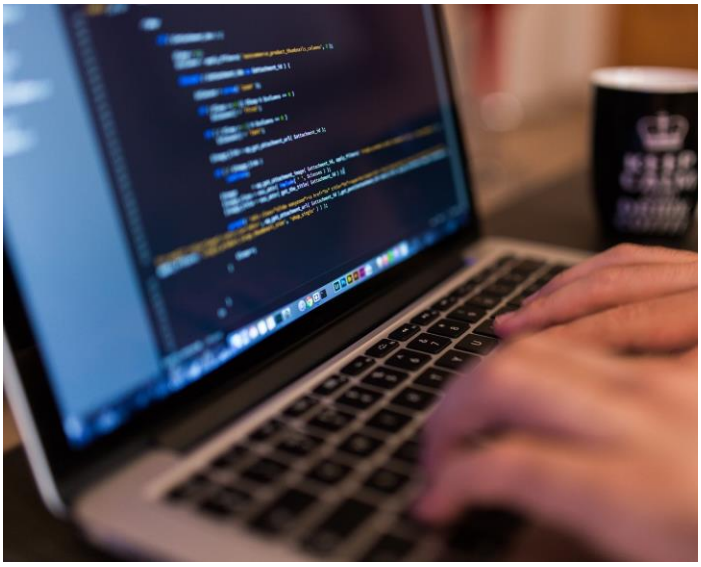
Rapport du Projet Architecture sécurisée



Rapport du Projet : Audit D'architecture

Nom 1 : ZAGHOUINI	Nom 2 : Bouachour
Prénom 1 : Redwane	Prénom2 : Mohamed Anouar

Nom 3 : SOLEIMAN
Prénom 3: Rabab

Enseignant : Cédric PINTO

Partie 1 : Analyse de l'existant

Travail demandé

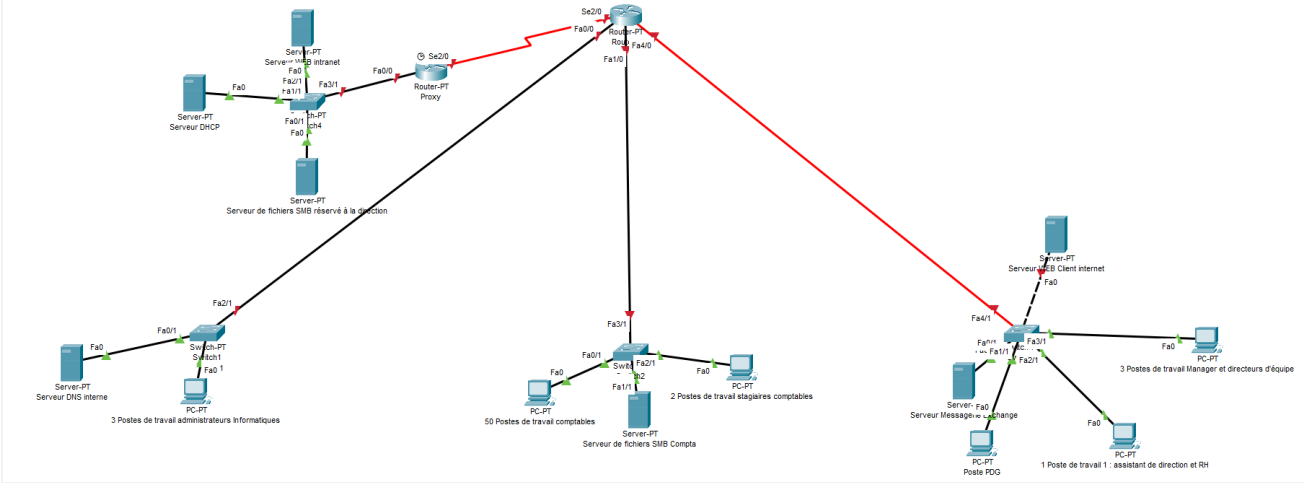
Partie 1 : Analyse de l'existant

1- **L'entreprise ne dispose pas de schéma d'architecture, votre première mission consiste à en produire un.**

- Réaliser un schéma d'architecture en se basant sur les éléments communiqués par le client
- Préciser l'adressage IP de chaque élément, les flux ainsi que les protocoles utilisés
- **Décrire les éléments de votre schéma en expliquant leur rôle**

Réponse

Schéma d'architecture (Architecture possible pour la suitesans ajout de composant)



