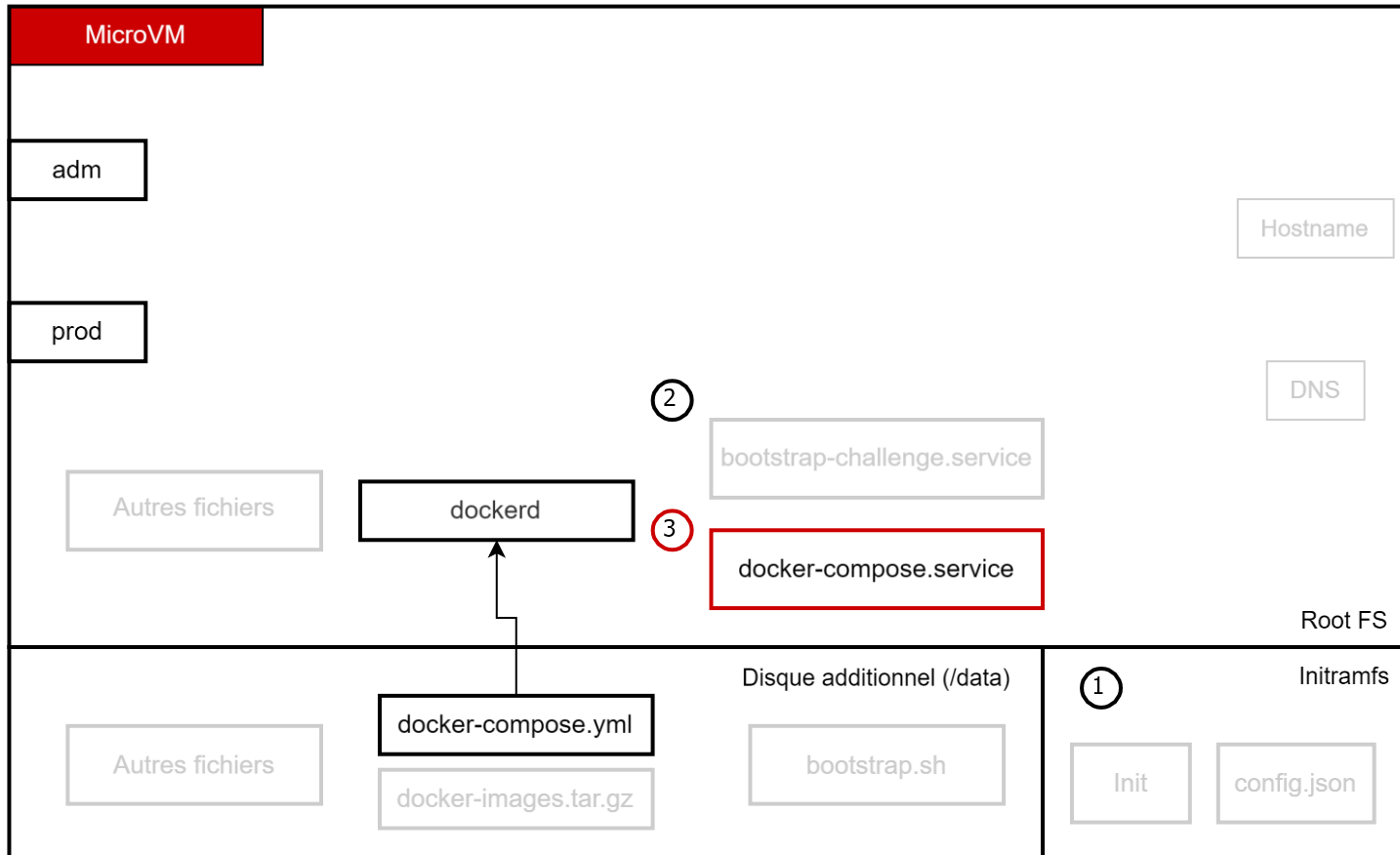


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

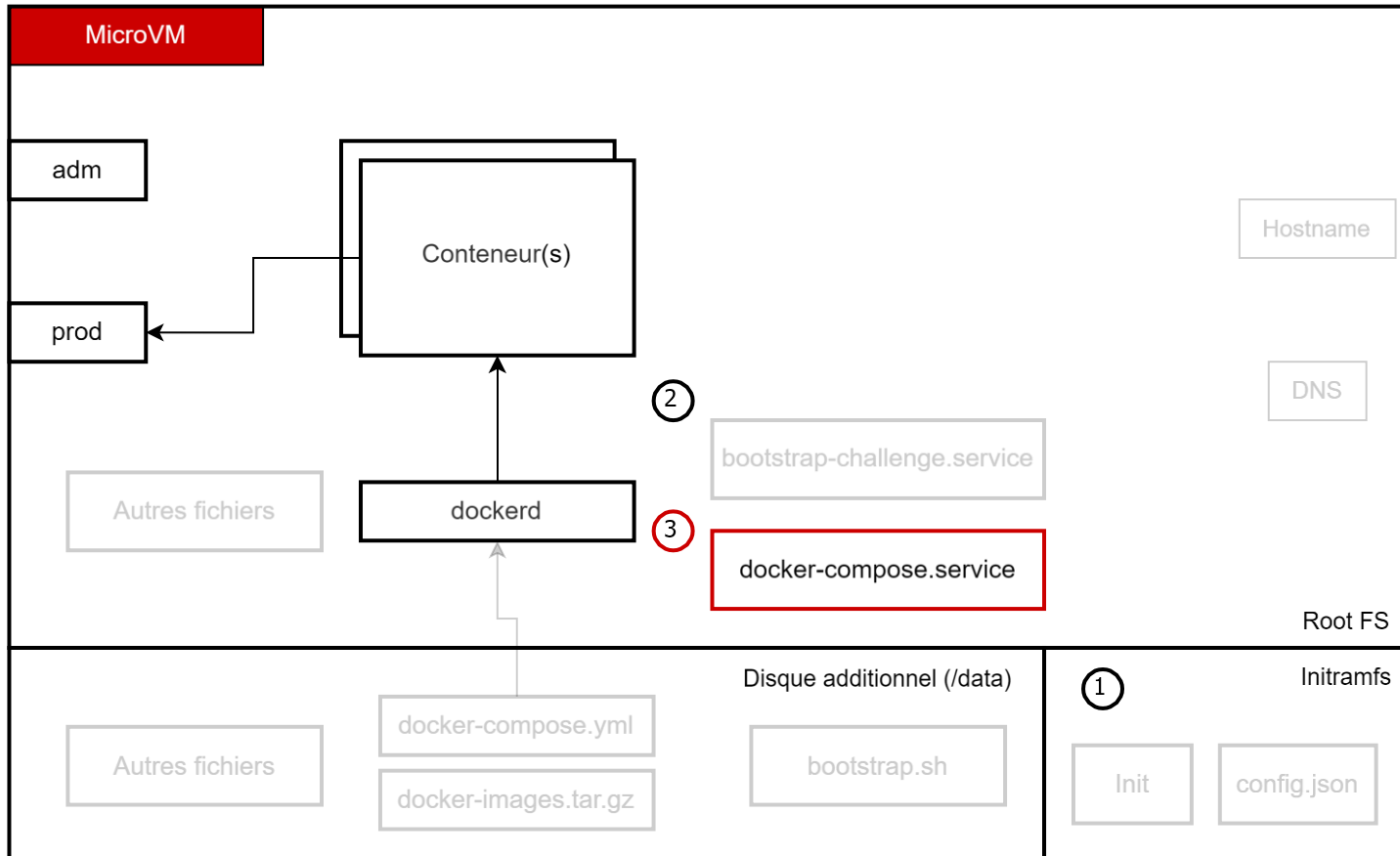


```
{
  "id": "file-checker",
  "vm_type": "firecracker",
  "hostname": "file-checker",
  "interfaces": [
    {
      "guest_dev": "eth0",
      "host_dev": "file-chk-p",
      "ip_configs": [
        {
