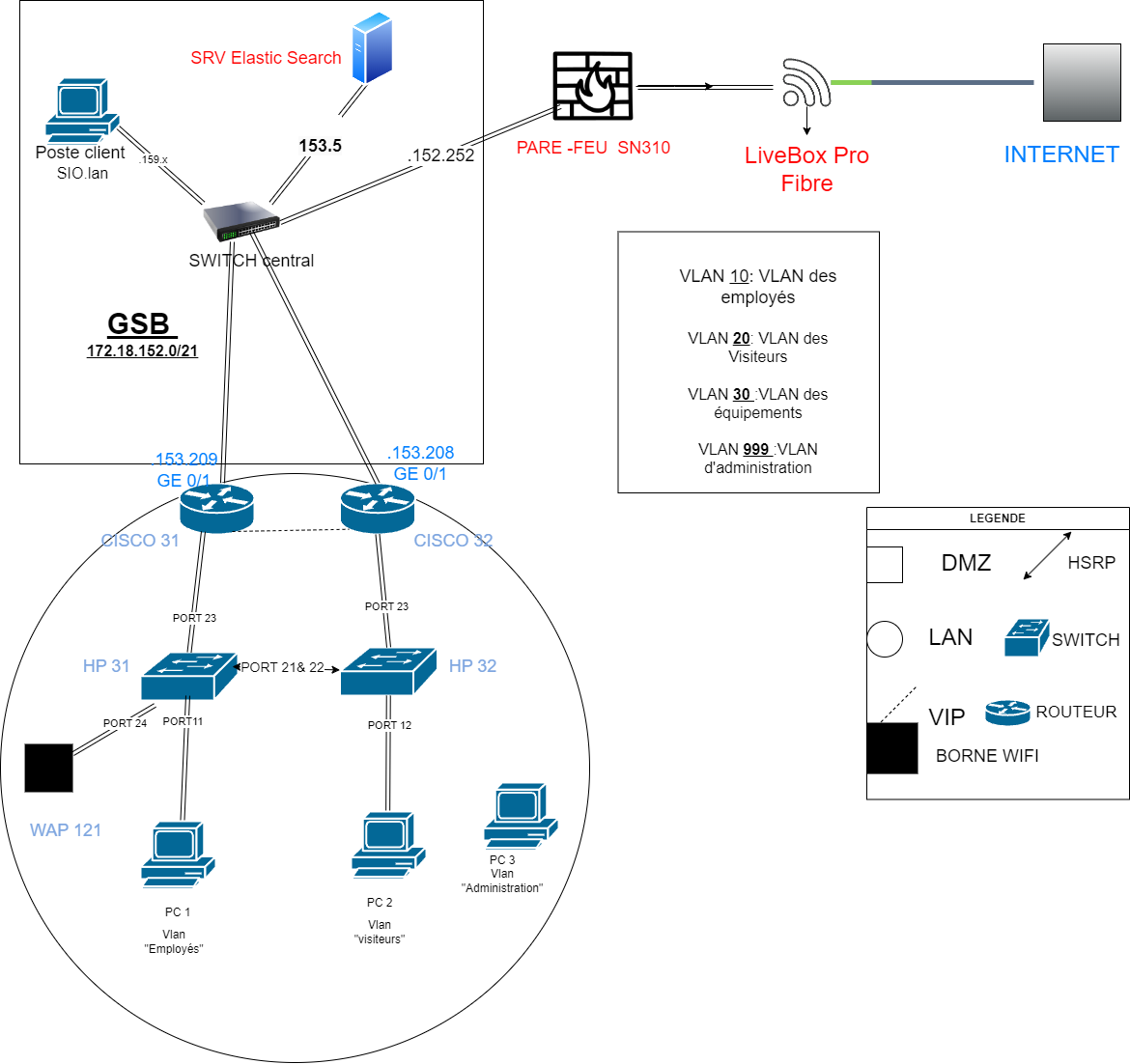
Manguilesy Corentin

Fiche Projet Reseau BTS SIO SISR - Mise en Place

1. OBJECTIF DU PROJET
   * Mettre en place une infrastructure reseau multi-VLAN avec redondance via HSRP
   * Fournir l'acces Internet, le Wi-Fi segmente, DHCP et la supervision reseau (Elasticsearch + Packetbeat)

Schéma réseau :



