PROJET ITWAY

Réalisé par Firas JEMAA, Najet BOUKADOUR

SOMMAIRE

Contexte

Contexte et enjeux

L'infrastructure actuelle de ITWay présente certaines limites en termes de performance, de sécurité et d'évolutivité. La nouvelle infrastructure vise à :

- **Améliorer la sécurité:** En mettant en place des mesures de protection rigoureuses pour prévenir les risques cyber et garantir la confidentialité des données.
- **Augmenter la disponibilité:** En assurant une haute disponibilité des services critiques pour minimiser les temps d'arrêt.
- **Optimiser les performances:** En déployant des technologies performantes et en optimisant l'utilisation des ressources.
- **Faciliter la collaboration:** En offrant des outils collaboratifs performants et en simplifiant l'accès aux informations.
- **Réduire les coûts:** En optimisant l'utilisation des ressources et en adoptant des solutions économiques.

Effectifs

- Collaborateurs : 50 utilisateurs.
- Direction administratif : 9 utilisateurs.
- Commerciaux : 6 utilisateurs.
- Production : 30 (dev, système, réseaux).

- IT : 5 utilisateurs (infra. interne, niv.1 & 2, maintenance).

Architecture proposée

L'architecture réseau proposée se compose de trois segments distincts :

- **Réseau SRV:** Destiné à héberger les serveurs critiques de l'entreprise, ce segment sera strictement isolé et sécurisé.
- **Réseau DMZ :** Ce segment accueillera les services accessibles depuis l'extérieur (serveurs web, messagerie) et sera protégé par un pare-feu applicatif.
- **Réseau LAN:** Dédié aux postes de travail des employés, il sera segmenté en VLAN pour améliorer la sécurité et la performance du trafic.

Fonctionnalités clés

La nouvelle infrastructure intègrera les fonctionnalités suivantes :

- **Gestion des identités et des accès:** Un système d'authentification centralisé permettra de contrôler finement les accès aux ressources.
- **Stockage centralisé:** Un système de stockage sécurisé permettra de centraliser les données de l'entreprise et de faciliter la collaboration.
- **Accès à distance sécurisé:** Les employés pourront accéder aux ressources de l'entreprise en toute sécurité depuis l'extérieur.
- **Communication unifiée:** Un système de messagerie performant et sécurisé sera mis en place pour faciliter les échanges.
- **Gestion de l'infrastructure:** Des outils d'automatisation et de supervision permettront de simplifier la gestion et la maintenance de l'infrastructure.

Phases du projet

Le projet sera mené en trois phases distinctes :

1. **Phase d'analyse et de conception:** Étude détaillée des besoins, choix des technologies, élaboration de l'architecture détaillée.
2. **Phase de déploiement:** Mise en œuvre de l'infrastructure, tests et recette.
3. **Phase de maintenance et d'évolution:** Surveillance, maintenance et amélioration continue de l'infrastructure.

Bénéfices pour l'entreprise

La mise en place de cette nouvelle infrastructure apportera de nombreux avantages à ITWay, notamment :

- **Amélioration de la sécurité des données :** Protection renforcée contre les cybermenaces.
- **Augmentation de la productivité des collaborateurs :** Grâce à des outils collaboratifs performants et à une meilleure disponibilité des services.
- **Réduction des coûts d'exploitation:** Optimisation de l'utilisation des ressources et réduction des coûts de maintenance.
- **Amélioration de l'image de marque:** Démonstration d'un engagement en faveur de la sécurité, de l'innovation et de développement durable.

Schéma réseau

Adressage

Réseau	Description	Adresse IP de base	CIDR	Nombre d'IP disponibles (nombre IP total - réseau et broadcast)
SRV	Réseau SRV	172.16.85.0	/27	30
	SRV-ADS	172.16.85.10		
	SRV-RADIUS	172.16.85.11		
	SRV-LOGS	172.16.85.12		
DMZ	Réseau DMZ	172.16.84.0	/28	14
	DMZ-DNS	172.16.84.2		
	DMZ-WEB	172.16.84.3		
	DMZ-MAIL	172.16.84.4		
LAN	Réseau LAN	192.168.84.0	/24	254

Moins il y a de machines, plus la gestion de la sécurité est facile (moins de points d’entrée pour une attaque).

Limiter le serveur DMZ à 14 adresses IP est une **mesure de sécurité** qui vise à :

- Restreindre le nombre de machines autorisées dans la DMZ.

