BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

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 : MALAUSSENA Maxence **N° candidat :**

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒ **Date : 10 / 04 / 2026**

Organisation support de la réalisation professionnelle

Suite à un audit de l'infrastructure informatique du port de Cherbourg, John, l'administrateur réseau, a identifié un point de défaillance unique (SPOF) critique au niveau du pare-feu : un seul équipement assure l'intégralité du filtrage et du routage entre le LAN, la DMZ et le WAN. Toute panne ou redémarrage de cet équipement entraîne une interruption totale des services en ligne (réservations, informations trafic, gestion des escales), accessibles 24h/24 par les clients et partenaires. L'absence de segmentation réseau correcte entre les zones accroît par ailleurs l'exposition aux risques en cas de compromission d'un service. John confie donc la mission de déployer un cluster de pare-feux pfSense en haute disponibilité, avec cloisonnement renforcé des flux réseau. Une fois cette première mission réalisée, une seconde mission portant sur la mise en cluster des serveurs web sera envisagée.

Intitulé de la réalisation professionnelle

Déploiement d'un cluster de pare-feux pfSense en haute disponibilité pour le port de Cherbourg

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 détaillant les exigences de haute disponibilité, de sécurité et de segmentation réseau
- Schéma de l'infrastructure réseau globale du port de Cherbourg (LAN, DMZ, WAN, interconnexions)
- Plan d'adressage IP et définition des VLAN utilisés (LAN, DMZ, synchronisation HA)
- Budget alloué à la mise en place du cluster de pare-feux

Résultats attendus :

- Mise en place d'un cluster de pare-feux pfSense garantissant la continuité du filtrage et du routage en cas de panne d'un pare-feu
- Maintien de l'accessibilité des services réseau et de la DMZ en cas de défaillance d'un équipement
- Renforcement de la sécurité par une segmentation stricte des flux via des règles de filtrage par VLAN
- Rédaction de documents techniques détaillant l'architecture mise en place, la configuration du cluster et les procédures de bascule

Description des ressources documentaires, matérielles et logicielles utilisées

Ressources matérielles :

- 2 machines physiques/VM dédiées aux pare-feux pfSense (cluster haute disponibilité)
- Infrastructure virtualisée reproduisant les zones LAN, DMZ, WAN pour tests et validation
- Commutateurs administrables gérant les VLAN et la segmentation des flux entre les zones

Ressources logicielles :

- pfSense CE : haute disponibilité (CARP, pfsync, XMLRPC), filtrage des flux, gestion du NAT
- Documentation officielle pfSense, cahier des charges, documentation technique interne

Modalités d'accès aux productions et à leur documentation

https://mm-bsio.fr/?page_id=1211

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, le port de Cherbourg a sollicité une intervention à la suite d'un audit de sécurité ayant mis en évidence deux points de défaillance uniques critiques au sein de son infrastructure : le pare-feu unique et le serveur web unique. L'absence de redondance sur ces équipements expose l'établissement à un risque d'interruption totale des services en ligne (réservations, informations trafic, gestion des escales), accessibles 24h/24 par les clients, compagnies maritimes et agents portuaires.

L'objectif principal est de garantir la continuité des services réseau et applicatifs en supprimant ces points de défaillance. La solution retenue prévoit :

- un cluster de pare-feux pfSense permettant la tolérance aux pannes au niveau du filtrage et du routage réseau,
- une segmentation renforcée des flux via des règles de filtrage strictes par VLAN (LAN employés, LAN clients, DMZ),
- en perspective, le déploiement d'un cluster de serveurs web avec répartition de charge afin d'éliminer le dernier SPOF identifié lors de l'audit.