1. VLANs

- VLAN 10 : Employes - 192.168.1.0/27

- VLAN 20 : Invites - 192.168.2.0/27

- VLAN 30 : Equipements - 192.168.3.0/27

- VLAN 999 : Admin - 192.168.99.0/27

# ROUTEURS CISCO (HSRP + DHCP)

* + IP virtuelle VLAN 10 : 192.168.1.30
  + IP virtuelle VLAN 20 : 192.168.2.30
  + IP virtuelle VLAN 30 : 192.168.3.30

- IP virtuelle VLAN 999 : 192.168.99.30

Cisco31 (principal) : IPs .1 + DHCP

hostname Cisco31

service dhcp

interface GigabitEthernet0/0

no shutdown

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.1 255.255.255.224

standby 10 ip 192.168.1.30

standby 10 priority 110

standby 10 preempt

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.1 255.255.255.224

standby 20 ip 192.168.2.30

standby 20 priority 110

standby 20 preempt

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.1 255.255.255.224

standby 30 ip 192.168.3.30

standby 30 priority 110

standby 30 preempt

interface GigabitEthernet0/0.999

encapsulation dot1Q 999

ip address 192.168.99.1 255.255.255.224

standby 1 ip 192.168.99.30

standby 1 priority 110

standby 1 preempt

interface GigabitEthernet0/1

ip address 172.18.153.209 255.255.255.0

no shutdown

ip route 0.0.0.0 0.0.0.0 172.18.153.1

ip dhcp pool EMPLOYES

network 192.168.1.0 255.255.255.224

default-router 192.168.1.30

dns-server 8.8.8.8

ip dhcp pool INVITES

network 192.168.2.0 255.255.255.224

default-router 192.168.2.30

dns-server 8.8.8.8

ip dhcp pool EQUIPEMENTS

network 192.168.3.0 255.255.255.224

default-router 192.168.3.30

dns-server 8.8.8.8

ip dhcp pool ADMIN

network 192.168.99.0 255.255.255.224

default-router 192.168.99.30

dns-server 8.8.8.8

Cisco32 (secondaire) : IPs .3 + DHCP

hostname Cisco32

service dhcp

interface GigabitEthernet0/0

no shutdown

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.1.3 255.255.255.224

standby 10 ip 192.168.1.30

standby 10 priority 100

standby 10 preempt

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.2.3 255.255.255.224

standby 20 ip 192.168.2.30

standby 20 priority 100

standby 20 preempt

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.3 255.255.255.224

standby 30 ip 192.168.3.30

standby 30 priority 100

standby 30 preempt

interface GigabitEthernet0/0.999

encapsulation dot1Q 999

ip address 192.168.99.3 255.255.255.224

standby 1 ip 192.168.99.30

standby 1 priority 100

standby 1 preempt

interface GigabitEthernet0/1

ip address 172.18.153.208 255.255.255.0

no shutdown

ip route 0.0.0.0 0.0.0.0 172.18.153.1

# SWITCHS HP

* + HP31 et HP32 avec les VLANs 10, 20, 30, 999

hostname "HP31"

ip default-gateway 192.168.99.30

vlan 10

name "EMPLOYES"

untagged 2-10

tagged 23

vlan 20

name "INVITES"

untagged 11-15

tagged 23

vlan 30

name "EQUIPEMENTS"

untagged 16-20

tagged 23

vlan 999

name "ADMIN"

untagged 21

tagged 22-23

ip address 192.168.99.2 255.255.255.224

HP32

hostname "HP32"

ip default-gateway 192.168.99.30

vlan 10

name "EMPLOYES"

untagged 2-10

tagged 23

vlan 20

name "INVITES"

untagged 11-15

tagged 23

vlan 30

name "EQUIPEMENTS"

untagged 16-20

tagged 23

vlan 999

name "ADMIN"

