11/12/2024

PROJET ASSURANCEPLUS

Livrable 3

Bloc Sécurité et Administration

BAUDRY Lilian
BOULITEAU Mattéo
CALVO Alban
COUGNY Alexandre
FOURNIER Timon

Table des matières

Contexte

Le groupe ASSURANCEPLUS a été victime d'une attaque par rançongiciel. Une de leurs agences est paralysée pendant 10 jours. Le groupe possède actuellement neuf agences, mais compte en ouvrir d'autres. En tant qu'ingénieur, nous faisons partie de l'ESN Numerica, et nous devons fournir des solutions pour ASSURANCEPLUS.

Objectifs du livrable

Les objectifs de ce second livrable sont de présenter :

- Les solutions de supervision et d'infrastructure ;
- Une maquette du nouveau système d'information ;
- Une justification de l'infrastructure logique et physique ;
- L'administration système ;
- La sécurité réseau ;
- La cryptographie et la sécurité des données ;
- Une évaluation du bilan carbone de notre solution technique.

Contraintes du livrable

Il faudra adapter les solutions aux contraintes suivantes :

- Présenter les éléments complémentaires à la maquette impossible à maquetter ;
- L'administration système doit garantir la confidentialité, l'intégrité, la disponibilité des données et des services, ainsi que la traçabilité des actions ;
- Le bilan carbone de la solution technique comprendra les postes utilisateurs.

Administration système

Un changement a été effectué dans la vue d'administration. La gestion par OU a été remplacée par une gestion par sous-domaines. Dans les versions précédentes, les agences étaient matérialisées par des OU et étaient répliquées sur les DC joints au domaine. Dorénavant, chaque agence possède un DC avec un sous domaine comme agence2.assurancesplus.fr. Les OU, les utilisateurs, les groupes et les dossiers partagés sont créés par des scripts PowerShell.

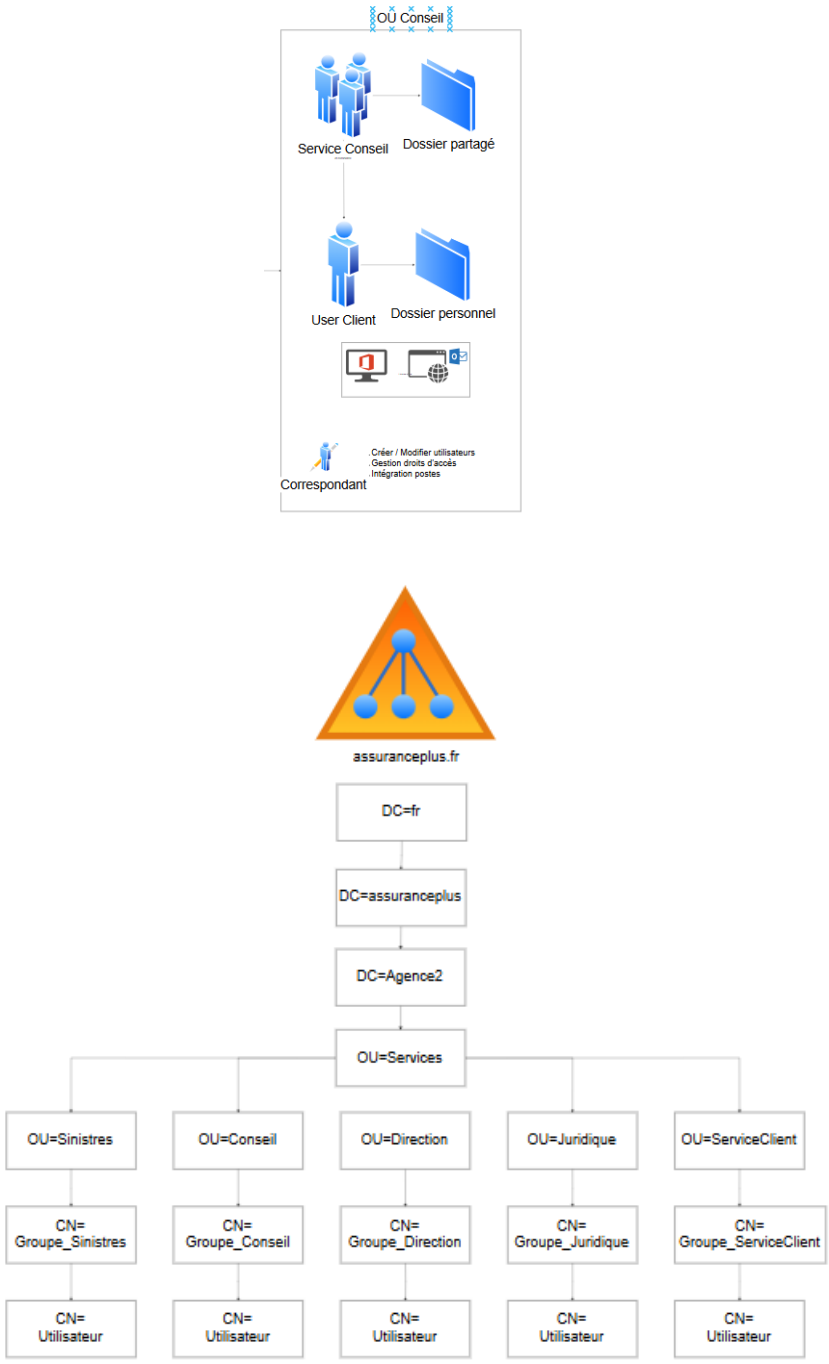

Figure 1 : Vue administration du système d'information de ASSURANCESPLUS.

Infrastructure logique

Le déroulement du projet étant basé sur la découverte de nouvelles notions au fil des différents prosit étudiés, plusieurs changements ont été apportés. Le présent livrable présente la version finale de l'infrastructure logique.

