BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2026

ANNEXE VII-1-A : 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 : RONFORT Maxence	**N° candidat :**
Épreuve ponctuelle ☐	**Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....

Organisation support de la réalisation professionnelle

Alicante.local

Intitulé de la réalisation professionnelle

Solution de travail à distance pour les utilisateurs ayant les habilitations :

- Inclus le serveur de bureau à distance
- Inclus la partie Active Directory et serveur de fichier pour la gestion des utilisateurs et des habilitations
- Inclus la partie stratégie de groupe pour l'automatisation
- Inclus la partie réseau pour la gestion du VPN SSL et pour la segmentation

Période de réalisation : 2026-2027 Lieu : UFA Robert Schuman Metz
Modalité : ☐ **Seul(e)** ☐ **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)

Objectifs et résultats attendus :
Mettre en place une infrastructure d'authentifications centralisées et sécurisée basées sur Active Directory
Intégrer un pare-feu Stormshield avec l'annuaire AD pour appliquer des règles d'accès en fonction des profils d'utilisateur
Interféré GLPI avec Active Directory

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

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

1. Objectif

Mettre en place une solution sécurisée de travail à distance permettant aux utilisateurs d'accéder aux ressources de l'entreprise et de leur fournir une connexion sécurisée.

Pourquoi : L'entreprise ne possède pas de solution de connexion à distance et sécuriser.

A quoi cela sert : Cela permettrait aux utilisateurs de travailler à distance avec une connexion sécurisée et fiable.

Comment : En utilisant les technologies mit en place par StormShield, il est possible de créer des tunnels sécurisés. Il faudra mettre en place un VPN SSL sur le SNS interne et déclarer sur le SNS externe les routes et protocoles afin que les utilisateurs puissent s'authentifier.

L'objectif final :
Assurer un accès distant sécurisé par VPN SSL pour les utilisateurs en utilisant les technologies fournis par Stormshield Network Security.

2. Compétences principales

Les principales compétences mobilisées dans cette activité sont :

- Choix des éléments nécessaires pour assurer la qualité et la disponibilité d'un service
- Installation et configuration des éléments nécessaires pour assurer la continuité des services
- Test d'intégration et d'acceptation d'une solution d'infrastructure
- Identification, qualification, évolution et réaction face à un incident ou un problème
- Evaluation, maintiens et amélioration de la qualité de service

Définitions et normes du domaine :
Les principaux éléments de l'authentification informatique sont :

- L'annuaire LDAP et Active Directory

- Système centralisé de gestion des comptes d'utilisateurs, de groupes et des droits d'accès.

  - Permet d'authentifier les utilisateurs et leurs habilitations. GLPI peut s'interfacer avec l'annuaire Active Directory pour synchroniser les comptes d'utilisateurs.

- Le pare-feu Stormshield Network : Intégré avec l'annuaire LDAP, il permet d'appliquer des règles d'accès et de filtrage en fonction des groupes et des profils utilisateur.

- SSL permettant d'encrypter les données

- Un Virtual Private Network permettant aux utilisateurs d'accéder au réseau interne de l'entreprise
- LAPS : Outil permettant de gérer de manière sécurisé les mots de passes des comptes d'administrations locaux sur les postes de travails.

Contexte :

Le contexte est celui d'une entreprise ou il faut sécuriser l'accès des ressources informatiques (serveurs fichiers, messageries, applications métiers, etc..) Une authentification centralisée et sécurisée est nécessaire pour garantir la confidentialité et l'intégrité des données.

Les ressources utilisées sont :

- Deux serveurs Actives Directory
- Un Stormshield externe
- Un Stormshield interne avec une solution VPN SSL
- Un client Windows 11

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

"Portolio" ----> à faire
Les différents accès login : Administrateur / MDP : Azerty123!
Login : Maxence / MDP : Azerty123!
Login : vpn / MDP : Azerty123!

