

Mise en oeuvre d'une solution d'hébergement intranet

Projet BTS SIO Option A - SISR

Contexte général

Nature du projet

Vous êtes chargé de mettre en œuvre une solution d'hébergement d'applications web en intranet pour une petite entreprise. Ces applications peuvent être de diverses natures : sites internet (wordpress), applications métiers auto-hébergées, etc.

Il s'agira donc, dans le cadre de ce projet, de fournir un prototype viable, respectant l'état de l'art, dont l'ensemble des aspects fonctionnels fondamentaux est couvert. Votre travail doit s'effectuer sur un ensemble d'axes :

1. **Sécurité.** La solution doit être sécurisée au possible, en faisant appel à un pare-feu applicatif interne, un système de ban-IP, des accès SSH et l'utilisation des protocoles dérivés de SSH pour le transfert de fichiers : SCP / SFTP, couplé à l'isolation du réseau privé qu'elle occupe (cf. point 6)
2. **Hébergement d'applications web.** La solution devra permettre l'hébergement d'applications web écrites en PHP et utilisant MariaDB ou MySQL pour leurs bases de données. Cet hébergement doit se faire dans le cadre d'un domaine interne dédié (intranet.local) avec sa propre zone DNS.
3. **Automatisation / scripting.** Certaines opérations complexes gagneraient à être automatisées par l'écriture de scripts.
4. **Supervision.** Votre solution pourra se voir adjoindre une ou plusieurs solutions complémentaires de supervision ainsi que de centralisation des logs, avec la visualisation associée.
5. **Sauvegardes.** Votre solution peut rencontrer des erreurs critiques ou subir des pannes destructrices. Il est donc important d'envisager des solutions de sauvegarde adaptées.
6. **Isolation du réseau intranet.** L'utilisation d'un pare-feu frontal et de redirections de ports est stipulé dans la demande initiale.

Bien qu'à priori le cœur fonctionnel représente l'allocation d'une machine dédiée (virtuelle ou physique), les solutions de supervision et de sauvegarde devraient être séparées dans une deuxième machine. Faites donc attention à l'utilisation de ressources et tentez de rester raisonnables pour la démonstration du prototype.

Livrables / Attendus

Ce projet constitue la première phase d'un long fil-rouge s'étendant sur les deux années. Il sera à présenter dans son état d'avancement à l'épreuve blanche du BTS blanc ayant lieu fin mai 2026. Dans ce contexte, les livrables sont :

- La fiche projet requise pour le BTS, remplie de manière conforme
- Toute documentation additionnelle du travail mené, au format PDF, dans un document séparé

Veillez noter que ce projet étant à cheval sur les deux années, il est inutile de tenter de tout réaliser pour le premier BTS blanc, faites au mieux et sélectionnez un ensemble de tâches que vous jugez adaptées au temps imparti.

En l'état, nous pensons que se concentrer sur le coeur fonctionnel et la sécurité de la solution est prioritaire, le développement de l'automatisation, des sauvegardes et de la supervision peuvent être réalisés dans un second temps.

NOTE : Les hypothèses de travail pour le développement se basent sur VirtualBox. Ceux d'entre vous qui utilisent VMWare devront surement adapter les opérations à cet environnement.

