Projet n°1 de Cyber sécurisation des Infrastructures et Projets

M. Raphael, L. Tilio, L. Jeankien, L. Thomas

Schéma d'architecture réseau :

Moins de 6 IPs utilisables nécessaires pour VLAN 1, 2, 3 et 4 donc on fait un masque en /29 (6= (2^3) -2 donc masque = 32-3 = 29)

Masque sous réseaux 1,2,3,4 : 255.255.255.248

WAN :
IP via DHCP

DMZ : VLAN 2
10.0.2.0/29
10.0.2.7 (broadcast)

Plage : 10.0.2.1 - 10.0.2.6

Passerelle Pfsense:10.0.2.1/29

HAproxy 1 : 10.0.2.2/29
HAproxy 2 : 10.0.2.3/29

address VIp: 10.0.2.4/29

Backend : VLAN 3

10.0.3.0/29

10.0.3.7 (broadcast)

Plage : 10.0.3.1 - 10.0.3.6

Passerelle Pfsense:10.0.3.1/29

web Server : 10.0.3.2/29

BDD : VLAN 4
10.0.4.0/29
10.0.4.7 (broadcast)

Plage : 10.0.4.1 - 10.0.4.6

Passerelle Pfsense: 10.0.4.1/29
BDD : 10.0.4.2/29

Pour le VLAN 99 pour avoir une marge on a laissé 30 IPs utilisables donc on fait un masque en /27 (30= (2^5) -2 donc masque = 32-5 = 27)

Masque sous réseaux 5 : 255.255.255.224

Management : VLAN99
10.0.99.0/27
10.0.99.31 (broadcast)

