Cahier des Charges Technique

Infrastructure Système et Réseau Sécurisée

Entreprise ITWay SAS

18 mars 2025

Table des matières

1 Introduction

1.1 Contexte

L'entreprise ITWay souhaite mettre en place une infrastructure système et réseau sécurisée pour répondre à ses besoins opérationnels actuels et futurs. Cette infrastructure est destinée à remplacer l'infrastructure actuelle qui n'est pas optimisée et ne respecte pas l'état de l'art en termes d'efficacité, d'accessibilité et de sécurité en environnement professionnel.

2 Architecture de l'infrastructure

2.1 Schéma général

L'infrastructure système et réseau de la société ITWay est composée de plusieurs éléments interconnectés. Voici un schéma général de l'architecture de l'infrastructure :

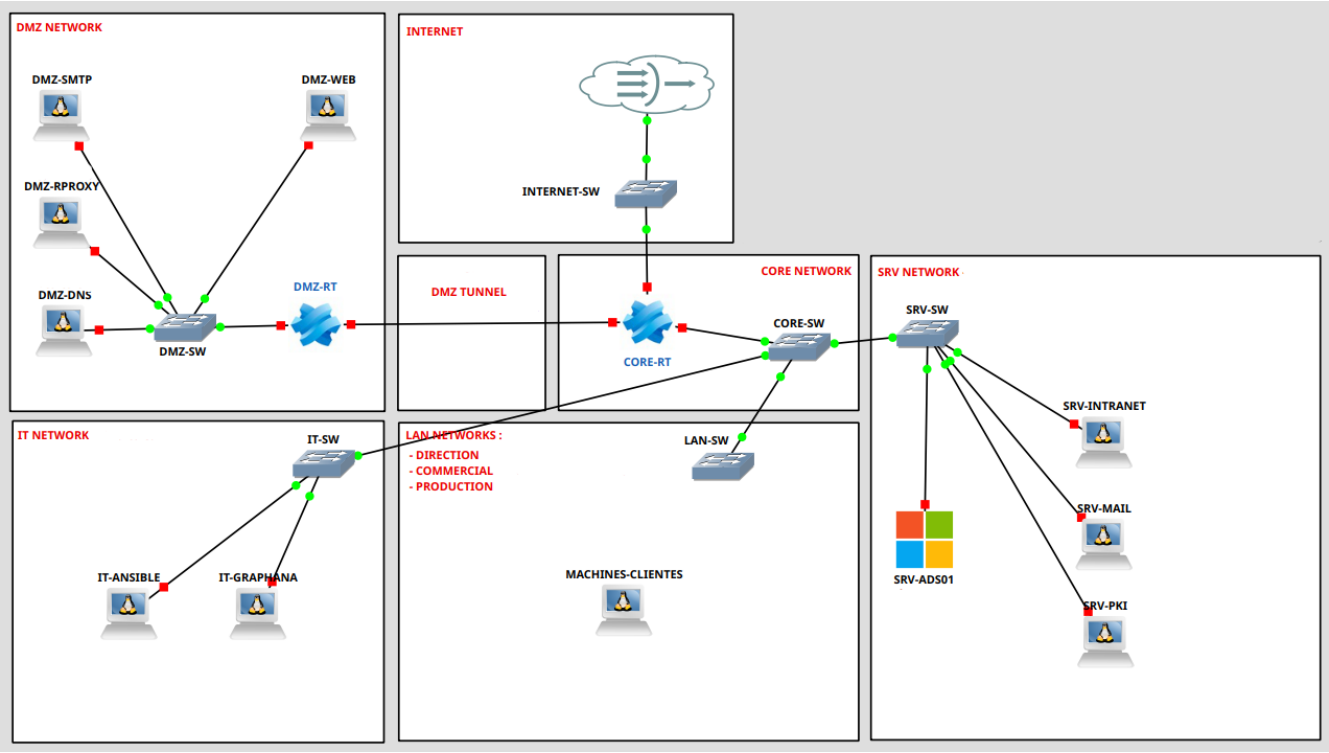

FIGURE 1 – Schéma général de l'infrastructure

Cette infrastructure est constituée d'un seul site principal, segmenté en plusieurs sous-réseaux, charge à vous de déterminer la politique d'accès entre ces sous-réseaux en fonction de la criticité des services et des données.