Autres remarques à caractère général

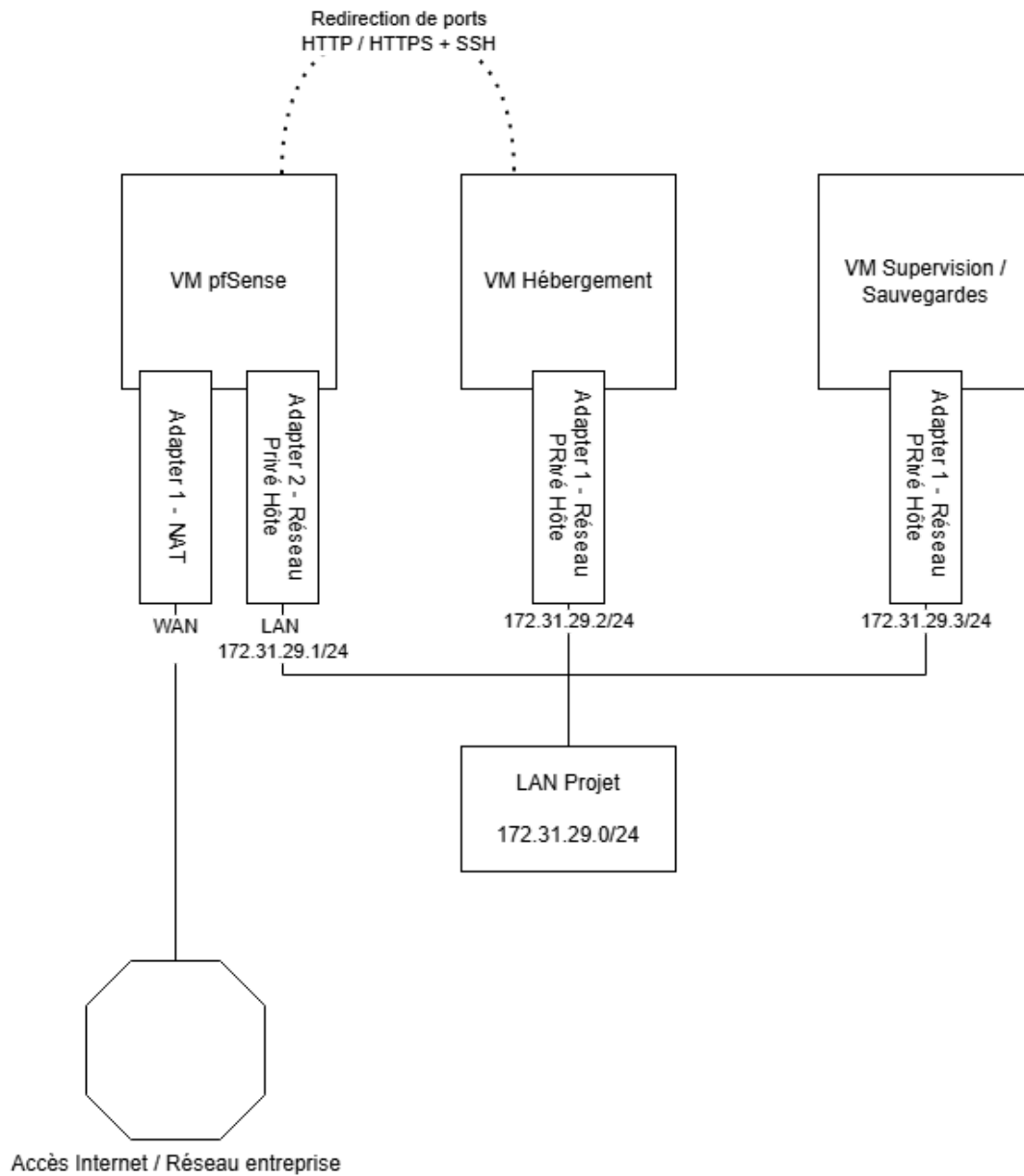
Vous êtes libre de proposer des axes de travail complémentaires si vous le jugez utile et nécessaire. Le présent document établit un ensemble de besoins fonctionnels que vous pouvez tout à fait étendre.

Soyez proactifs et créatifs !