- Réduire la surface d’attaque (moins de machines exposées = moins de vulnérabilités).
- Mieux contrôler l’accès et détecter plus facilement les anomalies.

Analyse cahier des charges

Plan de gestion de projet

Nous avons décidé de mener ce projet entièrement en binôme et de partager ainsi chacune des tâches en fonction de l’avancée afin de pouvoir comprendre si ce n’est maîtriser chacune d’elles. Cette manière de travailler permettra de pouvoir apporter des compétences complémentaires et s’imprégner du projet dans son entièreté, le but étant de pouvoir répondre l’un et l’autre à toutes les questions de notre client.

Cela signifie que pendant que l’un d’entre nous effectue la tâche 1, le second effectue la tâche 2, et ainsi de suite. Mais tout en ayant un regard réciproque sur ce que chacun fait en cas de besoin ou de question de la part de notre binôme.

Plan d'Action

Voici le rétroplanning que nous avons prévu de suivre.

Les outils utilisés

- **Documentation** : Notion
- **Calendrier & planification** : Trello
- **Schéma infrastructure** : Draw.io
- **Réunion de travail à distance** : Google Meet

Diagramme infrastructure

Solution proposées

Sécurité et surveillance

Voir : "Tableau comparatif des solutions".

- Serveur **SIEM** combiné pour la gestion des logs et la détection d'incidents comme :
  - **Splunk** (version gratuite) ou **octopussy** ou **graylog** pour la gestion centralisée des logs.
  - **Wazuh** (EDR+SIEM) en monitoring des fichiers pour détecter les altérations.
  - **suricata** ou **snort** en IDS/IPS pour détecter et bloquer les menaces.
  - **zabbix** ou **prometheus** en network monitor.
- Serveur de certificats (open PKI) : intégré à l'AD pour la gestion des certificats internes

Routeur

Notre proposition : **Stormshield**

- Solution européenne (validée par l'Anssi).
- Plusieurs rôles : **routeur**, **pare-feu, VPN IPSec** et **proxy** (solution plus éco-responsable).

Active directory + RADIUS

- Activer les profils utilisateur itinérants dans AD DS sur les comptes d'utilisateur.
- Pour limiter le stockage des utilisateurs et éviter de saturer le serveur de données, nous utiliserons une **GPO** pour mettre en place des quotas de stockage.
- Pour filtrer sur les extensions afin d'éviter l'ajout de malwares dans un répertoire, nous pouvons utiliser la stratégie de restriction logicielle dans les GPO. Cette stratégie permet de bloquer l'exécution de certains types de fichiers en ajoutant des extensions spécifiques à la liste des fichiers désignés.
- Chiffrement des données : Une Autorité de Certification interne est préférable pour générer des certificats pour tout le monde au sein de l'organisation car elle offre un contrôle total et une meilleure sécurité. L'utilisation d'une AC intermédiaire est souvent recommandée car elle

hérite de la confiance de la racine publique, ce qui permet de minimiser les risques d'exposition de l'AC racine en la laissant éteinte (voir documentation ANSSI).

- Synchronisation des droits pour une authentification unifiée avec RADIUS : configurer le serveur RADIUS pour qu'il utilise Active Directory comme base de données d'identification. Il faut également configurer le rôle Network Policy Server (NPS) sur le serveur Windows pour qu'il agisse en tant que serveur RADIUS et prenne en charge l'authentification RADIUS.
- Gestion des identités et des accès :
  - Centralisation des utilisateurs :
  - Mise en place des politiques de mots de passe robustes (Conforme au recommandation de l'ANSSI) :
    - **Complexité** : minimum 12 caractères, mélange de lettres, chiffres, et symboles.
    - **Expiration régulière** : 90 jours.
  - Configuration des accès en fonction des rôles (principe du moindre privilège).

Accès distant et mobilité

Le VPN IPsec de Stormshield connecté à l'annuaire Active Directory (pour gérer les utilisateurs et les groupes) est une solution de sécurité réseau qui permet de créer des tunnels sécurisés entre deux réseaux ou entre un réseau et un utilisateur nomade.

Il offre des fonctionnalités telles que le chiffrement et l'intégrité des données.

Les journaux de logs pour le VPN IPsec de Stormshield enregistrent les événements, notamment ceux liés à la phase de négociation d'un tunnel VPN IPsec, les erreurs de configuration et les activités d'administration afin de surveiller le fonctionnement du tunnel VPN. De plus, il analyse les problèmes rencontrés ainsi que les connexion utilisateurs.