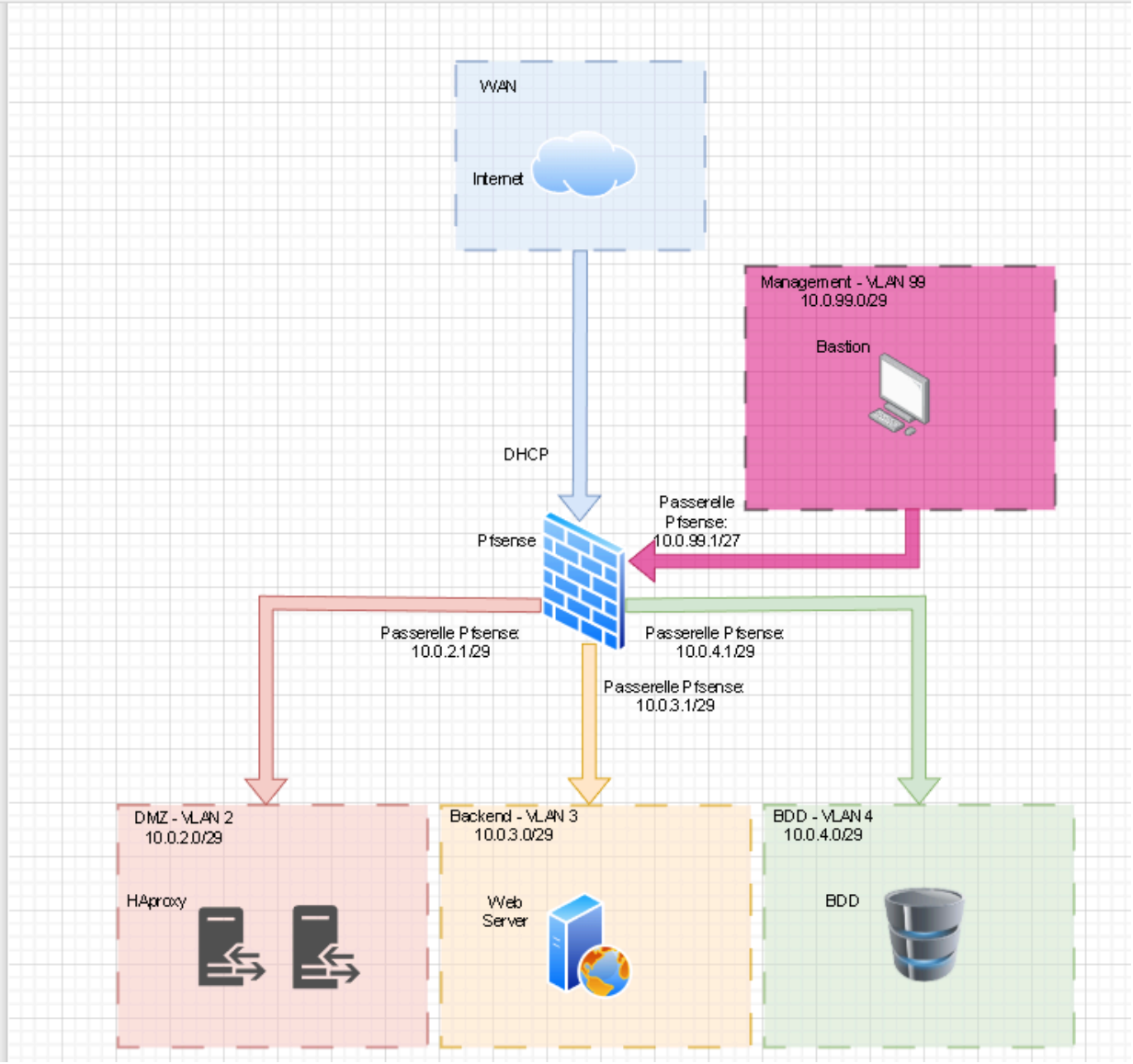
Plage : 10.0.99.1 - 10.0.99.30

Passerelle Pfsense: 10.0.99.1/27
HAproxy1 management : 10.0.99.2/27
HAproxy2 management : 10.0.99.3/27
Web Server management : 10.0.99.4/27

BDD management : 10.0.99.5/27

Bastion SSH management : 10.0.99.6/27

Schéma infra



Matrice de flux réseau :

Accès Internet :

Source	Destination	Service utilisé	Port	Protocole	Explication/Etat
Internet	HAProxy HTTPS	HTTPS	443	TCP	Accès public
HAProxy	WEB	HTTP	80	TCP	Reverse Proxy
HAProxy	WEB	HTTP	80	TCP	Réseau Interne

Flux admin vers toutes les machines + panel Admin en SSH :

Admin	Bastion	SSH	22	TCP	Accès Admin
Bastion	Toutes les machines	SSH	22	TCP	Administration

Accès et flux SQL

Web	MySQL	MySQL	3306	TCP	Accès DB
MySQL	Internet	x	x	x	Interdit

Threat Modeling avec STRIDE

Tableau STRIDE

Source impactée	Menace	STRIDE	Impact	Probabilité	Risque	Contre Mesures
HAProxy	Spoofing IP	S	3	3	9	Validation headers, ACL
Web	Injection SQL	T	4	3	12	WAF, requêtes préparées
MySQL	Vol de données	S	4	2	8	Vault, rotation secrets
pfSense	Load trop haut	D	3	3	9	Limite state table
Web	Bruteforce	S	3	4	12	Fail2ban

Priorisation des risques

À la suite de l'analyse des menaces, plusieurs niveaux de risques ont été identifiés. Les risques les plus critiques concernent principalement les attaques par injections SQL ainsi que les tentatives de pivot réseau depuis une zone compromise vers d'autres segments de l'infrastructure. Ces menaces présentent à la fois un impact élevé et une probabilité importante, ce qui nécessite une prise en charge prioritaire.

Les risques de niveau élevé incluent notamment les attaques par usurpation d'identité ainsi que les tentatives d'élévation de privilèges. Bien que légèrement moins probables que les risques critiques, leurs conséquences peuvent rester significatives en cas d'exploitation réussie.

Les risques de niveau moyen sont essentiellement liés à la journalisation, par exemple une insuffisance ou une mauvaise exploitation des logs, pouvant compliquer la
détection et l'analyse des incidents de sécurité. Enfin, les risques considérés comme faibles concernent la surveillance globale du système, qui reste nécessaire mais moins urgente par rapport aux autres menaces identifiées.

Contre-mesures globales

Afin de réduire les risques identifiés, plusieurs contre-mesures ont été définies. Sur le plan préventif, l'architecture repose sur une segmentation stricte du réseau à l'aide de VLANs, permettant d'isoler les différentes zones de sécurité. Le firewall stateful assure un contrôle précis des flux autorisés entre ces zones. L'accès à la zone de management est renforcé par l'utilisation d'une authentification forte, et le durcissement des
systèmes est réalisé en suivant les recommandations des benchmarks CIS.

En matière de détection, des mécanismes de supervision sont mis en place afin d'identifier rapidement les comportements anormaux. Des solutions de type IDS/IPS sont utilisées pour détecter les tentatives d'intrusion, tandis que les journaux sont centralisés afin de faciliter l'analyse des événements de sécurité. Des alertes
spécifiques permettent également de repérer rapidement les attaques par déni de service.

Enfin, des mesures de réaction sont prévues en cas d'incident de sécurité. Elles incluent l'isolement rapide de la zone compromise afin de limiter la propagation de l'attaque, la rotation des identifiants et des secrets potentiellement exposés, ainsi que la restauration des systèmes et des données à partir de sauvegardes fiables.