Schéma architectural de principe

Environnement de production

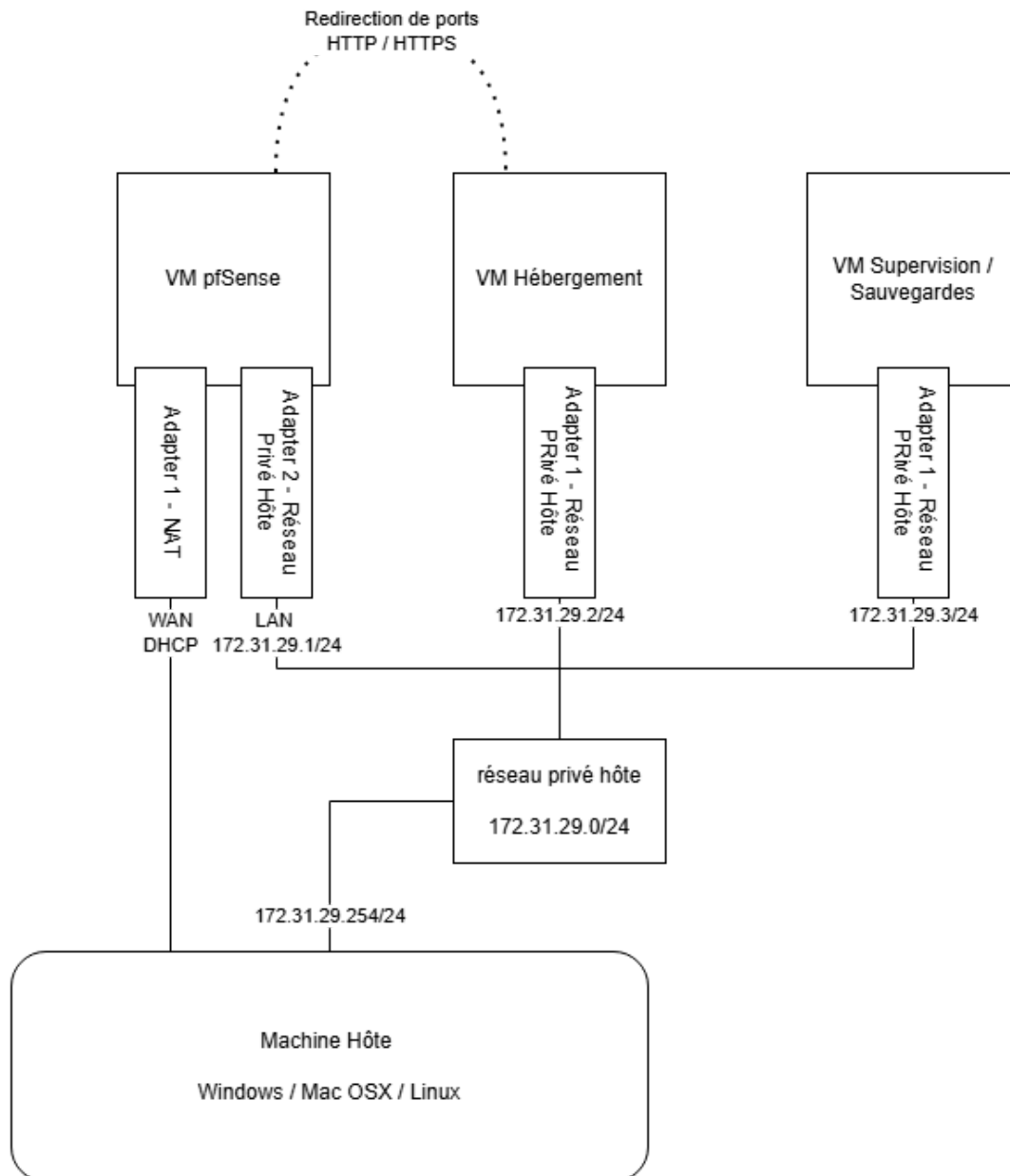
L'environnement est séparé du reste du réseau de l'entreprise par un pare-feu pfSense.



Environnement de développement

Hypothèse de travail : utilisation de VirtualBox.

Cette approche simplifie le développement de la solution en intégrant la machine hôte de développement dans le sous-réseau du projet.



