DOSSIER DE MISSION PROFESSIONNELLE – ÉPREUVE E5

Refonte et sécurisation de l'infrastructure réseau

Mise en place d'une approche Zero Trust adaptée aux besoins de l'entreprise

Candidat : Nils HAMITOUCHE

Formation : BTS SIO – Option SISR

Session : 2025 – 2027

Année de réalisation : 2026

Entreprise d'accueil : Intersport France – Siège de Longjumeau

Lieu : Longjumeau

TABLE DES MATIÈRES

PARTIE 1 – PRÉSENTATION DU CONTEXTE PROFESSIONNEL

1. Présentation de l'entreprise

Intersport France est un acteur majeur de la distribution d'articles de sport sur le territoire national. L'entreprise s'appuie sur un vaste réseau de magasins et sur une organisation structurée autour d'un siège social situé à Longjumeau. Ce siège centralise les fonctions stratégiques : direction générale, services financiers, ressources humaines, logistique, service offre et marketing et direction des systèmes d'information.

La direction des systèmes d'information constitue un pilier essentiel de l'activité. Il permet la gestion des stocks, le suivi des ventes, l'administration des ressources humaines, la supervision des flux logistiques ainsi que la communication interne et externe.

2. Organisation du service infrastucture

Le service est organisé en plusieurs pôles : support utilisateurs/gestionnaire de parcs, techniciens exploitation, infrastructure et réseaux, cybersécurité et gestion de projets. L'équipe infrastructure assure l'administration des serveurs, du réseau, de la virtualisation et des solutions de sauvegarde.

Dans ce contexte, la sécurisation du réseau est un enjeu stratégique. Une interruption ou une compromission du système pourrait avoir des impacts financiers, organisationnels et juridiques importants.

3. Situation initiale et constats

L'infrastructure réseau existante reposait sur un modèle traditionnel où le réseau interne était considéré comme fiable par défaut. Les équipements principaux étaient vieillissants et la segmentation des flux restait limitée.

Plusieurs limites ont été identifiées : visibilité partielle sur les flux internes, règles de filtrage insuffisamment granulaires, absence d'authentification renforcée pour certains accès sensibles et manque de centralisation des journaux d'événements.

PARTIE 2 – ANALYSE DES BESOINS ET OBJECTIFS DU PROJET

1. Objectifs principaux

L'objectif principal du projet était de moderniser l'infrastructure réseau afin d'améliorer la sécurité, la performance et la résilience du système d'information.

Il s'agissait également d'anticiper l'évolution des usages : télétravail, mobilité des collaborateurs, augmentation des équipements connectés et recours croissant aux services Cloud.

2. Contraintes identifiées

Le projet devait respecter plusieurs contraintes : continuité d'activité, budget défini, migration progressive sans interruption significative des services, et accompagnement des utilisateurs.

3. Analyse des risques

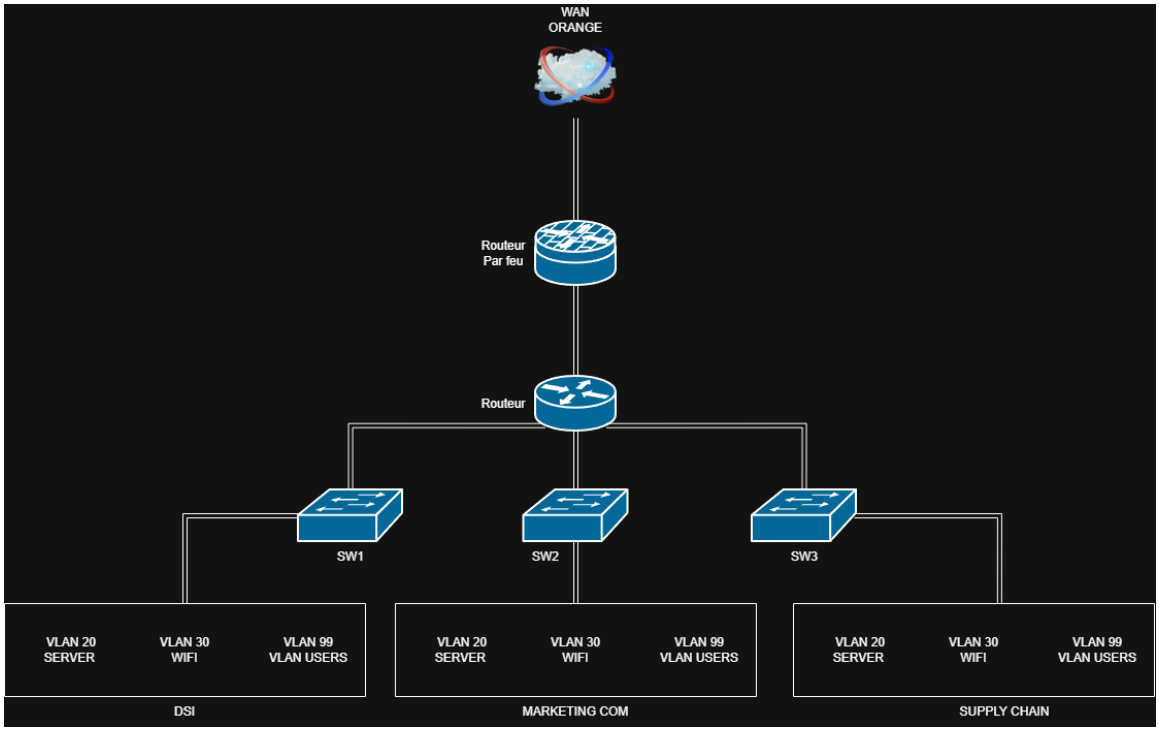
Une analyse des risques a permis d'identifier les menaces potentielles : attaque par ransomware, vol de données sensibles, compromission d'un compte utilisateur ou exploitation d'un équipement mal sécurisé. Une cyberattaque dû à une attaque par phishing arrivé en février 2026 est aussi une des causes pour laquelle Intersport a déciéder de moderniser son infrascture et lancé une campagne de sensibilation à la cybersécurité

