EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

# Egide, yet another security box…


Jérémy De Cock

jdecock@cyberzen.com


14/02/2023

cyberzen

# QUI SUIS-JE ?

## $ whoami

- Jérémy DE COCK, 23 ans
- Consultant en cybersécurité

## $ mount –o nosuid,nodev,noexec /life

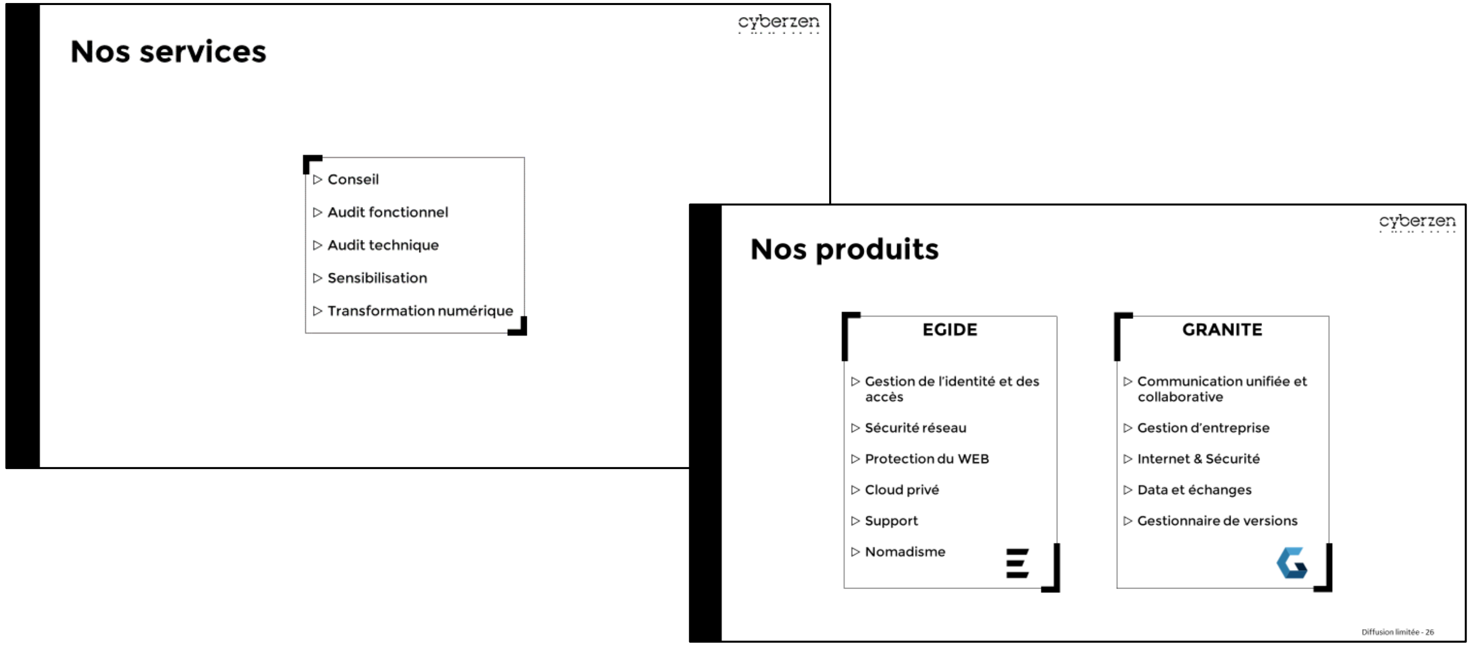
- Master of Science Management de la Cybersécurité
  - Alternance chez Cyberzen (1 an)
- MS-SIS « Expert de la Sécurité des Systèmes d'Informations »
  - Stage chez Cyberzen (6 mois)
- Passionné par les travaux de Alan Turing
  - Sujet de mémoire de Master
- Passionné de CTF
  - En préparation de l'OSCP
  - {Pentesterlab, Root-me, Hackthebox} certified


https://www.cyberzen.com/

@Alguna_Pseudo

linkedin.com/in/jeremy-dc

# PRÉSENTATION DE CYBERZEN



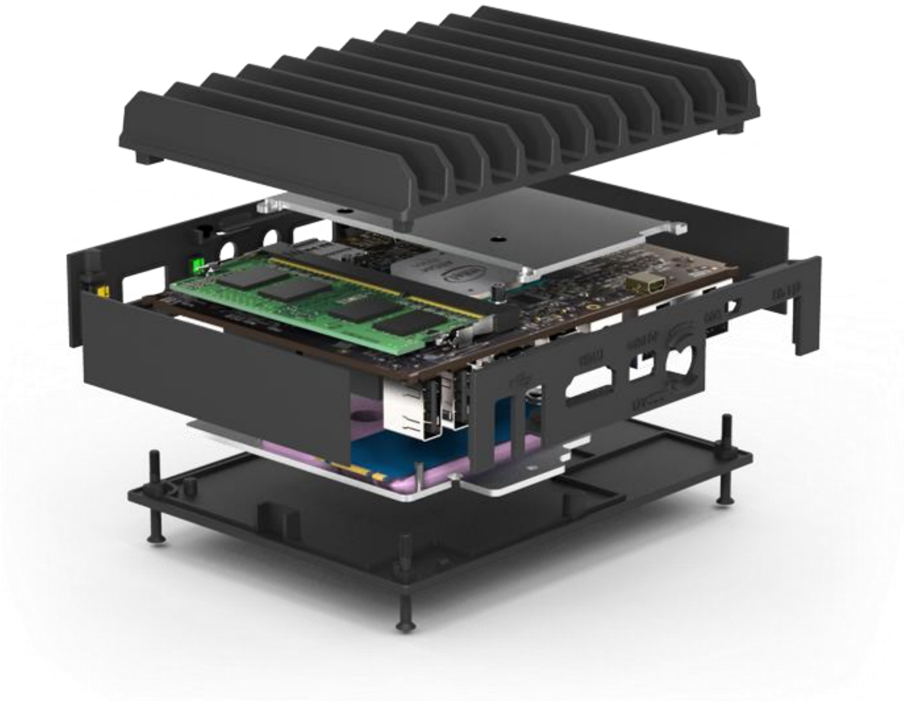
# « Mon stage »

# 3615 ma vie… chez Cyberzen

- En **alternance**, j'ai travaillé sur l'établissement des bases du boîtier Egide : virtualisation, pare-feu, DHCP, gestionnaire de mots de passe, VPN…

