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 :

Nom, prénom : NICOLAU Noah **N° candidat :**

Épreuve ponctuelle **Contrôle en cours de formation** **Date :** 16 / 12 /25

Organisation support de la réalisation professionnelle

Le port de Cherbourg gère un flux constant de passagers et de marchandises. L'infrastructure supporte 150 collaborateurs et des bornes wifi publiques pour les clients. Le besoin principal est de garantir une disponibilité 24h/24 des services de réservation et de sécuriser les données face à l'augmentation des cybermenaces maritimes.

Intitulé de la réalisation professionnelle

Mise en œuvre d'une architecture réseau hautement disponible et sécurisation périmétrique automatisée.

Période de réalisation : 05/09/25 – 22/05/26 **Lieu :** Saint Raphaël

Modalité : X Seul(e) **En équipe**

Compétences travaillées

X Concevoir une solution d'infrastructure réseau

X Installer, tester et déployer une solution d'infrastructure réseau

X Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation (ressources fournies, résultats attendus)

Ressources fournies :

- Cahier des charges (Port de Cherbourg) : Document définissant les besoins de continuité de service et les exigences de sécurité pour le trafic portuaire.
- Infrastructure de virtualisation : Accès à un serveur physique hébergeant un hyperviseur pour le déploiement des machines virtuelles.
- Accès internet dédié : Pour le téléchargement des packages (pfSense, Ansible) et la consultation des documentations techniques.

Résultat attendu :

- Cluster Haute Disponibilité : Mise en place de deux pare-feux pfSense redondés et d'un cluster de serveurs Web pour éliminer les SPOF.
- Sécurisation active/passive : Déploiement d'un IDS/IPS et d'un SIEM pour détecter et centraliser les tentatives d'intrusion.
- Automatisation & Déploiement : Utilisation d'Ansible pour la configuration de sécurité et d'un serveur FOG pour le déploiement rapide des OS clients.

Description des ressources documentaires, matérielles et logicielles utilisées

Ressources Documentaires :

- Documentation Netgate (pfSense) : Référentiel technique utilisé pour la configuration du protocole HA.
- Documentation Ansible Galaxy : Pour l'installation de Ansible et la recherche de rôles communautaires.
- Documentation FOG Project : Guide d'installation pour la gestion du déploiement PXE et le partitionnement des images systèmes.

Matériel spécifique utilisé :

- Serveur physique : Hôte de virtualisationalloué pour supporter l'ensemble des services.
- Switch Cisco: Équipement permettant la segmentation du réseau en VLAN

Production finale

- pfSense (Cluster HA) : Solution de pare-feu redondée assurant la sécurité périmétrique et la répartition de charge via HAProxy.
- Serveur FOG : Solution de clonage et déploiement réseau permettant une restauration rapide des postes de travail après incident.
- Ansible : Moteur d'automatisation utilisé pour le déploiement cohérent des services et la mise en conformité des serveurs de sécurité.
- SIEM & IDS/IPS : Couple d'outils permettant une vision total des menaces
- Cluster Web & BDD : Architecture redondante garantissant la disponibilité des services de réservation du port, même en cas de panne serveur

Modalités d'accès aux productions et à leur documentation

https://noah-nicolau.fr/

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

Plan proposée :

Le Port de Cherbourg gérait jusqu'alors ses services (site web de réservation, base de données) sur des serveurs isolés, sans aucune redondance. Cette architecture présentait de nombreux **SPOF.** La panne d'un seul équipement entraînait l'arrêt total des services portuaires. De plus, l'augmentation du trafic maritime et des cyberattaques ciblées rendait l'infrastructure actuelle vulnérable et instable lors des pics de connexion.

Solution envisagée :

- Haute disponibilité : Cluster de pare-feux (pfSense) et répartition de charge (HAProxy).
- Déploiement : Mise en place d'un serveur FOG (Open Source) ou d'une solution propriétaire WDS/MDT.
- Sécurité : Déploiement d'un IDS/IPS couplé à un SIEM pour la visibilité des logs, avec une automatisation via Ansible.

Solution Retenue :

Les solutions retenues visent à maximiser la résilience tout en maîtrisant les coûts :

- Serveur FOG & Active Directory : Choisi pour sa flexibilité et sa rapidité de déploiement via le réseau (PXE), permettant de restaurer un poste de travail en quelques minutes.
- Cluster pfSense : L'utilisation du protocole CARP permet une bascule transparente entre deux pare-feux en cas de panne matérielle.
- IDS/IPS & SIEM (Wazuh/ELK) via Ansible : Cette solution permet de centraliser les alertes de sécurité sur un tableau de bord unique, tout en garantissant une configuration homogène sur tout le parc grâce aux playbooks Ansible.

La réalisation :

La mise en œuvre a été découpée en trois phases techniques majeures :

1. Industrialisation du déploiement : Installation du serveur FOG et liaison avec l'Active Directory existant pour l'intégration automatique des machines au domaine après clonage.
2. Sécurisation et Supervision : Déploiement automatisé des agents de détection (IDS) sur les serveurs critiques et configuration du SIEM pour la corrélation des logs en temps réel.
3. Continuité de service : Configuration du cluster pfSense (synchronisation XMLRPC) et mise en place de HAProxy pour distribuer le trafic sur un pool de serveurs Web redondés.

Conclusion :

Cette modernisation transforme une infrastructure fragile en une solution résiliente et évolutive. L'entreprise dispose désormais d'une visibilité totale sur sa sécurité. En cas d'incident sur un poste ou un serveur, les procédures de déploiement automatisées et la haute disponibilité permettent une reprise d'activité quasi instantanée, minimisant les pertes d'exploitation pour le Port de Cherbourg.