          "host_net": "10.20.2.1/24",
          "guest_net": "10.20.2.2/24"
        }
      ]
    },
    {
      "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

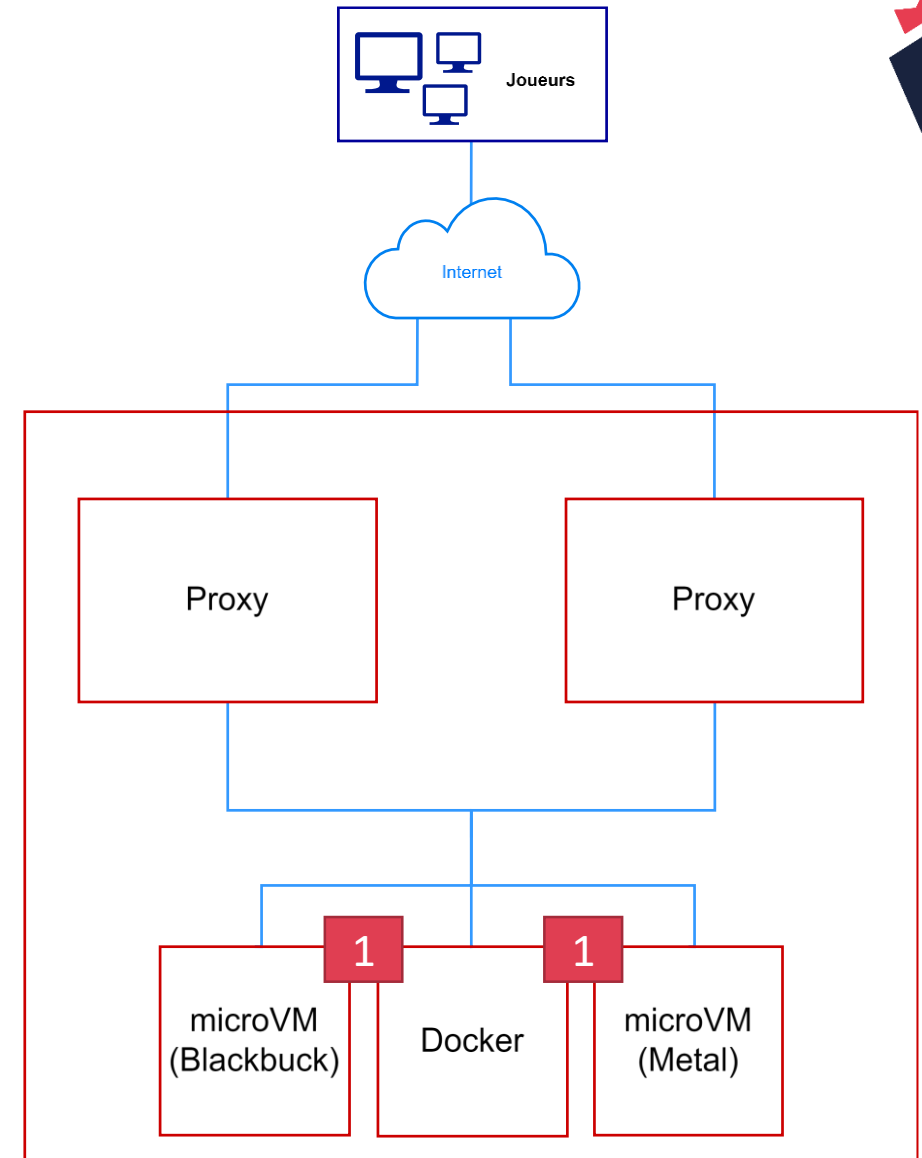


> Édition 2023

- Hybride conteneurs / microVM
- Solutions de microVM interchangeables

> Retour d'expérience

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