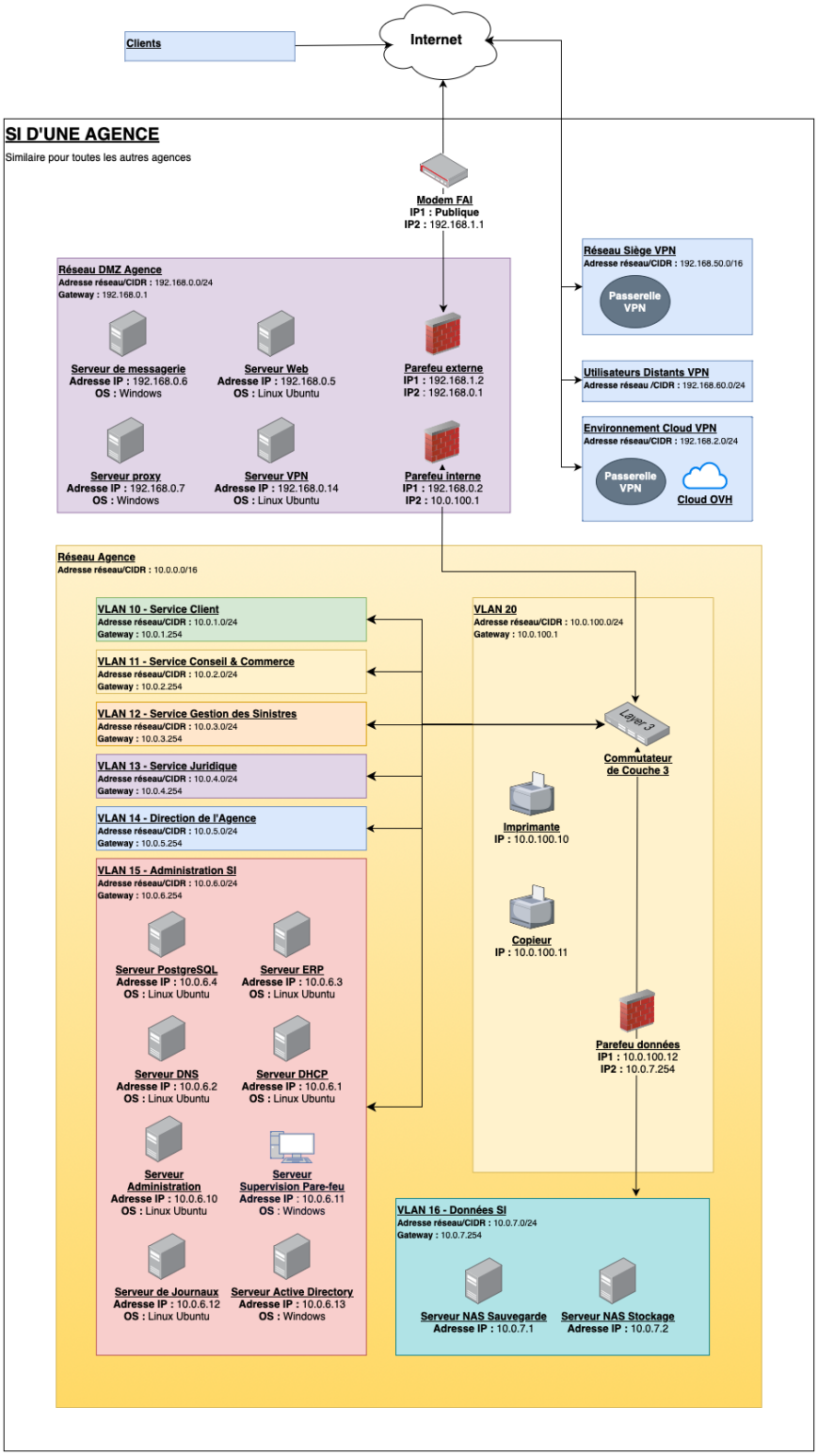

Figure 2 : Vue logique du système d'information de ASSURANCESPLUS.

Il existe quelque changement par rapport à la première version :

- Des adresses IP de certaines interfaces ont été détaillés ;
- Un nouveau VLAN a été ajouté pour isoler certains périphériques ;
- La sécurisation de la DMZ a été revu, notamment la liaison entre le routeur et le pare-feu 1.

Infrastructure physique

L'infrastructure physique, liée à l'infrastructure logique, a également subit quelques changements et est présente en version définitive ci-dessous. Les ajustements se fondent sur la vue logique corrigé de la partie précédente.

