DIAGRAMME DES FLUX PLEIADE

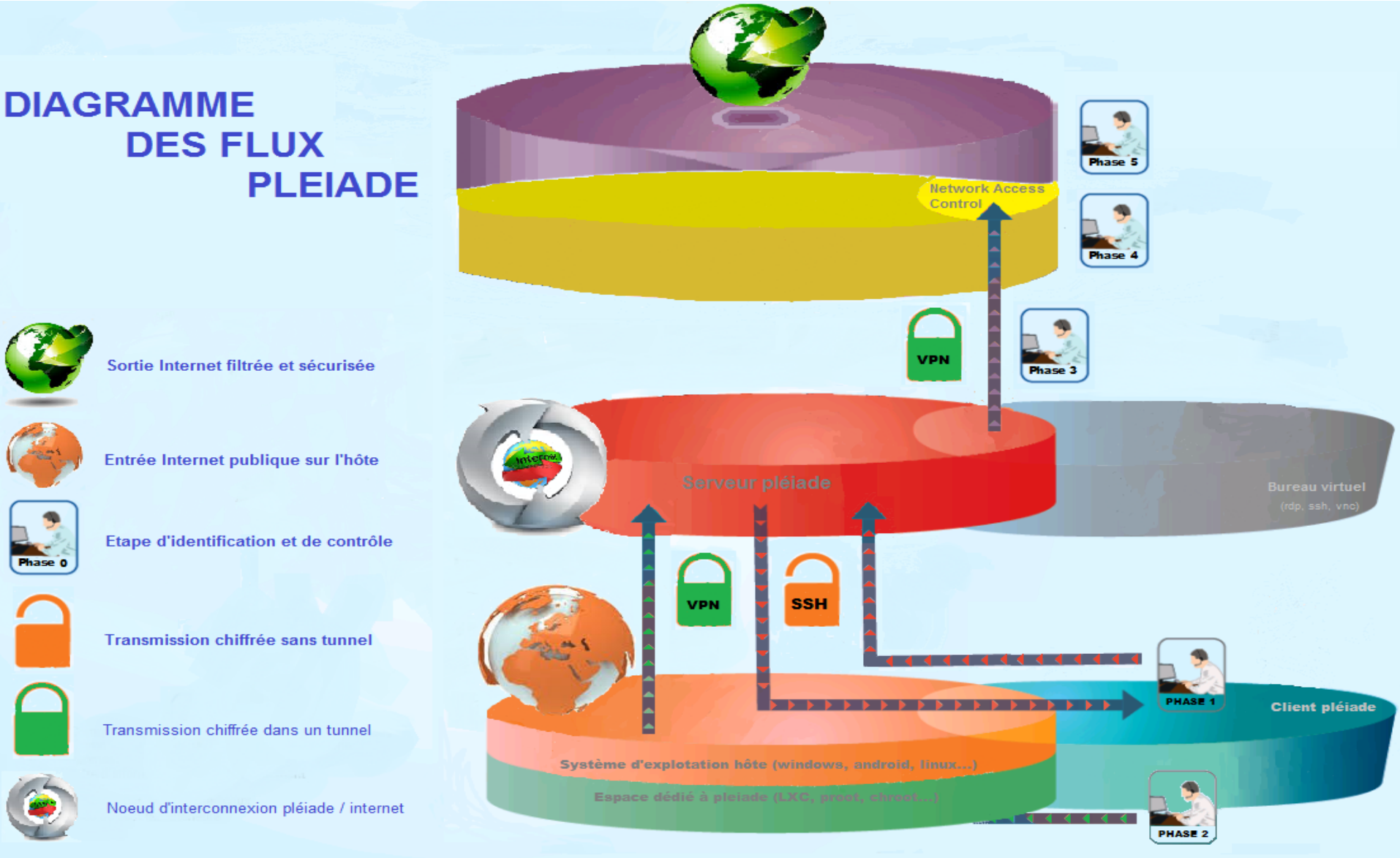

DIAGRAMME DES FLUX PLÉIADE CLIENT / SERVEUR

1. L'utilisateur, après avoir connecté le système hôte de son ordinateur à internet sur un accès public (wifi d'une gare, d'un hôtel, de son domicile etc.), va lancer l'application « client pléiade ». Le client « pléiade » va tenter de se connecter via SSH (port 22) au serveur « pléiade » auquel il a été relié à l'installation. Après reconnaissance de la station cliente par le serveur, une archive contenant la configuration temporaire lui est envoyée. Quand cette archive est reçue la connexion Secure SHell se ferme.

2. Le « client pléiade » va relancer une tentative de connexion en utilisant la configuration qu'il vient de recevoir par SSH, lui permettant d'ouvrir un tunnel VPN jusqu'au « serveur pléiade ». Ce tunnel est ouvert entre le container client et le container serveur afin d'assurer l'étanchéité du réseau.

3. Le serveur « pleiade », suivant le profil du client qui vient de se connecter va envoyer directement un bureau (mode kiosk), va envoyer un écran d'information (perte ou vol) ou envoyer une interface d'authentification s'il s'agit d'une session « utilisateur ». Dans ce dernier cas, la source de validation sera le serveur N.A.C. en utilisant les méthodes radius, apache, AD, ldap. Cette validation se fait à travers une connexion « TUN/TAP » demandé par le serveur « pléiade » au serveur Network Access Control.

4. Quand la connexion est validée et établie par le N.A.C. une session virtuelle est ouverte dans le réseau consultation (identique à celle d'un client physique connecté directement au portail captif) fournissant les mécanismes de fail2ban et d'anti-spoofing.

5. La phase 5 donne l'accès à internet en passant au travers du pare-feu dynamique avec tous les mécanismes de sécurité (liste noire, liste blanche, antivirus de proxie, etc...).

ATTENTION : Le serveur N.A.C utilisé dans la représentation de ce diagramme de flux est le serveur « alcasar ». D'autres serveurs peuvent être utilisés comme Network Access Control, mais il se peut que les fonctions diffèrent sur les protocoles d'authentification, de filtrage web et d'interception des requêtes de connexions.