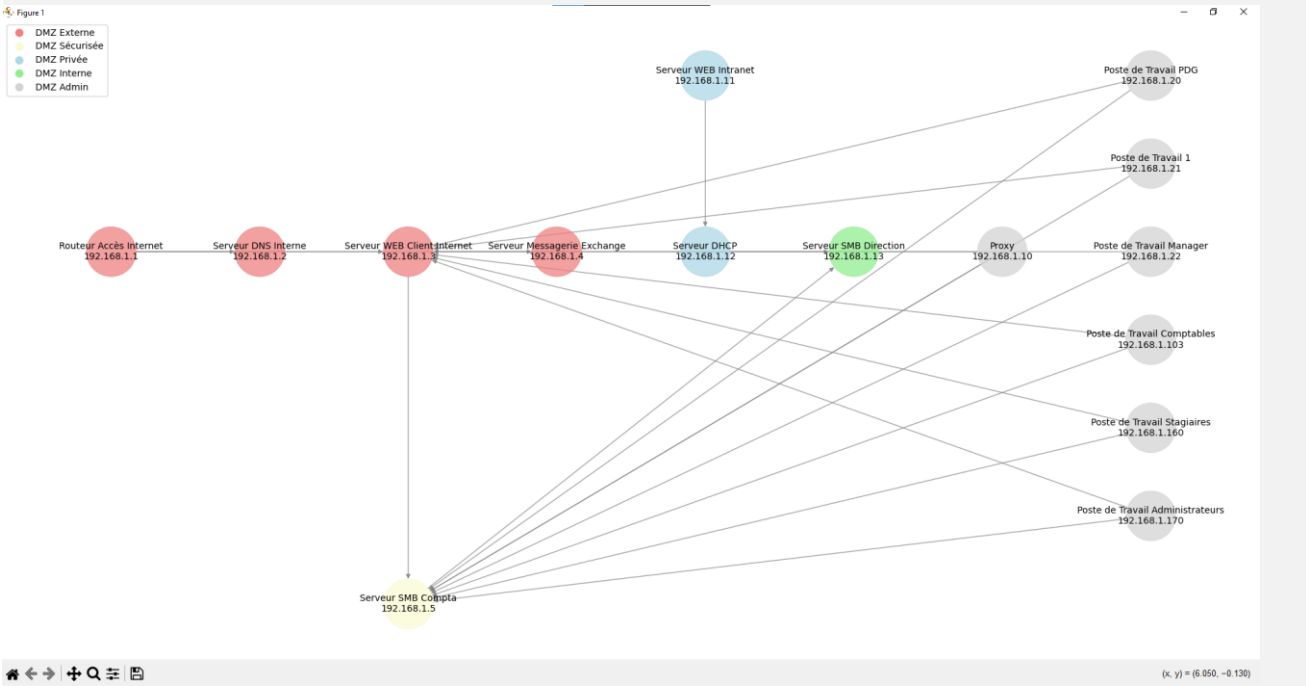


Table d’adressage ip/flux/protocole

Composant	Adresse IP	Système	Protocoles Utilisés
Routeur accès internet	192.168.1.1		
Serveur DNS interne	192.168.1.2	Windows Server 2003	DNS
Serveur WEB Client internet	192.168.1.3	Linux Debian & Apache	HTTP, HTTPS
Serveur Messagerie Exchange	192.168.1.4	Windows Server 2019	SMTP, IMAP, POP3
Serveur de fichiers SMB Compta	192.168.1.5	Windows Server 2000	SMB v1
Proxy	192.168.1.10	Linux Debian	HTTP, HTTPS
Serveur WEB intranet	192.168.1.11	Linux Debian & Apache	HTTP
Serveur DHCP	192.168.1.12	Linux Debian	DHCP
Serveur de fichiers SMB (direction)	192.168.1.13	Windows Server 2019	SMB
Poste de travail PDG	192.168.1.20	Windows 10 Pro	
Poste de travail assistant de direction et RH	192.168.1.21	Windows XP	
Postes de travail Managers et directeurs	192.168.1.22 - 192.168.1.24	Windows 10 Pro	
Postes de travail comptables	192.168.1.103 - 192.168.1.152	Windows 10 Pro	
Postes de travail stagiaires comptables	192.168.1.160 - 192.168.1.161	Windows XP	
Postes de travail administrateurs informatiques	192.168.1.170 - 192.168.1.172	Windows 10 Pro	
Switchs Cisco			

Description des Éléments du schéma

- **Routeur accès internet (192.168.1.1) :**

Rôle : Connecte le réseau interne de Cube-IT à Internet.
Protocole : Interface interne.

- **Serveur DNS interne (192.168.1.2) :**

Rôle : Fournit la résolution de noms DNS pour le réseau interne.
Protocole : DNS.

- **Serveur WEB Client internet (192.168.1.3) :**

Rôle : Héberge les espaces clients, la base de données clients et l'outil de traitement de la comptabilité.
Protocole : HTTP, HTTPS.

- **Serveur Messagerie Exchange (192.168.1.4) :**

Rôle : Fournit les services de messagerie pour l'entreprise.
Protocole : SMTP, IMAP, POP3.

- **Serveur de fichiers SMB Compta (192.168.1.5) :**

Rôle : Stocke les documents clients et les résultats de comptabilité.
Protocole : SMB v1.

- **Proxy (192.168.1.10) :**

Rôle : Intermédiaire pour les requêtes HTTP/HTTPS pour améliorer la sécurité et les performances.
Protocole : HTTP, HTTPS.

- **Serveur WEB intranet (192.168.1.11) :**

Rôle : Héberge les processus internes et les guides de prestations.
Protocole : HTTP.

- **Serveur DHCP (192.168.1.12) :**

Rôle : Attribue des adresses IP dynamiques aux appareils du réseau.
Protocole : DHCP.

- **Serveur de fichiers SMB (direction) (192.168.1.13) :**

Rôle : Stocke des données stratégiques de la direction.
Protocole : SMB.