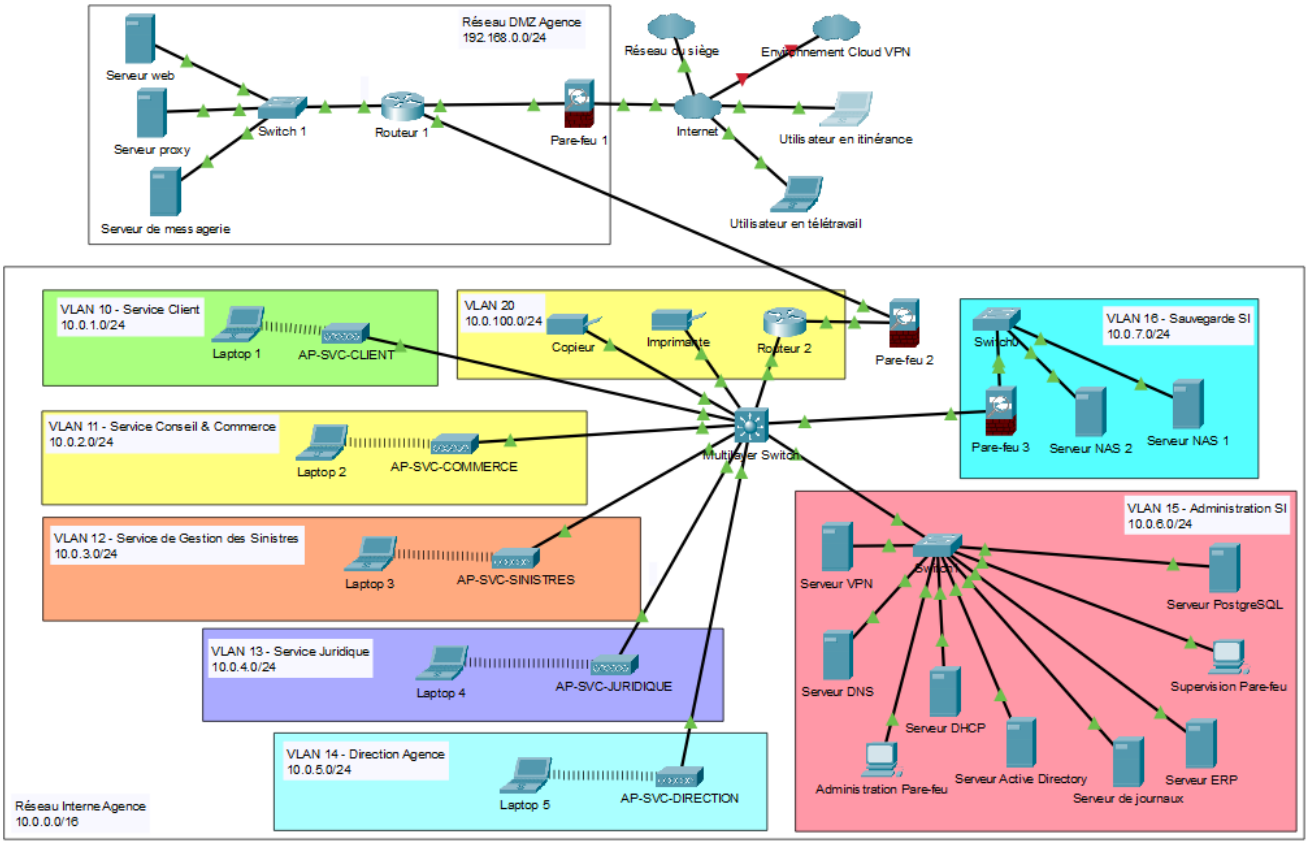

Figure 3 : Vue physique du système d'information de ASSURANCESPLUS.

Sécurité du réseau

Les changements dans la vue logique apportent également des changements dans la sécurité du réseau. La politique de filtrage ci-dessous est la dernière version.

Il est également nécessaire de rajouter qu'un antivirus comme Windows Defender est indispensable pour posséder une protection contre les virus et ransomwares sur le matériel Windows.

1. Politique de filtrage de la DMZ

1.1. Règles d'autorisation des flux à destination du pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur Administration Pare-feu – *10.0.6.10*	Interface admin. – *192.168.12.2*	SSH, HTTPS	Autoriser	Oui	Administration du pare-feu
Serveur Supervision Pare-feu – *10.0.6.11*	Interface admin. – *192.168.12.2*	get-snmp	Autoriser	Oui	Supervision du pare-feu

1.2. Règles d'autorisation des flux émis par le pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Interface admin. – *192.168.12.2*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Non	Journalisation des événements de pare-feu
Interface admin. – *192.168.12.2*	Serveur Supervision Pare-feu – *10.0.6.11*	trap-snmp	Autoriser	Oui	Notifications asynchrones initiées par le pare-feu
Interface admin. – *192.168.12.2*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu
Interface admin. – *192.168.12.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu

1.3. Règle de protection du pare-feu

Source	Destination	Service	Action	Journalisation
Toutes	Passerelle pare-feu	Tous	Interdire	Oui

1.4. Règles d'autorisation des flux métiers

1.4.1. Flux d'accès au serveur web

Source	Destination	Service	Action	Journalisation	Commentaires
Toutes	Serveur web - *192.168.0.5*	HTTPS	Autoriser	Oui	Connexions web entrantes
Serveur web – *192.168.0.5*	Toutes	HTTPS	Autoriser	Oui	Connexions web sortantes

1.4.2. Flux d'accès au serveur de messagerie

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur de messagerie – *192.168.0.6*	Toutes	SMTP	Autoriser	Oui	Envoi de mails
Toutes	Serveur de messagerie – *192.168.0.6*	SMTP, IMAP	Autoriser	Oui	Réception et récupération de mails

1.4.3. Flux d'accès au serveur proxy

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur proxy – *192.168.0.7*	Toutes	HTTPS	Autoriser	Oui	Connexions web sortantes
Toutes	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexions web entrantes

1.5. Règles « antiparasites »

Source	Destination	Service	Action	Journalisation
Aucune				

1.6. Règle d'interdiction finale

Source	Destination	Service	Action	Journalisation
Toutes	Toutes	Tous	Interdire	Oui

2. Politique de filtrage du pare-feu 1

2.1. Règles d'autorisation des flux à destination du pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur Administration Pare-feu – *10.0.6.10*	Interface admin. – *192.168.10.2*	SSH, HTTPS	Autoriser	Oui	Administration du pare-feu
Serveur Supervision Pare-feu – *10.0.6.11*	Interface admin. – *192.168.10.2*	get-snmp	Autoriser	Oui	Supervision du pare-feu

2.2. Règles d'autorisation des flux émis par le pare-feu

Source	Destination	Service	Action	Journalisation	Commentaire
Interface admin. – *192.168.10.2*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Non	Journalisation des événements de pare-feu
Interface admin. – *192.168.10.2*	Serveur Supervision Pare-feu – *10.0.6.11*	trap-snmp	Autoriser	Oui	Notifications asynchrones initiées par le pare-feu
Interface admin. – *192.168.10.2*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu
Interface admin. – *192.168.10.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu

2.3. Règle de protection du pare-feu

Source	Destination	Service	Action	Journalisation
Toutes	Passerelle pare-feu	Tous	Interdire	Oui

2.4. Règles d'autorisation des flux métiers

2.4.1. Flux d'accès au serveur ERP

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur ERP – *10.0.6.3*	Serveur web - *192.168.0.5*	HTTPS	Autoriser	Oui	Connexion entre le serveur de présentation web et le serveur de contrôle ERP
Serveur web – *192.168.0.5*	Serveur ERP – *10.0.6.3*	HTTPS	Autoriser	Oui	
Réseau siège – 192.168.50.0	Serveur ERP – *10.0.6.3*	HTTPS	Autoriser	Oui	Connexion entre le serveur ERP et le réseau siège pour synchronisation siège
Serveur ERP – *10.0.6.3*	Réseau siège – 192.168.50.0	HTTPS	Autoriser	Oui	
Serveur ERP – *10.0.6.3*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur ERP

2.4.2. Flux d'accès au serveur d'administration pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur Administration Pare-feu – *10.0.6.10*	Interface admin. Pare-feu DMZ – *192.168.12.2*	SSH, HTTPS	Autoriser	Oui	Administration du pare-feu de la DMZ

