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 : Metreau Nicolas	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....

Organisation support de la réalisation professionnelle

Le port de Cherbourg dispose d'un système d'information utilisé par plusieurs services (administration, surveillance et Wi-Fi public). L'infrastructure réseau existante repose sur des équipements virtualisés et des services centralisés. Le directeur des systèmes d'information souhaite renforcer la sécurité du réseau, assurer la continuité de service des équipements critiques et mettre en place une haute disponibilité des services.
Il est également nécessaire de proposer un accès distant sécurisé pour les administrateurs et les utilisateurs nomades, tout en améliorant la gestion centralisée des accès.

Intitulé de la réalisation professionnelle

Mise en place d'une infrastructure réseau sécurisée et hautement disponible intégrant un cluster pfSense, un Active Directory redondant et un accès distant sécurisé via OpenVPN

Période de réalisation : ..... **Lieu :** .....

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, - Schéma réseau existant, - Environnement de virtualisation, - Serveurs et postes clients

Résultats attendus :

- Haute disponibilité du pare-feu, - Redondance des services Active Directory, - Accès distant sécurisé, - Tests de continuité de service, - Documentation technique

Description des ressources documentaires, matérielles et logicielles utilisées

Matérielles :

- Serveurs virtualisés, - Postes clients

Logicielles :

- pfSense, - Windows Server (Active Directory, DNS), - Linux (OpenVPN)

Documentaires :

- Documentation officielle pfSense, - Documentation Microsoft Active Directory, - Documentation OpenVPN

Modalités d'accès aux productions et à leur documentation

- Schémas réseau, - Procédures d'installation et de configuration, - Documentation technique numérique

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

Partie 1 – Besoins spécifiques de l'entreprise

L'entreprise devait garantir la continuité de service de son système d'information afin d'éviter toute interruption des services réseau critiques. La sécurisation des flux réseau constituait un besoin essentiel afin de limiter les risques d'intrusion et d'accès non autorisés. Une segmentation du réseau était nécessaire pour isoler les différents services et améliorer le contrôle des communications internes et externes. L'entreprise souhaitait également centraliser l'authentification des utilisateurs afin de faciliter l'administration et la gestion des droits d'accès. Enfin, la mise en place d'un accès distant sécurisé était indispensable pour permettre aux administrateurs et aux utilisateurs autorisés d'accéder au réseau depuis l'extérieur en toute sécurité.

Partie 2 – Solutions envisageables

Plusieurs solutions ont été étudiées pour répondre aux besoins exprimés. La mise en place d'un pare-feu unique a d'abord été envisagée, mais elle ne garantissait pas une continuité suffisante en cas de panne.
L'utilisation d'un serveur VPN intégré ou indépendant a également été analysée, ainsi que différentes solutions d'authentification centralisée.
Après comparaison, il est apparu nécessaire de privilégier une solution combinant haute disponibilité, sécurité renforcée et évolutivité du système d'information.

Partie 3 – Solutions retenues

La solution retenue repose sur un cluster de pare-feu pfSense configuré en haute disponibilité, assurant la continuité du service réseau.
Elle intègre un Active Directory redondant pour garantir la disponibilité des services d'authentification et DNS et centraliser la gestion des utilisateurs.
Enfin, un serveur OpenVPN sous Linux a été déployé pour offrir un accès distant sécurisé, chiffré et contrôlé.
Cette architecture améliore la sécurité, la disponibilité et la gestion globale du système d'information.

Partie 4 – Mise en œuvre des solutions

La mise en œuvre a commencé par le déploiement de deux pare-feu pfSense configurés en cluster avec CARP et synchronisation des règles.
Une segmentation du réseau a été réalisée, incluant la création de VLAN et la mise en place d'une DMZ pour isoler les services exposés.
Deux contrôleurs de domaine Active Directory ont été installés pour assurer la réplication des données et la tolérance de panne.
Un serveur OpenVPN chiffré a été mis en place avec authentification centralisée pour sécuriser les accès distants.
Des règles de filtrage et une journalisation des accès ont été configurées afin d'assurer la traçabilité.

Partie 5 – Améliorations futures

Plusieurs améliorations pourraient être envisagées, comme la haute disponibilité du serveur VPN, le renforcement de la supervision réseau et l'ajout de mécanismes de détection et prévention d'intrusion.
L'automatisation des sauvegardes et l'amélioration des outils de reporting pourraient également être mises en œuvre pour optimiser la maintenance.

Partie 6 – Conclusion

Pour conclure, la mise en place du cluster pfSense, de l'Active Directory redondant et du serveur OpenVPN offre une solution complète et sécurisée. Elle garantit la continuité des services critiques, renforce la sécurité des flux par le filtrage et la segmentation, et permet un accès distant sécurisé. La journalisation assure une traçabilité en cas d'incident et facilite la maintenance et la supervision.