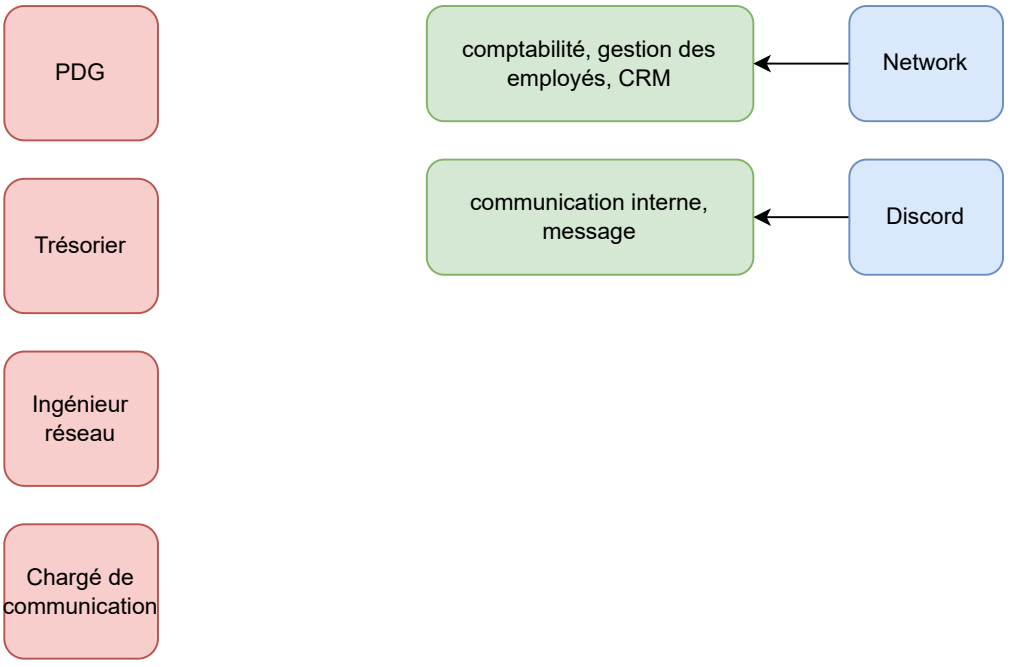
