Segmentation & Firewalling avec pfSense et VLAN

Dans le cadre de ma formation BTS SIO option SISR, j'ai mené un projet essentiel axé sur la segmentation réseau et la sécurisation du trafic à l'aide de pfSense. Ce projet m'a permis de développer une compréhension approfondie des infrastructures réseau sécurisées.

Un Objectif Crucial : Reproduire une Infrastructure d'Entreprise Sécurisée

L'objectif principal de ce projet était de reproduire fidèlement une infrastructure d'entreprise. Pour ce faire, j'ai procédé à une séparation rigoureuse des différents types de machines sur des réseaux distincts, visant à :

1

Améliorer la Sécurité

Renforcer la protection contre les menaces internes et externes.

2

Contrôler les Communications

Gérer précisément les flux de données entre les différentes zones du réseau.

3

Limiter la Propagation d'Incidents

Contenir les éventuels problèmes au sein d'une seule section du réseau.

Mise en Place de pfSense : Le Cœur de la Sécurité

La première étape cruciale fut l'installation de pfSense, une solution de pare-feu open source reconnue pour sa robustesse et sa flexibilité. Il a été configuré comme le pare-feu principal de l'infrastructure virtuelle, agissant comme le point de contrôle central pour tout le trafic réseau.

- Sécurité Périmétrique
- Filtrage de Paquets Avancé
- Haute Disponibilité

Création de VLAN et Sous-Réseaux : Une Segmentation Logique

Pour atteindre les objectifs de sécurité, j'ai procédé à la configuration de plusieurs réseaux distincts à l'aide de VLAN (Virtual Local Area Networks). Cette approche permet d'isoler logiquement les différents groupes de machines, même si elles partagent la même infrastructure physique.

Réseau Utilisateurs

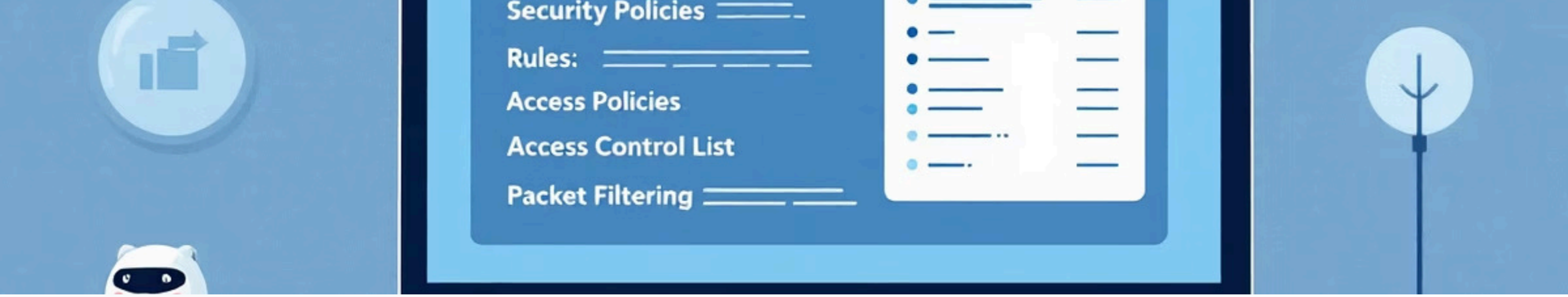
Accès contrôlé pour les employés.

Réseau Serveurs

Hébergement des applications et données critiques.

Réseau Administration

Accès privilégié pour les administrateurs système.

