BTS SIO – Épreuve E6 – Option SISR – Session 2025
FICHE RESSOURCE
Mise en place d'un cluster de pare-feu Stormshield – Port de Cherbourg

1. Informations générales

Candidat	Enzo FAUDON
Réalisation n°	1
Date	16 / 12 / 2025
Modalité	Épreuve ponctuelle + Contrôle en cours de formation
Organisation support	Port de Cherbourg – Contact : M. Gérard, administrateur réseau
Lieu de réalisation	Lycée Saint-Exupéry, Saint-Raphaël
Période	05/09/2025 → 26/05/2026
Modalité de travail	Seul(e)
Productions accessibles	https://efportfoliobtssio.fr/ap4-realisations-professionnelles/

2. Compétences travaillées

- Concevoir une solution d'infrastructure réseau
- Installer, tester et déployer une solution d'infrastructure réseau
- Exploiter, dépanner et superviser une solution d'infrastructure réseau

3. Contexte et problématique

M. Gérard, administrateur réseau du port de Cherbourg, a réalisé un audit de sécurité qui a mis en évidence des failles critiques sur l'infrastructure réseau. Le réseau repose sur un seul pare-feu gérant l'ensemble du trafic, avec des règles trop permissives représentant un point de défaillance unique (SPOF).

3.1 Comparatif avant / après

AVANT (existant)	APRES (solution)
✗ Pare-feu unique (SPOF)	✓ Cluster actif/passif (haute disponibilité)
✗ Règles trop permissives	✓ Politique de filtrage restrictive par VLAN
✗ Pas de segmentation réseau	✓ Séparation clients / employés / internes
✗ Aucune tolérance de panne	✓ Bascule automatique en cas de défaillance

4. Déroulé technique de la réalisation

N°	Etape	Description
1	**Analyse de l'existant**	Lecture du schéma réseau et du cahier des charges. Identification des points critiques : SPOF, règles laxistes, absence de segmentation VLAN.
2	**Conception de la solution**	Architecture cluster Stormshield actif/passif avec lien de synchronisation dédié. Séparation logique des flux (clients / employés / internes / Internet).
3	**Mise en oeuvre technique**	Installation des 2 pare-feux (entrée/sortie). Configuration du lien de synchronisation, association des interfaces, synchronisation automatique des règles.
4	**Politique de filtrage**	Blocage des accès non autorisés, restriction par VLAN, autorisation des seuls protocoles nécessaires, règles dédiées à l'administration réseau.
5	**Tests et validation**	Simulation de panne d'un pare-feu, vérification de la bascule automatique, contrôle du maintien des règles de filtrage après basculement.

5. Ressources utilisées

5.1 Ressources matérielles

- Deux pare-feux Stormshield (entrée et sortie du réseau)
- Infrastructure réseau simulée avec des machines virtuelles dans chaque réseau

5.2 Ressources logicielles et documentaires

- Documentation complète sur les règles de filtrage (NAT, filtrage de base, filtrage de contenu, haute disponibilité)
- Documentation de base mise à jour en fonction des changements réseau réalisés
- Cahier des charges fourni par le client

6. Conditions de réalisation

6.1 Ressources fournies

- Cahier des charges précisant les attentes du client et les contraintes techniques
- Schéma de l'infrastructure réseau globale du port et des connexions entre les points d'accès
- Outils de sécurité déjà mis en place pour adapter la solution existante
- Budget alloué à la réalisation du projet

6.2 Résultats attendus

- Mise en place d'un cluster de pare-feu interconnecté assurant la haute disponibilité et la tolérance de panne
- Déploiement de règles de filtrage adaptées aux différentes zones du port
- Rédaction de documents techniques relatifs aux pare-feux et aux règles de filtrage