Architecture 2024

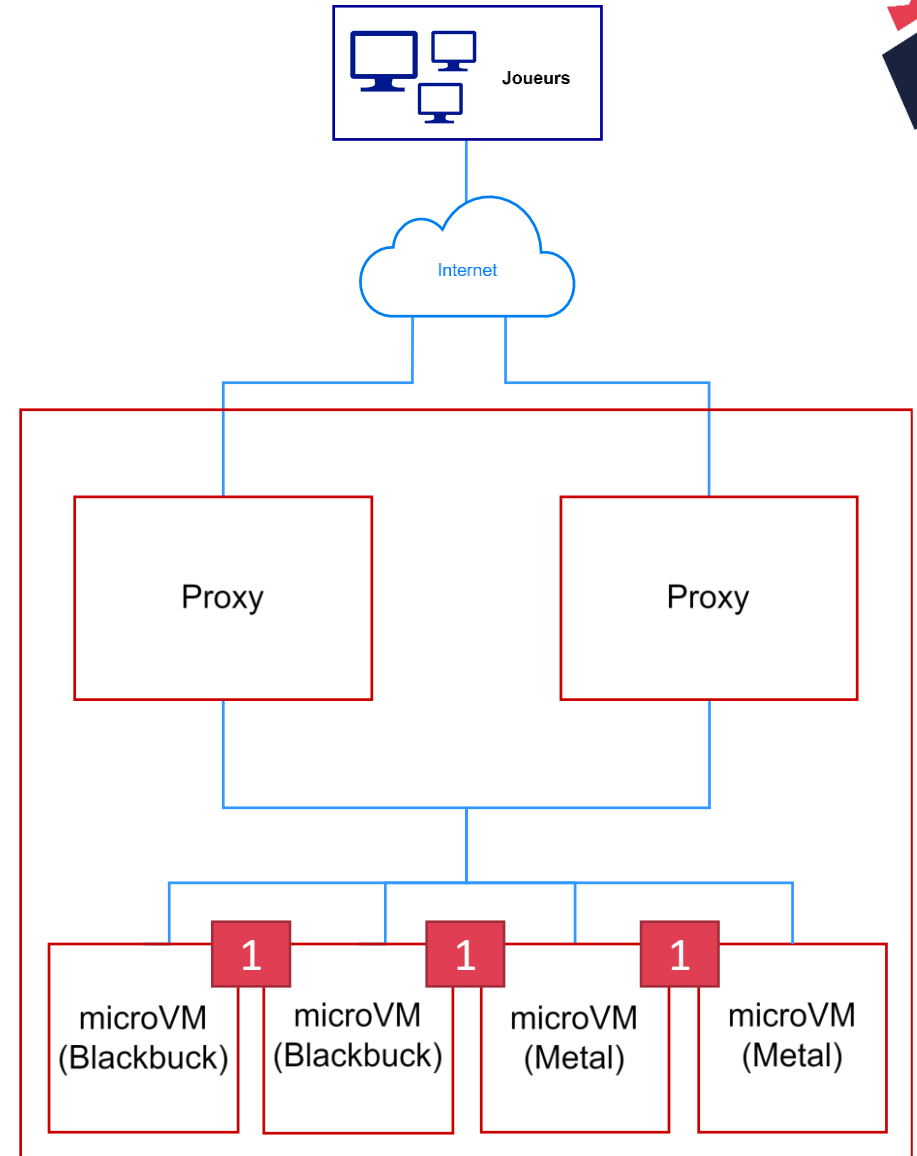


> 2024

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

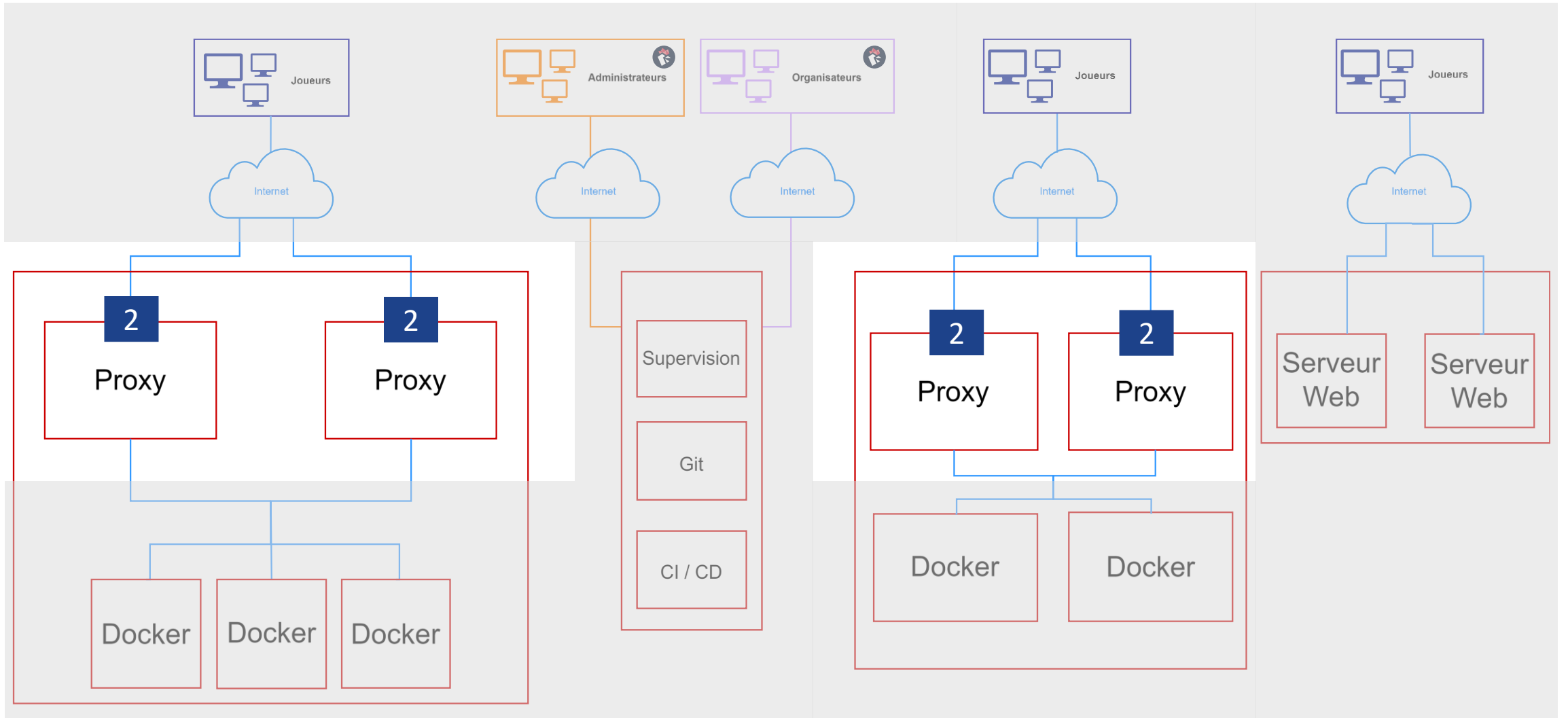
> Par serveur physique

- 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

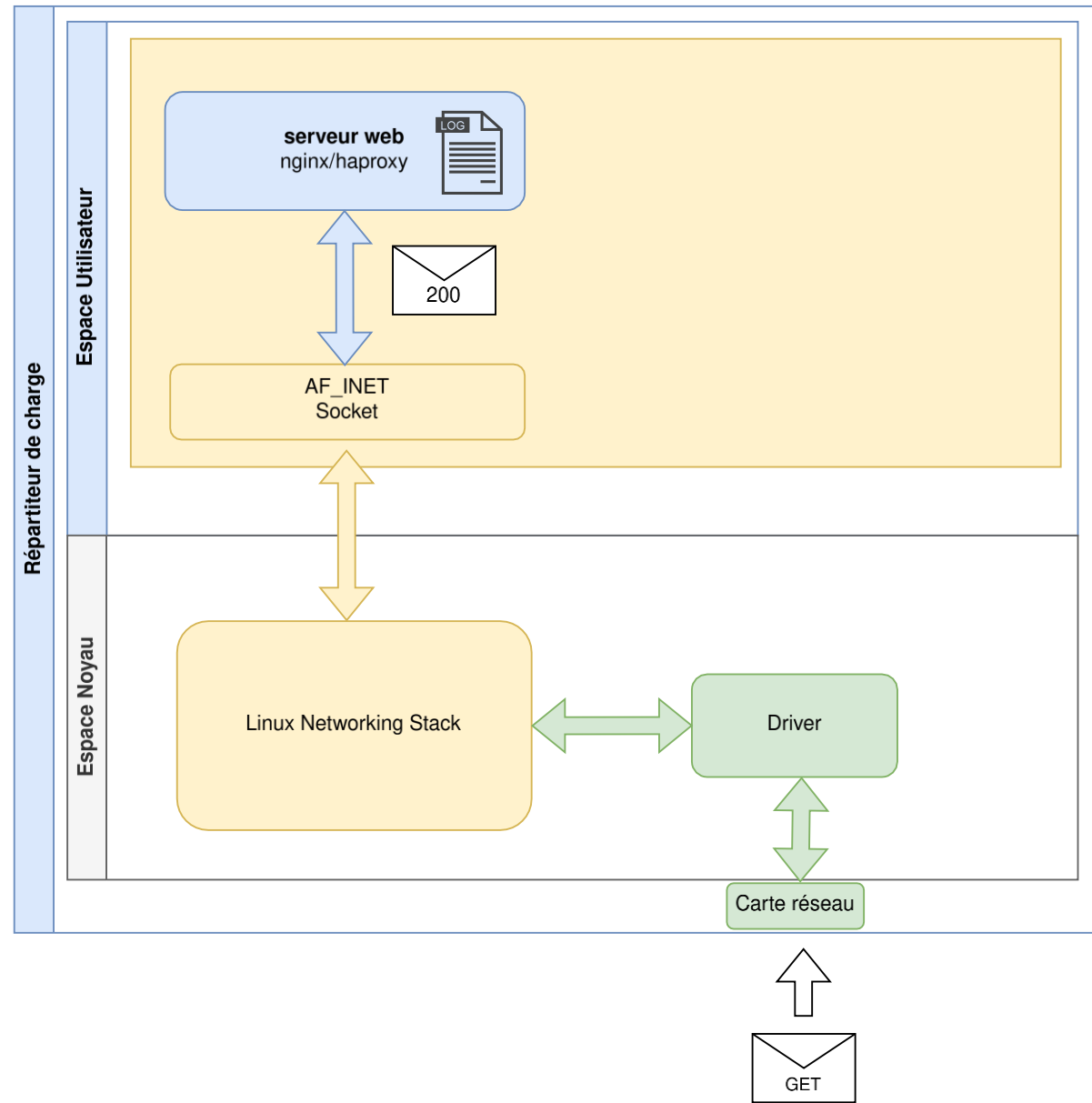
- Actif **avant** la protection réseau hébergeur