2.4.3. Flux d'accès au serveur de supervision pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur Supervision Pare-feu – *10.0.6.11*	Interface admin. Pare-feu DMZ – *192.168.12.2*	get-snmp	Autoriser	Oui	Supervision du pare-feu de la DMZ
Interface admin. Pare-feu DMZ – *192.168.12.2*	Serveur Supervision Pare-feu – *10.0.6.11*	trap-snmp	Autoriser	Oui	Notifications asynchrones du pare-feu de la DMZ au serveur de supervision

2.4.4. Flux d'accès au serveur de journaux

Source	Destination	Service	Action	Journalisation	Commentaires
Interface admin. Pare-feu DMZ – *192.168.12.2*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Oui	Journalisation des événements du pare-feu de la DMZ
Serveur de journaux – *10.0.6.12*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur de journaux
Serveur web - *192.168.0.5*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Oui	Journalisation des événements du serveur web
Serveur de messagerie – *192.168.0.6*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Oui	Journalisation des événements du serveur de messagerie
Serveur proxy – *192.168.0.7*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Oui	Journalisation des événements du serveur proxy

2.4.5. Flux d'accès au serveur de sauvegarde NAS1

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur web - *192.168.0.5*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde du serveur web
Serveur proxy – *192.168.0.7*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde de la configuration du serveur proxy
Serveur de messagerie – *192.168.0.6*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde du serveur de messagerie
Interface admin. Pare-feu DMZ – *192.168.12.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu DMZ

2.4.6. Flux d'accès au serveur Active Directory

Source	Destination	Service	Action	Journalisation	Commentaires
Réseau siège – 192.168.50.0	Serveur AD - *10.0.6.13*	HTTPS, ldaps	Autoriser	Oui	Synchronisation AD avec le siège
Serveur AD - *10.0.6.13*	Réseau siège – 192.168.50.0	HTTPS, ldaps	Autoriser	Oui	Synchronisation AD avec le siège
Serveur AD – *10.0.6.13*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur AD
Serveur de messagerie – *192.168.0.6*	Serveur AD – *10.0.6.13*	ldaps	Autoriser	Oui	Authentification des comptes de messagerie depuis l'annuaire AD

2.4.7. Flux d'accès au serveur VPN

Source	Destination	Service	Action	Journalisation	Commentaires
Toutes	Serveur VPN - *10.0.6.14*	HTTPS	Autoriser	Oui	Authentification des utilisateurs VPN
Serveur VPN - *10.0.6.14*	Utilisateurs distants VPN – *192.168.1.0*	HTTPS	Autoriser	Oui	Passerelle VPN
Utilisateurs distants VPN – *192.168.60.0*	Serveur VPN - *10.0.6.14*	HTTPS	Autoriser	Oui	Passerelle VPN
Serveur VPN - *10.0.6.14*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur VPN

2.4.8. Flux d'accès au serveur DNS

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur VPN - *10.0.6.14*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur DNS

2.4.9. Flux d'accès au VLAN 10 – Service client

Source	Destination	Service	Action	Journalisation	Commentaires
VLAN 10 – *10.0.1.0*	Utilisateurs distants VPN – *192.168.60.0*	HTTPS	Autoriser	Oui	Connexion distante VPN au VLAN
Utilisateurs distants VPN – *192.168.60.0*	VLAN 10 – *10.0.1.0*	HTTPS	Autoriser	Oui	
VLAN 10 – *10.0.1.0*	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexion du VLAN au proxy pour les requêtes web entrantes et sortantes
Serveur proxy – *192.168.0.7*	VLAN 10 – *10.0.1.0*	HTTPS	Autoriser	Oui	

2.4.10. Flux d'accès au VLAN 11 – Service conseil et commerce

Source	Destination	Service	Action	Journalisation	Commentaires
VLAN 11 – *10.0.2.0*	Utilisateurs distants VPN – *192.168.60.0*	HTTPS	Autoriser	Oui	Connexion distante VPN au VLAN
Utilisateurs distants VPN – *192.168.60.0*	VLAN 11 – *10.0.2.0*	HTTPS	Autoriser	Oui	
VLAN 11 – *10.0.2.0*	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexion du VLAN au proxy pour les requêtes web entrantes et sortantes
Serveur proxy – *192.168.0.7*	VLAN 11 – *10.0.2.0*	HTTPS	Autoriser	Oui	

2.4.11. Flux d'accès au VLAN 12 – Service gestion des sinistres

Source	Destination	Service	Action	Journalisation	Commentaires
VLAN 12 – *10.0.3.0*	Utilisateurs distants VPN – *192.168.60.0*	HTTPS	Autoriser	Oui	Connexion distante VPN au VLAN
Utilisateurs distants VPN – *192.168.60.0*	VLAN 12 – *10.0.3.0*	HTTPS	Autoriser	Oui	
VLAN 12 – *10.0.3.0*	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexion du VLAN au proxy pour les requêtes web entrantes et sortantes
Serveur proxy – *192.168.0.7*	VLAN 12 – *10.0.3.0*	HTTPS	Autoriser	Oui	

2.4.12. Flux d'accès au VLAN 13 – Service juridique

Source	Destination	Service	Action	Journalisation	Commentaires
VLAN 13 – *10.0.4.0*	Utilisateurs distants VPN – *192.168.60.0*	HTTPS	Autoriser	Oui	Connexion distante VPN au VLAN
Utilisateurs distants VPN – *192.168.60.0*	VLAN 13 – *10.0.4.0*	HTTPS	Autoriser	Oui	
VLAN 13 – *10.0.4.0*	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexion du VLAN au proxy pour les requêtes web entrantes et sortantes
Serveur proxy – *192.168.0.7*	VLAN 13 – *10.0.4.0*	HTTPS	Autoriser	Oui	

2.4.13. Flux d'accès au VLAN 14 – Service direction de l'agence

Source	Destination	Service	Action	Journalisation	Commentaires
VLAN 14 – *10.0.5.0*	Utilisateurs distants VPN – *192.168.60.0*	HTTPS	Autoriser	Oui	Connexion distante VPN au VLAN
Utilisateurs distants VPN – *192.168.60.0*	VLAN 14 – *10.0.5.0*	HTTPS	Autoriser	Oui	
VLAN 14 – *10.0.5.0*	Serveur proxy – *192.168.0.7*	HTTPS	Autoriser	Oui	Connexion du VLAN au proxy pour les requêtes web entrantes et sortantes
Serveur proxy – *192.168.0.7*	VLAN 14 – *10.0.5.0*	HTTPS	Autoriser	Oui	