Tranches et livrables

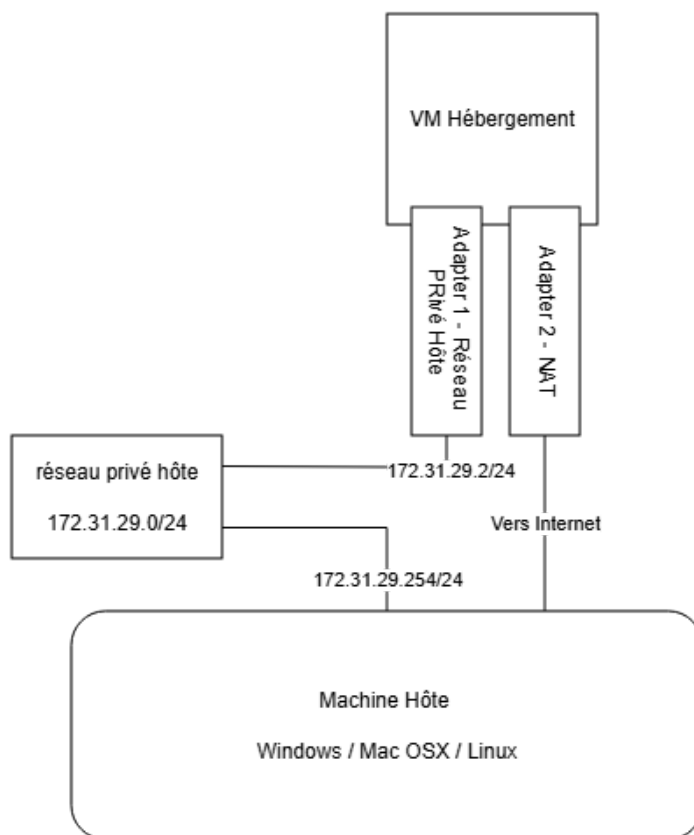
Principe de découpage

Le projet est découpé en tranches, chacune représentant un jalon dans le projet

Tranche 1 - Coeur fonctionnel

Pour cette tranche, il s'agit de livrer la machine dédiée à l'hébergement, conformément aux besoins exprimés.

Dans ce contexte et dans l'hypothèse de travail sous VirtualBox, cette machine dédiée utilisera une interface réseau en mode NAT en plus du réseau privé hôte. Comme montré ci-dessous.



La tranche 1 est estimée achevée dès lors que les services s'articulent correctement et que l'hébergement d'applications / sites au sein du domaine intranet.local

Tranche 2 - Sécurité

Cette tranche concerne le déploiement et la configuration de pfSense, afin de créer le réseau privé dédié à la solution. Dans cet esprit, la machine dédiée à l'hébergement bascule en réseau privé hôte pour modéliser la LAN intranet de production.

Cette tranche est considérée comme achevée dès lors que la machine dédiée à l'hébergement peut accéder à internet depuis son LAN (conformément au schéma de principe).

Tranche 3 - Supervision et Sauvegardes

Cette tranche suppose la mise en oeuvre de la supervision et des sauvegardes afin d'assurer la disponibilité de la solution. Les besoins en haute-disponibilité (HA) n'étant pas spécifiés, un mécanisme de sauvegarde et compression est suffisant, associé à la surveillance des machines et des applicatifs et services.

Cette tranche est estimée achevée lorsque la machine de supervision et sauvegarde est paramétrée et fonctionnelle, et que les procédures de sauvegarde de la machine d'hébergement sont qualifiées et rédigées.

Tranche 4 - Automatisation et scripting

Une fois l'infrastructure en place, il s'agira d'automatiser par l'écriture de scripts les procédures principales nécessaires à l'administration et la maintenance de la solution.

Opérations à réaliser

Caractérisation des opérations

Les opérations décrites ci-après sont réparties par tranche, elles constituent des jalons intermédiaires à documenter pendant leur élaboration.

Ces opérations doivent être vues comme des guides généraux pour atteindre les objectifs fonctionnels et opérationnels de la solution décrite dans ce document, vous pouvez y ajouter toute opération que vous jugez utile.