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

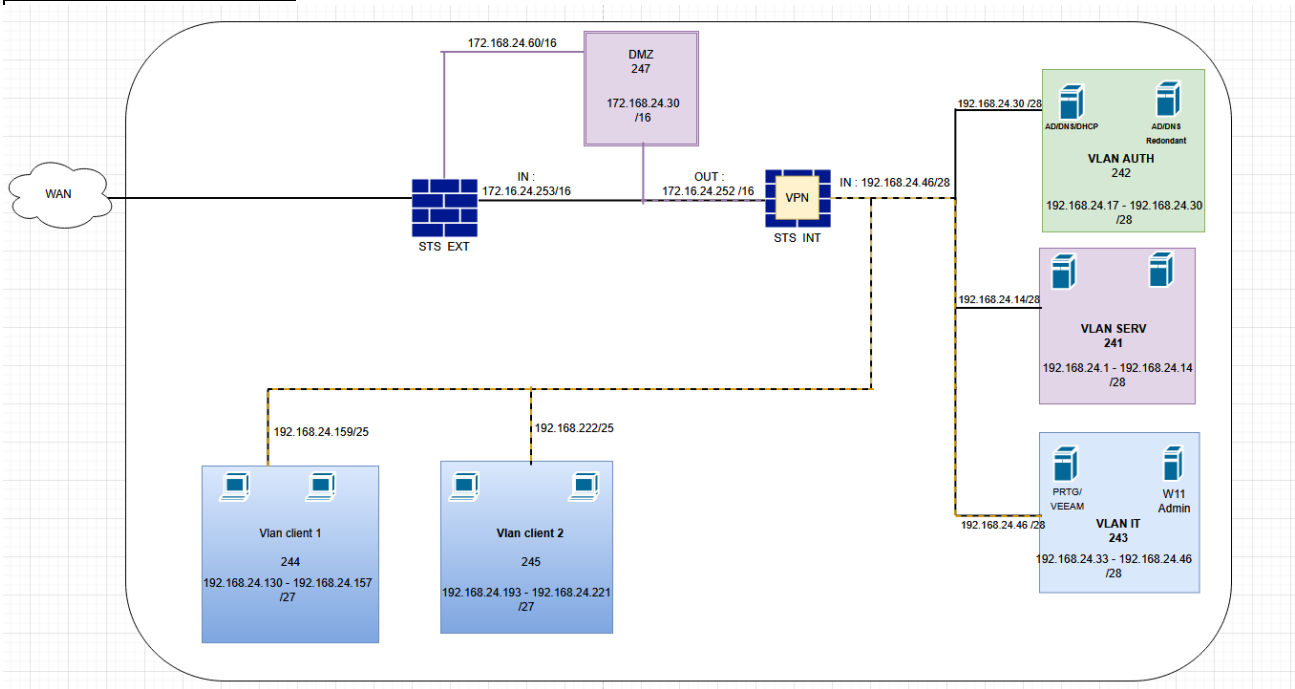
Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

RONFORT
Maxence

Schéma et maquettes de l'infrastructure :

	VLAN	Nom machine	IP	MASQUE	Passerelle
Serveur	AUTH 242	AD/DNS/DHCP	192.168.24.17	/28	192.168.24.30
		AD 2	192.168.24.18		192.168.24.30
	Serveur 241	RDS	192.168.24.23	/28	192.168.24.14
		Fichier	192.168.24.25		192.168.24.14
	IT 243	PRTG/VEEAM	192.168.24.34	/28	192.168.24.46
		Stormshield Int	192.168.24.46		192.168.24.46
		CLIENT W11 Admin	192.168.24.45		192.168.24.46
Utilisateur	CLIENT1 244	Utilisateur	192.168.24.130 - 157	/27	192.168.24.158
	CLIENT2 245	Utilisateur	192.168.24.193 - 221	/27	192.168.24.222
DMZ	DMZ 247	192.168.24.0	172.168.24.59	/28	172.168.24.60

PLAN D'ADRESSAGE :