Hodor est né !

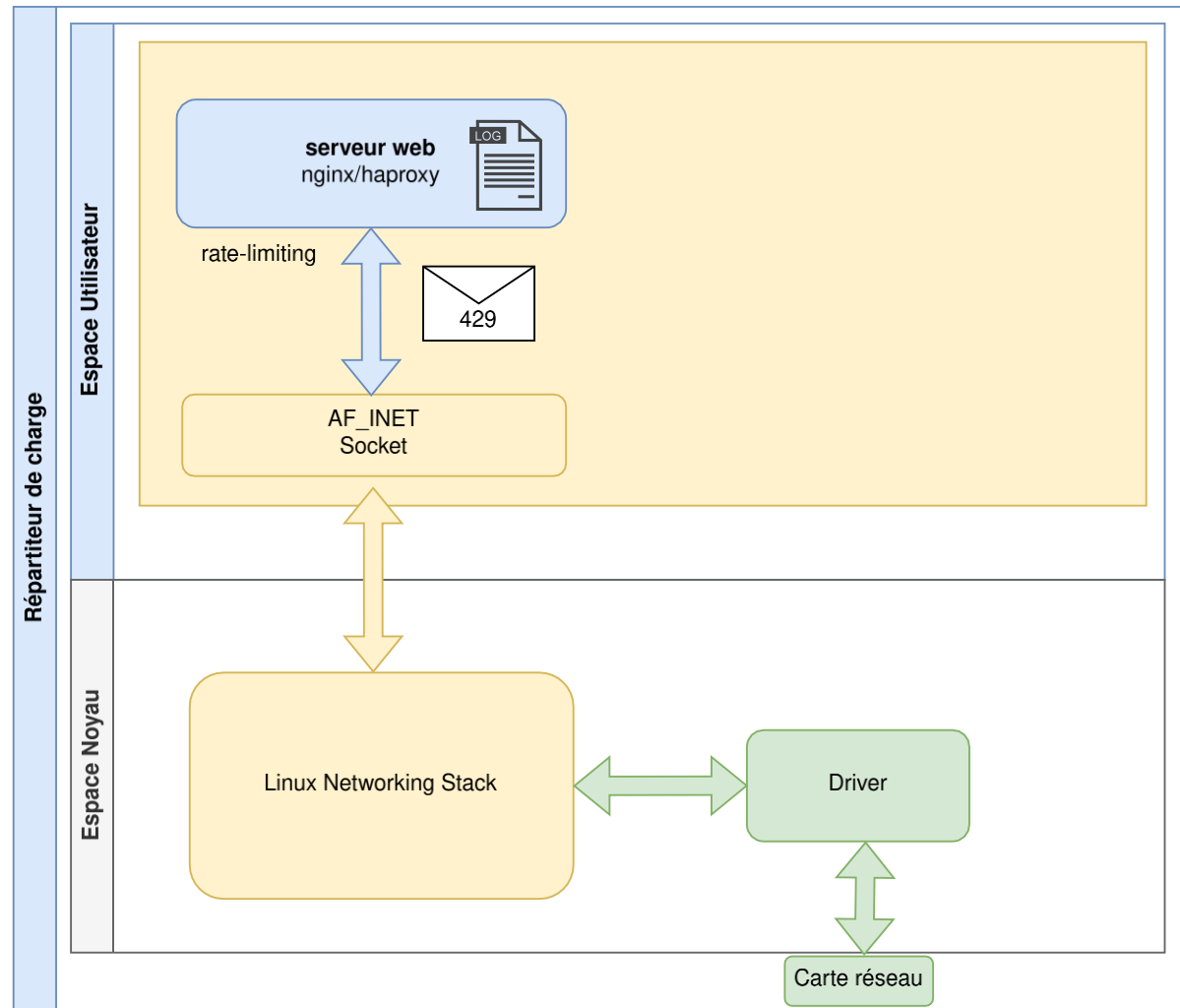
Protection DDoS - Hodor

> Trafic légitime, sans Hodor



Protection DDoS - Hodor

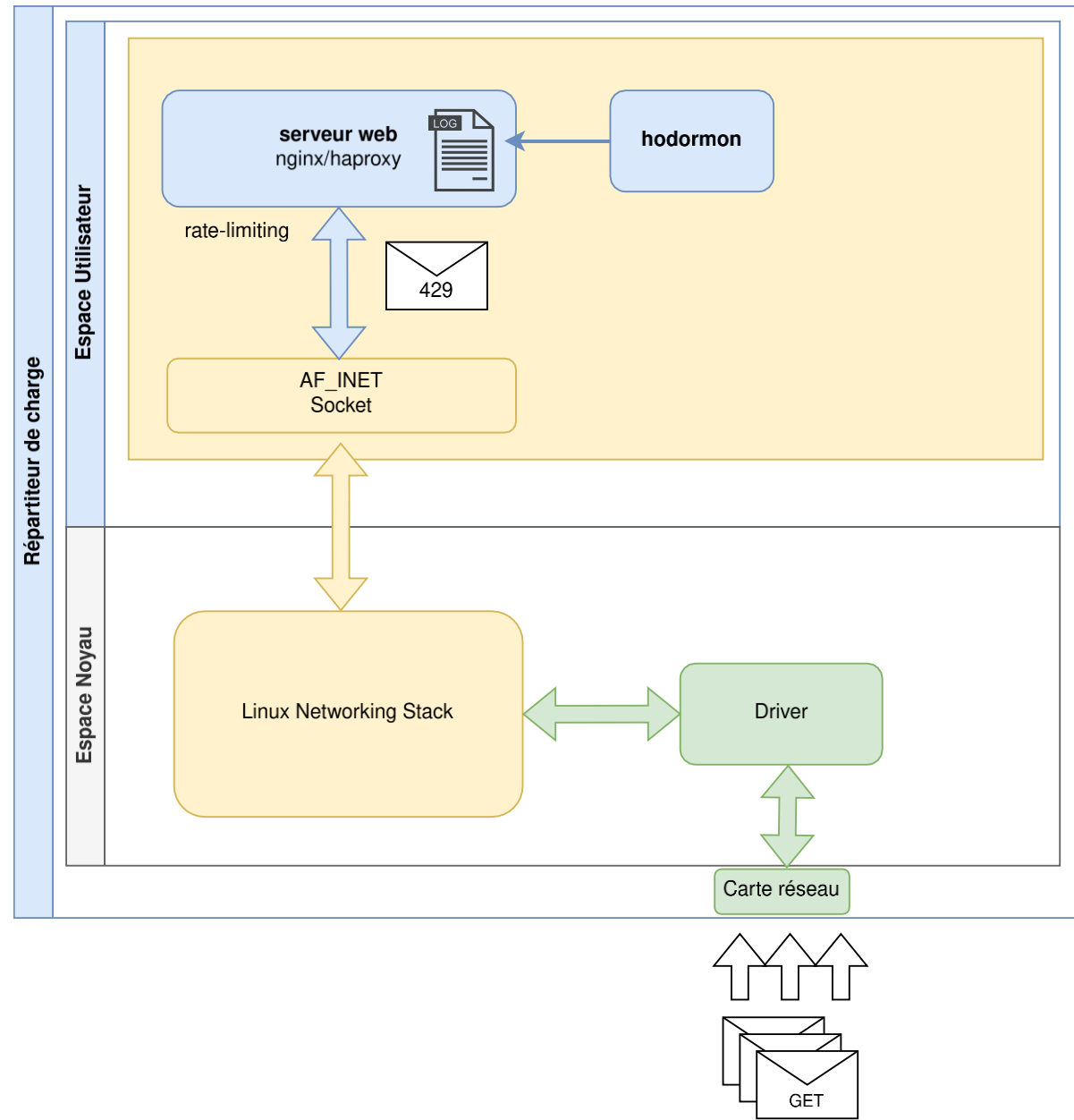
> Pic de trafic, sans Hodor



Protection DDoS - Hodor

> Hodormon

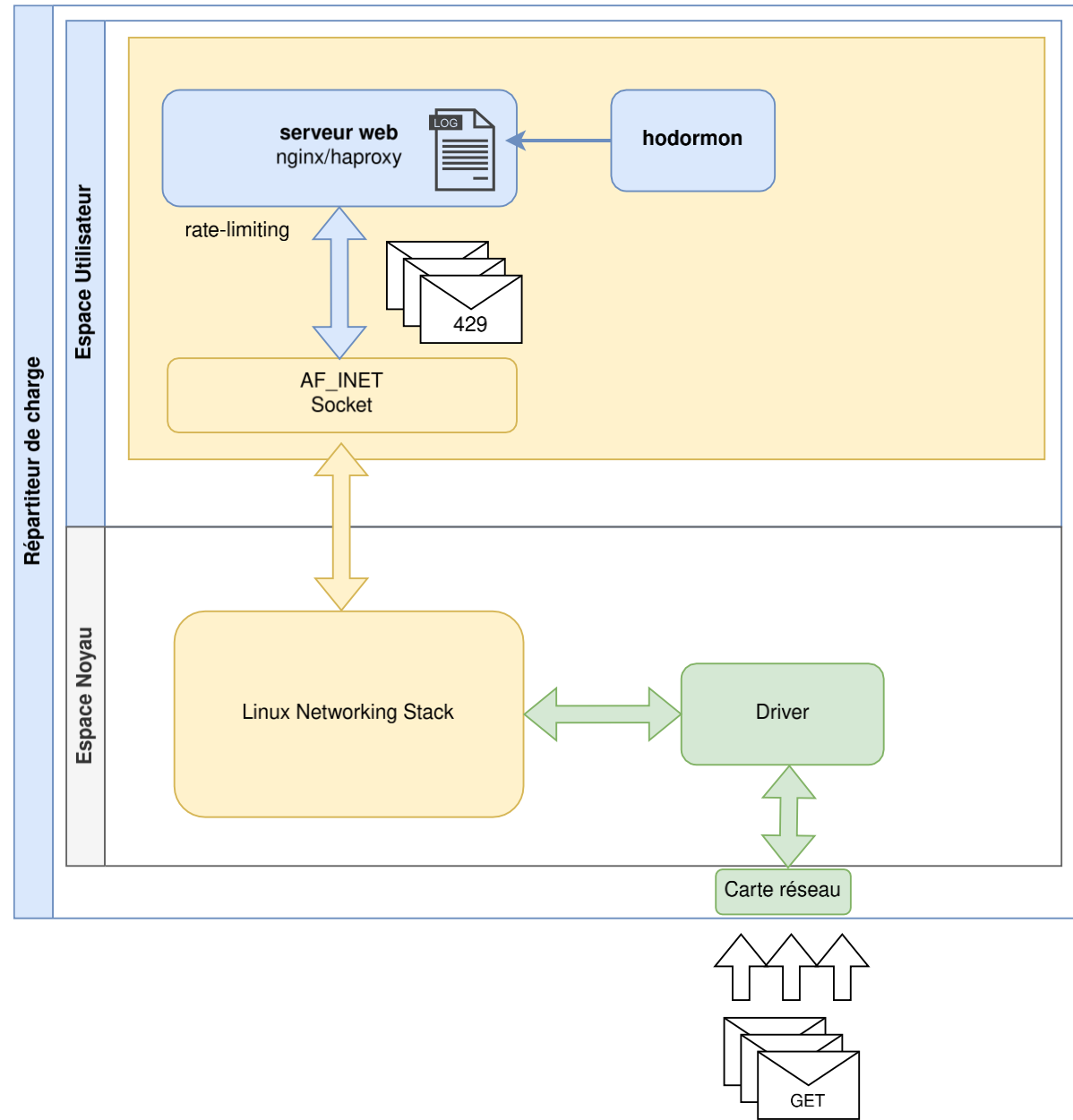
- Surveillance logs web
- Capacité : +300k logs/s