2.4.14. Flux d'accès au cloud VPN de sauvegarde

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur web - *192.168.0.5*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur web
Serveur proxy – *192.168.0.7*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde de la configuration du serveur proxy
Serveur de messagerie – *192.168.0.6*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde du serveur de messagerie
Interface admin. Pare-feu DMZ – *192.168.0.10*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu DMZ

2.5. Règles « antiparasites »

Source	Destination	Service	Action	Journalisation
Aucune				

2.6. Règle d'interdiction finale

Source	Destination	Service	Action	Journalisation
Toutes	Toutes	Tous	Interdire	Oui

3. Politique de filtrage du pare-feu 2

3.1. Règles d'autorisation des flux à destination du pare-feu

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur Administration Pare-feu – *10.0.6.10*	Interface admin. – *10.0.8.1*	SSH, HTTPS	Autoriser	Oui	Administration du pare-feu
Serveur Supervision Pare-feu – *10.0.6.11*	Interface admin. – *10.0.8.1*	get-snmp	Autoriser	Oui	Supervision du pare-feu

3.2. Règles d'autorisation des flux émis par le pare-feu

Source	Destination	Service	Action	Journalisation	Commentaire
Interface admin. – *10.0.8.1*	Serveur de journaux – *10.0.6.12*	syslog	Autoriser	Non	Journalisation des événements de pare-feu
Interface admin. – *10.0.8.1*	Serveur Supervision Pare-feu – *10.0.6.11*	trap-snmp	Autoriser	Oui	Notifications asynchrones initiées par le pare-feu
Interface admin. – *10.0.20.21*	Cloud VPN – *192.168.2.0*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu
Interface admin. – *10.0.20.21*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde de la configuration du pare-feu

3.3. Règle de protection du pare-feu

Source	Destination	Service	Action	Journalisation
Toutes	Passerelle pare-feu	Tous	Interdire	Oui

3.4. Règles d'autorisation des flux métiers

3.4.1. Flux d'accès au serveur de sauvegarde NAS1

Source	Destination	Service	Action	Journalisation	Commentaires
Serveur web - *192.168.0.5*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	Sauvegarde des configurations et des données
Serveur AD - *10.0.6.13*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur de journaux – *10.0.6.12*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur DNS – *10.0.6.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur ERP – *10.0.6.3*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur PostgreSQL – *10.0.6.4*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur VPN - *10.0.6.14*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur de messagerie – *192.168.0.6*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Serveur proxy – *192.168.0.7*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Interface admin. Pare-feu DMZ – *192.168.12.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	
Interface admin. Pare-feu 1 – *192.168.10.2*	Serveur de sauvegarde NAS1 – *10.0.7.1*	SSH	Autoriser	Oui	

3.5. Règles « antiparasites »

Source	Destination	Service	Action	Journalisation
Aucune				

3.6. Règle d'interdiction finale

Source	Destination	Service	Action	Journalisation
Toutes	Toutes	Tous	Interdire	Oui

Cryptographie et sécurité des données

La sécurisation des données repose sur des mécanismes robustes combinant confidentialité, intégrité et disponibilité. Cette stratégie inclut plusieurs niveaux de protection et des pratiques adaptées aux besoins métiers.

Confidentialité et sécurité des données

- **Chiffrement et sécurité réseau** : Toutes les communications sont protégées par des protocoles sécurisés, garantissant la confidentialité des données en transit.
    - **IPSec comme VPN client-to-site** : Ce standard mondialement reconnu assure une connexion sécurisée entre les utilisateurs distants et l'infrastructure interne.
    - **HTTPS avec certificats Let's Encrypt** : Permet un accès sécurisé aux serveurs web depuis Internet. Les certificats Let's Encrypt offrent une solution économique et fiable pour un chiffrement SSL/TLS.
- **Authentification unifiée** :
    - Mise en œuvre de **LDAPS** et **SSO** pour centraliser l'authentification des utilisateurs. Ces solutions simplifient la gestion des accès tout en renforçant la sécurité par des mécanismes d'authentification forts (authentification multifactorielle, par exemple).

Stratégie de sauvegarde et conservation

La stratégie de sauvegarde repose sur l'utilisation de **Veeam Backup & Replication**, combinée à un stockage en RAID 10 local, un NAS WORM hors-site et un cloud OVH. Ces mécanismes garantissent redondance et récupération rapide en cas d'incident.

Type de sauvegarde	Fréquence	Durée de rétention	Description
Incrémentale	Horaires	24 heures	Sauvegarde des changements récents (logs et modifications de fichiers).
Différentielle	Quotidienne	15 jours	Sauvegarde intermédiaire pour restaurations rapides sur une courte période.
Complète	Hebdomadaire	1 an	Sauvegarde intégrale pour assurer une base stable et fiable.
Structurelle	Annuelle	5 ans	Copie complète de l'ensemble du système d'information pour conformité légale.

Éléments sauvegardés et cas d’utilisation

La stratégie inclut plusieurs niveaux de sauvegarde adaptés à différents scénarios :

1. **Sauvegarde au niveau de l’image (Image Level)** :
    - **Définition** : Copie complète d'une machine virtuelle, incluant le système d'exploitation, les applications et les données.
    - **Cas d’utilisation** :
        - Restauration d’un serveur complet en cas de panne majeure.
        - Migration d’un environnement virtuel (VMware, Hyper-V) vers une nouvelle plateforme.
    - **Limitation** : Espace de stockage conséquent, récupération granulaire non disponible.
2. **Sauvegarde au niveau des volumes (Volume Level)** :
    - **Définition** : Sauvegarde ciblée sur des volumes spécifiques.
    - **Cas d’utilisation** :
        - Protection de bases de données critiques ou de volumes métiers.
        - Restauration partielle pour minimiser l’impact sur la continuité d’activité.
    - **Limitation** : Risque d’omission de volumes essentiels.
3. **Sauvegarde au niveau des fichiers (File Level)** :
    - **Définition** : Copie de fichiers ou répertoires spécifiques.
    - **Cas d’utilisation** :
        - Sauvegarde des documents partagés et fichiers utilisateurs.
        - Restauration rapide de fichiers individuels supprimés ou modifiés accidentellement.
    - **Limitation** : Incapacité à restaurer un système complet.