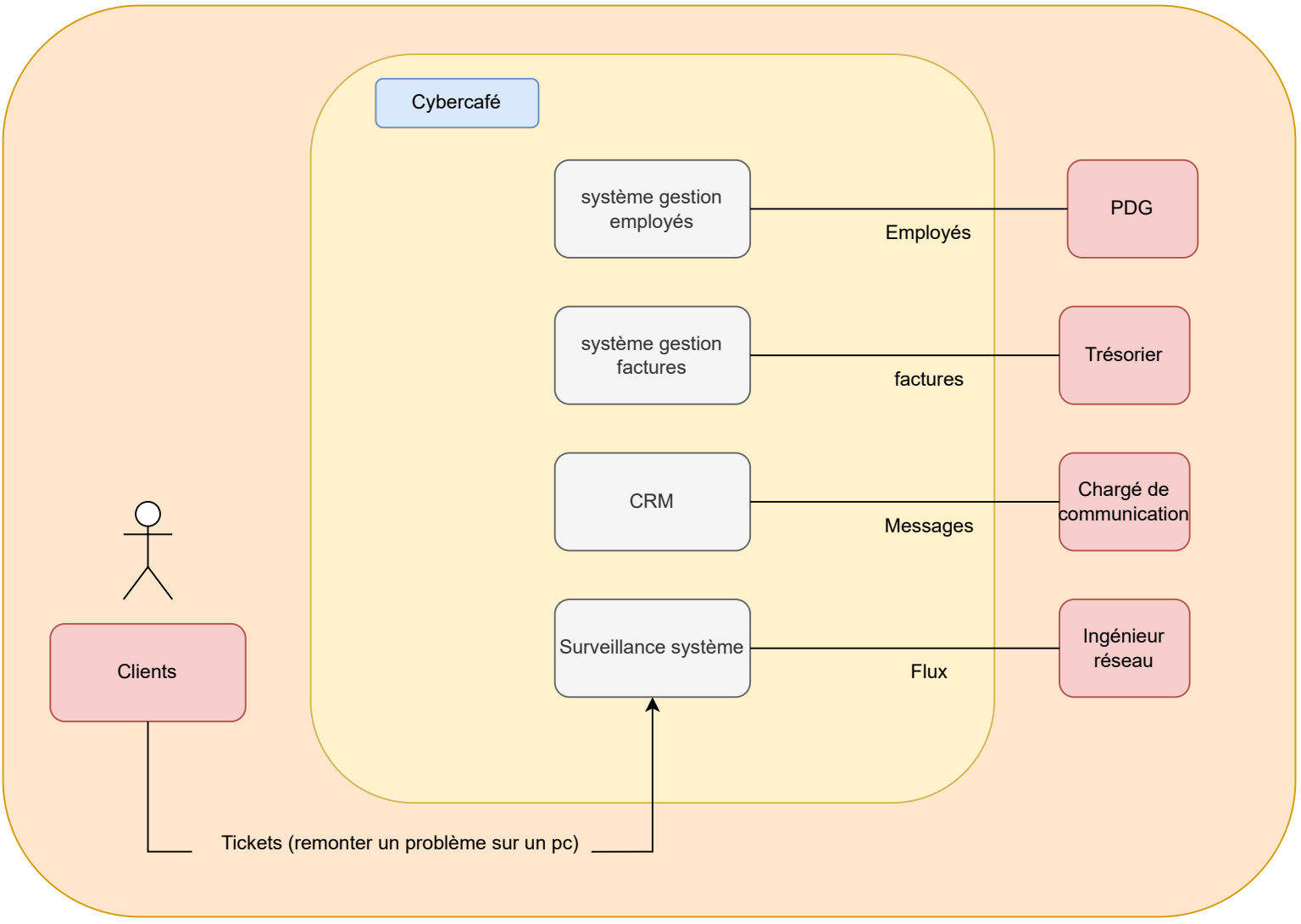

