STAGE FOLIATEAM

SERVICE INFORMATIQUE SI INTERNE

- ***Procédure configuration PC :***

  → Allumage PC BIOS (F12)
  → Installez driver
  → Installation des pilotes manquants
  → Changer domaine (win + R) « sysdm.cpl »
  → Intégration dans bureau à distance via dsa.msc
  Member of : gu-do
  Déplacer dans Foliateam > Computers
  → Activer licence Windows
  vivaldi>Applications > logiciels > OS > Activation-Windows11 (exécute en admin)
  → Installation VPN Stormshield
  Planificateur tache : importer tache
  → Bitlocker config mdp : 87654321
  → Supprimer le compte de config (sysdm.cpl)

- ***Service Informatique Foliateam (Garibaldi) :***

  → Création compte User
  Administration des droits
  → Résolution des tickets
  → Gérer le stock/inventaire du matériel
  Arrivé/sortie/changement
  → Gestion des sauvegardes/copies des backups

- ***Logiciels/programmes utilisés :***

  → WIPSOS
  → GLPI
  → Centreon
  → BitLocker
  → Stormshield
  → Mail in Black

SERVICE RUN OPERATEUR

- ***Fonctionnement FOLATEAM OPERATEUR***

➔ Accès Internet :

→ Requête client passe par un routeur PE d'un opérateur déjà établi (Orange, SFR…)
→ La requête est envoyée dans l'écosystème FOLIATEAM via un routeur qui redirige ensuite vers Orange qui fournit l'accès à la requête du client.

➔ Accès Data (sur serveur interne à FOLIATEAM) :

→ Dans le cas où le client veut accéder à de la data :
→ Requête client passe par un routeur PE d'un opérateur déjà établi (Orange, SFR…)
→ La requête est envoyée dans l'écosystème FOLIATEAM via un routeur qui redirige ensuite vers le data center interne de FOLIATEAM.

➔ Accès Voix IP :

→ Requête client passe par ….
→ Utilisation des protocoles nécessaires

- ***Protocoles utilisés FOLIATEAM***
  - Internet : BGP
  - VPN (télétravail /interco-site) : MPLS
  - Voix IP : signalisation SIP
  - Voix : RTP
  -
- ***Clients***
  - Uniquement entreprises/professionnels
  - FOLIATEAM propose des services en fonction des besoins des clients. Donc possibilité de problématique techniques si on sort des process habituels. → Garder une certaine logique.

- ***SERVICE RUN***
  - Résolution ticket (problématique d'un client)

Cas incident client :

Lenteur réseaux, problèmes impression et envoi et/ou réception des requetés retardées.

Procédure de solution :

→ Passer par le prestataire informatique du client (s'il en a un)

- Attendre son compte-rendu sur la situation.

→ Vérifier par étape le problème (toujours remonter par niveau = respect du modèle OSI).

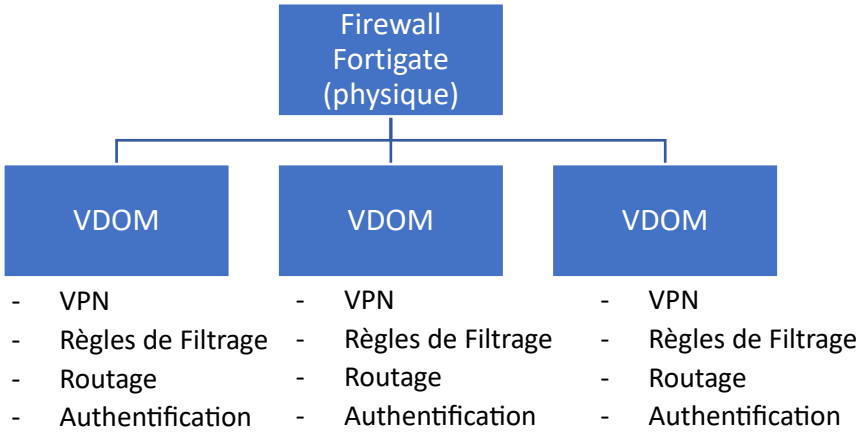
- *Niveau 1 :*
  - Vérifier le matériels/équipements clients.
  - Modèles switch pour vérifier la capacités des flux (10/100/1000 Mbps)
  - Mode de raccordement avec le routeur (Ethernet ou gigabit).
  - Utilisation de Hub (matériel moins performant)

- Niveau 2 :
  - Vérification du LAN
  - Vitesse des flux (s'il y a une perte de paquets ou ralentissement réseaux).
  - Vérification des QoS (priorités sur le réseau).