untagged 21

tagged 22-23

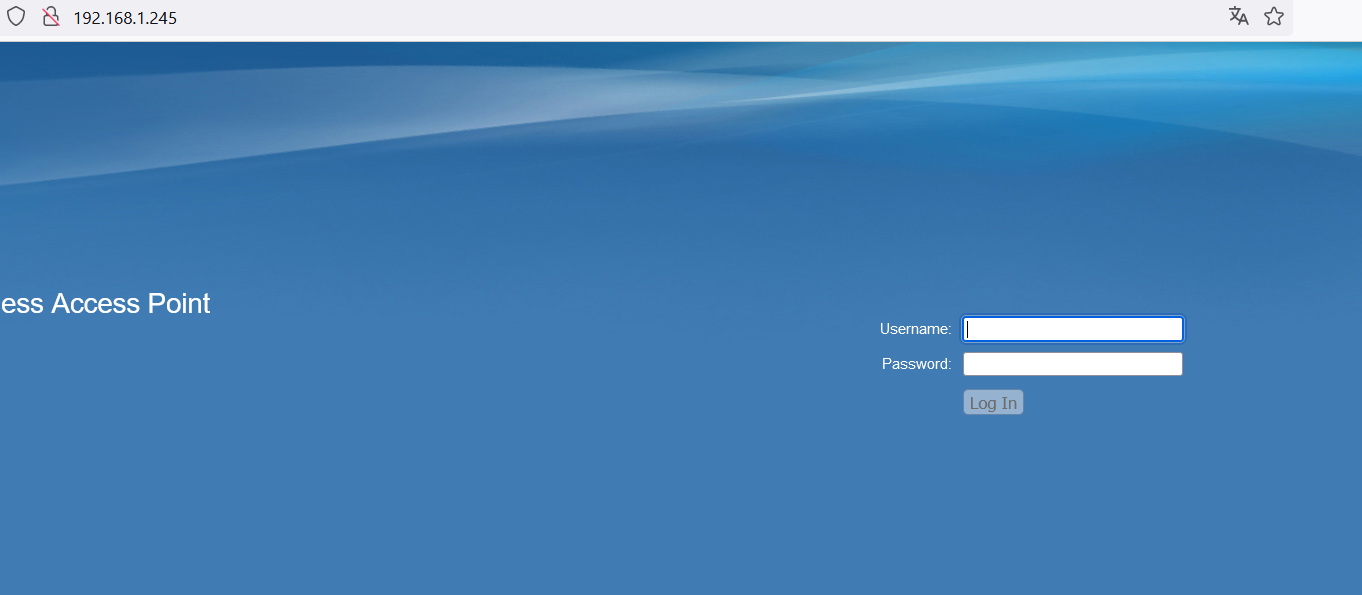
ip address 192.168.99.3 255.255.255.224

# BORNE WI-FI

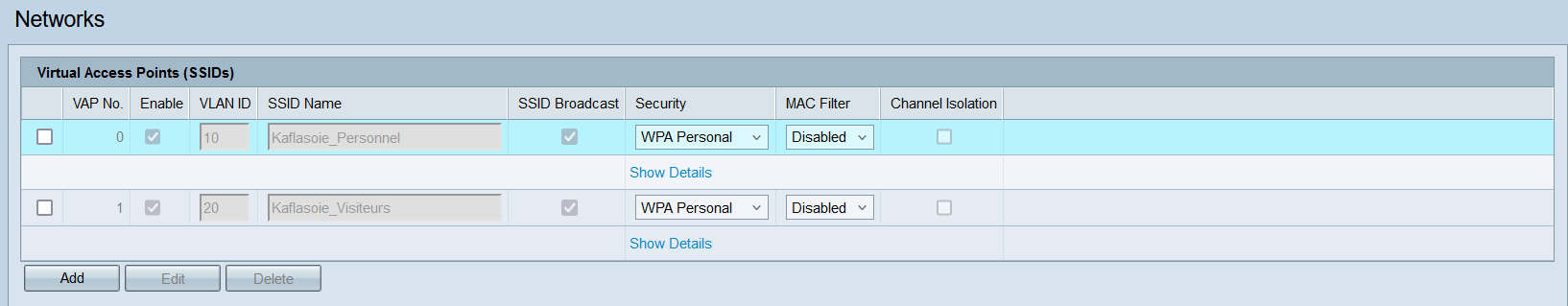
* + SSID KaflaSoie\_Personnel (VLAN 10)
  + SSID KaflaSoie\_Visiteurs (VLAN 20)

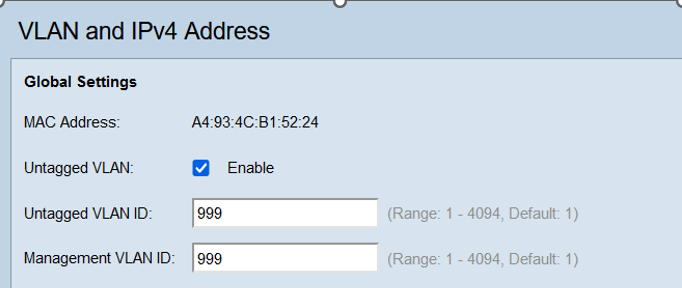
- IP de gestion : 192.168.99.4

Configuration de la borne wifi :