- **Poste de travail PDG (192.168.1.20) :**

Rôle : Utilisé par le PDG pour les activités quotidiennes.
Protocole : -

- **Poste de travail assistant de direction et RH (192.168.1.21) :**

Rôle : Utilisé par l'assistant de direction et RH pour les tâches administratives.
Protocole : -

- **Postes de travail Managers et directeurs (192.168.1.22 - 192.168.1.24) :**

Rôle : Utilisés par les managers et les directeurs pour leurs activités.
Protocole : -

- **Postes de travail comptables (192.168.1.103 - 192.168.1.152) :**

Rôle : Utilisés par les comptables pour réaliser leurs missions comptables.
Protocole : -

- **Postes de travail stagiaires comptables (192.168.1.160 - 192.168.1.161) :**

Rôle : Utilisés par les stagiaires pour des tâches comptables.
Protocole : -

- **Postes de travail administrateurs informatiques (192.168.1.170 - 192.168.1.172) :**

Rôle : Utilisés par les administrateurs pour gérer et maintenir l'infrastructure informatique.
Protocole : -

- **Switchs Cisco :**

Rôle : Interconnectent les divers appareils du réseau local.
Protocole : -

Travail demandé

2- Évaluation du niveau de sécurité de l'architecture

- Commencer par critiquer l'architecture mise en place en précisant au moins 5 constats problématiques de non-conformité aux bonnes pratiques de sécurité (Préciser vos constats en détail)

Réponse

1. Exposition des Serveurs Critiques à Internet

Constat :
Le serveur Web Client Internet (hébergeant les espaces clients, la base de données client, et l'outil de comptabilité) et le serveur SMB Compta (stockant des documents et résultats de comptabilité) sont exposés directement à Internet.

Problématique :
- Exposition Inutile : Exposer ces serveurs à Internet augmente considérablement le risque d'attaques externes. Les attaquants peuvent tenter des exploitations de vulnérabilités dans le serveur Web ou dans le protocole SMB pour accéder aux données sensibles.
- Absence de Pare-feu : Il semble qu'il n'y ait pas de pare-feu configuré pour protéger ces serveurs contre les accès non autorisés, ce qui est une pratique de sécurité essentielle.

Bonne Pratique :
- Utiliser une DMZ (zone démilitarisée) pour isoler les serveurs accessibles depuis Internet des serveurs internes.
- Configurer un pare-feu pour filtrer le trafic entrant et sortant.

2. Utilisation de Protocole SMB v1

Constat :
Le serveur SMB Compta utilise SMB v1, un protocole obsolète et connu pour ses vulnérabilités (par exemple, WannaCry exploitait SMB v1).

Problématique :
- Vulnérabilités Connues : SMB v1 présente des vulnérabilités critiques qui peuvent être exploitées par des attaquants pour accéder aux données ou infecter le réseau.
- Absence de Support : Le protocole n'est plus supporté par Microsoft, rendant le serveur vulnérable à des attaques que les mises à jour de sécurité ne couvrent pas.

Bonne Pratique :
Mettre à jour vers SMB v2 ou v3 pour bénéficier des améliorations en termes de sécurité et de performance.

3. Accès Non Filtré au Serveur SMB Compta

Constat :
Le serveur SMB Compta est accessible depuis Internet sans authentification ni filtrage.

Problématique :
- Accès Insecure : Les utilisateurs externes peuvent accéder à ce serveur sans aucune restriction, mettant en danger les documents sensibles stockés dessus.
- Manque de Contrôle d'Accès : Aucun contrôle d'accès basé sur les adresses IP ou sur les utilisateurs n'est en place, ce qui est une faille de sécurité importante.

Bonne Pratique :
Restreindre l'accès au serveur SMB Compta en utilisant un VPN ou en configurant un pare-feu pour limiter l'accès uniquement aux adresses IP autorisées.

4. Utilisation de Comptes Administratifs Génériques

Constat :
Les administrateurs partagent un fichier Excel avec les comptes Root/admin de toutes les machines et utilisent ces comptes génériques pour les tâches d'administration.

Problématique :
- Sécurité Compromise : L'utilisation de comptes administratifs génériques augmente le risque de compromission car un seul compte compromis peut mettre en danger l'ensemble du réseau.
- Gestion Inappropriée des Identifiants : Le partage du fichier Excel sur un serveur accessible à tous les administrateurs expose ces identifiants à un risque de vol ou de fuite.

Bonne Pratique :
Utiliser des comptes individuels pour chaque administrateur avec des permissions spécifiques et un système d'audit pour surveiller les accès.
Stocker les identifiants dans un coffre-fort de gestion des mots de passe sécurisé.

5. Manque de Sécurité pour les Requêtes HTTP Malformées

Constat :
L'entreprise reçoit des requêtes HTTP malformées contenant des caractères spéciaux dans l'entête HTTP, causant des bugs sur le site Web. Les administrateurs redémarrent le serveur à chaque fois.

Problématique :
- Absence de Protection Contre les Attaques : Les requêtes malformées peuvent être une tentative d'attaque, et le fait de redémarrer le serveur plutôt que d'implémenter une solution de sécurité est une pratique inadéquate.
- Manque de Surveillance et d'Analyse : L'absence d'outils de surveillance (comme un IDS/IPS) pour analyser ces requêtes et bloquer les tentatives malveillantes expose le serveur à des attaques potentielles.

Bonne Pratique :
Mettre en place un IDS/IPS pour surveiller et filtrer les requêtes HTTP.
Configurer des règles de filtrage sur le serveur Web pour empêcher les requêtes malformées d'affecter le service.