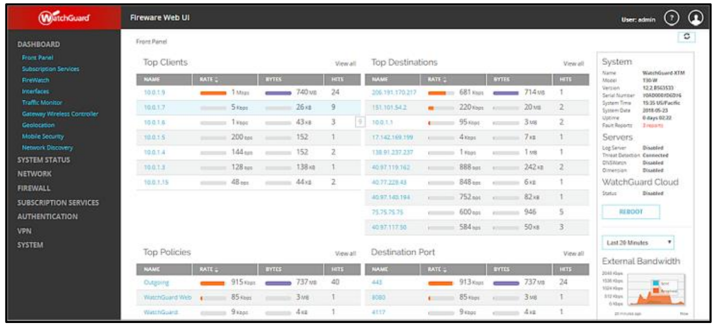
- En **stage**, j'ai pu continuer mon travail sur un boîtier qui avait bien avancé en mon absence…

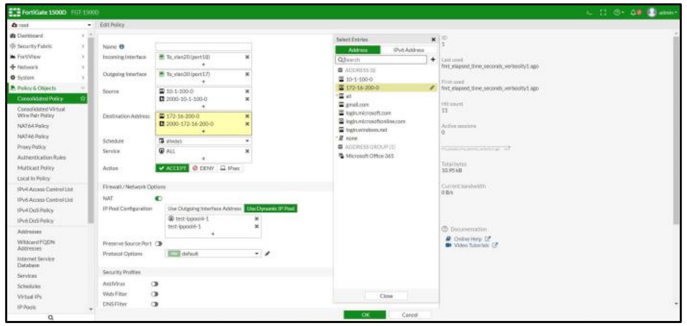
# PRÉSENTATION D’EGIDE
## Version simplifiée



- → Protège les données
- → Segmente le réseau
- → Autorise et supervise les flux
- → Est supervisé 24h/24 et bien plus encore…

# UN ECOSYSTÈME TRÈS PRESENT





*Ou encore…*

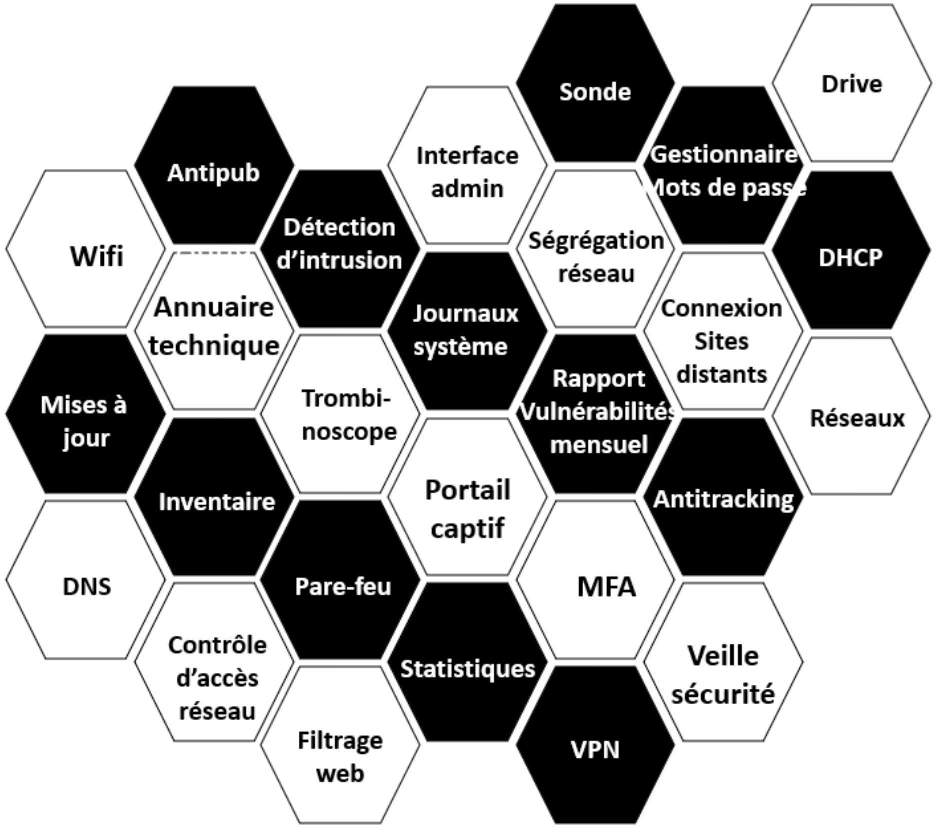
Bitdefender BOX

# POURQUOI UN NOUVEAU BOÎTIER ?

- Une technicité préalable importante et nécessaire
- Des boîtiers pensés globalement pour la sécurité de l'infrastructure, pas pour les usagers
- Des interfaces par des admins pour des admins
- Des besoins de mises à jour non gérés avec des coûts de licences pouvant être importants
- Des technos internes obscures qui s'appuient souvent sur l'open source sans jamais vouloir le dire
- En général, des technos non européennes
- On pourrait en parler pendant des heures…