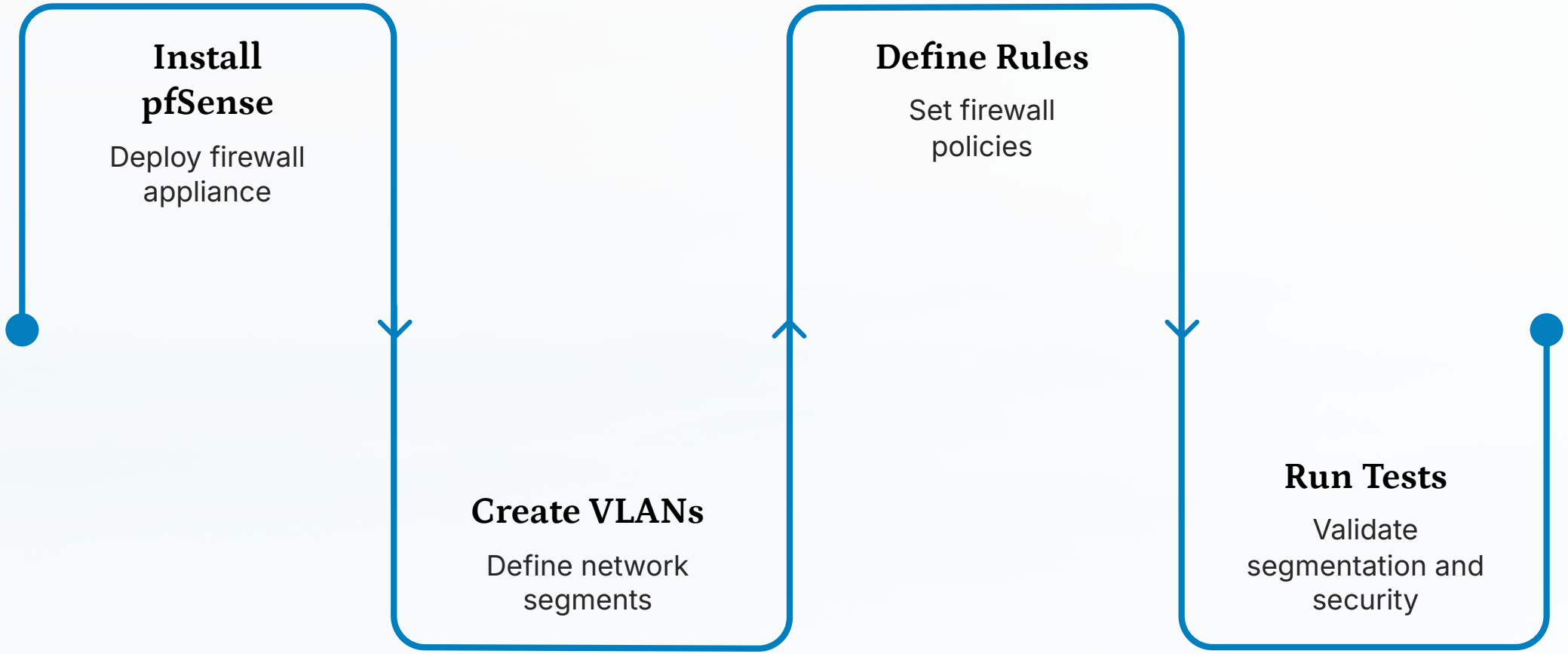


Règles de Filtrage (Firewall) : Le Contrôle d'Accès Granulaire

La mise en place de règles de filtrage précises sur pfSense a été essentielle pour contrôler les accès et les communications entre les VLANs. Chaque règle a été conçue pour garantir que seul le trafic autorisé puisse circuler.

- **Isolation des Utilisateurs :** Les utilisateurs n'ont pas d'accès direct aux serveurs sensibles.
- **Services Autorisés :** Seuls des services spécifiques (DNS, HTTP/S, Active Directory) sont permis.
- **Accès Administrateurs :** L'administration est strictement réservée à un réseau spécifique et sécurisé.