Tranche 1 - Coeur fonctionnel

Voici les tâches jugées essentielles pour la réalisation de cette tranche

Opération	Description / Spécifications / Contraintes
Installation	Debian 13, minimal, ligne de commande, pas d'interface graphique, utilitaires usuels du système uniquement.
Configuration initiale	Configuration réseau, installation paquets utilitaires complémentaires (htop, sudo, serveur ssh, ...)
Installation pile LAMP	Installation des services : Apache2, PHP, MySQL / MariaDB pour former une pile LAMP (Linux Apache MySQL PHP)
Sécurisation	Sécurisation de la machine : installation et configuration du pare-feu UFW, installation et configuration de fail2ban, sécurisation du serveur MariaDB / MySQL. On cherche ici à réduire la surface d'attaque sur le système.
Service DNS	Installation et configuration de Bind9 et configuration de la zone DNS "intranet.local", puis configuration de la machine hôte pour utiliser ce serveur DNS.
Déploiement portail intranet	Le portail intranet est un site wordpress simple. Déployez wordpress selon la documentation disponible. Utilisez la dernière version de wordpress depuis https://wordpress.org. Le portail intranet sera sur le sous-domaine http://intranet.local
Déploiement service NextCloud	Déployez NextCloud sur le sous-domaine http://cloud.intranet.local De la même manière que pour wordpress, utilisez les documentations de NextCloud pour mener à bien l'opération.

Le test du service DNS devra se faire en ajoutant l'IP de la machine hôte comme serveur DNS dans la configuration de l'interface dédiée au réseau privé hôte.

Les opérations de déploiement nécessitent de nombreuses actions qu'il vous faudra qualifier en fonction de vos recherches personnelles sur les services mentionnés. Wordpress est un site-builder populaire (70% du web environ) et NextCloud est une solution open-source de cloud d'entreprise.

Tranche 2 - Sécurité

Voici les tâches jugées essentielles pour la réalisation de cette tranche

Opération	Description / Spécifications / Contraintes
Installation	Installation de pfSense
Configuration initiale	Configuration initiale, règles de pare-feu
DNS Resolver	Mise en place du service DNS Resolver de manière à garantir l'accès internet à la machine d'hébergement et aussi à permettre la diffusion de la zone DNS intranet.local à l'extérieur du LAN.
Redirection de ports	Mise en place de la redirection de ports vers la machine d'hébergement (DNS, HTTP, HTTPS, SSH)
Modification de la configuration réseau de la machine d'hébergement	Le pare-feu pfSense sert désormais de routeur pour les machines présentes dans le réseau privé LAN intranet. Il est donc nécessaire de modifier la configuration réseau de la machine d'hébergement en conséquence.

Tranche 3 - Supervision et sauvegardes

Voici les tâches jugées essentielles pour la réalisation de cette tranche

Opération	Description / Spécifications / Contraintes
Installation	Installation de Debian 13 (mêmes contraintes que pour la machine d'hébergement)
Configuration initiale	Configuration réseau, installation paquets utilitaires complémentaires (htop, sudo, serveur ssh, ...)
Sécurisation	Sécurisation de la machine : installation et configuration du pare-feu UFW, installation et configuration de fail2ban, sécurisation du serveur MariaDB / MySQL. On cherche ici à réduire la surface d'attaque sur le système.
Déploiement Zabbix	Installation et configuration des prérequis pour l'installation de Zabbix Installation de Zabbix Configuration des agents Zabbix sur les deux machines debian Activation de SNMP sur le parefeu pfSense + sonde SNMP Zabbix Paramétrage de dashboards pour le relevé des métriques des machines
Sauvegardes	Élaboration d'un protocole de sauvegarde des bases de données de la machine d'hébergement, ainsi que des applications de l'intranet. Proposition de procédure viable et testée

Journaux Système	Mise en place d'un serveur RSyslog et paramétrage en tant que client rsyslog des autres machines de l'infrastructure. Mise en place d'une stratégie de rotation des journaux. Déploiement d'une solution de visualisation des logs (loganalyzer).
------------------	---

Tranche 4 - Automatisation

Voici les tâches jugées essentielles pour la réalisation de cette tranche

Opération	Description / Spécifications / Contraintes
Scripts de sauvegarde	Après la formalisation du (des) protocole(s) de sauvegarde dans la phase 3, rédaction d'un script permettant l'automatisation des sauvegardes, devant être exécuté toutes les nuits à 3h33 du matin.
Scripts pour l'ajout d'un nouveau sous-domaine	La modification de la zone DNS intranet.local peut s'avérer fastidieuse. Rédigez un script permettant d'ajouter un sous-domaine et de déployer une application pour ce sous-domaine.