Le choix des plans d'adressage et des numéros de VLAN est laissé libre. Il est cependant nécessaire de respecter les noms de réseaux et le nom des machines indiqués sur le schéma.

2.2 CORE-NETWORK

Le cœur du réseau est d'un routeur principal Stormshield (CORE-RT) qui assure la connexion entre les différents sous-réseaux. Il est connecté à un switch principal (CORE-SW) qui assure la distribution des connexions aux différents sous-réseaux.

2.2.1 CORE-RT

Nom d'hôte	Domaine	OS
CORE-RT	core-rt.itway.local	Stormshield EVA

Le routeur **CORE-RT** est en charge de la segmentation des réseaux internes et de la fourniture de la connexion Internet. Il servira les réseaux suivants :

- **SRV-NET** - Réseaux contenant les serveurs internes
- **LAN-NET-DIR** - Réseau des utilisateurs du service commercial
- **LAN-NET-COM** - Réseau des utilisateurs du service communication
- **LAN-NET-PROD** - Réseau des utilisateurs du service production
- **IT-NET** - Réseau des administrateurs du service informatique
- **DMZ-TUNNEL** : Réseau menant vers le routeur de la DMZ

Un service **VPN SSL** sera mis en place pour permettre aux utilisateurs de se connecter à distance au réseau de l'entreprise. Il sera accessible à l'adresse **vpn.itway.fr** et donnera accès aux seuls serveurs et réseaux nécessaires à l'activité des utilisateurs.

D'autres spécifications sont à prendre en configuration pour la configuration du routeur :

- L'accès à l'interface WEB se fera en HTTPS exclusivement.
- L'interface WEB et SSH seront accessibles uniquement depuis le réseau IT-NET.
- L'authentification sur l'interface WEB pourra se faire avec un compte local et avec les comptes AD membres du groupe GRP-SECU-IT.
- Les certificats VPN et WEB seront signés par l'autorité de certification interne.
- La politique globale de sécurité sera configurée pour bloquer tout trafic entrant non sollicité. Le protocole ICMP sera autorisé en tout sens. Et vous mettrez en place une politique de filtrage cohérente pour les services internes.
- La politique de NAT sera configurée pour permettre la translation d'adresses pour les services internes.
- Les services DHCP seront configurés pour les services internes.

2.2.2 SWITCHS

Chacun des commutateurs de l'infrastructure fonctionneront sous Cisco et seront paramétrés en mode L2. Les switchs seront manageable par SSH à partir du réseau IT-NET uniquement.

2.3 SRV-NETWORK

2.3.1 SRV-INTRANET

Nom d'hôte	Domaine	OS
SRV-INTRANET	intranet.itway.local	Debian

Le serveur **SRV-INTRANET** est un serveur web interne qui héberge le site intranet de l'entreprise qui sera développé par vos soins. Il est accessible depuis l'ensemble des réseaux internes de confiance.

Vous utiliserez au choix NGINX ou APACHE2 pour servir le site intranet. Vous mettrez en place un certificat SSL signé par l'autorité de certification interne pour sécuriser les échanges avec le serveur.

Le site web intranet sera développé avec la technologie de votre choix et devra proposer un système de publication des actualités de l'entreprise avec authentification LDAP. Le tout développé en respectant les bonnes pratiques en termes de sécurité.

Les actualités seront visibles sur la page d'accueil du site et seront classées par date de publication.