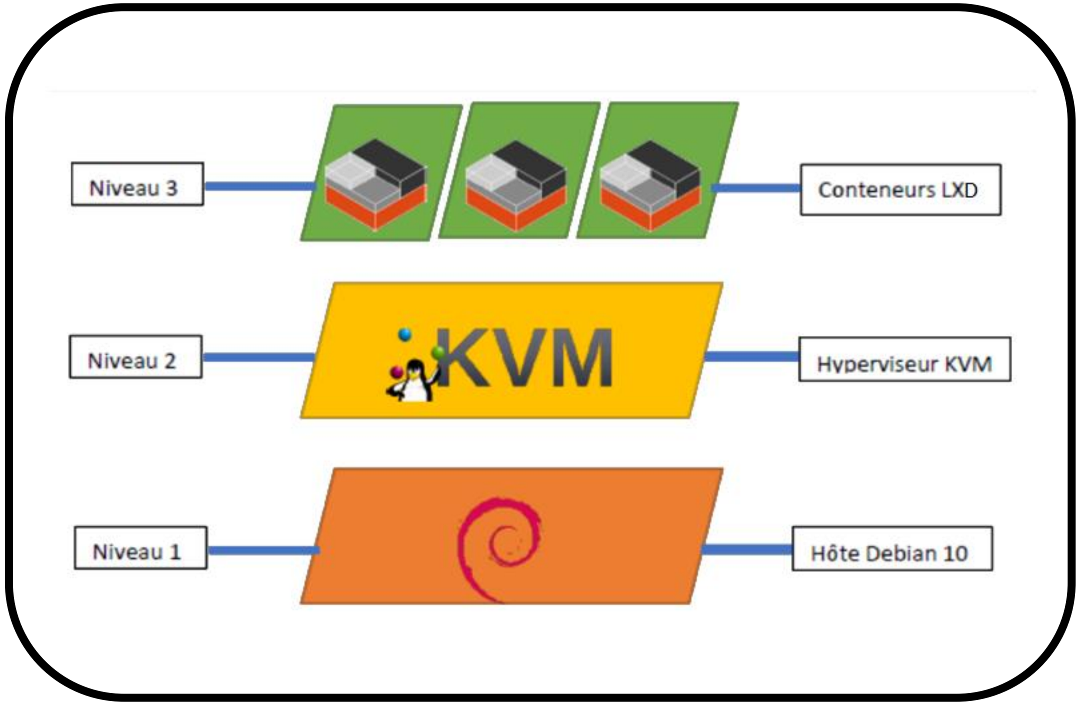
***DU PRAGMATISME !***

# PRÉSENTATION D'EGIDE
## Version détaillée




- → Gestion de l'identité et des accès
- → Sécurité réseau
- → Protection du web
- → Cloud privé
- → Nomadisme
- → Support

# ARCHITECTURE
## Virtualisation




→ Le reste : 1 applicatif / **LXD**

→ **DNS** , **VPN** & **pare-feu** sur la **KVM**

→ **DHCP** & **pare-feu** sur l’hôte

# ARCHITECTURE
## Hôte vs KVM

| ***NIVEAU 1 - HÔTE*** |
|---|
| Interface de configuration de Netfilter |
| Serveur DHCP |
| Serveur SSH léger utilisé pour le déchiffrement |
| Binaire minimum compilé statiquement |
| Emule le processeur et les périphériques |

| ***NIVEAU 2 - KVM*** |
|---|
| Interface de configuration de Netfilter |
| Gestionnaire de conteneurs |
| Serveur DNS |
| Serveur VPN |
| Serveur Reverse-Proxy |

# ARCHITECTURE
## LXD disponibles

| *Que pouvons-nous retrouver dans les LXD ?* |
| --- |
| Gestionnaire de mots de passe |
| Serveur d’inventaire |
| Serveur d’annuaire |
| Serveurs pots de miel : HTTP, SSH, FTP, VNC, RDP, MySQL, etc. |
| Contrôleur de domaine : DNS, LDAP, Kerberos, RPC, SMB 3.0 |
| Scanneur de vulnérabilités |
| Interface web d’administration |

Une application = un conteneur LXD !

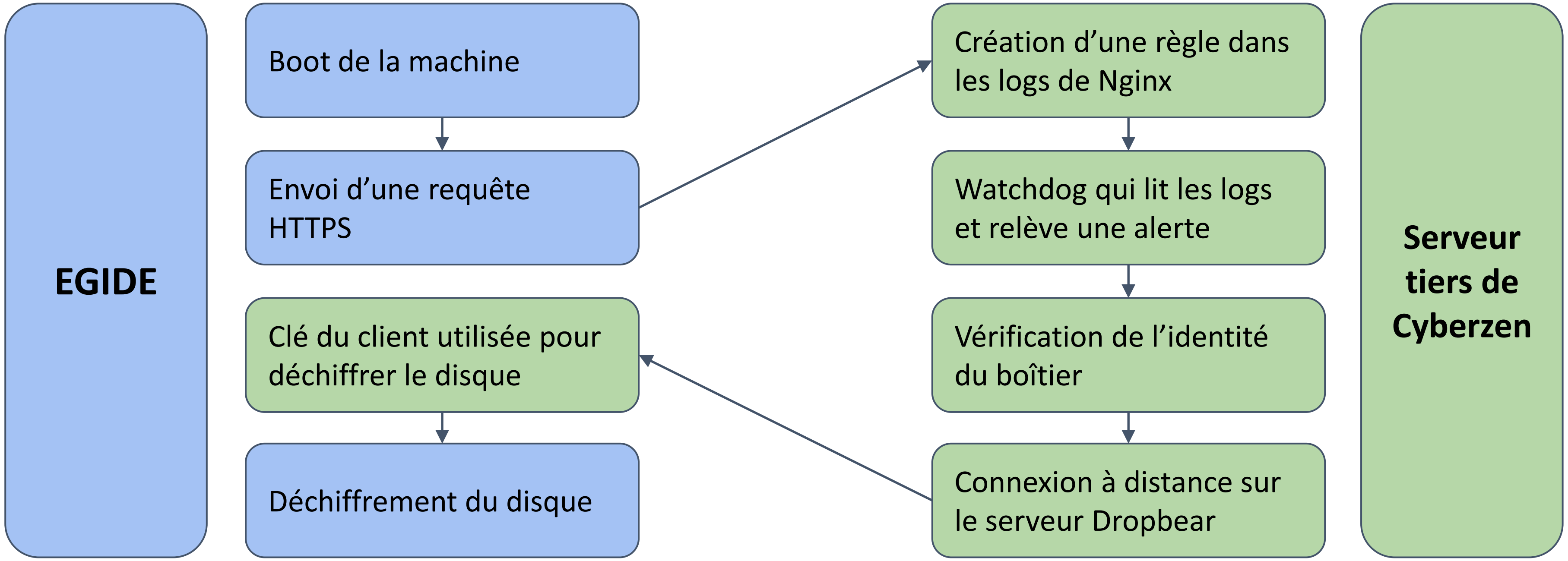
# ARCHITECTURE
# Logiciels présents à chaque niveau

| *Qu'avons-nous partout ?* |
| --- |
| Gestionnaire d'accès applicatifs |
| Utilitaire gérant la rotation automatique des logs |
| Utilitaire transférant les logs |
| Composant de Saltstack qui exécute des tâches définies par son Master |
| Utilitaire chiffrant une archive .tar.gz avec GPG |
| Shell de conteneurs / service SSH |
| Utilitaire qui permet de maintenir l'horloge système "à l'heure" |

Ces listes sont non exhaustives.