Accès Web

- **Serveur web** : NGINX en tant que serveur web (open source, performant, grand nombre de connexions simultanées, permet de servir plus de clients

avec moins de ressources), et reverse proxy (si besoin pour répartir efficacement le trafic).

- **Serveur Reverse Proxy :** NGINX qui sert de WAF :
  - Mise en cache du contenu,
  - Protection contre attaques DDoS, XSS, SQL Injection, LFI, etc...,
  - Limitation du trafic malveillant (IP bannies, protection DDoS de base),
  - Vérification des requêtes avant qu'elles n'atteignent le serveur web,
  - Gestion du SSL/TLS pour sécuriser les connexions HTTPS.

Surveillance et Contrôle des Connexions

Pour surveiller les connexions à distance pour garantir la conformité et détecter les activités suspectes :

- Logs et surveillance des connexions :
  - Configurer les logs sur le reverse proxy (Nginx/HAProxy) et le serveur web pour suivre les accès et erreurs.
  - Détecter les connexions suspectes (tentatives répétées, accès depuis des IP inconnues).
  - Générer des alertes en cas d'anomalies.
- Outils de Supervision et Analyse des Logs :
  - ELK Stack (Elasticsearch, Logstash, Kibana) ou Graylog pour collecter et analyser les logs.
  - Grafana + Prometheus pour surveiller les performances et générer des alertes.
- Blocage Automatique des Tentatives Suspectes :
  - Reverse Proxy avec WAF (ex. ModSecurity) pour filtrer les attaques web.
  - Fail2Ban pour bloquer automatiquement les tentatives de connexions malveillantes.
  - Restrictions d'accès (ex. autoriser uniquement certaines IP ou pays).

Services de communication internes et externes

- Messagerie : **Postfix** (messagerie uniquement) ou **Nextcloud** (solution + complète avec des fonctionnalités autres : stockage et partage de fichiers, synchronisation, gestion de contacts et d'agenda, visioconférence, permet également le travail collaboratif et dispose d'une application cliente sur tous les OS).
- Sécurité avec un anti-spam : **SpamAssassin** à paramétrer.
- Site web : Serveur **NGINX** en HTTPS.
- Authentification Multi-Facteurs (MFA) : Pour renforcer la sécurité des accès à distance via une application d'authentification à deux facteurs open source (**Open Authenticator**). C'est essentiel pour limiter les risques d'accès non autorisé.

Gestion de l'Infrastructure

- Automatisation des déploiements : Vagrant pour créer et gérer des environnements de VM, Ansible pour les provisionner automatiquement en configurant et en installant des logiciels et des configurations nécessaires.
- Versionning et documentation : GitHub

Résolution de noms et gestion des certificats

Services de résolution

- Service de résolution de nom interne : DNS de l'AD.
- Service de résolution de nom externe : serveur DNS.
- **Fiabilité et performance :**
  - Surveillance et alertes : outil type Zabbix pour surveiller la santé des serveurs DNS.
  - Optimisation des réponses : Activer EDNS (Extended DNS) qui permet d'envoyer et recevoir des paquets DNS plus grands que la limite standard.

    - Caches DNS : Implémenter un serveur DNS cache (comme Unbound ou Dnsmasq) pour réduire les temps de réponse en interne.
- Sécurité :
    - Filtrage ACL : règles pour limiter l’accès au serveur DNS (Autoriser uniquement les machines internes pour les résolutions internes / Bloquer les requêtes provenant d’adresses IP non autorisées).
    - Protection contre les attaques DoS/DDoS : Implémentation d’un outil type Fail2Ban ou règles pare-feu pour détecter et bloquer les attaques DNS.
    - Logs et audit : journalisation des requêtes DNS pour analyser les activités et détecter les anomalies.
    - Intégrité : Signature cryptographique avec le protocole DNSSEC pour éviter les altérations, falsifications et contre le spoofing.

Gestion des certificats

Essentielle pour sécuriser les services HTTPS, VPN, etc..

Déployer une infrastructure PKI interne pour gérer les certificats SSL/TLS (Voir la solution OpenSSL) : il faudra configurer les modèles de certificats (serveur web, client, email, etc.).

1. **Sécurisation des communications** :

L'objectif est de chiffrer les communications entre les utilisateurs et les services pour garantir la confidentialité et l'intégrité des données.

Services à sécuriser :

- Serveur web (HTTP → HTTPS).
- Messagerie (IMAP/SMTP avec TLS).
- VPN (chiffrement des connexions).
- Nginx : Ajouter les fichiers de certificat dans le fichier de configuration.