Protection DDoS - Hodor

> Hodormon

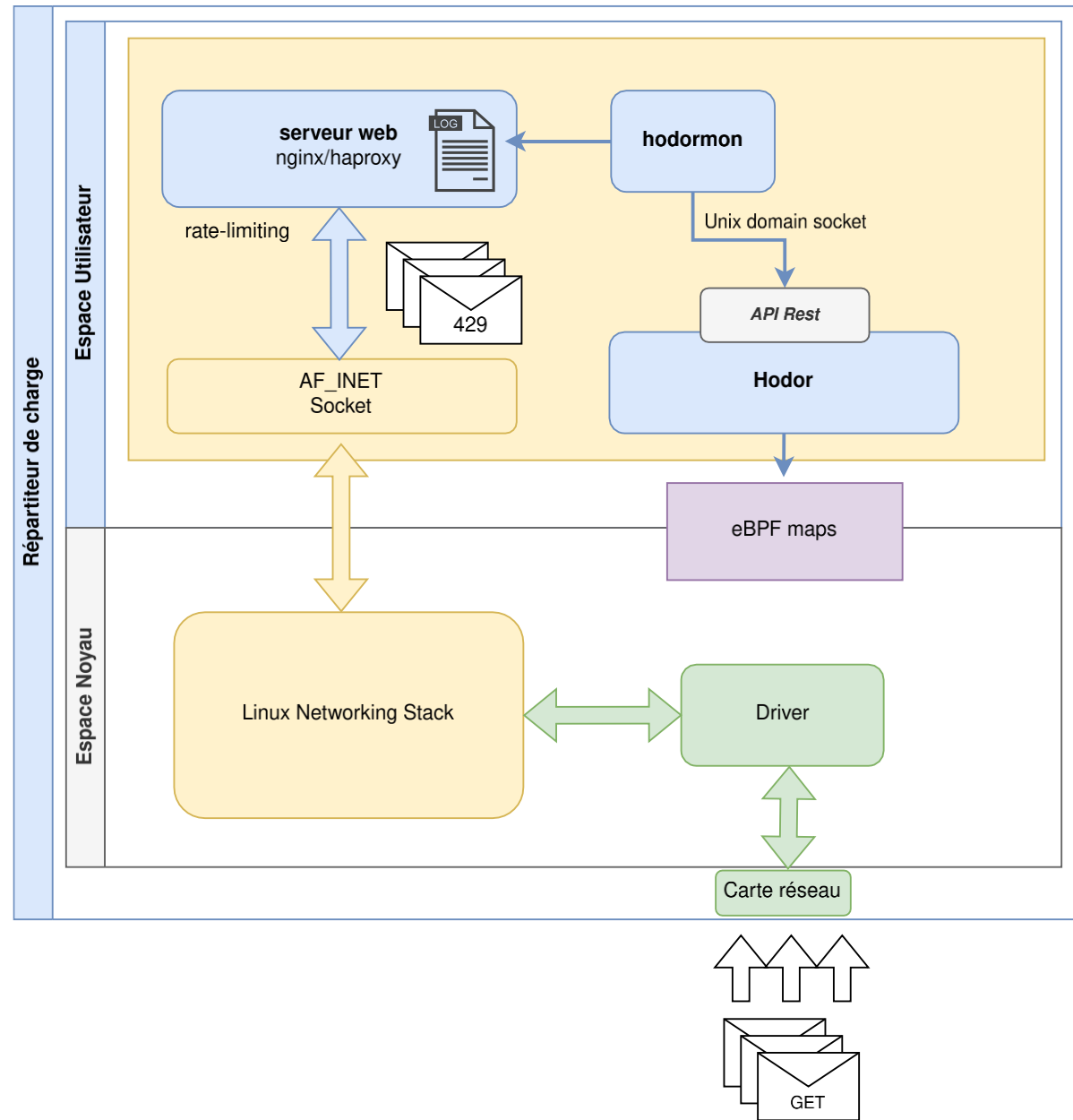
- Détection de nombreux dépassements du *rate-limiting* (429)



Protection DDoS - Hodor

> Hodormon

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



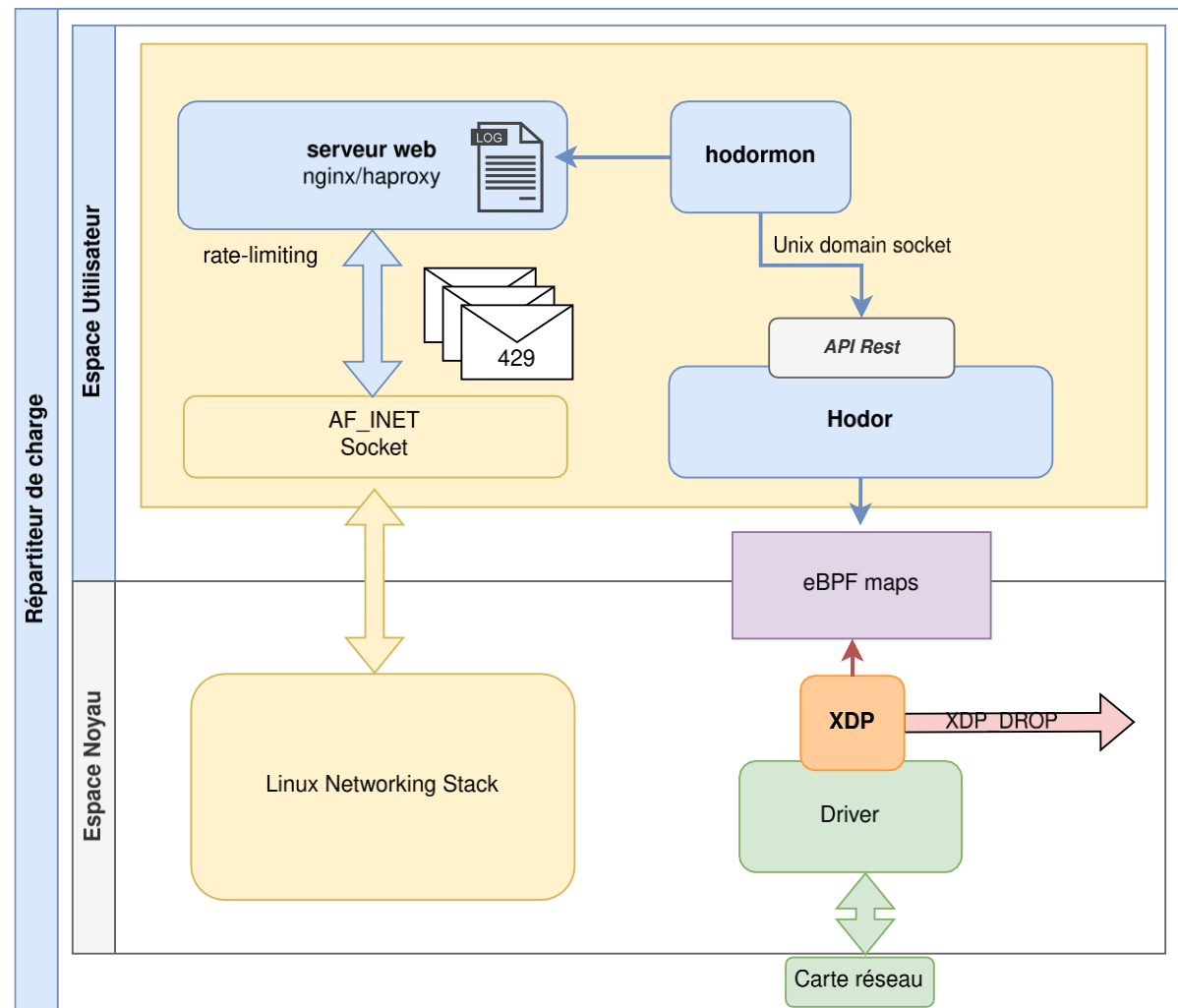
Protection DDoS - Hodor

> 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)