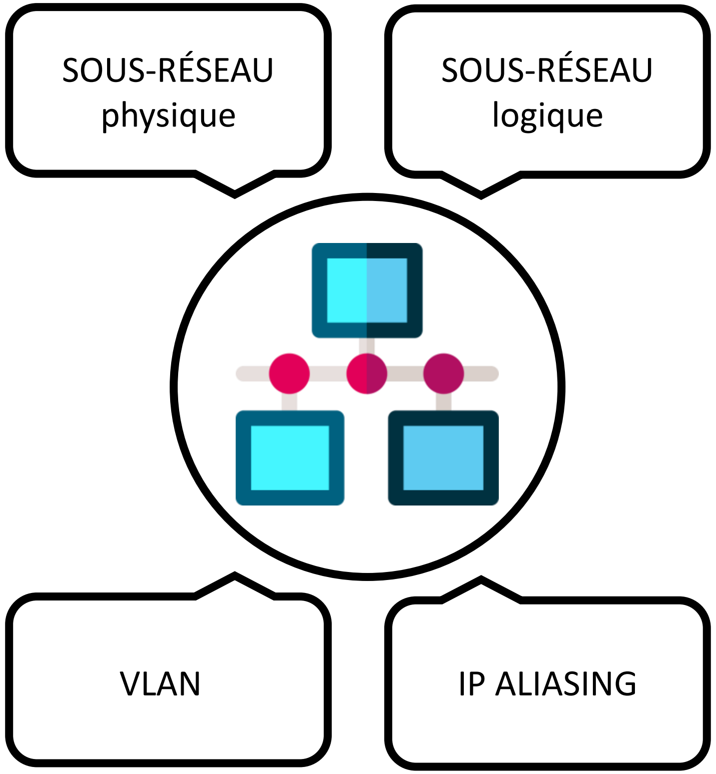
# FONCTIONNALITÉS
## Déchiffrement à distance du disque

*“Le contenu du disque est chiffré. Lorsque le boîtier redémarre, comment effectuer le déchiffrement automatiquement ?”*



# FONCTIONNALITÉS
## Segmentation du réseau

*“Le boîtier dispose de deux interfaces physiques. Comment mettre en place 3, 4 ou 10 sous-réseaux ?”*



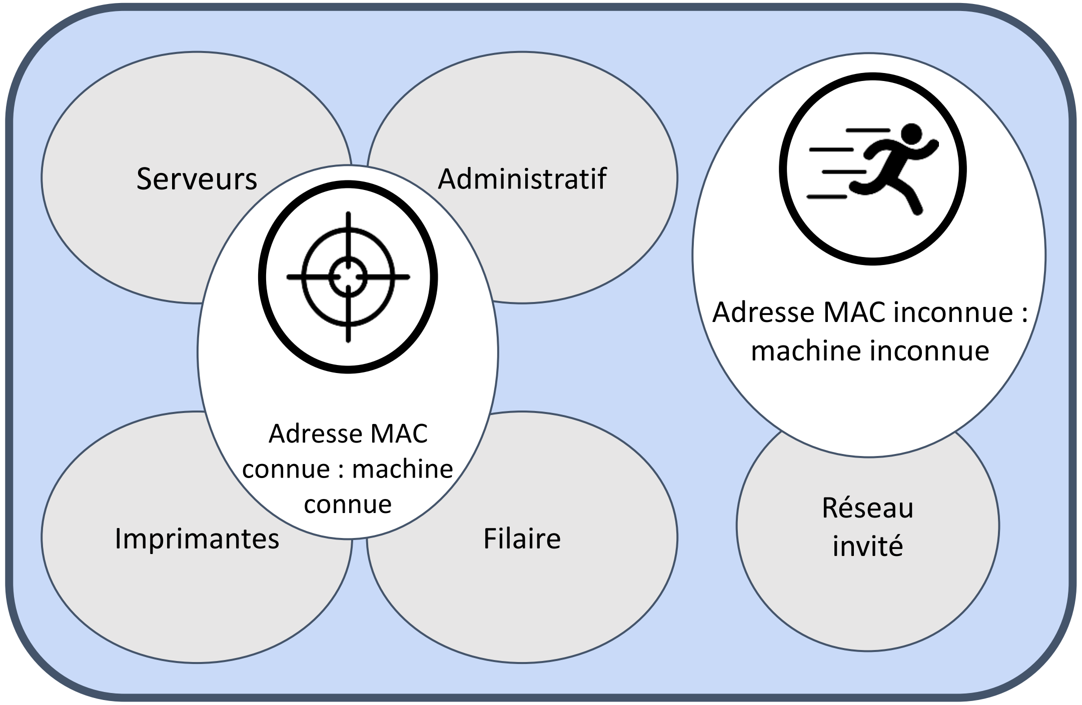

```
auto eno1
iface eno1 inet static
        address 192.168.1.1/24
        dns-nameservers 1.1.1.1
        dns-search cloudflare.com
        post-up ifup eno1:100
        post-up ifup eno1:110

iface eno1:100 inet static
        address 192.168.2.1/24

iface eno1:110 inet static
        address 192.168.3.1/24
```

*/etc/network/interfaces*

→ eno1 : 192.168.1.0/24
→ eno1:100 : 192.168.2.0/24
→ eno1:110 : 192.168.3.0/24

# FONCTIONNALITÉS
## Sous-réseau par défaut

*“Si une personne malveillante se connecte en filaire sur le réseau de l’entreprise avec sa machine, comment l’isoler ?”*



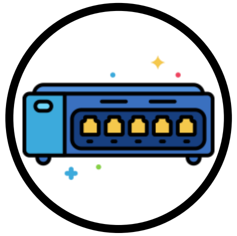

```
shared-network eno2_default {
        boot-unknown-clients on;

        subnet 192.168.50.0 netmask 255.255.255.0 {
                option routers 192.168.50.1;
                option domain-name-servers 1.1.1.1;
                range 192.168.50.10 192.168.50.100;
        }
}
```

*/etc/dhcp/dhcp.conf*

# FONCTIONNALITÉS
## Pourquoi les adresses MAC ?

*“Si une personne malveillante se connecte, elle va pouvoir utiliser de l’ARP spoofing, c’est nul comme protection”*


802.1x



BON EQUIPEMENT ?

# FONCTIONNALITÉS : Gestion des zones DNS par ACL

*"Le boîtier fournit un service DNS. Peut-on restreindre la résolution de certains noms à certaines adresses IP ?"*

- On a définit des ACLs →

```
acl my_net_1 { 192.168.1.0/24; };
acl my_net_2 { 192.168.2.0/24; };
acl my_net_3 { 192.168.3.0/24; };
```

- On a configuré des vues DNS →

```
view trusted {
        match-clients { my_net_1 ; };
        allow-recursion { my_net_1; };
        include "/etc/bind/named.conf.default-zones";
        include "/etc/bind/zones.rfc1918";
        include "/etc/bind/zones.cyberzen";
        response-policy { "test.cyberzen.com"; };
};
```

- On a configuré des DNS menteurs →

```
zone "test.cyberzen.com" { type master; file "/etc/bind/db.testzone"; };
```

- Et on a finalement créé nos zones DNS : enregistrements A, CNAME, etc.