2. **L’Autorité de certification** doit être interne pour générer des certificats pour tout le monde (autorité intermédiaire préférable car c’est le certificat racine qui est de confiance, l’autorité racine est éteinte pour éviter les risques).

- **Outil type** : OpenSSL
- **interface graphique pour gérer une Autorité de certification** : ADCS pour Windows AD, ou XCA.

Système de sauvegarde

La sauvegarde doit être immuable afin de pouvoir éviter son chiffrement : Par exemple un outil du type **Bacula** en open source permet de se prémunir contre une modification ou une suppression ou un chiffrement des données pour une période de temps prédéfinie. Elle permet de définir des politiques de rétention et de sécuriser les sauvegardes contre les modifications non autorisées.

Exigences de performance et de disponibilité

voir 3.2 (page 6)

- **Disponibilité des services** :
    - Identifier avec le client les services critiques à surveiller en priorité.
    - Mettre en place un monitoring proactif avec Zabbix ou Prometheus pour suivre l’état des services et du réseau, avec alertes en cas d’anomalie.
    - Assurer des sauvegardes automatiques et régulières des configurations et appliances.
    - Clustering GNS3 sur plusieurs serveurs pour limiter les interruptions et configuration de protocoles de redondance (IP virtuelle) pour les routes critiques.
    - Prévoir un second contrôleur de domaine (AD) pour garantir la redondance.
    - Documenter toutes les configurations et procédures (sauvegarde, déploiement) pour une réactivité optimale en cas d’incident.

- Optimisation du serveur web avec Nginx, capable de gérer un grand nombre de connexions simultanées avec une faible consommation de ressources.

- **Performances :**
  - Maximiser l'usage de Linux pour minimiser la consommation de ressources.
  - Implémenter des règles QoS sur routeurs et switches pour prioriser le trafic critique.
  - Réduire l'impact des processus inutiles (ex. éviter les interfaces graphiques sur les serveurs).
  - Mettre en place du Load Balancing via Nginx pour répartir les requêtes entre plusieurs serveurs (ex. en cas de forte affluence sur le serveur web).
  - Effectuer des tests de latence pour identifier les éventuels goulets d'étranglement.
- **Évolutivité :**
  - Utiliser Ansible pour automatiser et accélérer les déploiements.
  - Adapter l'infrastructure selon les besoins en allouant dynamiquement les ressources (ex. ajustement des quotas de stockage par utilisateur dans l'AD pour éviter les abus).
  - Exploiter le mode serveur distribué de GNS3 pour ajouter des nœuds facilement.
  - Nettoyer régulièrement l'AD en supprimant les profils et comptes obsolètes pour optimiser les performances.
- **Redondance et Tolérance aux Pannes :**
  - Prévoir des chemins de communication alternatifs pour assurer la continuité de service en cas de panne réseau.
  - Effectuer des snapshots réguliers des machines pour permettre un retour rapide en cas de dysfonctionnement.
  - Tester la résilience de l'infrastructure en simulant des pannes (ex. désactivation d'un routeur ou d'un lien critique).

    - Configurer un système de sauvegarde automatique pour les données critiques avec des solutions comme rsync ou BorgBackup.
    - Mettre en place une infrastructure redondante pour minimiser les interruptions, tout en optimisant l'utilisation de l'espace disponible.

Conformité et éthique

- Conformité règlementaire : RGPD, classement des données sensibles et ACL pour restreindre accès aux données sensibles, minimiser la collecte de données au strict autorisé, contrôler la charte informatique, utilisation de protocoles sécurisés pour les communications, réduire les risques de fuite avec des mesures de sécurité (vlan, règles de pare feu), stockage des journaux (voir la durée).
- Respect de la vie privée : confidentialité et intégrité des données utilisateurs et entreprise. Respect des données sensibles et personnelles.
- Approche écoresponsable : optimisation des ressources en installant un maximum de services Linux et le moins de Windows possible entre autres (solutions + légères), conteneurisation, en isolant les applications dans des conteneurs légers permettant de réduire significativement l'empreinte des applications et d'optimiser l'utilisation des ressources, implémentation d'un outil de monitoring pour surveiller la santé des services, réduire le nombre de VM s'il est possible de mutualiser des services, songer éventuellement à arrêter certains services en dehors des heures de bureau si possible, et allouer dynamiquement les ressources pour éviter la surconsommation.