Ces risques ont justifié la mise en place d'une architecture plus segmentée et d'un contrôle d'accès renforcé.

PARTIE 3 – SOLUTION PROPOSÉE ET ARCHITECTURE CIBLE

1. Principe général de la nouvelle architecture

La nouvelle architecture repose sur une organisation en couches : une sécurité renforcée en frontière réseau, un cœur de réseau performant et une segmentation logique des différents services.



Le schéma a été simplifié

2. Segmentation du réseau

Le réseau a été segmenté en plusieurs VLAN afin d'isoler les différents types d'équipements : serveurs, utilisateurs, téléphonie, IoT et administration.

Cette segmentation permet de limiter les communications aux seuls flux nécessaires et de réduire les risques de propagation en cas d'incident.

Segmentation :

- VLAN 20 est utilisé par les serveurs et n'utilise pas le service DHCP
- VLAN 30 est utilisé pour les bornes Wi-Fi du site
- VLAN 99 est utilisé par les utilisateurs de l'entrerprise en guise d'accès sans fil pour pouvoir travailler partout sans avoir besoin d'un câble cuivre type RJ45

3. Mise en place d'une approche Zero Trust

L'approche **Zero Trust** repose sur le principe fondamental suivant : ne jamais accorder de confiance implicite, y compris au sein du réseau interne de l'entreprise. Contrairement aux modèles traditionnels où le réseau local est considéré comme sécurisé par défaut, le modèle Zero Trust considère que toute tentative d'accès doit être vérifiée, quel que soit son point d'origine.

Ainsi, chaque accès à une ressource (serveur, application, base de données ou service interne) est systématiquement soumis à un processus d'authentification, de vérification et d'autorisation. Ces contrôles sont adaptés au profil de l'utilisateur, à son rôle dans l'entreprise et au niveau de sensibilité de la ressource demandée. Cette logique permet d'appliquer le principe du **moindre privilège**, c'est-à-dire d'accorder uniquement les droits strictement nécessaires à l'exercice des missions professionnelles.

Dans ce cadre, l'authentification multifacteur (MFA) a été déployée pour les comptes sensibles ainsi que pour les accès distants. Ce mécanisme renforce significativement la sécurité en ajoutant un second facteur de validation (application d'authentification, code temporaire, validation mobile, etc.) en complément du mot de passe. Cela permet de réduire fortement les risques liés au vol ou à la compromission d'identifiants.

Actuellement, Intersport s'appuie sur des **groupes de sécurité** afin de contrôler l'accès aux ressources et aux données. Cette gestion des droits par appartenance à un groupe permet de structurer les autorisations selon les services, les fonctions et les responsabilités des collaborateurs. Cette organisation facilite l'administration des accès tout en garantissant une cohérence globale des permissions attribuées.

L'outil central utilisé pour cette gestion est le service d'annuaire LDAP de Microsoft, nommé **Active Directory**. Il permet d'administrer les comptes utilisateurs, les postes de travail, les serveurs, les groupes de sécurité et les stratégies de configuration. Active Directory joue un rôle clé dans la gestion des identités et constitue le socle de l'authentification au sein du système d'information.

L'intégration d'Active Directory dans une logique Zero Trust représente une première étape structurante dans le projet global de sécurisation. En s'appuyant sur une gestion centralisée des identités et des groupes, il devient possible de renforcer progressivement les contrôles d'accès, d'améliorer la traçabilité des connexions et de faire évoluer l'infrastructure vers un modèle plus résilient et mieux adapté aux menaces actuelles.

