BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation : 1

Nom, prénom : Enzo FAUDON **N° candidat :**

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒ **Date : 16 / 12 / 2025**

Organisation support de la réalisation professionnelle

M. GÉRARD, administrateur réseau du port de Cherbourg, a réalisé un audit de sécurité concernant l'infrastructure réseau. Cet audit a permis de mettre en évidence des failles de sécurité majeures pouvant nuire au bon fonctionnement du réseau. Suite à ce constat, il fait appel à nos services afin de proposer et mettre en œuvre des solutions adaptées. Des failles critiques, telles que des règles de filtrage trop permissives sur l'unique pare-feu gérant le trafic, doivent être corrigées dans les plus brefs délais afin d'assurer la sécurité de l'ensemble du réseau.

Intitulé de la réalisation professionnelle

Mise en place d'un cluster de pare-feu et d'une nouvelle politique de filtrage renforcée pour le réseau

Période de réalisation : 05/09/2025-26/05/2026 **Lieu :** Lycée Saint-Exupéry, Saint-Raphaël

Modalité : ☐ **Seul(e)** ☒ **En équipe**

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

Conditions de réalisation (ressources fournies, résultats attendus)

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

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 afin d'améliorer la sécurité
- Rédaction de documents techniques relatifs aux pare-feux et aux règles de filtrage

Description des ressources documentaires, matérielles et logicielles utilisées

Ressources matérielles :
- Deux pare-feux Stormshield en sortie et entrée du réseau
- Infrastructure réseau simulée avec des machines virtuelles présentent dans chaque réseaux

Ressources logicielles/documentaires :
- Documentation complète sur les règles de filtrage globales (NAT, filtrage de base, filtrage de contenu, haute disponibilité…) ainsi que leurs explications détaillées correspondant aux différents services du port
- Documentation de base améliorée dans le cas où des changements sur le réseau ont été faits
- Cahier des charges

Modalités d'accès aux productions et à leur documentation

https://efportfoliobtssio.fr/ap4-realisations-professionnelles/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (verso)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte et objectifs de la réalisation

Dans le cadre de cette réalisation professionnelle, M.GÉRARD demande d'intervenir sur l'infrastructure réseau du port de Cherbourg à la suite d'un audit de sécurité réalisé par l'équipe d'administration réseau. Cet audit a mis en évidence plusieurs failles de sécurité critiques, notamment l'utilisation de règles de filtrage trop permissives sur un pare-feu unique, représentant un point de défaillance majeur pour l'ensemble du réseau.

L'objectif principal de cette réalisation est donc de renforcer la sécurité du réseau tout en assurant la continuité de service. Pour répondre à ces besoins, la solution retenue consiste à mettre en place un cluster de pare-feu Stormshield en mode actif/passif, permettant à la fois la haute disponibilité, la tolérance de panne et une répartition de la charge, ainsi que définir une nouvelle politique de filtrage plus restrictive et adaptée aux différents réseaux et VLANs du port.

Analyse de l'existant

Avant toute mise en œuvre, une analyse de l'infrastructure existante est réalisée à partir du schéma réseau et du cahier des charges fournis.
Le réseau repose sur un seul pare-feu en sortie, assurant l'ensemble des fonctions de filtrage et de protection. Cette architecture présente plusieurs limites :
- Absence de haute disponibilité en cas de panne matérielle ou logicielle
- Règles de filtrage trop générales, autorisant des flux non nécessaires
- Manque de segmentation claire entre les différents réseaux (clients, employés, services internes)

Cette analyse permet d'identifier les points critiques à corriger et de définir les exigences techniques de la nouvelle solution.

Conception de la solution

La solution conçue repose sur la mise en place d'un cluster de pare-feu Stormshield en mode actif/passif, interconnectés par un lien dédié permettant la synchronisation des états et des règles. Ce mode de fonctionnement permet aux deux pare-feux de traiter simultanément le trafic réseau tout en garantissant la continuité de service en cas de défaillance de l'un des équipements.

La politique de sécurité est repensée en tenant compte de l'ensemble des réseaux et VLANs présents sur l'infrastructure, avec une séparation logique des flux selon leur usage (réseaux clients, réseaux employés, ressources internes et accès Internet).

Mise en œuvre technique - Installation et configuration du cluster

Deux pare-feux Stormshield vont être installés en entrée et sortie du réseau.
La configuration du cluster actif/passif est réalisée en définissant :
- Le lien de synchronisation entre les deux pare-feux
- Les interfaces réseau associées aux différents flux
- La synchronisation automatique des règles de filtrage et des configurations

Une fois le cluster opérationnel, les pare-feux fonctionnent ensemble et assurent une protection continue du réseau, en entrée comme en sortie.

Mise en place des règles de filtrage

Une nouvelle politique de filtrage est définie afin de limiter les flux au strict nécessaire.
Les règles sont organisées par réseaux et VLANs afin d'améliorer la lisibilité et la sécurité globale.

Parmi les règles à mettre en place :
- Blocage de l'accès à certains sites distants non autorisés depuis les réseaux clients
- Restriction de l'accès aux ressources internes en fonction des VLANs (clients / employés)
- Autorisation uniquement des protocoles et services nécessaires au bon fonctionnement des activités du port
- Mise en place de règles spécifiques pour l'administration réseau

Cette approche permet de réduire significativement la surface d'attaque et d'améliorer le contrôle des flux réseau.

Tests et validation

Une phase de tests va être réalisée afin de valider le bon fonctionnement de la solution.
Les tests effectués prendraient en compte notamment :
- La coupure volontaire d'un des deux pare-feu afin de vérifier la continuité de service
- La vérification du maintien des communications réseau durant la bascule
- Le contrôle du bon fonctionnement des règles de filtrage après la défaillance simulée

Les résultats restent encore à déterminer mais doivent pouvoir conclure que le cluster assure correctement la haute disponibilité et que les règles de filtrage restent pleinement fonctionnelles en cas de panne.

Résultats obtenus et bénéfices pour le client

À l'issue de cette réalisation, le réseau du port de Cherbourg disposera alors :
- D'un cluster de pare-feu actif/passif opérationnel, garantissant la haute disponibilité et la tolérance de panne
- D'une politique de filtrage renforcée, adaptée aux différents réseaux et VLANs
- D'une infrastructure plus sécurisée et plus résiliente face aux incidents matériels ou aux menaces réseau

La solution mise en place permettra donc de renforcer grandement la sécurité dans l'entièreté du réseau du port de Cherbourg, réduisant ainsi les tentatives d'attaques et par conséquent, permet également de renforcer la protection et l'intégrité des diverses données stockées.