Processus de Réalisation du Projet

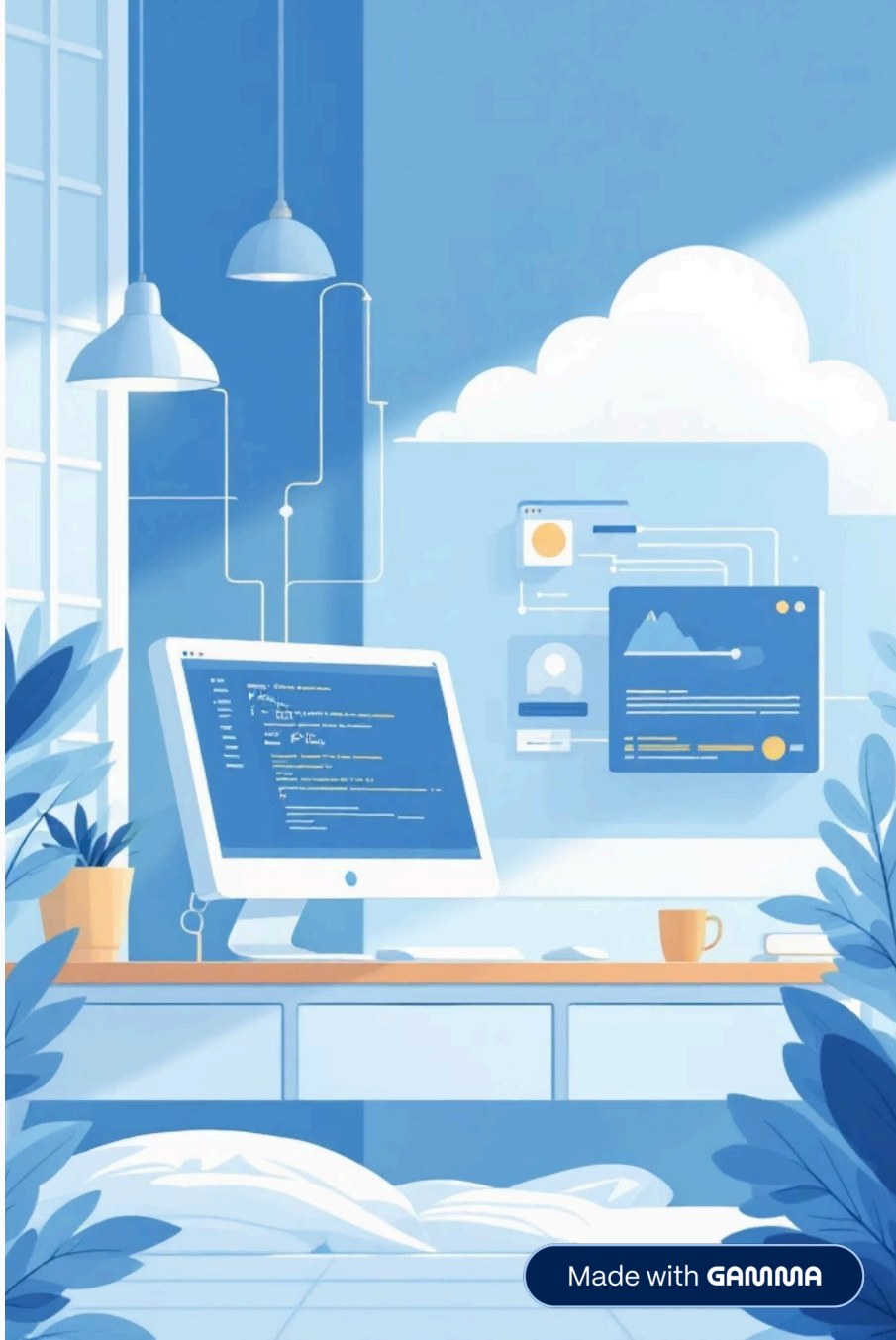


Ce diagramme illustre les étapes clés de la mise en œuvre du projet, de l'initialisation du pare-feu à la validation finale de la segmentation et des règles de sécurité.

Tests de Validation : Assurer l'Efficacité des Mesures

Pour garantir le bon fonctionnement de la configuration, des tests rigoureux ont été effectués. Ces validations ont permis de confirmer que la segmentation réseau et les règles de filtrage opéraient comme prévu, bloquant les accès non autorisés et permettant les communications légitimes.

- Tests de connectivité (ping)
- Vérification des accès aux ressources
- Tests de blocage des flux non autorisés



Un Résultat Tangible : Infrastructure Sécurisée et Structurée

Ce projet a abouti à la création d'un environnement réseau sécurisé et bien structuré, qui reflète fidèlement les architectures rencontrées en entreprise. Cette réalisation est une preuve concrète de ma capacité à concevoir et à implémenter des solutions de sécurité réseau complexes.

> "Ce projet m'a permis de mettre en place un réseau sécurisé et structuré, proche des pratiques utilisées en entreprise."

Compétences Développées : Une Expertise Approfondie

La réalisation de ce projet a été l'occasion de renforcer et d'acquérir des compétences essentielles pour un professionnel des systèmes d'information.

Maîtrise de pfSense

Configuration avancée et gestion des fonctionnalités de sécurité.

VLAN et Segmentation Réseau

Conception et implémentation de réseaux logiquement isolés.

Firewalling et Contrôle d'Accès

Définition de règles granulaires pour la sécurisation du trafic.

Architecture Sécurisée

Conception de solutions robustes en environnement professionnel.

Prochaines Étapes : Vers de Nouveaux Défis

Fort de cette expérience, je suis prêt à relever de nouveaux défis dans le domaine de la cybersécurité et de l'administration réseau. Mon objectif est de continuer à développer mes compétences et à contribuer à la sécurisation des infrastructures numériques de demain.

SÉCURITÉ RÉSEAU

ADMINISTRATION SYSTÈME

CYBERSÉCURITÉ