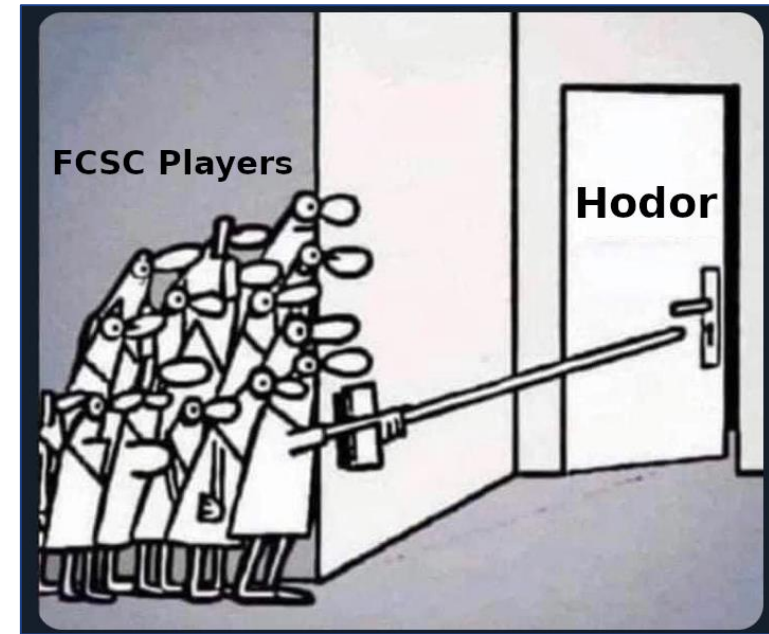
> Notification rapide (quelques secondes maximum)



hodor APP 29/03/2024 08:28

🔥 Hodor successfully banned **1** IPs during last 4s

```
🇫🇷 x.x.x.x on [france-cybersecurity-challenge.fr] banned for 376s:  
"GET /_flash HTTP/1.1" "gobuster/3.5"
```

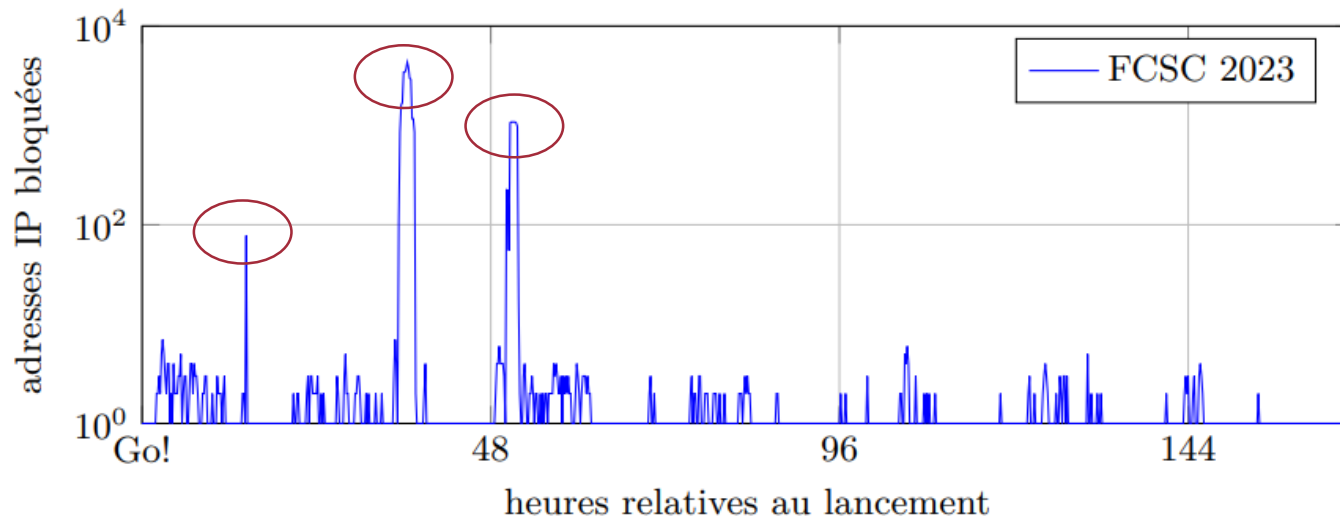


Protection DDoS – Blocage de vrais DDoS



> 2023 : vagues de DDoS successives

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



hodor BOT 23/04/2023 00:08

🔥 Hodor successfully banned **398 IPs** during last 4s
<https://www.youtube.com/watch?v=lnBZINtS0ec>

🔍 Temporarily turning off detail notifications under DDoS

YouTube

M-M-M-M-MONSTER KILL!