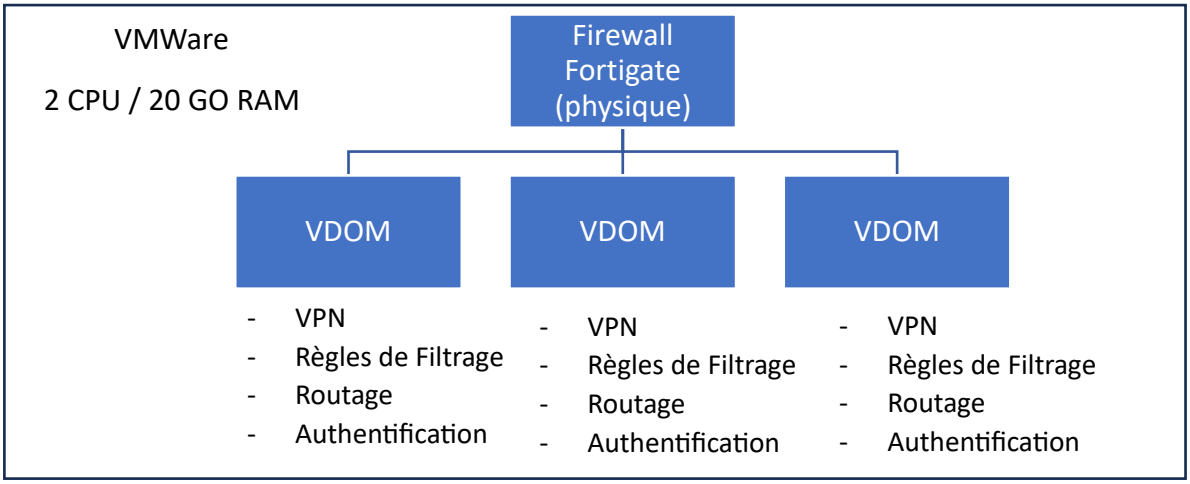
- Niveau 3 :
  - Vérification du SD WAN
  - Vérification du WAN

SERVICE SU RESEAU & SECURITE

- Infrastructure d'un Firewall physique :



- Infrastructure d'un Firewall virtuel :



- Explications :

- Le Firewall peut être physique ou virtuel. Si virtuel il se trouve dans VMWare.
- VDOM est un sous firewall crée dans un Firewall. (max 25 sous firewall mais possibilité de faire plus selon la licence).
- Chaque VDOM peut être configuré différemment et inclure jusqu'à 31 clients chacun.

Logiciel Wireshark :

Wireshark peut récupérer l'ensemble des paquets d'un appel et les convertir en audio.

= possible d'écouter une conversation si elle n'est pas sécurisée.

Gestion par le protocole RTP.

- ***Langages utilisés switch :***

  → Linux
  → R6 ou R8 pour la config de switch
  → Utilisation de Alcatel / Aruba

  + config de FW STORMSHIELD

- ***Modèle OSI***

  7- Application (http/SMTP/)
  6- Presentation
  5-Session
  4- TCP / UDP
  3- IP / ICMP(ping)
  2- MAC / Ethernet
  1- Optique / cuivre / Herstein

- ***Pen test***

Les tests de pénétration, également connus sous le nom de tests d'intrusion ou « pen test » en abrégé, sont des évaluations de sécurité informatique qui consistent à simuler des attaques ciblées sur un système informatique pour identifier ses vulnérabilités et déterminer la façon dont un pirate informatique pourrait y pénétrer.

Les « pen test » peuvent être réalisés de différentes manières. Les approches "white box" (boîte blanche), "grey box" (boîte grise) et "black box" (boîte noire) sont des méthodes différentes utilisées lors des tests de pénétration pour évaluer la sécurité d'un système. Voici une explication de chacune de ces approches :

1. Approche "White box" (boîte blanche) : Dans cette approche, le testeur dispose d'une connaissance détaillée et complète du système ou de l'application qu'il teste. Le testeur a accès à des informations internes, telles que le code source, les diagrammes d'architecture, les configurations et autres détails techniques. Cette approche permet au testeur d'analyser en profondeur le système, d'identifier les failles de sécurité potentielles et de vérifier si les meilleures pratiques de sécurité sont suivies.

2. Approche "Grey box" (boîte grise) : Cette approche se situe entre les approches "white box" et "black box". Le testeur dispose d'un niveau d'accès partiel au système, ce qui signifie qu'il a une connaissance limitée de son fonctionnement interne. Il peut avoir accès à certaines informations, telles que la documentation du système, les identifiants d'utilisateur, les spécifications techniques, etc. L'objectif est de simuler une attaque menée par une personne ayant un certain niveau de connaissance du système. Cette approche permet de découvrir les vulnérabilités qui pourraient être exploitées par un attaquant avec une connaissance partielle du système.

3. Approche "Black box" (boîte noire) : Dans cette approche, le testeur n'a aucune connaissance préalable du système ou de l'application qu'il teste. Il agit comme un attaquant externe sans aucune information interne. Cette approche permet d'évaluer la résistance d'un système face à une attaque de la part d'un individu n'ayant aucune connaissance préalable. Le testeur découvre les vulnérabilités à partir de zéro, en utilisant des techniques d'analyse et des outils de test standards.

Il convient de noter que chaque approche a ses avantages et ses inconvénients. L'approche "white box" offre une connaissance approfondie du système, mais elle ne reproduit pas fidèlement la perspective d'un attaquant réel. L'approche "black box" imite mieux une situation réelle, mais elle peut être limitée en termes de couverture des tests en raison du manque de connaissances internes. L'approche "grey box" offre un équilibre entre les deux, en fournissant une connaissance partielle pour reproduire une attaque plus réaliste tout en permettant une couverture plus large des tests. Le choix de l'approche dépendra des objectifs du test de pénétration et des ressources disponibles.