**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS** **SESSION 2025**

**ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate**

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

# CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

## En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

| | | | |
|---|---|---|---|
| **Identification**[1] | Nom : Akhbouche Prénom : Issam<br>N° d'inscription : 2045539097<br>Centre de formation : CNED | Voie d'accès à l'examen : Candidat individuel<br>Académie : Lyon | **SISR** |

## 1. Environnement commun aux deux options

### 1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

| **Éléments** | **Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)** | **Remarques de la commission d'interrogation** |
|---|---|---|
| Un service d'authentification | Simulé via documentation dans le compte rendu du projet (création d'OUs, GPO, utilisateu Tracer). | |
| Un SGBD | Aucun SGBD utilisé dans le projet. | |
| Un accès sécurisé à internet | Simulé avec routage NAT et ACL dans Cisco Packet Tracer. | |
| Un environnement de travail collaboratif | Serveur de messagerie simulé dans Packet Tracer, documentation du fonctionnement. | |
| Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)* | - Tous les serveurs sont simulés dans Packet Tracer (Linux et Windows représentés par leur rôle logique). | |

[1] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

**ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel**

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

| **Éléments** | **Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)** | **Remarques de la commission d'interrogation** |
|---|---|---|
| Une solution de sauvegarde | Non simulée dans le projet. | |
| Des ressources dont l'accès est sécurisé et soumis à habilitation | Contrôle des accès simulé via configuration d'ACL. | |
| Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette) | Uniquement des postes clients simulés dans Packet Tracer (pas de smartphones). | |

### 1.2 Des outils sont mobilisés pour la gestion de la sécurité :

| **Éléments** | **Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)** | **Remarques de la commission d'interrogation** |
|---|---|---|
| Gestion des incidents | Documentée théoriquement dans le compte rendu (problèmes de connectivité, DNS). | |
| Détection et prévention des intrusions | Non utilisée. | |
| Chiffrement | Utilisation de HTTPS sur le site WordPress (SSL activé sur Hostinger).<br>Sensibilisation à la protection des données utilisateurs. | |
| Analyse de trafic | Non réalisée (Wireshark non utilisé). | |

**Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.**

**ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel**

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

## 2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : **« *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »**

### 2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

| **Éléments** | **Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)** | **Remarques de la commission d'interrogation** |
|---|---|---|
| Un réseau comportant plusieurs périmètres de sécurité | Réseau simulé sur Cisco Packet Tracer avec plusieurs VLANs (DMZ, administration, utilisateurs). Routage inter-VLAN configuré sur le routeur, ACL appliquées pour filtrer les flux. | |
| Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité | Simulation d'un serveur Web et d'un serveur de messagerie dans une DMZ. Accès simulé via NAT et ACL dans Packet Tracer. Pas de supervision réelle. | |
| Un logiciel d'analyse de trames | Non utilisé. Aucune analyse de paquets réalisée dans ce projet. | |
| Un logiciel de gestion des configurations | Configuration manuelle des équipements dans Cisco Packet Tracer. Aucun outil de gestion centralisée utilisé. | |
| Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès | Non simulée. Pas d'utilisation de SSH ni d'accès distant réel. | |
| Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes | Non utilisée. Aucun outil de supervision (type Centreon) n'a été mis en œuvre. | |
| Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet) | Accès simulé à un serveur Web via NAT et filtrage ACL dans Packet Tracer. Le serveur DNS est également simulé. | |

| Éléments | Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques) | Remarques de la commission d'interrogation |
|---|---|---|
| Une solution garantissant la continuité d'un service | Non simulée. La continuité de service n'a pas été intégrée dans le projet. | |
| Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion | Simulée dans Packet Tracer : deux routeurs configurés avec HSRP pour assurer une bascule automatique en cas de panne. | |
| Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion | Non simulée. Aucun load balancing mis en place. | |

**2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :**

| Éléments | Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques) | Remarques de la commission d'interrogation |
|---|---|---|
| Une solution permettant la connexion sécurisée entre deux sites distants | Non réalisée. Aucun VPN simulé ni tunnel entre routeurs. | |
| Une solution permettant le déploiement des solutions techniques d'accès | Configuration manuelle dans Packet Tracer. Aucun outil de déploiement ou TFTP utilisé. | |
| Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting* | Non utilisées. Aucun script bash ou automatisation n'a été mis en œuvre. | |
| Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau | Non réalisée. Aucun test d'intrusion ni outil d'analyse de trames utilisé (Wireshark non utilisé). | |