Rétention et immutabilité

Toutes les sauvegardes sont :

- **Chiffrées** : Garantissant la confidentialité des données en stockage et en transit.
- **Immuables** : Les données ne peuvent être modifiées ou supprimées prématurément.
- **Journalisées** : Chaque opération de sauvegarde est tracée pour assurer un suivi complet.
- **Intégrité vérifiée** : Des tests réguliers garantissent la validité et la restauration des sauvegardes.

Virtualisation

La virtualisation optimise les systèmes d'information en améliorant la gestion des ressources, la sécurité et la résilience :

- **Virtualisation du réseau** : Grâce aux **VLANs**, elle segmente le réseau pour isoler les flux critiques, améliorer les performances et renforcer la sécurité.
- **Virtualisation des serveurs** : Permet de consolider plusieurs services sur une seule infrastructure, avec une allocation dynamique des ressources et une flexibilité pour déployer ou migrer des machines virtuelles (VMs).
- **Avantages clés** :
    - **Isolation des services** : Garantit leur disponibilité en évitant les conflits.
    - **Facilité de gestion** : Sauvegardes rapides (images complètes) et restaurations efficaces.
    - **Résilience accrue** : Réplication et migration à chaud pour minimiser les interruptions.
    - **Tests sécurisés** : Création d'environnements isolés pour essais.

Traçabilité

La traçabilité consiste à suivre et enregistrer les actions et événements dans un système, afin de garantir la transparence, la conformité et la résolution rapide des incidents.

Monitoring par Zabbix

Le **monitoring** consiste à surveiller en temps réel les performances des systèmes, réseaux et applications afin de détecter rapidement les anomalies, prévenir les pannes et garantir la disponibilité optimale des services.

La **supervision du système** permet :

- Un suivi des serveurs physiques ou virtuels via la surveillance de l'état général des serveurs et la détection des défaillances matérielles et logicielles ;
- Une visualisation des indicateurs types, sur l'utilisation du CPU, de la mémoire, du taux d'utilisation du disque et l'uptime (temps de disponibilité).

Critère	Description	Warning	Critique
Utilisation du CPU	Surveillance de l'utilisation des ressources CPU	> 75% d'utilisation pendant plus de 5 minutes	> 90% d'utilisation pendant plus de 2 minutes
Utilisation de la mémoire	Surveillance de l'utilisation de la mémoire RAM	> 80% de mémoire utilisée	> 95% de mémoire utilisée
Utilisation du disque	Surveillance de l'espace disque disponible	> 80% de l'espace disque utilisé	> 90% de l'espace disque utilisé
Température du serveur	Surveillance de la température des composants matériels	> 70°C	> 85°C
Uptime des serveurs	Suivi de la disponibilité des serveurs (durée sans redémarrage)	Redémarrage prévu dans les 24 heures	Serveur en panne ou redémarré sans raison apparente
État des services critiques	Vérification des services essentiels (ex: SSH, HTTP)	Service indisponible pendant plus de 2 minutes	Service indisponible pendant plus de 5 minutes

La **supervision du réseau** apporte :

- Une surveillance des équipements réseau, impliquant un suivi des routeurs, des commutateurs et des firewalls via SNMP, ainsi que la mesure de la connectivité, de la bande passante et des pertes de paquets ;
- Une observation d'indicateurs types, comme la latence, la perte de paquets, le débit (bande passante) et la disponibilité des équipements.

Critère	Description	Warning	Critique
Latence du réseau	Mesure du temps de réponse entre les équipements	> 100 ms (interne), > 250 ms (externe)	> 500 ms
Perte de paquets	Proportion de paquets perdus durant la transmission	> 1% de perte de paquets pendant 5 minutes	> 5% de perte de paquets pendant 1 minute
Débit / Bande passante	Surveillance de la bande passante des équipements	> 80% de la bande passante utilisée	> 95% de la bande passante utilisée
Disponibilité des équipements	Suivi de la disponibilité des équipements réseau	Équipement inactif pendant 5 minutes	Équipement inactif pendant 10 minutes
Utilisation des interfaces	Suivi de l'état des interfaces réseau (up/down)	Une interface réseau en statut down pendant 5 minutes	Une interface réseau en statut down pendant 10 minutes

La **supervision applicative** consiste à :

- Analyser des performances applicatives, comprenant le suivi des applications métiers (temps de réponse et disponibilité des services) et la vérification des communications entre applications (APIs, bases de données) ;
- Obtenir des indicateurs types sur le temps de réponse, la disponibilité des services (*health checks*), le taux de transactions réussies et l'état des bases de données.

Critère	Description	Warning	Critique
Temps de réponse des applications	Temps que met l'application pour répondre aux requêtes	> 3 secondes	> 10 secondes
Disponibilité des services métiers	Vérification de la disponibilité des services métiers	Service indisponible pendant plus de 2 minutes	Service indisponible pendant plus de 5 minutes
Taux de transactions réussies	Proportion de transactions traitées avec succès	< 95% de transactions réussies	< 90% de transactions réussies
État des bases de données	Vérification du fonctionnement des bases de données	Temps de réponse > 5 secondes pour les requêtes critiques	Temps de réponse > 10 secondes pour les requêtes critiques
Vérification des APIs	Vérification des appels API entre applications	Temps de réponse des API > 3 secondes	Temps de réponse des API > 10 secondes
Santé des services	Test de la disponibilité des services via des health checks	Un ou plusieurs services non accessibles	Un ou plusieurs services critiques non accessibles

Suivi des logs Elastic Search

Un suivi des logs par Elastics Search permet :

- L'indexation et le stockage des logs, qui fonctionne avec une base de données pour centraliser les logs issus des différents systèmes et applications tout en gérant les logs non structurés provenant de bases non relationnelles ;
- Une recherche et analyse via un moteur de recherche performant, identifiant rapidement les anomalies tout en facilitant l'analyse des causes racines et des éléments pouvant déclencher des incidents en chaîne.