# FONCTIONNALITÉS :
# Environnement isolé (chroot)

*“Est-il possible de lancer un service dans un environnement isolé du reste ? Pour Rsyslog par exemple ?”*

PARTITION /CHROOT

DÉPENDANCES ?

→ **ldd** : librairies nécessaires
→ **strace** : complément à ldd

GO TO /chroot/…

Exemple de dépendances pour Rsyslog :

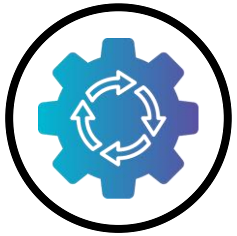
```
cp /usr/sbin/rsyslogd /chroot/rsyslog/usr/sbin/rsyslogd
cp /lib64/ld-linux-x86-64.so.2 /chroot/rsyslog/lib64
cp /lib/x86_64-linux-gnu/libz.so.1 /chroot/rsyslog/lib/x86_64-linux-gnu
cp /lib/x86_64-linux-gnu/libpthread.so.0 /chroot/rsyslog/lib/x86_64-linux-gnu
```

# FONCTIONNALITÉS :
## Hardening du boîtier

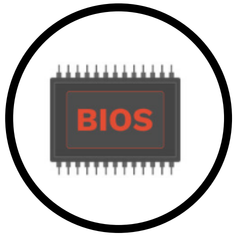
*"L'ANSSI a rédigé un guide sur les recommandations de sécurité relatives à un système GNU/Linux. Suivons-le !"*


80 RÈGLES

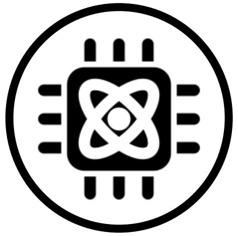
SCRIPTS HARDENING & KERNELGEN



CHANGEMENT PRODUCTION




BIOS



KERNEL


RECOMMANDATIONS DE CONFIGURATION D'UN SYSTÈME GNU/LINUX

GUIDE ANSSI

PUBLIC VISÉ :

Administrateur RSSI

Dernière version : 03/10/2022

# FONCTIONNALITÉS :
## Filtrage des paquets .deb

*"Tout ce qui est présent actuellement sur le boîtier, est-il encore nécessaire ?"*

- Utiliser **deborphan** pour lister les paquets non essentiels
- Utiliser **debsecan** pour lister les vulnérabilités concernant les paquets présents sur la machine
- Mettre en place un miroir APT

```
deb http://ftp.fr.debian.org/debian stable main contrib
deb-src http://ftp.fr.debian.org/debian stable main contrib
```

→

```
deb [trusted=yes] http://[IP CYBERZEN]/ stable main
```

*/etc/apt/mirror.list : avant / après*

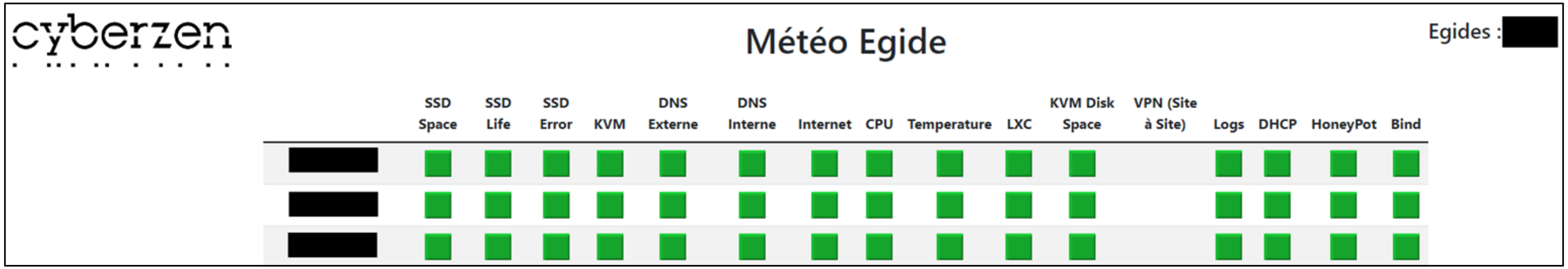
# FONCTIONNALITÉS :
## Monitoring des activités

*“Est-ce qu’une attaque est en cours sur le réseau ? Avons-nous des logs ? Avons-nous des backups ? Egide fonctionne t-il ?”*

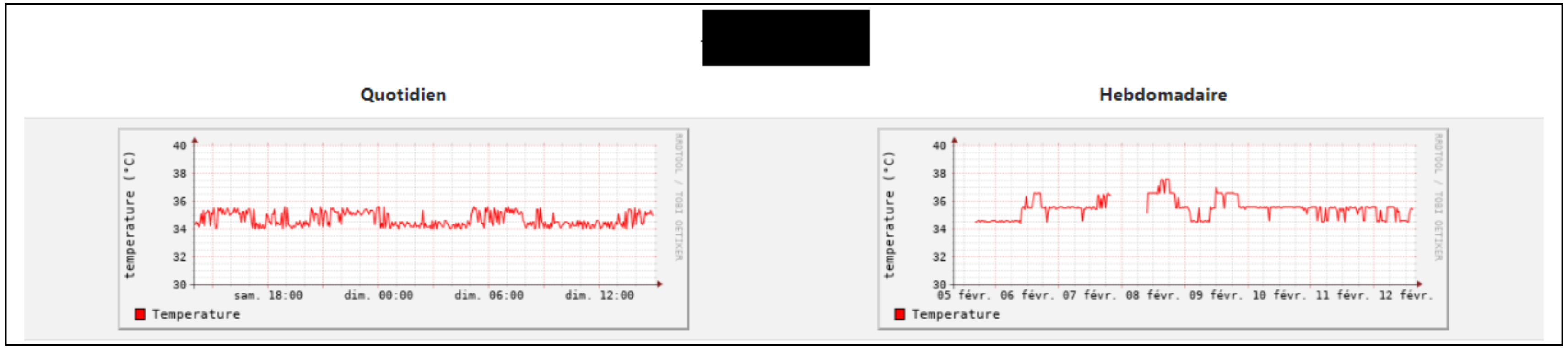
PROGRAMMES PYTHON

→ **Backup** (chiffrée avec GPG) : Succès ? Taille cohérente ?
→ **Météo** : Egide allumé ? Activité suspecte ? Tout fonctionne ?