2.3.2 SRV-MAIL

Nom d'hôte	Domaine	OS
SRV-MAIL	srv-mail.itway.local	Debian

Le serveur **SRV-MAIL** est un serveur de type MDA - Mail Delivery Agent et IMAP/POP qui assure la réception et la distribution des courriers électroniques des utilisateurs de l'entreprise. Il est accessible depuis l'ensemble des réseaux internes de confiance et le serveur DMZ-SMTP pourra contacter ce serveur pour y distribuer les mails.

Son rôle est de stocker les mails des utilisateurs et de les distribuer aux clients de messagerie des utilisateurs.

Il disposera des services suivants :

- Postfix - en mode MDA
- Dovecot - serveur IMAP/POP
- MySQL/MariaDB pour le stockage des utilisateurs
- PostfixAdmin pour la gestion des domaines et des utilisateurs

DMZ-SMTP lui fera office de relais SMTP, passerelle d'entrée/sortie du courrier et relaiera donc le courrier à SRV-MAIL.

2.3.3 SRV-PKI

Nom d'hôte	Domaine	OS
SRV-PKI	srv-pki.itway.local	Debian

Le serveur **SRV-PKI** est un serveur de gestion de clés publiques et privées qui assure la gestion des certificats de l'entreprise. Il est accessible depuis le réseau IT pour l'administration du serveur et la génération des certificats, et accessible uniquement pour consulter la liste de révocation des certificats depuis les autres réseaux internes.

2.3.4 SRV-ADS01

Nom d'hôte	Domaine	OS
SRV-ADS01	srv-ads01.itway.local	Windows Server 2022

Le serveur **SRV-ADS01** est un contrôleur de domaine Active Directory qui assure l'authentification des utilisateurs et des machines de l'entreprise. Il est accessible depuis l'ensemble des réseaux internes de confiance.

L'architecture du serveur Active Directory est laissé à votre discrétion, mais il devra être capable de gérer les utilisateurs, les groupes, les machines et les stratégies de groupe de l'entreprise, le tout structuré de manière cohérente.

Les groupes de sécurité suivants devront être créés :

- GRP-SECU-IT : Groupe des administrateurs du service informatique
- GRP-SECU-COM : Groupe des administrateurs du service communication
- GRP-SECU-DIR : Groupe des administrateurs du service commercial
- GRP-SECU-PROD : Groupe des administrateurs du service production

D'autres groupes de sécurité seront à créer en fonction des besoins de l'entreprise.

En complément, il faudra effectuer les paramétrages suivants :

- Configuration des profils itinérants pour les utilisateurs dans un dossier dédié.
- Chaque profil disposera d'un lecteur X : personnel et monté automatiquement.
- Chaque dossier personnel disposera d'un quota de 100 Mo de stockage.
- Bloquer toute tentative d'enregistrement de fichiers exécutables sur les lecteurs réseaux.
- Créer un message d'accueil pour les utilisateurs lors de leur connexion : "Les accès à ce poste de travail sont réservés aux utilisateurs autorisés. Toute tentative d'accès non autorisée sera sanctionnée."
- Configurer les stratégies d'audit des connexions/déconnexions.
- Configurer les stratégies d'audit des modifications des politiques.
- Régler les mécanismes de chiffrement du protocole RDP à un niveau élevé.
- Désactiver le compte invité sur l'ensemble des postes.
- Implémenter les communications IPSec avec authentification Kerberos.
- Les pare-feu Windows seront configurés pour n'autoriser que WINRM, RDP, Remote Assistance, Network Discovery et tout autre service nécessaire.
- Chaque machine interne devra disposer d'une entrée DNS statique sur le serveur DNS interne.
- Les zones DNS inverses devront être configurées pour les réseaux internes.