Personnel responsable

Lors des incidents ou anomalies, il est nécessaire de joindre certains membres clés du personnel pour intervenir :

- **Administrateurs système** : En charge de la gestion des serveurs et des équipements, ils doivent être alertés rapidement en cas de défaillance système ou réseau.
- **Équipes réseau** : Responsables de la connectivité, elles doivent être informées en cas de problèmes affectant la bande passante, la latence ou la disponibilité des équipements réseau.
- **Développeurs ou équipes applicatives** : En cas de défaillance liée à une application, un service ou une base de données, ils doivent être avertis pour diagnostiquer et résoudre rapidement les problèmes.
- **Responsables opérationnels** : Les managers ou responsables d'équipes doivent être tenus informés des incidents critiques afin d'assurer la continuité des opérations.

Méthodes de notification

Joindre efficacement le personnel responsable est une tâche fondamentale, qui doit être la plus rapide possible. Les méthodes les plus utilisés sont :

- **Alertes par courriel :** Informer les administrateurs et équipes avec des détails sur le problème (indicateurs, gravité, impact) ;
- **SMS :** Utilisé pour les alertes critiques nécessitant une réponse rapide ;
- **Messagerie instantanée :** Notifier les équipes en temps réel via Slack, Teams ou Telegram, pour des actions immédiates ;
- **Tableaux de bord :** Visualiser l'état des systèmes et les alertes critiques en temps réel via des outils comme Zabbix ;
- **Escalade automatique :** Si aucune action n'est prise, notifier un responsable hiérarchique pour garantir une réponse rapide.

Protocole de réponse à l'alerte

Lorsque le personnel responsable du bon fonctionnement du système d'information évalue le problème rencontré, il doit suivre certaines étapes clés :

- **Évaluation de la gravité :** Identifier rapidement si l'alerte est critique ou non pour définir les actions à entreprendre ;
- **Temps de réponse :** Les alertes critiques nécessitent une réaction immédiate, tandis que les alertes moins graves peuvent être traitées plus tard ;
- **Suivi et résolution :** Confirmer la résolution de l'incident et notifier les parties concernées lorsque le problème est résolu.

Système de mise à jour

WSUS (Windows Server Update Services) est un outil qui permet d'automatiser la gestion des mises à jour Windows, en offrant un contrôle sur les mises à jour à appliquer ou restreindre :

- **Automatisation des mises à jour** : Gère et planifie les mises à jour des systèmes de manière centralisée ;
- **Validation administrative** : Offre la possibilité de valider ou de rejeter les mises à jour avant leur déploiement pour garantir la stabilité des systèmes ;
- **Gestion granulaire** : Permet de restreindre certaines mises à jour ou d'en forcer d'autres en fonction des priorités et des exigences de sécurité.

Bilan carbone

Équipements existants

La liste suivante comprend tous les équipements déjà présents au sein d'une agence type :

- 50 PC portables ;
- 50 écrans ;
- Routeur
- 1 Serveur virtualisant plusieurs services (Active Directory, l'ERP, la messagerie, la BDD PostgreSQL, le serveur web) ;
- Copieur multifonction ;
- Imprimante couleur ;
- Pare-feu ;
- 1 Switch de l'agence.

Équipements supplémentaires

La liste ci-dessous contient le matériel physique que notre solution ajouterait :

- Switch de la DMZ ;
- Routeur de la DMZ ;
- 2 pares-feux ;
- 8 switches ;
- 1 Serveur qui virtualise plusieurs services (le DNS ; le DHCP, l'administration du pare-feu, la supervision du pare-feu, les logs, Active Directory, le VPN, le proxy) ;
- 2 NAS de sauvegarde ;
- 2 onduleurs.

Émissions de CO2

La fabrication et le transport du matériel informatique doit être pris en compte dans nos calculs. L'unité sera la masse de CO2 émis dans l'atmosphère, et on suppose que les transports se font par voie maritime.

- Commutateur de la DMZ ;
  - Fabrication : 100 kg,
  - Transport : 2 kg,
- Routeur de la DMZ ;
  - Fabrication : 42 kg,
  - Transport : 0.2 kg,
- 2 pares-feux
  - Fabrication : 2 x 360kg,
  - Transport : 2 x 1kg,

- 8 commutateurs de l'agence ;
  - Fabrication : 8 x 100 kg,
  - Transport : 8 x 2 kg,
- 2 onduleurs ;
  - Fabrication : 2 x 75 kg,
  - Transport : 2 x 3 kg,
- Serveur (DNS et DHCP) et 2 NAS de sauvegarde.

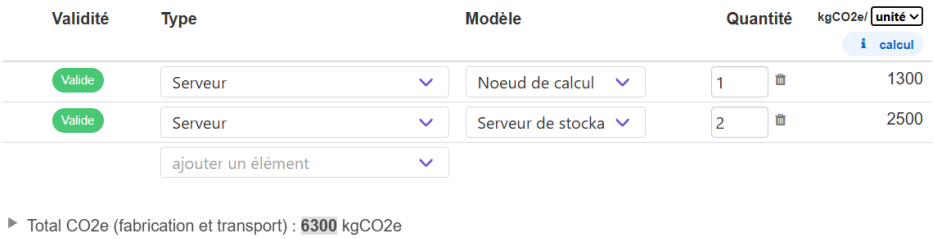

Figure 4 : Estimation de l'impact du serveur et des NAS via l'outil EcoDiag.

À partir de ces données, on détermine que la fabrication et le transport des nouveaux équipements produira :

$$Impact_{commutateurs} + Impact_{routeur} + Impact_{pares-feux} + Impact_{onduleurs}$$
$$+(Impact_{serveur} + Impact_{NAS})$$
$$= (9 \times 100 + 9 \times 2) + (42 + 0.2) + (2 \times 360 + 2 \times 1) + (2 \times 75 + 2 \times 3) + (6300)$$
$$= 8138{,}2\ kg$$

Les émissions de CO2 pour la production et la livraison des équipements est estimé à 8138.2 kg par agence, soit 73513.8 kg au total (pour les 9 agences).

