

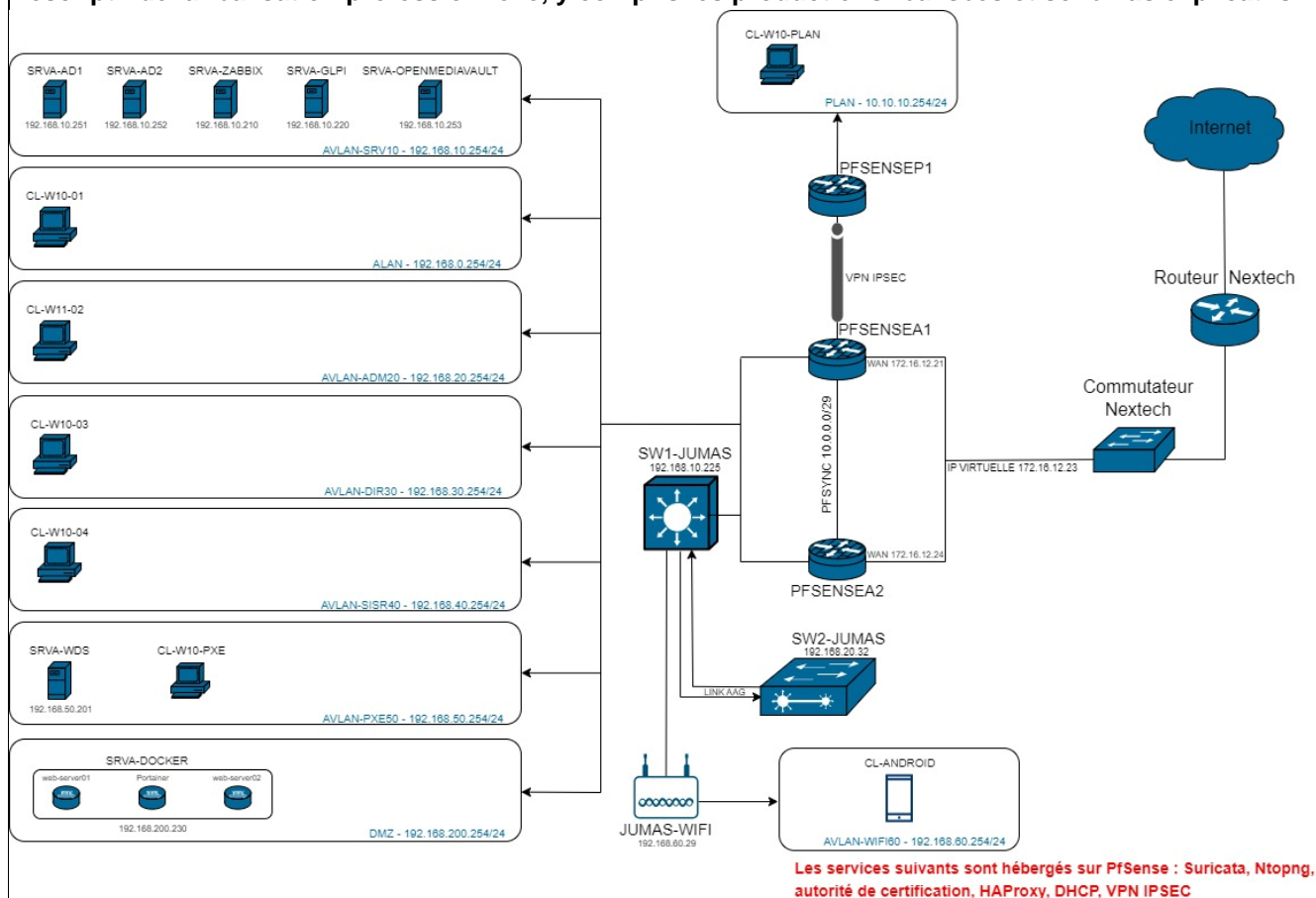
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2024
Épreuve E5 - Administration des systèmes et des réseaux (option SISR)	
ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)	

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 2
Nom, prénom : TRINEL Jules		N° candidat : 02341341637
Épreuve ponctuelle <input checked="" type="checkbox"/>	Contrôle en cours de formation <input type="checkbox"/>	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 : CFA A.P.I - C.F.A.I. 84 - AVIGNON (NEXTECH), 60 chemin de Fontanille, Campus Agroparc 84140 Avignon Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (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, un switch Alcatel-Lucent, Une borne WiFi, un switch TP-LINK. 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 utilisées² 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, un switch Alcatel-Lucent, un switch TP-LINK. 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 productions³ et à leur documentation⁴ Documentation accessible sur le portfolio à l'adresse suivante : https://f4doli.github.io/situations-form/windows_serveur/durcissement-ad/		

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

**Étapes 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 au sein du centre de collaboration Google Apps :

https://drive.google.com/drive/folders/1sfti5c3VCCP6gRIKT7CmzagHBi00HRpB?usp=drive_link

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://drive.google.com/drive/folders/1sfti5c3VCCP6gRIKT7CmzagHBi00HRpB?usp=drive_link