MAIL




*Vue côté Cyberzen*




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| SSD Space : 12 | SSD Life : 100 | SSD Errors : 0 | KVM : On | DNS Externe : On | DNS Interne : On | Internet : On | VPN (Site à Site) : On | CPU (idle) : 99 | Temperature : 35 |

| | | | | |
|---|---|---|---|---|
| Machines : 192.168.1.254, [redacted] | eno1 RX : 5987149662 | eno1 TX : 50984684295 | enp2s0 RX : 51077871924 | enp2s0 TX : 6347599274 |

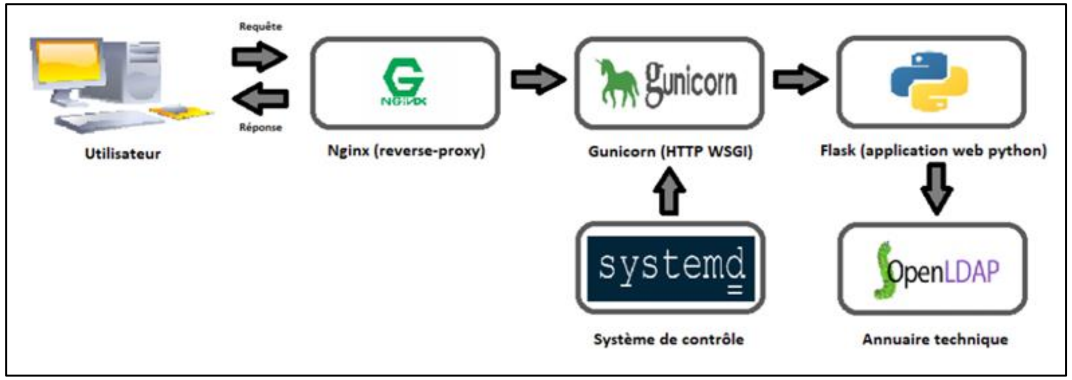
| | | | |
|---|---|---|---|
| Uptime : 04 jours 05 heures 44 minutes 58 secondes | LXC : bitwarden, canary, ldap, ocs | KVM Disk Space : 62 | DHCP : 0 |

| | SSD Space | SSD Life | SSD Error | KVM | DNS Interne | DNS Externe | Internet | CPU | Temperature | LXC | KVM Disk Space | VPN (Site à Site) | DHCP |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **2023-02-12 14:58:02** | | | | | | | | | | | | | |
| **2023-02-12 14:56:01** | | | | | | | | | | | | | |

*Vue côté Cyberzen et vue du client*

# FONCTIONNALITÉS
## Interface d'administration

*"Nous pouvons recevoir plusieurs tickets par jour liés à la création de certificats VPN, création de compte dans le gestionnaire de mots de passe, enregistrements dans notre DHCP, etc. Doit-on obligatoirement nous connecter sur le boîtier et naviguer entre les couches de virtualisation pour effectuer les actions demandées ?"*

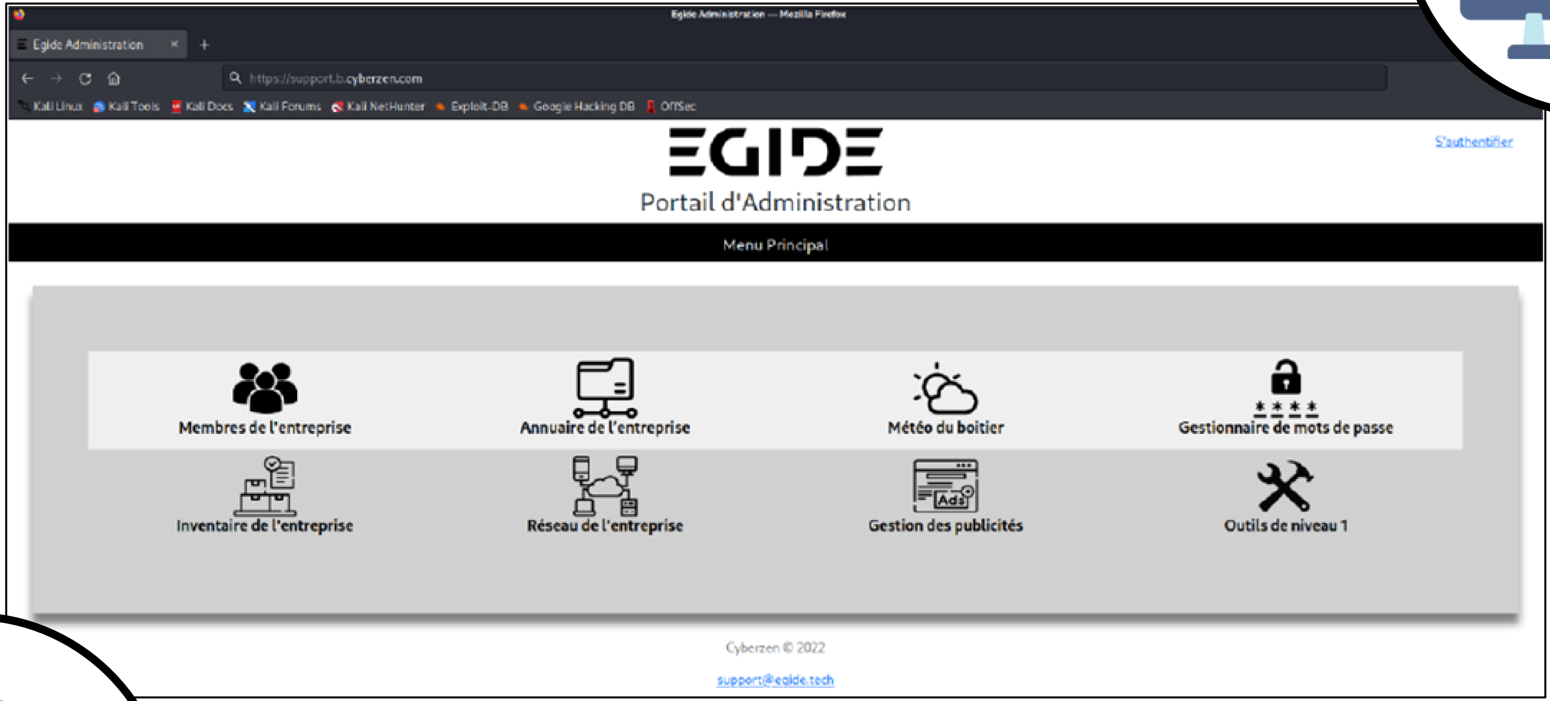



*Architecture choisie*

PBKDF2

MFA

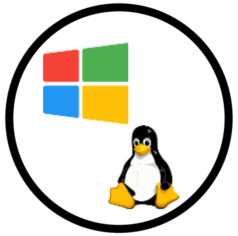
SCAPY




*Interface web du site hébergé sur Egide*

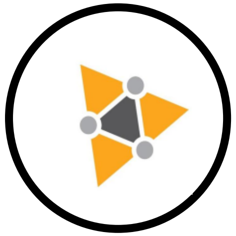
# FONCTIONNALITÉS
## “Active Directory full open-source”