Travail demandé

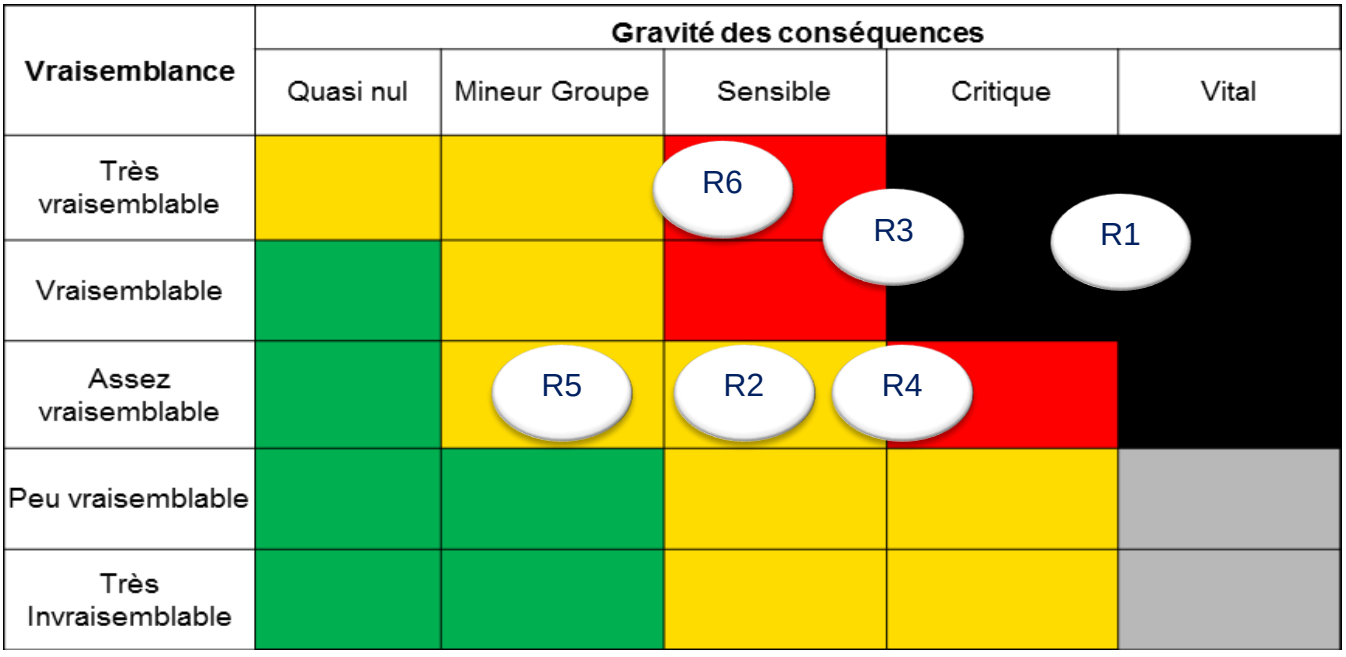
- Réaliser une analyse de risque sur cette architecture en précisant :
  - Intitulé du risque identifié
  - Menace
  - Vulnérabilité
  - L'impact
  - Les critères DIC impactés
  - Probabilité (sur une échelle de 1 à 5)
  - Niveau de risque (sur une échelle de 1 à 5)
  - Action de remédiation

Réponse

Identification des risques sur l'architecture

Num	Risque	Vulnérabilités	Menaces	D	I	C	Impacts potentiels
R1	Exposition directe des serveurs critiques à Internet	Les serveurs sont directement accessibles depuis Internet sans filtrage adéquat.	Attaque externe (par exemple,DDoS, exploitation de vulnérabilités	X		X	Compromission des données sensibles, interruption de service.
R2	Utilisation de SMB v1 pour le serveur de fichiers Compta	Utilisation d'un protocole obsolète avec des failles de sécurité connues.	Exploitation de vulnérabilités SMB v1 (comme le ransomware WannaCry)		X	X	Accès non autorisé aux documents sensibles, propagation de logiciels malveillants.
R3	Accès non filtré au serveur SMB Compta depuis Internet	Absence de filtrage et d'authentification appropriée.	Accès non autorisé et potentiel vol ou altération des données		X	X	Compromission des documents clients et des résultats comptables, perte de données.
R4	Partage de comptes administratifs génériques	Gestion inappropriée des identifiants administratifs, partage de fichiers non sécurisés	Compromission des identifiants administratifs, utilisation abusive des privilèges		X	X	Accès non autorisé aux systèmes, altération ou suppression de données importantes.
R5	Requêtes HTTP malformées causant des bugs	Absence de filtrage et d'analyse des requêtes HTTP.	Attaques de type HTTP flood ou injection, perturbation du service Web	X			Interruption de service, déni de service (DoS), affectation de la disponibilité du serveur.
R6	Utilisation de postes de travail obsolètes	Absence de mises à jour et de support pour les systèmes d'exploitation vieillissants.	Exploitation de vulnérabilités connues dans les systèmes d'exploitation obsolètes.	X	X	X	Compromission du système, propagation de logiciels malveillants, perte de données.