Les Deux SSID :





Connectee sur un port trunk ( Fa0/11 HP31)

# BRANCHEMENTS CLES

- Cisco31 Gi0/0 <-> HP31 Fa0/23

- Cisco32 Gi0/0 <-> HP32 Fa0/23

- HP31 Fa0/24 <-> HP32 Fa0/24

* Cisco31 et Cisco32 Gi0/1 <-> WAN
* Borne Wi-Fi <-> HP31 Fa0/11 (trunk)
* PCs et Serveur selon VLANs

# SUPERVISION (ELK)

* + Serveur avec Elasticsearch + Kibana + Packetbeat
  + IP dans VLAN 999, acces via navigateur sur :5601
  + Packetbeat envoie vers Elasticsearch (localhost:9200)

Procédure d’installation d’elasticsearch :

Prérequis :

Installer apt-transport-https et les paquets nécessaires :



Importer la clé PGP Elasticsearch :



* Ajouter le **dépot** elastic :



* Installer **Elasticsearch** et noter le **mot de passe super-utilisateur** :



* editer le fichier **/etc/elasticsearch/elasticsearch.yml** pour paramétrer l'**interface d'écoute** :

network.host: 0.0.0.0

* Démarrer le **service elasticsearch** :

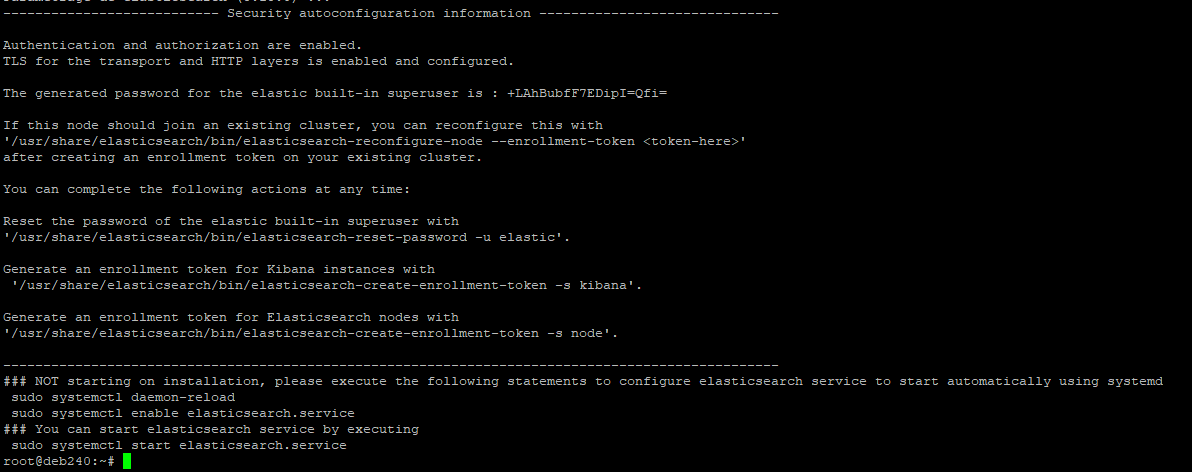
root@host:~# systemctl start elasticsearch.service

ensuite taper :

curl --cacert /etc/elasticsearch/certs/http\_ca.crt -u elastic https://localhost:9200

Enter host password for user 'elastic': **elastic\_password;)**

{



* Éditer le fichier **/etc/kibana/kibana.yml** pour paramétrer l'**adresse d'écoute** sur «toutes les adresses» :

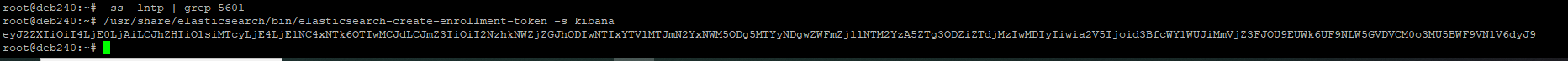
server.host: "0.0.0.0"

server.publicBaseUrl: [http://**X.X.X.X**:5601](http://X.X.X.X:5601)