PDG
Trésorier
Ingénieur réseau
Chargé de communication
comptabilité, gestion des employés, CRM
Network
communication interne, message
Discord

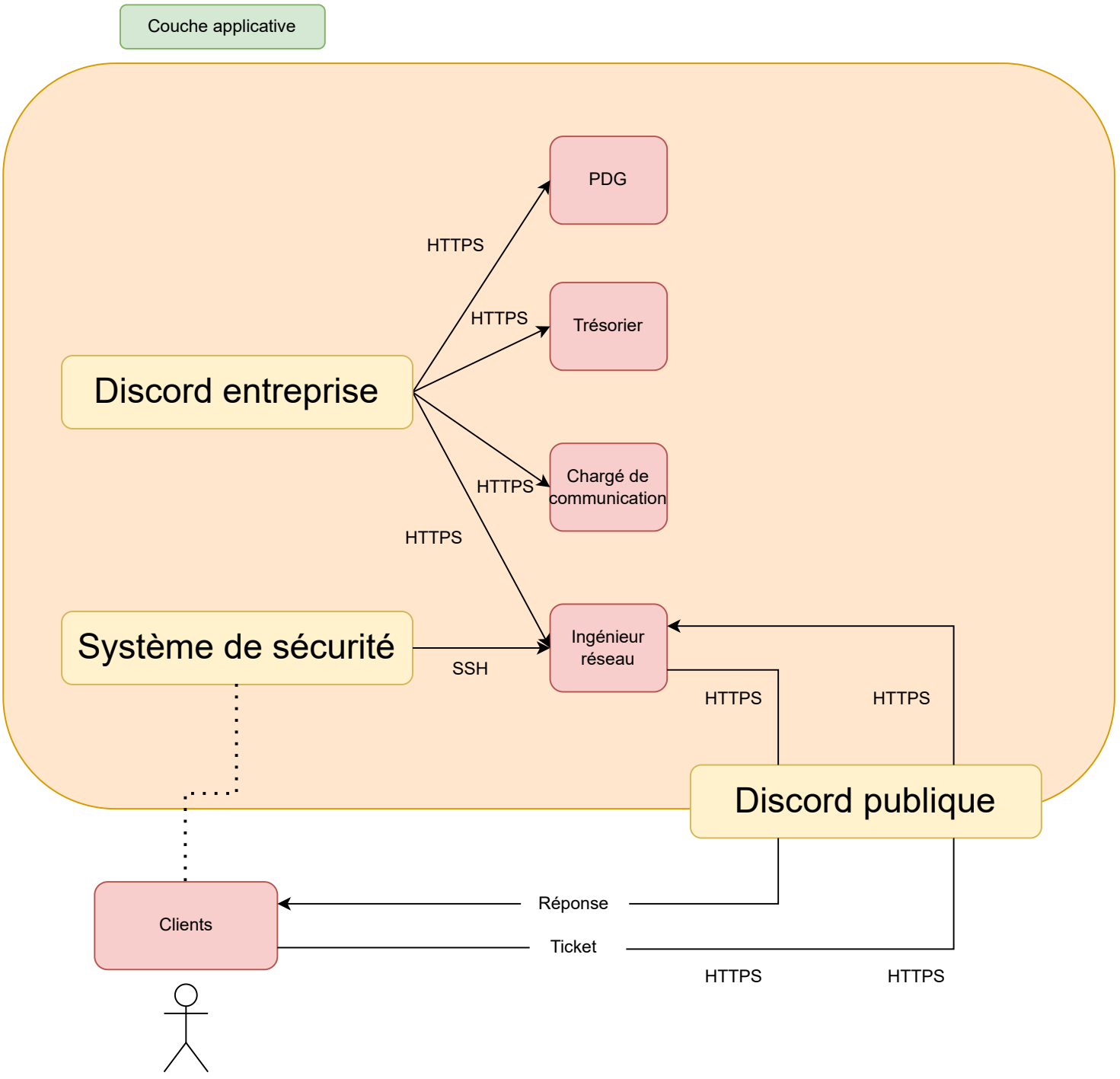
Couche fonctionnelle



Système de tickets : Nous avons chois d'utiliser un système de tickets pour la remontée de problèmes/bugs parce que c'est le système de remontée le plus "facile et pratique" pour l'utilisateur, surtout si celui-ci n'a pas l'habitude d'utiliser un ordinateur. La création/gestion/fermeture de tickets sera gérée par le bot discord Ticket Tool, un bot connu par la communauté discord pour être performant et fiable.

Messages : Nous avons chois d'utiliser la plateforme de communication Discord pour l'envoi de messages et la communication entre les employés du cybercafé parce qu'il est de plus en plus utilisé et qu'il faut vivre avec son temps (même si MSN > all)

Surveillance système : Pour le surveillance système, nous avons choisi de stocker les flux de données et les logs sur un serveur sécurisé accessible par l'ingénieur réseau et le PDG.



Discord entreprise : Chaque employé aura accès au discord entreprise où ils pourront tous communiquer les uns avec les autres. La communication se fera via des requêtes HTTPS puisque c'est simplement le protocole de communication par défaut de discord.

Les clients auront accès au discord publique pour pouvoir échanger, faire remonter des bugs et/ou autres avec le système de tickets expliqué plus haut. Les tickets seront lisibles par l'intégralité des employés de l'entreprise. Suivant le problème la réponse et/ou la solution sera envoyée au client par l'employé le plus qualifié pour y répondre. Nous utiliserons également les requêtes HTTPS pour les mêmes raisons citées au dessus.

Système de sécurité : Pour parler du système de sécurité, il est lié à la surveillance système. Nous avons choisi le protocole de communication SSH parce que c'est à la fois un protocole de communication sécurisé et un programme informatique. Le protocole de communication impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer.

Architecture Réseaux