2.4 IT-NETWORK

2.4.1 IT-ANSIBLE

Nom d'hôte	Domaine	OS
IT-ANSIBLE	it-ansible.itway.local	Debian

Le serveur **IT-ANSIBLE** est un serveur de gestion de configuration qui assure le déploiement et la configuration (dans la mesure du possible) de l'ensemble des équipements de l'entreprise. Il est accessible depuis le réseau IT pour l'administration du serveur et la gestion des playbooks, et accessible depuis les autres réseaux internes pour le déploiement des configurations.

2.4.2 IT-GRAPHANA

Nom d'hôte	Domaine	OS
IT-GRAPHANA	it-graphana.itway.local	Debian

Le serveur **IT-GRAPHANA** est un serveur de monitoring qui assure la supervision de l'ensemble des équipements de l'entreprise. Il est accessible pour son interface WEB depuis le réseau IT uniquement. Il est configuré pour superviser l'ensemble des équipements de l'entreprise.

2.4.3 IT-MGMT

Nom d'hôte	Domaine	OS
IT-MGMT	it-mgmt.itway.local	Windows 11 Pro Evaluation

Le poste **IT-MGMT** est un poste de travail pour l'administration de l'infrastructure IT-WAY. Il est accessible depuis le réseau IT uniquement et est configuré pour permettre l'administration des équipements de l'entreprise. Il disposera de tout les outils nécessaires à l'administration de l'infrastructure.

2.5 DMZ-NETWORK

2.5.1 DMZ-SMTP

Nom d'hôte	Domaine	OS
DMZ-SMTP	mail.itway.fr	Debian

Le serveur **DMZ-SMTP** est un serveur de messagerie qui assure la réception et la distribution des courriers électroniques de l'entreprise. Il est accessible depuis l'ensemble des réseaux internes de confiance et depuis Internet. Il est configuré pour recevoir les mails de l'extérieur et les distribuer aux serveurs internes.

Il disposera des services suivants :

- Postfix - en mode Relais SMTP
- SpamAssassin pour le filtrage des spams
- Roundcube pour la consultation des mails (accessible via ReverseProxy)

Le webmail Roundcube sera installé sur le serveur pour permettre aux utilisateurs de consulter leurs mails depuis l'intérieur et l'extérieur.

Flux de communication

Mail entrant

- **SMTP** : Internet → Postfix (DMZ) → Postfix (Interne) → Dovecot (stockage et accès)

Mail sortant

- **SMTP** : Postfix (Interne) → Postfix (DMZ) → Internet

Accès utilisateurs

- **IMAP/POP3 - Interne uniquement** : Clients Mail (Thunderbird, Outlook, Mobile, Webmail) → Dovecot (Serveur Interne)
- **SMTP Auth - Interne uniquement** : Clients Mail → Postfix (Interne) → Postfix (DMZ) → Internet
- **Webmail - Externe/Interne** : Clients Web → Roundcube (DMZ) → Postfix (Interne) → Dovecot (Serveur Interne)

2.5.2 DMZ-RPROXY

Nom d'hôte	Domaine	OS
DMZ-RPROXY	itway.fr/webmail.itway.fr	Debian

Le serveur **DMZ-RPROXY** est un serveur Reverse Proxy qui assure la sécurisation de l'accès aux services de l'entreprise. Il est accessible depuis Internet et depuis l'ensemble des réseaux internes de confiance.

Il doit permettre l'accès à itway.fr et webmail.itway.fr depuis Internet et rediriger les requêtes vers les serveurs internes correspondants.

2.5.3 DMZ-WEB

Nom d'hôte	Domaine	OS
DMZ-WEB	itway.fr/dmz-web.int.itway.fr	Debian

Le serveur **DMZ-WEB** est un serveur web qui assure la publication du site principal de l'entreprise. Il est accessible depuis Internet et depuis l'ensemble des réseaux internes de confiance.

Vous installerez sur ce serveur un site web vitrine de l'entreprise en utilisant Wordpress. Vous utiliserez au choix NGINX ou APACHE2 pour servir le site web.