Matrice des risques : positionner les risques sur cette matrice



Plan d'action de remédiation des risques

Num	Risque	Actions de remédiation
R1	Exposition directe des serveurs critiques à Internet	**Action 1.1 : Mise en place d'une DMZ** Description : Configurer une zone démilitarisée (DMZ) pour isoler les serveurs exposés (Serveur WEB Client internet, Serveur de fichiers SMB Compta) du réseau interne de l'entreprise. **Action 1.2 : Configuration des pares-feux** Description : Déployer des pares-feux pour filtrer le trafic entrant et sortant sur les serveurs exposés à Internet. Configurer les règles pour autoriser uniquement les connexions nécessaires.
R2	Utilisation de SMB v1 pour le serveur de fichiers Compta	**Action 2.1 : Mise à jour du protocole SMB** Description : Mettre à jour le serveur de fichiers SMB Compta pour utiliser SMB v2 ou v3 et désactiver SMB v1. **Action 2.2 : Audit de la configuration SMB** Description : Réaliser un audit pour vérifier que tous les systèmes utilisent les versions sécurisées de SMB.
R3	Accès non filtré au serveur SMB Compta depuis Internet	**Action 3.1: Mise en place d'une DMZ** Description : Configurer un VPN sécurisé pour restreindre l'accès au serveur SMB Compta. Seules les connexions VPN authentifiées doivent pouvoir accéder au serveur. **Action 3.2 : Configuration des règles de pare-feu** Description : Configurer les pare-feux pour limiter l'accès au serveur SMB Compta à des plages IP spécifiques ou à des adresses IP autorisées.
R4	Partage de comptes administratifs génériques	**Action 4.1 : Implémentation d'une gestion des identifiants** Description : Mettre en place un système de gestion des identifiants sécurisés avec des comptes individuels pour chaque administrateur. Supprimer les comptes génériques et attribuer des droits spécifiques. **Action 4.2 : Stockage sécurisé des identifiants** Description : Utiliser un coffre-fort sécurisé pour stocker les informations sensibles comme les mots de passe administratifs. Assurer l'accès contrôlé et journalisé.
R5	Requêtes HTTP malformées causant des bugs	**Action 5.1 : Déploiement d'un IDS/IPS** Description : Installer un système de détection et de prévention d'intrusions (IDS/IPS) pour surveiller et filtrer les requêtes HTTP malformées. **Action 5.2 : Configuration des règles de sécurité du serveur Web** Description : Mettre en place des règles de sécurité sur le serveur Web pour valider et filtrer les requêtes HTTP entrantes, bloquant celles qui sont malformées.

R6	**Utilisation de postes de travail obsolètes (Windows XP)**	**Action 6.1 : Mise à jour des postes de travail** Description : Remplacer ou mettre à jour les postes de travail Windows XP vers des versions supportées comme Windows 10. Assurer la compatibilité des applications et des systèmes. **Action 6.2 : Isolation des postes obsolètes** Description : Si la mise à jour n'est pas possible, isoler les postes de travail Windows XP dans un réseau séparé avec des restrictions d'accès sévères.

Partie 2 : Proposition d'une architecture sécurisée

Travail demandé

Partie 2 : Proposition d'une architecture sécurisée

Proposition une architecture réseau plus conforme à l'état de l'art en matière de sécurité

- Préciser la liste des éléments nécessaires à acheter par l'entreprise pour remédier au problème de sécurité, ainsi que les éléments à remplacer ! (**Précision** : Cube-IT ne prévoit pas de migrer vers un cloud, cette technologie est écartée de l'étude)
- Préciser les principes de sécurité d'architecture que vous souhaitez appliquer sur la nouvelle architecture (Filtrage réseau, Filtrage applicatif,...etc.)
- Réaliser un nouveau schéma d'architecture sécurisée ainsi que la matrice des flux correspondante. (en cas de besoin, utiliser ce lien : https://app.diagrams.net/)
- Proposer un plan d'action de sécurisation des éléments contenus dans votre architecture afin de renforcer sa sécurité : Durcissement des OS, configuration des éléments de filtrage,... Cette liste pourrait être appliquée par les administrateurs internes de l'entreprise.

Réponse

1. Liste des Éléments à Acheter et à Remplacer

Éléments à Acheter :

1. Pare-feu (Firewall) de Nouvelle Génération : Pour filtrer le trafic réseau en fonction des politiques de sécurité définies.
2. Système de Détection et de Prévention des Intrusions (IDS/IPS) : Pour surveiller et analyser le trafic réseau et détecter les comportements suspects.
3. Serveur de Gestion des Identités et des Accès (IAM) : Pour gérer les utilisateurs et les accès aux ressources réseau.
4. Système de Gestion des Journaux de Sécurité (SIEM) : Pour collecter, analyser et corréler les journaux de sécurité.
5. Switches et Routeurs avec Fonctionnalités de Sécurité Avancées : Pour segmenter le réseau et appliquer des politiques de sécurité.
6. VPN pour Connexions à Distance Sécurisées : Pour permettre aux employés de se connecter en toute sécurité depuis l'extérieur du réseau de l'entreprise.

7. Antivirus et Antimalware : Pour protéger les terminaux et les serveurs contre les logiciels malveillants.
8. Solutions de Sauvegarde et de Récupération : Pour assurer la continuité des affaires en cas de sinistre.

Éléments à Remplacer :

1. Pare-feu Existants : Remplacer les pares-feux obsolètes par des pares-feux de nouvelle génération avec des capacités avancées de filtrage.
2. Switches et Routeurs Vieillissants : Remplacer les équipements vieillissants qui ne supportent pas les fonctionnalités modernes de sécurité comme VLAN, ACL (Listes de Contrôle d'Accès), etc.

2. Principes de Sécurité d'Architecture

Filtrage Réseau :

- Pare-feu pour contrôler le trafic entrant et sortant en appliquant des règles basées sur des critères tels que les adresses IP, les ports, et les protocoles.
- Segmentations avec VLANs pour isoler les différentes zones du réseau (par exemple, réseau interne, DMZ, réseau de gestion).

Filtrage Applicatif :

- Pare-feu d'Application Web (WAF) pour protéger les applications web contre les attaques telles que les injections SQL, XSS, etc.
- Analyse des applications pour identifier et corriger les vulnérabilités dans les logiciels internes.