Analyse de l'existant

Avant toute mise en œuvre, une analyse de l'infrastructure existante a été réalisée à partir du schéma réseau et du rapport d'audit. L'infrastructure actuelle présente plusieurs limites :

- Un pare-feu unique assurant l'intégralité du filtrage et du routage entre le LAN, la DMZ et le WAN, sans aucune redondance : toute panne ou redémarrage entraîne une coupure totale des services, sans mécanisme de bascule automatique.
- L'absence de segmentation réseau correcte entre les zones LAN, DMZ et Internet permet à un attaquant ayant compromis un service web d'accéder directement au réseau interne. Les règles de filtrage trop permissives laissent passer des flux non nécessaires.
- Un serveur web unique, sans mécanisme de bascule ni répartition de charge, identifié comme SPOF supplémentaire lors de l'audit, dont le traitement est prévu dans une phase ultérieure.

Conception de la solution

La solution adoptée repose sur :

- La mise en place d'un cluster de deux pare-feux pfSense synchronisés via CARP (adresses IP virtuelles partagées), pfsync (synchronisation des états de connexion) et XMLRPC (réplication des règles de filtrage), formant un équipement logique capable de maintenir le réseau opérationnel en cas de panne de l'un des membres du cluster.
- Le déploiement d'une segmentation stricte par VLAN (LAN employés, LAN clients, DMZ, synchronisation HA) avec des règles de filtrage adaptées, réduisant significativement la surface d'attaque.
- La mention, comme perspective d'évolution, de la mise en cluster des serveurs web avec HAProxy afin de compléter l'élimination des SPOF identifiés lors de l'audit.

Mise en œuvre technique – Installation et configuration

- Cluster de pare-feux pfSense

-Acquisition et installation de deux pare-feux pfSense sur machines dédiées.

- Configuration du protocole CARP : adresses IP virtuelles partagées sur chaque interface (LAN, DMZ, WAN) permettant un basculement automatique en moins de 2 s.
- Configuration de pfsync : synchronisation temps réel des tables d'états TCP/UDP entre le MASTER et le BACKUP via un VLAN dédié, garantissant la transparence du basculement pour les sessions actives.
- Configuration de XMLRPC : réplication automatique des règles de filtrage et NAT du MASTER vers le BACKUP, éliminant tout risque de divergence de configuration.
- Définition des règles de filtrage strictes par VLAN : LAN employés, LAN clients, DMZ, synchronisation HA.

Tests et validation

Des tests ont été réalisés pour vérifier le fonctionnement de la solution :

- Simulation de panne du pare-feu MASTER pour vérifier le basculement automatique vers le BACKUP sans interruption des sessions actives (RTO inférieur à 2 s).
- Vérification de la synchronisation des règles de filtrage et NAT après basculement, sans régression de sécurité constatée.
- Contrôle de la cohérence des états de connexion après bascule et du bon fonctionnement de l'ensemble des services réseau.
- Vérification du retour en production du pare-feu MASTER et de la reprise correcte de son rôle dans le cluster.

Ces tests ont permis de confirmer que le cluster pfSense garantit la tolérance aux pannes et la continuité de service attendues.

Résultats obtenus et bénéfices pour le client

À l'issue de la réalisation, le port de Cherbourg dispose :

- d'un cluster de pare-feux pfSense opérationnel, éliminant le point de défaillance unique au niveau du filtrage et du routage réseau,
- d'un basculement automatique MASTER vers BACKUP transparent pour les sessions actives (RTO inférieur à 2 s),
- d'une politique de filtrage renforcée par VLAN, réduisant significativement la surface d'attaque et cloisonnant correctement les zones LAN, DMZ et WAN, - -
d'une infrastructure documentée (schémas, procédures de bascule) accessible sur mm-bsio.fr,
- d'une base solide pour la prochaine étape identifiée lors de l'audit : la mise en cluster des serveurs web avec HAProxy.

Perspective d'évolution

Suite à la validation de cette première mission, John envisage de confier une seconde réalisation portant sur la mise en cluster des serveurs web : déploiement de deux serveurs Debian en DMZ hébergeant Apache, et mise en place de HAProxy en frontal avec algorithme round-robin, health checks actifs et détection automatique des pannes. Cette évolution viendra compléter l'architecture haute disponibilité en éliminant le dernier SPOF identifié lors de l'audit, au niveau de la couche applicative.