2.5.4 DMZ-DNS

Nom d'hôte	Domaine	OS
DMZ-DNS	dns.itway.fr	Debian

Le serveur **DMZ-DNS** est un serveur DNS qui assure la résolution des noms de domaines de la zone itway.fr. Il est accessible depuis Internet et depuis l'ensemble des réseaux internes de confiance.

Vous utiliserez BIND pour la configuration du serveur DNS et vous configurerez les enregistrements nécessaires pour la résolution des noms de domaines de l'entreprise.

Il servira les domaines suivants :

- itway.fr
- dmz-web.int.itway.fr
- dmz-rt.int.itway.fr
- webmail.itway.fr
- mail.itway.fr

int.itway.fr se devra d'être une zone distincte de itway.fr et ne sera pas accessible depuis Internet. Seul la zone itway.fr sera accessible depuis Internet.

Aucune communication ne doit être possible entre le DNS de la DMZ et le DNS interne.

2.5.5 DMZ-RT

Nom d'hôte	Domaine	OS
DMZ-DNS	dmz-rt.int.itway.fr	Stormshield EVA

Le routeur **DMZ-RT** est un routeur qui isole la DMZ du reste de l'infrastructure, pour mener à Internet il devra passer par le routeur CORE-RT. Il sera manageable depuis le réseau IT uniquement.

3 Pour rappel - Phase 2 : Conception, Développement, Déploiement et Maintenance

3.1 Objectifs

Voici les objectifs à atteindre sur la phase 2 du projet, certains objectifs ne sont pas expliqués dans ce document, ils sont à déduire des informations fournies dans le cahier des charges.

- **Développement des Services** :
  - Concevoir et implémenter les services requis, en respectant les bonnes pratiques de conception et de développement.
- **Sécurité Intégrée** :
  - Appliquer les principes de sécurité dès la phase de conception (par exemple, compartimentage des réseaux, gestion des droits d'accès).
- **Tests et Recettes** :
  - Élaborer des plans de tests couvrant les aspects fonctionnels et non fonctionnels.
  - Réaliser des tests unitaires, d'intégration et des tests de sécurité (par exemple, tests de vulnérabilité).
  - Si des vulnérabilités sont découvertes, les corriger et les retester. Documenter l'ensemble des vulnérabilités et des corrections apportées.
- **Déploiement en Production** :
  - Mettre en place l'environnement de production en respectant les procédures établies.
  - Documenter le processus de déploiement pour faciliter les futures opérations.
- **Maintenance** :
  - Établir des procédures pour la maintenance corrective et évolutive.
  - Prévoir des mécanismes de sauvegarde et de restauration.

3.1.1 Livrables

Les livrables suivants devront êtres fournis à la fin de la phase 2 du projet :

- **Documentation Technique** :
  - Spécifications détaillées, manuels d'installation, guides d'utilisation.
- **Codes Sources et Configurations** :
  - Fournir tous les scripts, configurations et codes nécessaires à la reproduction de l'infrastructure.
- **Plans de Tests et Rapports** :
  - Documentation des tests effectués, des résultats et des actions correctives.
- **Procédures de Maintenance** :
  - Guides détaillés pour la maintenance quotidienne et les mises à jour.

3.1.2 Évaluation

Dans cette phase, différents aspects vont être évalués pour mesurer la qualité du travail fourni. Voici les critères d'évaluation qui seront pris en compte :

- **Travail en Équipe** :
  - Coordination efficace, respect des rôles et responsabilités, bonne répartition des tâches, investissement personnel.
- **Contribution Individuelle** :

  - Qualité du travail fourni, capacité à résoudre les problèmes rencontrés.
- **Qualité des Livrables** :
  - Fonctionnalité des services, conformité aux spécifications, qualité du code, qualité rédactionnelle.
- **Présentation Orale** :
  - Capacité à expliquer les choix techniques, les problématiques rencontrées, les corrections apportées, à démontrer le fonctionnement des services.