Zonage :

- Zone Démilitarisée (DMZ) : Zone isolée pour les serveurs accessibles depuis l'extérieur (ex. serveurs web, serveurs de messagerie) pour limiter l'impact en cas de compromission.
- Réseau Interne : Séparation entre les différents départements ou groupes de travail pour limiter les mouvements latéraux en cas de compromission.

Rupture de la Confiance :

- Principe du Moindre Privilège : Limiter les accès aux ressources réseau uniquement aux utilisateurs et services qui en ont besoin.
- Authentification Multi-Facteurs (MFA) : Pour renforcer l'accès aux systèmes critiques et aux interfaces d'administration.

3. Schéma d'Architecture Sécurisée et matrice des flux

Schéma d'architecture sécurisé

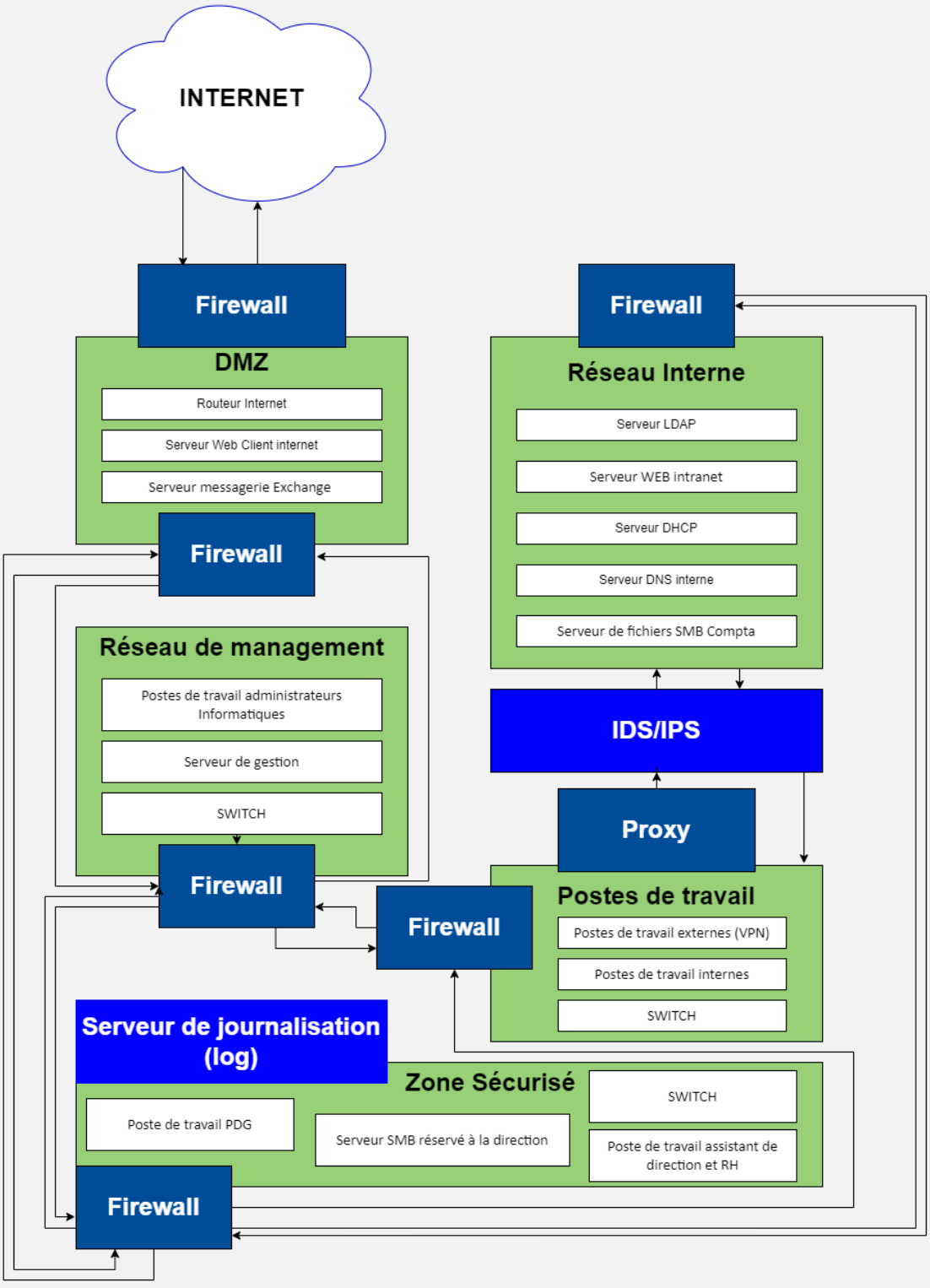
1. **DMZ (Zone Démilitarisée)** :
   - **Routeur Internet** : Point d'entrée depuis l'Internet.
   - **Serveur Web Client** : Héberge les espaces clients et l'outil de comptabilité, accessible via HTTPS.
   - **Serveur Messagerie** : Gère les communications par email, accessible via HTTPS.
2. **Réseau interne** :
   - **Serveur SMB Compta** : Stocke les documents clients, accessible uniquement depuis le réseau interne et via VPN.
   - **Serveur Web Intranet** : Partage les processus internes et les guides de prestations.
   - **Serveur DHCP** : Assigne les adresses IP aux postes de travail.
   - **Serveur LDAP** : Gère l'authentification centralisée.
   - **Serveur DNS interne** : Fournit la résolution de noms pour le réseau interne.
3. **Réseau de management** :
   - **Serveur de gestion** : Gestion sécurisée des comptes administrateurs.

