BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : TRINEL Jules	**N° candidat : 02341341637**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 05/06/2024

Organisation support de la réalisation professionnelle :
Nextech est un centre de formation qui permet aux entreprises de disposer des compétences dont elles ont besoin afin de mettre en œuvre leur stratégie et améliorer leur compétitivité. Le centre de formation utilise un serveur Active Directory afin de centraliser la gestion des ressources et Nextech souhaite améliorer la sécurité de ce serveur qui est un élément critique dans l'infrastructure informatique. L'utilisation d'une checklist sera nécessaire afin de valider les points les plus importants à sécurisés.

Intitulé de la réalisation professionnelle
Mise en place de deux serveurs Active Directory et création d'utilisateurs, de groupes, de GPO et utilisation d'un script pré-fait afin de contribuer à l'amélioration de la sécurité du domaine.

Période de réalisation : du 01/2024 au 04/2024 **Lieu :** Centre de formation Nextech, 84911 Avignon
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[1] (ressources fournies, résultats attendus)

Ressources fournies : Un schéma réseau, le contexte Nextech, un plan réseau, les identifiants, un serveur HP Proliant DL380 hébergeant l'hyperviseur Proxmox exécutant toutes l'infrastructure virtuelle répondant au référentiel de l'infrastructure commune du BTS SIO SISR.

Résultats attendus : Sécurisation renforcée de l'Active Directory en désactivant certains protocoles à l'aide de différentes GPO et en améliorant la sécurité du compte critique krgbt. Amélioration de la politique de mot de passe par défaut forçant ainsi l'utilisation d'un mot de passe robuste répondant aux critères de la CNIL.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources documentaires : Un schéma réseau comprenant l'infrastructure commune et la situation personnelle ainsi qu'une documentation technique décrivant la mise en place.

Ressources matérielles : Un serveur HP Proliant DL380 configuré en RAID 1 et hébergeant l'hyperviseur Proxmox dans lequel est exécuté toute l'infrastructure virtuelle.

Ressources logicielles : Hyperviseur Proxmox, Un serveur Active Directory principal avec comme OS Windows serveur 2022, Un deuxième serveur Active Directory secondaire avec comme OS principal Windows serveur 2022, Des machines clientes Windows 10 ou 11 disponibles dans les différents VLANs (machines virtuelles).

Modalités d'accès aux productions[3] et à leur documentation[4]

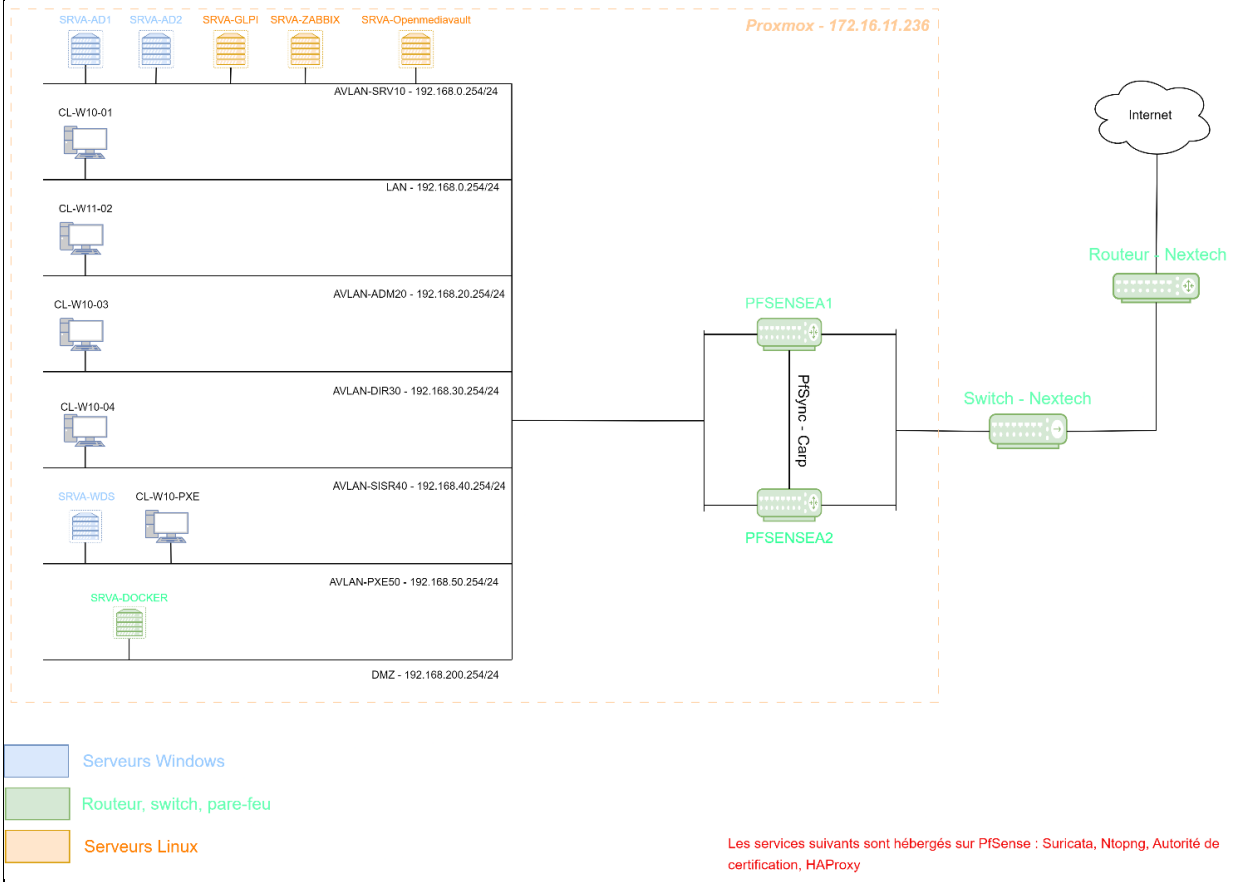
Documentation accessible sur le portfolio à l'adresse suivante : https://f4doli.github.io/situations-form/windows_serveur/durcissement-ad/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

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



Etapes de réalisation :

Première étape : Création des deux machines virtuelles Windows serveur 2022 et configuration des rôles AD DS, DNS et ajout des PC dans le domaine.
Deuxième étape : Création de plusieurs OU, utilisateurs et groupes de sécurité afin d'améliorer l'organisation de l'Active Directory.
Troisième étape : Création d'une checklist de 5 étapes comprenant certains des points les plus vulnérables au sein d'un Active Directory
Quatrième étape : Mise en place de la sécurisation en suivant la checklist : Amélioration de la stratégie de mot de passe, Désactivation du service Print Spooler, Désactivation de la version 1 de SMB, Désactivation de LLMNR et Netbios à l'aide de GPO, amélioration de la protection du compte krgbt à l'aide d'un script pré-fait PowerShell.
Cinquième étape : Vérification de l'application des GPO, de la désactivation du service Print Spooler et de la stratégie de mot de passe.

Plan réseau de tous les périphériques :

Le plan réseau de l'infrastructure est disponible sur mon portfolio à l'adresse suivante :
https://f4doli.github.io/situations-form/windows_serveur/durcissement-ad/

Identifiants de l'infrastructure :

Tous les identifiants permettant d'accéder et d'administrer l'infrastructure sont disponible sur mon portfolio à l'adresse suivante :
https://f4doli.github.io/situations-form/windows_serveur/durcissement-ad/