Cette démarche s'inscrit dans une stratégie d'amélioration continue de la sécurité, visant à protéger durablement les données et les ressources critiques de l'entreprise.

PARTIE 4 – DÉPLOIEMENT ET ACCOMPAGNEMENT

1. Phase de préparation

Une phase de préparation a été conduite afin d'assurer une migration sécurisée et maîtrisée. Elle a débuté par un inventaire précis des équipements réseau et serveurs, permettant d'identifier les éléments à conserver, à remplacer ou à reconfigurer.

Une analyse des flux existants a ensuite été réalisée afin de comprendre les communications essentielles entre les différents services et d'anticiper les impacts de la future segmentation.

Par ailleurs, les règles de sécurité ont été définies selon le principe du moindre privilège, afin de structurer les futurs contrôles d'accès.

Enfin, un planning de migration progressif a été établi, intégrant des phases de test et un plan de retour arrière, garantissant ainsi la continuité d'activité.

2. Migration progressive

La migration a été réalisée de manière progressive, étape par étape, afin de limiter les risques et de gérer efficacement les éventuelles difficultés liées aux changements d'infrastructure.

Chaque phase faisait l'objet de tests de validation avant mise en production, et un plan de retour arrière était systématiquement prévu en cas d'anomalie. Cette approche a permis d'assurer la continuité des services tout en maîtrisant les impacts techniques et organisationnels.

3. Communication et accompagnement

Une communication interne a été mise en place afin d'informer les collaborateurs des évolutions de l'infrastructure et des impacts sur leurs usages quotidiens. Cette démarche visait à anticiper les interrogations et à favoriser l'adhésion au projet.

Un accompagnement spécifique a été prévu pour la mise en œuvre de l'authentification multifacteur (MFA) ainsi que pour l'adoption des nouvelles procédures d'accès. Des explications claires et un support dédié ont permis de faciliter la transition et de limiter les résistances au changement.

PARTIE 5 – RÉSULTATS ET BILAN PROFESSIONNEL

1. Résultats obtenus

La nouvelle infrastructure permet une meilleure visibilité sur les flux réseau grâce à une segmentation claire et à un contrôle plus précis des communications internes. Cette amélioration renforce la capacité de supervision et facilite la détection d'éventuelles anomalies.

Par ailleurs, la segmentation mise en place réduit significativement la surface d'attaque en limitant les interactions entre les différents segments du réseau. En cas d'incident, les risques de propagation interne sont maîtrisés, ce qui améliore la protection des ressources et des données sensibles.

2. Apports personnels et compétences développées

Cette mission m'a permis de développer des compétences solides en analyse d'infrastructure, en conception d'architecture réseau et en sécurisation des accès au sein d'un environnement professionnel structuré. Elle m'a également donné l'opportunité de comprendre les enjeux concrets liés à la modernisation et à la protection d'un système d'information.

Par ailleurs, j'ai renforcé mes capacités d'organisation, de planification et de gestion des priorités. Le travail en équipe avec les différents intervenants du service informatique m'a permis d'améliorer ma communication professionnelle et ma capacité à collaborer efficacement dans un contexte réel.

3. Perspectives d'évolution

Des évolutions futures pourraient inclure la mise en place d'une solution de supervision avancée afin d'améliorer la détection des incidents, ainsi qu'un renforcement progressif des politiques de sécurité dans une logique d'amélioration continue. Le déploiement du modèle Zero Trust pourrait également être étendu aux autres sites de l'entreprise afin d'harmoniser le niveau de protection à l'échelle nationale.

Toutefois, l'approche Zero Trust, en restreignant fortement les accès par défaut, ne doit pas se limiter à une logique purement technique. Un dispositif de sécurité trop restrictif, s'il n'est pas accompagné d'explications adaptées, peut générer de l'incompréhension ou des contournements involontaires. Il est donc essentiel d'intégrer une dimension pédagogique au projet, en sensibilisant les collaborateurs aux enjeux de la cybersécurité, aux bonnes pratiques et aux raisons des nouvelles restrictions mises en place.

Cette démarche permet non seulement de renforcer l'efficacité du dispositif de sécurité, mais aussi de responsabiliser les utilisateurs, qui deviennent ainsi de véritables acteurs de la protection du système d'information.

CONCLUSION GÉNÉRALE

La refonte de l'infrastructure réseau constitue une étape stratégique pour sécuriser et moderniser le système d'information. L'adoption d'une architecture segmentée et d'une approche Zero Trust permet d'améliorer la protection des données tout en accompagnant l'évolution des usages professionnels.

Ce projet s'inscrit pleinement dans les compétences attendues d'un technicien supérieur SISR : analyser une situation, proposer une solution adaptée, la déployer et en assurer le suivi.