M-M-M-M-MONSTER KILL!

Disclaimer



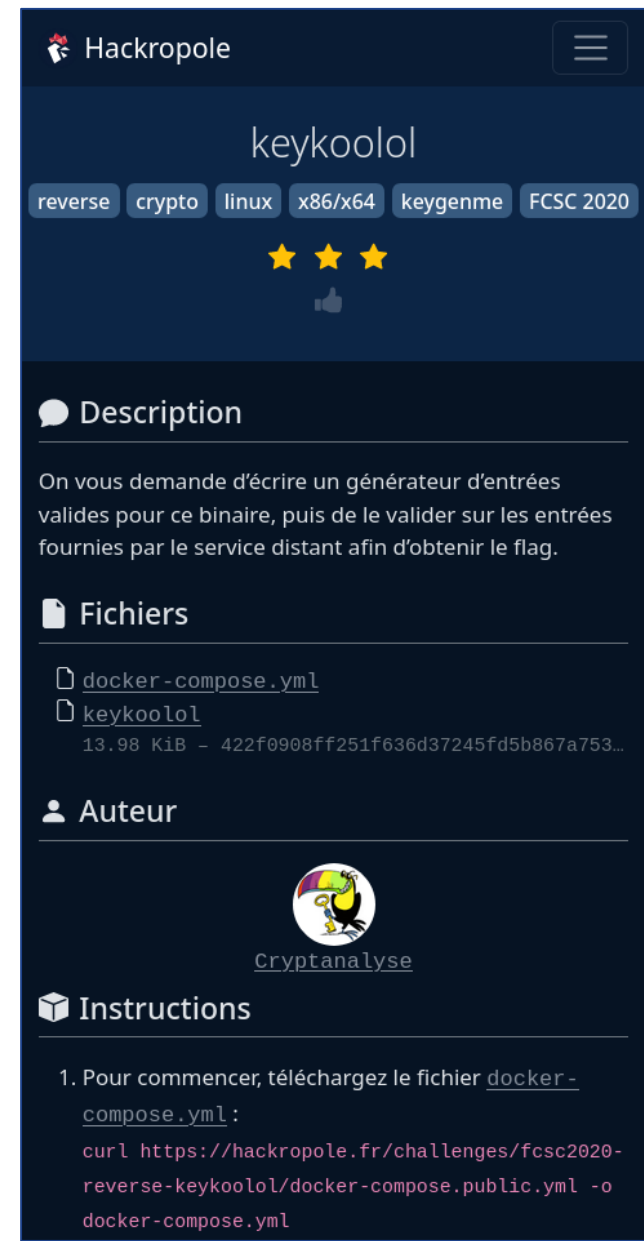
- Les solutions présentées ne constituent pas des recommandations de l'ANSSI
- Possible car c'est une infra temporaire (infra de CTF)
- Le but est de présenter des solutions possibles de cloisonnement d'applicatifs et d'anti-DDoS pour du CTF

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



The screenshot shows the Hackropole website interface. At the top, there is a navigation bar with the Hackropole logo, links for 'Épreuves', 'Statistiques', and 'FAQ', and a search bar containing the text 'Chercher une épreuve...'. Below the navigation bar, the main content area features the title 'Hackropole' in large black font. To the left of the title, there is a paragraph: 'Bienvenue sur Hackropole. Cette plateforme vous propose de rejouer les épreuves du France Cybersecurity Challenge tout au long de l'année dans le but de découvrir et de vous former à divers domaines de la cybersécurité.' Below this paragraph, there are two statistics: '431 épreuves de difficulté croissante.' and '327 solutions pour votre apprentissage.' A blue button labeled 'Explorer les épreuves' is positioned at the bottom left. On the right side of the main content area, there is a large illustration of a classical building with columns, rendered in a pixelated, digital style.



The screenshot shows the Hackropole challenge page for 'keykoolol'. The page has a dark blue background. At the top, the Hackropole logo is in the upper left, and a menu icon is in the upper right. The challenge title 'keykoolol' is centered. Below the title, there are tags: 'reverse', 'crypto', 'linux', 'x86/x64', 'keygenme', and 'FCSC 2020'. There are three yellow stars and a thumbs-up icon below the tags. The 'Description' section contains the text: 'On vous demande d'écrire un générateur d'entrées valides pour ce binaire, puis de le valider sur les entrées fournies par le service distant afin d'obtenir le flag.' The 'Fichiers' section lists two files: 'docker-compose.yml' and 'keykoolol', with the latter having a size of '13.98 KiB' and a hash '422f0908ff251f636d37245fd5b867a753...'. The 'Auteur' section shows the profile of 'Cryptanalyse', which includes a circular profile picture of a penguin and the name 'Cryptanalyse'. The 'Instructions' section contains a list with one item: '1. Pour commencer, téléchargez le fichier `docker-compose.yml`:' followed by a code block:

```
curl https://hackropole.fr/challenges/fcsc2020-reverse-keykoolol/docker-compose.public.yml -o docker-compose.yml
```



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 patches 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 alumni de la Team France