*“Nous rencontrons des clients qui sont intéressés par la mise en place d’un environnement Active Directory pour gérer facilement leurs comptes utilisateurs, leurs postes et les autorisations qui en découlent. Doit-on obligatoirement passer par la solution propriétaire de Microsoft ou avons-nous des alternatives ?“*

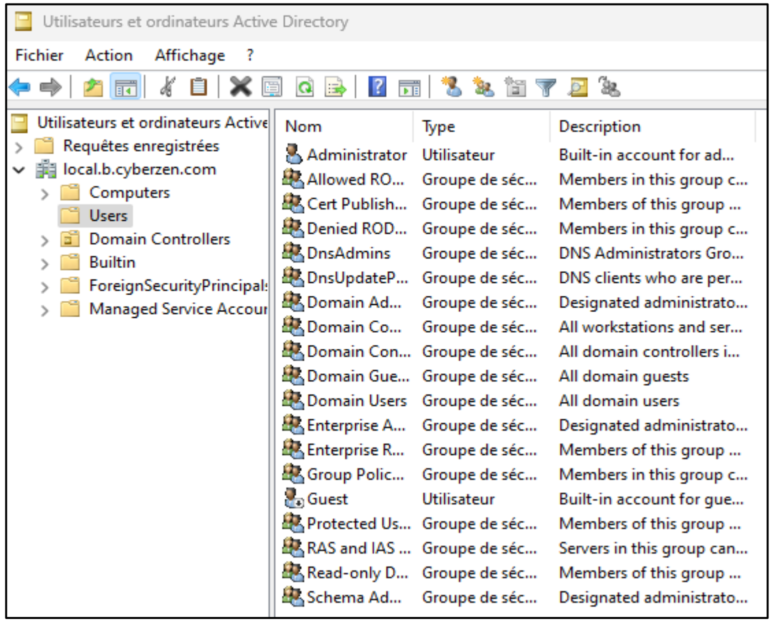


AUTHENTIFICATION
UNIX / WINDOWS

GPOs



HARDENING




*Gestion des objets (outils RSAT)*

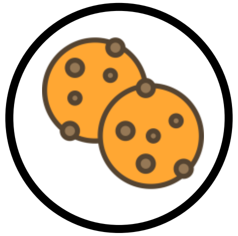
# FONCTIONNALITÉS
## Authentification MFA - VPN

*"Wireguard ne propose pas de MFA pour l'authentification des clients. Possibilité de le faire nous-même ?"*

- Portail captif mis à disposition sur un serveur web
- Tous les flux réseaux des utilisateurs (en VPN) sont redirigés vers le portail captif

Adresse mail / mot de passe

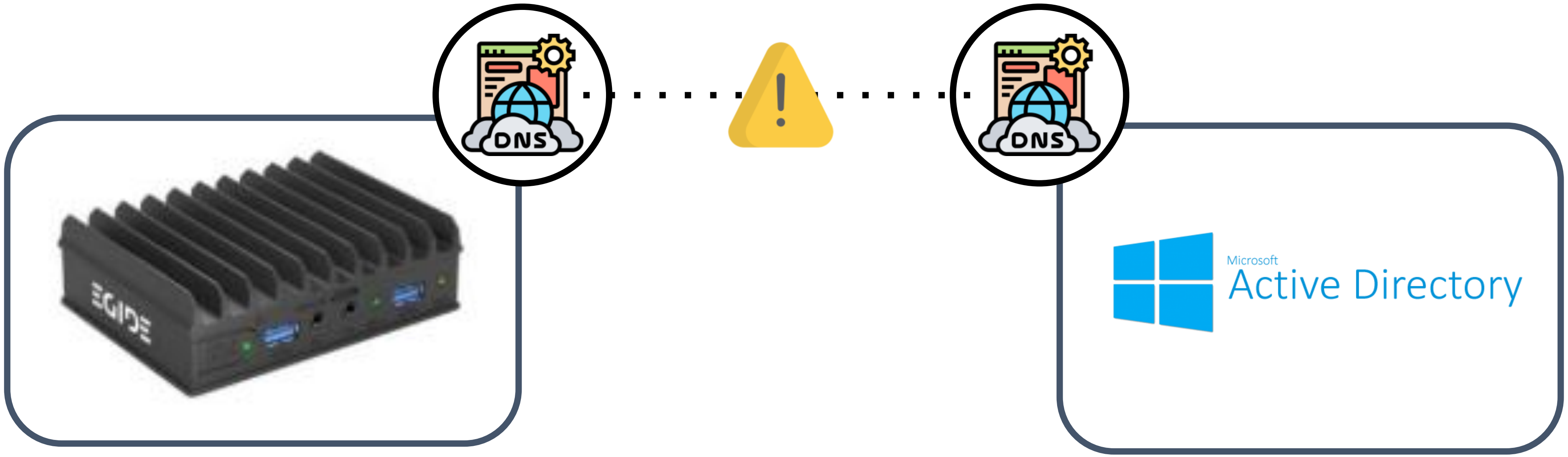
Vérification du certificat VPN utilisé



Session de 8 heures créée

- Une fois authentifié, des flux sont ajoutés automatiquement pour autoriser l'utilisateur à naviguer sur le réseau