- **Postes de travail administrateurs informatiques** : Utilisés par les administrateurs informatiques

4. **Postes de travail** :
   - **Postes de travail internes** : Utilisés par les comptables, les stagiaires comptables et les Manager et directeurs d'équipe
   - **Postes de travail externes (VPN)** : Utilisés par les comptables externes, accès via VPN.
5. **Postes de travail** :
   - **Postes de travail internes** : Utilisés par le PDG, la direction et le RH.
   - **Serveur SMB direction** : Stocke les données stratégiques, accessible uniquement aux postes autorisés.

Dispositifs de Sécurité

- Firewalls **: Séparent chaque segment de réseau pour contrôler les flux de trafic.**
- IDS/IPS **: Systèmes de Détection et de Prévention d'Intrusion pour surveiller et protéger le réseau.**
- Serveur de journalisation **: Enregistre les logs et événements pour analyse et audit.**



Matrice des flux

	Source	Destination	Protocole/Service	Port d'origine	Port de destination	Description	Action
1	Internet	Routeur Internet	HTTP	Any	80	Accès web depuis l'extérieur	Accept
2	Internet	Routeur Internet	HTTPS	Any	443	Accès web sécurisé depuis l'extérieur	Accept
3	Internet	Routeur Internet	SMTP	Any	25	Envoi d'e-mails	Accept
4	Internet	Routeur Internet	SMTPS	Any	465	Envoi d'e-mails sécurisé	Accept
5	Internet	Routeur Internet	IMAPS	Any	993	Accès aux e-mails sécurisé	Accept
6	Internet	Réseau Interne	Any	Any	Any	Tout accès direct depuis Internet au réseau interne	Deny
7	Internet	Réseau de Management	Any	Any	Any	Tout accès direct depuis Internet au réseau de management	Deny
8	Routeur Internet	Firewall DMZ	Any	Any	Any	Filtrage tout trafic entrant	Accept
9	Firewall DMZ	Serveur Web Client Internet	HTTP	Any	80	Connexion au serveur web client	Accept
10	Firewall DMZ	Serveur Web Client Internet	HTTPS	Any	443	Connexion sécurisée au serveur web client	Accept
11	Firewall DMZ	Serveur Messagerie Exchange	SMTP	Any	25	Connexion au serveur de messagerie	Accept
12	Firewall DMZ	Serveur Messagerie Exchange	SMTPS	Any	465	Connexion sécurisée au serveur de messagerie	Accept

13	Firewall DMZ	Serveur Messagerie Exchange	IMAPS	Any	993	Connexion sécurisée pour accès aux e-mails	Accept	
14	Firewall Réseau Interne	Serveur LDAP	LDAP	Any	389	Authentification centralisée	Accept	
15	Firewall Réseau Interne	Serveur LDAP	LDAPS	Any	636	Authentification sécurisée centralisée	Accept	
16	Firewall Réseau Interne	Serveur Web Intranet	HTTP	Any	80	Connexion au serveur intranet	Accept	
17	Firewall Réseau Interne	Serveur Web Intranet	HTTPS	Any	443	Connexion sécurisée au serveur intranet	Accept	
18	Firewall Réseau Interne	Serveur DHCP	DHCP	Any	67/68	Attribution des adresses IP	Accept	
19	Firewall Réseau Interne	Serveur DNS interne	DNS	Any	53 (TCP/UDP)	Résolution des noms de domaine	Accept	
20	Firewall Réseau Interne	Serveur de fichiers SMB Compta	SMB	Any	445	Connexion au serveur de fichiers	Accept	
21	Firewall Réseau de Management	Postes de travail administrateurs	RDP	Any	3389	Accès à distance pour administration	Accept	
22	Firewall Réseau de Management	Postes de travail administrateurs	SSH	Any	22	Connexion sécurisée pour administration	Accept	
23	Firewall Réseau de Management	Serveur de gestion	RDP	Any	3389	Accès à distance pour gestion	Accept	
24	Firewall Réseau de Management	Serveur de gestion	SSH	Any	22	Connexion sécurisée pour gestion	Accept	
25	Firewall Réseau de Management	Serveur de gestion	HTTP/HTTPS	Any	80/443	Administration web	Accept	
26	Réseau Interne	Réseau de Management	Any	Any	Any	Accès depuis le réseau interne vers le réseau de management	Deny	

27	Firewall	IDS/IPS	Any	Any	Any	Surveillance et détection	Accept	
28	Firewall	Proxy	HTTP Proxy	Any	8080	Proxy HTTP	Accept	
29	Firewall	Proxy	HTTPS Proxy	Any	8443	Proxy HTTPS	Accept	
30	VPN	Postes de Travail Externes	IPSec	Any	500/4500	Connexion VPN sécurisée	Accept	
31	VPN	Postes de Travail Externes	OpenVPN	Any	1194	Connexion VPN sécurisée	Accept	
32	VPN	Postes de Travail Externes	SSL VPN	Any	443	Connexion VPN sécurisée	Accept	
33	Switch	Postes de Travail Internes	Any	Any	Any	Connexions internes	Accept	
34	Firewall	Serveur de Journalisation	Syslog	Any	514 (UDP)	Envoi des logs	Accept	
35	Firewall	Serveur de Journalisation	Syslog sécurisé	Any	6514 (TCP)	Envoi sécurisé des logs	Accept	
36	Firewall	Serveur SMB réservé à la direction	SMB	Any	445	Connexion au serveur de fichiers direction	Accept	
37	Firewall	Poste de travail PDG	RDP	Any	3389	Accès à distance pour PDG	Accept	
38	Firewall	Poste de travail assistant direction et RH	RDP	Any	3389	Accès à distance pour direction	Accept	
39	Firewall	Poste de travail PDG	SSH	Any	22	Connexion sécurisée pour PDG	Accept	
40	Firewall	Poste de travail assistant direction et RH	SSH	Any	22	Connexion sécurisée pour direction	Accept	