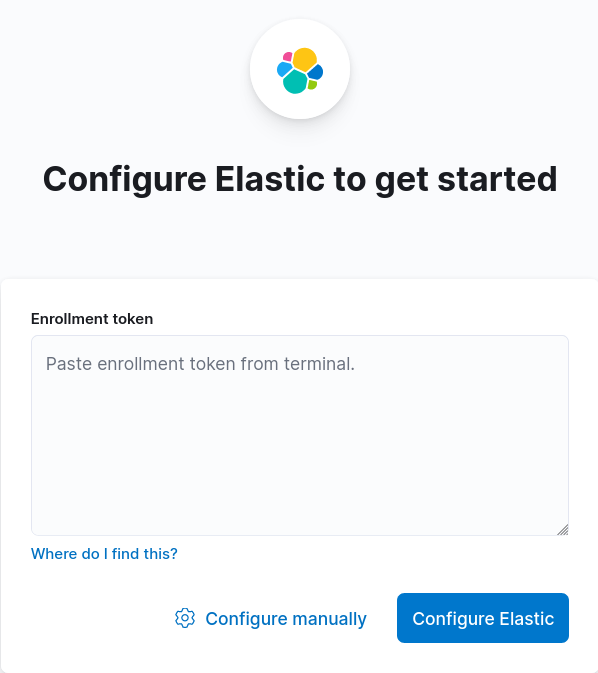
* Démarrer le **service** :

root@host:~# systemctl start kibana.service

* Créer le **jeton d'inscription** :

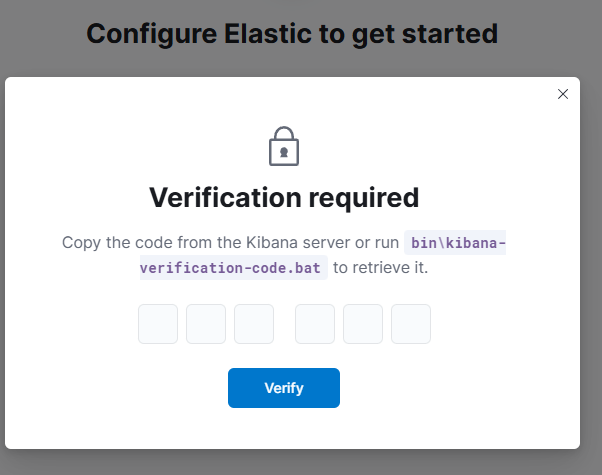


* Ouvrir **Firefox** à l'adresse **http://X.X.X.X:5601** et coller le **jeton d'inscription** puis cliquer sur **Configure Elastic** :

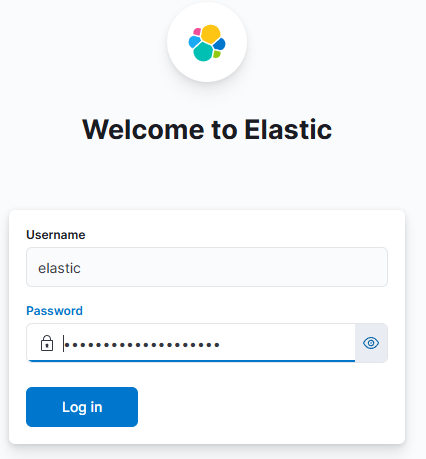


* Générer un **code** de vérification **Kibana** :
* 

Entrez le code :



Connectez vous avec le compte elastic et le mot de passe super user :



ElasticSearch est désormais accessible en http.

Installation de packetbeat:

**1. Ajouter le dépôt Elastic :**

-curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

-sudo apt install apt-transport-https

-echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

-sudo apt update

**2. Installer Packetbeat :**

sudo apt install packetbeat -y

**⚙️ CONFIGURATION DE PACKETBEAT**

**1. Fichier principal : /etc/packetbeat/packetbeat.yml**

packetbeat.interfaces.device: any

**Protocoles à surveiller (exemple DNS + HTTP) :**

packetbeat.protocols:

- type: dns

ports: [53]

- type: http

ports: [80, 8080, 8000, 5000, 8002]

**Connexion à Elasticsearch :**

output.elasticsearch:

hosts: ["localhost:9200"]

**Connexion à Kibana :**

setup.kibana:

host: ["localhost:5601"]

**▶️ DÉMARRER ET ACTIVER LE SERVICE**

sudo systemctl enable packetbeat

sudo systemctl start packetbeat

Vérifie qu’il tourne avec :

sudo systemctl status packetbeat

**📊 VISUALISER DANS KIBANA**

1. Lance Kibana : <http://localhost:5601>
2. Aller dans **Discover** ou **Dashboards**
3. Utilise les dashboards Packetbeat préconfigurés

sudo packetbeat setup --dashboards