# PROBLÈMES RENCONTRÉS
## AD en production chez le client




**test.cyberzen.com**

**contoso.com**

**Solution** :
Délégation de la zone du domaine de l’AD au DNS de l’AD

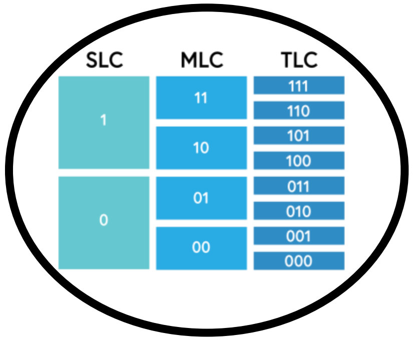
# PROBLÈMES RENCONTRÉS
## SSD HS

**3 ANS**

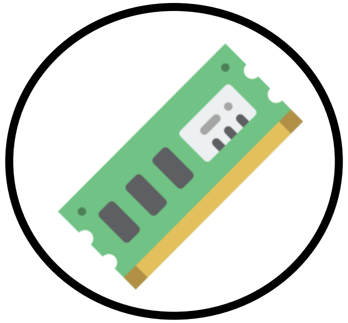
↓

**1 MOIS**

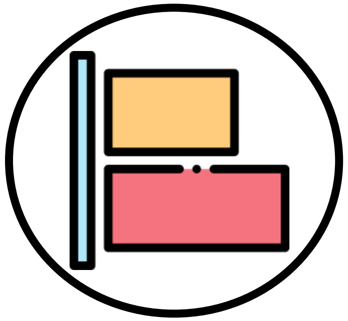

**Solutions :**



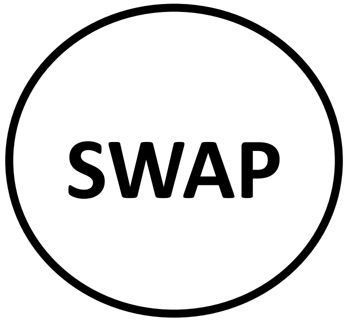

SLC ou MLC NAND



DRAM



ALIGNEMENT DES PARTITIONS



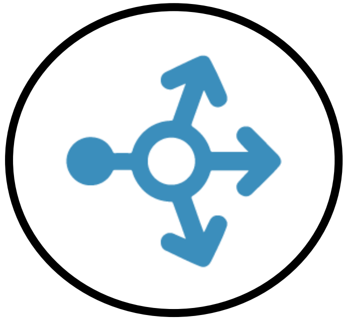

RAMDISK

# PROBLÈMES RENCONTRÉS
## High CPU usage


**Cause :**

CHECKER +2000 RÈGLES IPTABLES
À CHAQUE PAQUET REÇU

**Solutions :**



RÉPARTITION SUR TOUS
LES COEURS

OPTIMISATION DES
RÈGLES IPTABLES

# PROBLÈMES RENCONTRÉS
## IPV6


**Causes** :

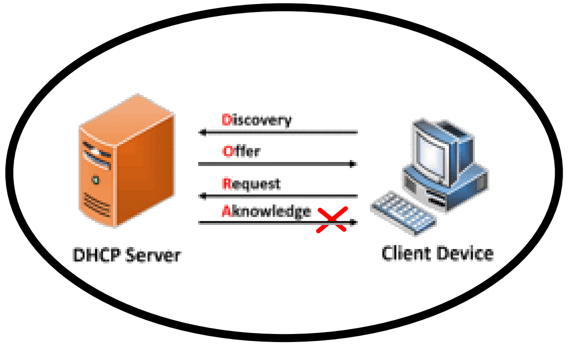

Le /56 n'en est pas un

Pas de délégation du DHCP

**Solution** :
Pas de solution = Pas d'IPv6 (pour l'instant)

# PROBLÈMES RENCONTRÉS
## Allocation Wi-Fi

**Cause** :




Les réponses DHCP sont perdues

**Solution** :
Selon le FAI du client, on propose à ce dernier d'utiliser des bornes Wi-Fi au lieu de celui de la box

# ROADMAP (aperçu)

SERVEUR OTP

PORT-KNOCKING

QOS

PORTAIL CAPTIF WIFI

IPV6

IA

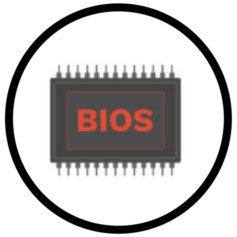
DNS OVER HTTPS

CROWDSEC

…

# BONUS : Préparation d’un boîter

MONTAGE DU BOÎTIER




CONFIGURATION DU BIOS

SCRIPTS PRÉPARATION

- CHROOTGEN
- KERNELGEN
- LXDGEN
- KVMGEN
- PRESEEDGEN


SERVEUR PXE

SCRIPT INSTALLATION

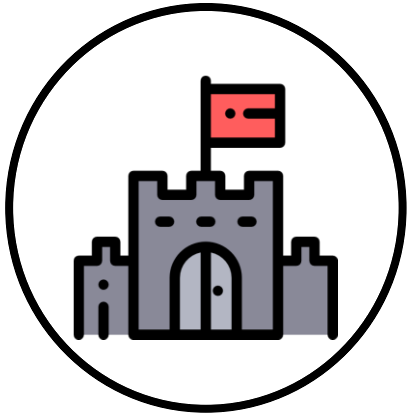

PROGRAMME MATRICE PARSER

| | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | id | objet | source | source port | destination | destination port | REQ | REP | NEW | EST | REL | action |
| 2 | | INPUT | | | | | | | | | | |
| 3 | 1 | Ping | gh-home | - | gh-egide | - | x | | | | | accept |
| 4 | 2 | Ping | n-internet | - | gh-egide | - | | x | | | | accept |
| 5 | 3 | DHCP/BOOTP | gn-allowed-to-local-dhcp | - | - | gs-dhcp | | | | | | accept |
| 6 | 4 | SSH | gh-home | - | h-egide | gs-ssh | | | | | | accept |

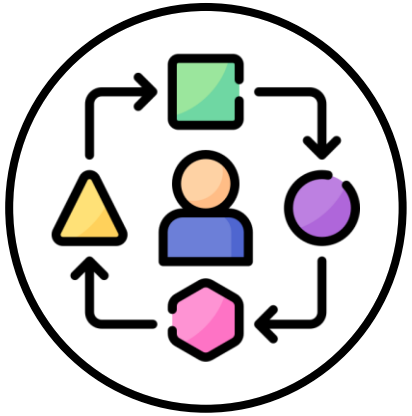
accueil | reseaux | groupes de reseaux | hotes | groupes d'hotes | services | groupes de services | flux egide | flux a la demande | flux client

*Extraits du fichier Excel utilisé par Matrice Parser*

# CONCLUSION



BOÎTIER **SOLIDE**



BOÎTIER **ADAPTATIF**

BOÎTIER **ÉVOLUTIF**

« Merci ! »

« Questions ? »