41	Postes de travail internes	Internet	Any	Any	Any	Accès direct des postes internes vers Internet	Deny	

4. Plan d'Action pour la Sécurisation

1. Durcissement des OS :
   - Désactiver les services inutilisés.
   - Installer les mises à jour de sécurité régulièrement.
   - Configurer les paramètres de sécurité selon les meilleures pratiques.

2. Configuration des Éléments de Filtrage :
   - Pare-feu : Définir des règles strictes pour autoriser seulement le trafic nécessaire.
   - WAF : Configurer les règles pour filtrer les requêtes web malveillantes.
   - IDS/IPS : Ajuster les règles de détection pour identifier les comportements suspects.

3. Gestion des Accès :
   - Mettre en œuvre des politiques de gestion des identités avec des permissions minimales.
   - Configurer l'authentification multi-facteurs pour les accès critiques.

4. Surveillance et Réponse aux Incidents :
   - Configurer le SIEM pour collecter les journaux et alerter sur les incidents de sécurité.
   - Développer un plan de réponse aux incidents et former le personnel.

5. Sauvegarde et Récupération :
   - Mettre en place des solutions de sauvegarde régulières et tester les procédures de récupération.

Partie 3 : Veille sécurité et supervision

Travail demandé

Partie 3 : Veille sécurité

Veille sécurité : Un élément de l'architecture mise en place par le client a fait l'objet durant la semaine du 02 mars 2021 d'une grande compagne d'attaque basée sur 4 failles zéro Day. En se basant sur les recherches internet :

- Préciser quel est élément concerné par cette attaque ?
- Décrire l'attaque qui a eu lieu brièvement et conseiller à votre client comment y remédier s'il est concerné !

Réponse

1. Élement Concerné par l'Attaque

Élément Concerné : Microsoft Exchange Server

Contexte :
Durant la semaine du 2 mars 2021, une grande campagne d'attaques a ciblé les serveurs Microsoft Exchange. Cette attaque est survenue en raison de l'exploitation de plusieurs failles de sécurité critiques, appelées failles "zero-day", dans Microsoft Exchange Server. Les failles découvertes ont été publiquement connues sous les noms de CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, et CVE-2021-27065.

2. Description de l'Attaque et Recommandations

Description de l'Attaque :

- Type d'Attaque : Les vulnérabilités permettaient l'exécution de commandes à distance (RCE), l'accès non autorisé aux e-mails et aux données des utilisateurs, ainsi que la possibilité de déployer des logiciels malveillants sur les serveurs Exchange.
- Exploitation des Failles : Les attaquants pouvaient exploiter ces vulnérabilités pour accéder aux serveurs Exchange via des requêtes HTTP spéciales, injecter des commandes dans les requêtes HTTP, et installer des portes dérobées pour maintenir un accès persistant.
- Conséquences : Les attaques pouvaient entraîner des fuites de données sensibles, un contrôle total sur les comptes de messagerie des utilisateurs, et potentiellement la compromission de l'ensemble du réseau interne de l'entreprise.

Recommandations pour Remédier à la Situation :

1. Application des Correctifs de Sécurité :
    - Mettre à Jour Microsoft Exchange : Assurez-vous que tous les serveurs Microsoft Exchange sont mis à jour avec les derniers correctifs fournis par Microsoft. Les correctifs pour ces vulnérabilités ont été publiés par Microsoft dans les mises à jour de sécurité de mars 2021.
2. Exécution d'une Analyse de Sécurité :
    - Vérification des Compromissions : Utilisez des outils de sécurité pour analyser les serveurs Exchange à la recherche de signes de compromission. Cherchez des anomalies dans les journaux de sécurité et des fichiers suspects.
    - Nettoyage des Backdoors : Si des logiciels malveillants ou des backdoors ont été installés, procédez à leur suppression et à la réinitialisation des mots de passe des comptes affectés.
3. Renforcement de la Sécurité :
    - Changer les Mots de Passe : Changez les mots de passe de tous les comptes administratifs et utilisateurs des serveurs Exchange.
    - Configurer une Surveillance Active : Déployez des solutions de surveillance et de détection des intrusions pour détecter toute activité suspecte en temps réel.
    - Renforcer les Accès Externes : Réduisez les points d'accès externe au serveur Exchange en utilisant des VPN, des pare-feu, et des contrôles d'accès supplémentaires.
4. Communication et Formation :
    - Informer les Utilisateurs : Avertissez les utilisateurs de l'entreprise des risques potentiels et des signes d'activité suspecte dans leurs comptes de messagerie.
    - Former le Personnel : Assurez-vous que les administrateurs système sont formés pour gérer les vulnérabilités de sécurité et pour répondre aux incidents de sécurité.
5. Plan de Réponse aux Incidents :
    - Établir un Plan de Réponse : Développez et testez un plan de réponse aux incidents pour traiter les incidents futurs efficacement. Assurez-vous que le personnel sait comment réagir en cas de nouvelle attaque.