Émissions lors de l'utilisation

Les émissions de CO2 par an lié à l'utilisation des équipements sont également à prendre en compte :

- 3 Pares-feux ;
  - 3 x 350 kg ;
- Commutateur de l'agence ;
  - 105 kg ;
- Commutateur de la DMZ ;
  - 105 kg ;
- Routeurs de la DMZ et de l'agence ;
  - 2 x 52 kg ;
- 8 commutateurs de l'agence ;
  - 8 x 105 kg,
- 2 onduleurs
  - 2 x 175 kg ;
- 50 PC, 50 écrans, copieur, imprimante, serveur, 2 NAS.

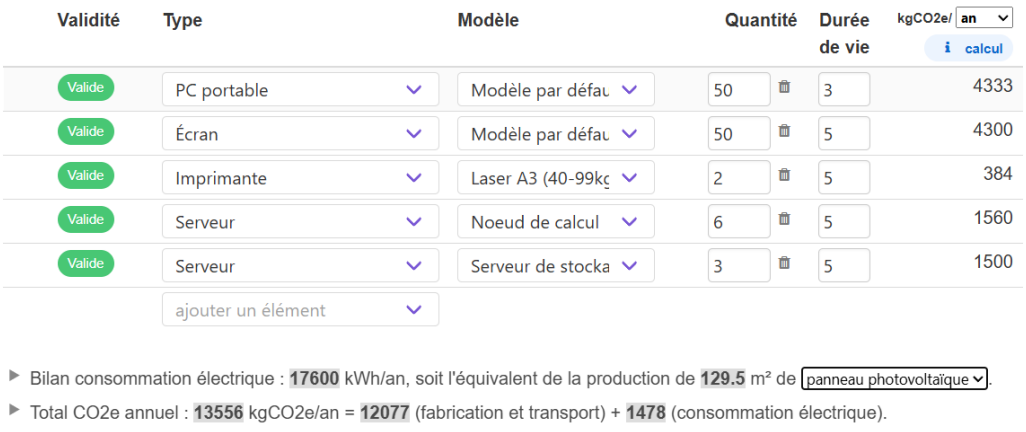

Figure 5 : Estimation de l'impact de plusieurs équipements via l'outil EcoDiag.

À partir de ces données, on peut déterminer que la consommation électrique des appareils aura une émission de :

$$Impact_{pares-feux} + Impact_{commutateurs} + Impact_{routeurs} + Impact_{onduleurs}$$
$$+ Impact_{PC} + Impact_{écrans} + Impact_{copieur} + Impact_{imprimante}$$
$$+ Impact_{serveur} + Impact_{NAS}$$
$$= 3 \times 350 + 10 \times 105 + 2 \times 52 + 2 \times 175 + 1478 = 4032\ kg$$

La consommation électrique du parc informatique émettra 4032 kg de CO2 par an.

Cloud

Le choix pour l'hébergeur Cloud s'est porté sur OVH, puisque sa localisation en France permet de garantir la législation sur les données.

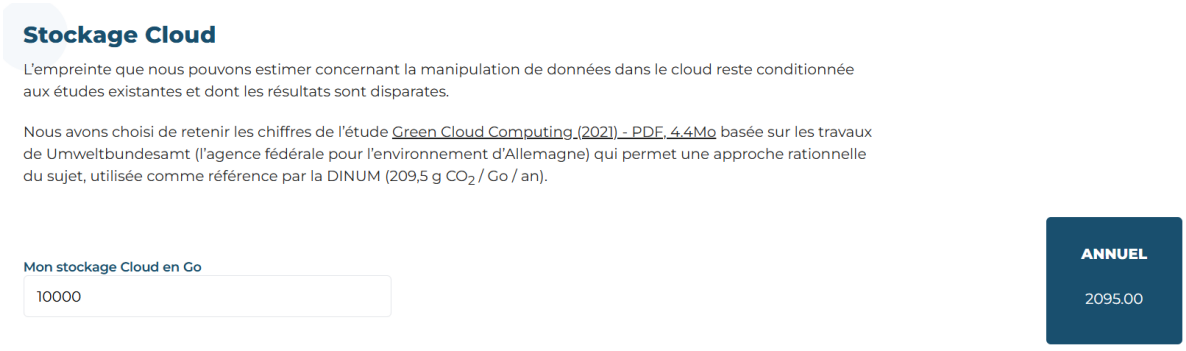

Figure 6 : Estimation des émissions du Cloud avec l'outil MyImpact.

Le stockage de 10 Téraoctets du cloud aura une émission annuelle de CO2 estimé à 2095 kg.

Total des émissions

Le total des émissions du parc informatique de notre solution se fonde sur ces données :

- Fabrication et transport des équipements : 8138.2 kg de CO2 ;
- Consommation annuelle des équipements : 4032 kg de CO2 ;
- Consommation annuelle du cloud : 2095 kg.

L'émission totale de CO2 de notre solution pour chaque agence sera donc 8138.2 kg avant la mise en service, et émettra 6127 kg de CO2 par an pour sa consommation électrique.

L'empreinte carbone de cette infrastructure est donc estimée à 122.54 kg de CO2 par an par salarié. En sachant qu'en moyenne, un employé consomme 350 kg de CO2 pour l'utilisation de matériels informatique[3], il est possible de qualifier notre solution comme moins polluante que la moyenne.

Maquette

Les maquettes présentes pour ce projet sont :

- Une maquette Packet Tracer permettant de tester les liaisons réseaux entres les différents équipements, ainsi que certaines règles de sécurité ;
- Une maquette sur VirtualBox, composé de trois machines virtuelles (un domaine racine, un sous-domaine, un poste utilisateur), attestant de la viabilité du système Active Directory qui doit être établis sur le réseau.

Bibliographie

1. Outil Ecodiag. 15 décembre 2020. [En ligne]. **EcoInfo**. Disponible sur <https://ecoinfo.cnrs.fr/ecodiag-calcul/>. Consulté le 10 décembre 2024.
2. Évaluation de mon empreinte environnementale professionnelle individuelle du numérique en kg eq. CO2. 1er juillet 2022. [En ligne]. **MyImpact**. Disponible sur <https://myimpact.isit-europe.org/fr/>. Consulté le 10 décembre 2024.
3. Quelle est l'empreinte carbone d'un salarié ? 13 mai 2022. [En ligne]. **Culture RH**. Disponible sur <https://culture-rh.com/empreinte-carbone-salarie/>. Consulté le 11 décembre 2024.