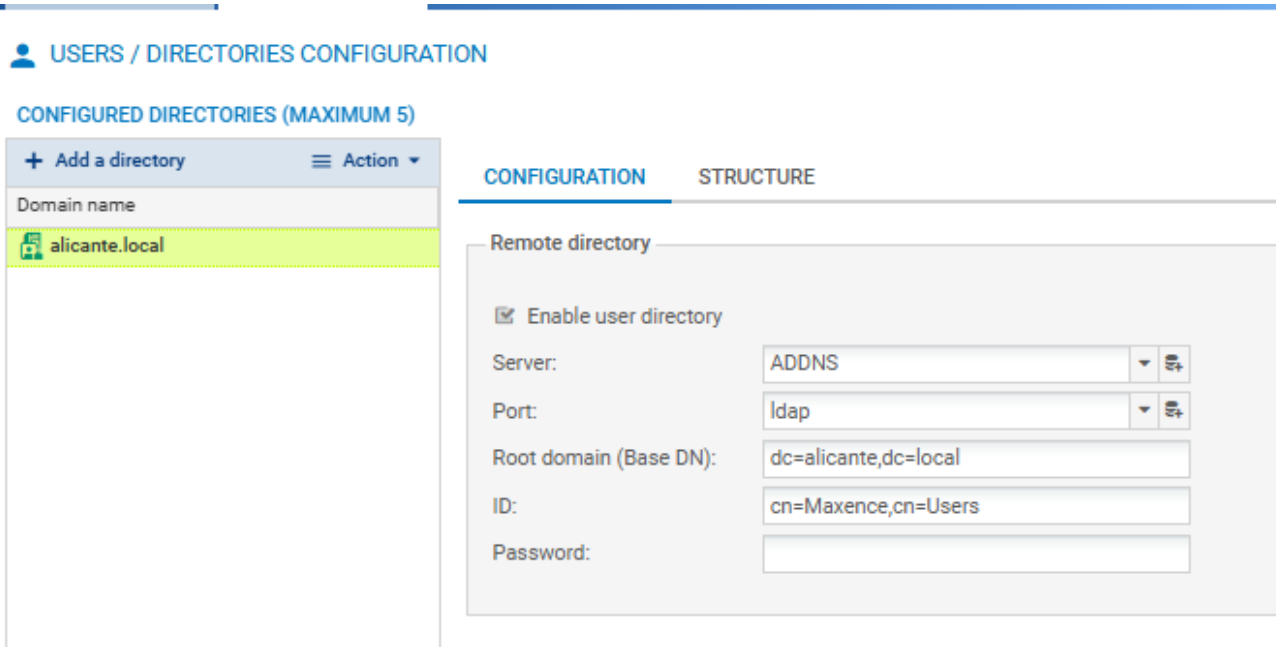


3. DOC TECHNIQUE :

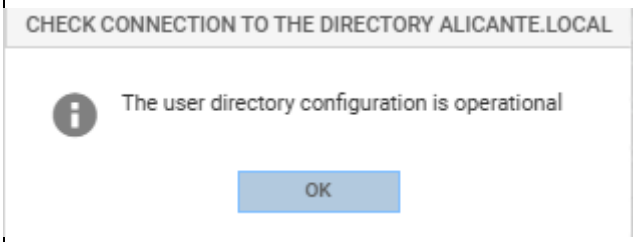
3.1 Connexion Stormshield avec LDAP

Une fois notre AD / DNS / DHCP / LDAP configuré, nous pouvons configurer le connecter à Stormshield qui effectuera l'authentification utilisateur par ce dernier.

Nous devons connecter Stormshield et l'annuaire LDAP en déclarant le nom de domaine ainsi qu'un administrateur afin d'accéder à l'annuaire LDAP.

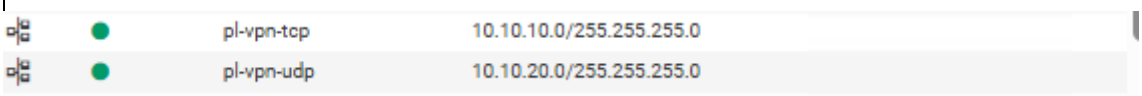


Une fois l'Active Directory configuré, nous nous assurons qu'il fonctionne bien en effectuant un 'check connexion' depuis le Stormshield interne :

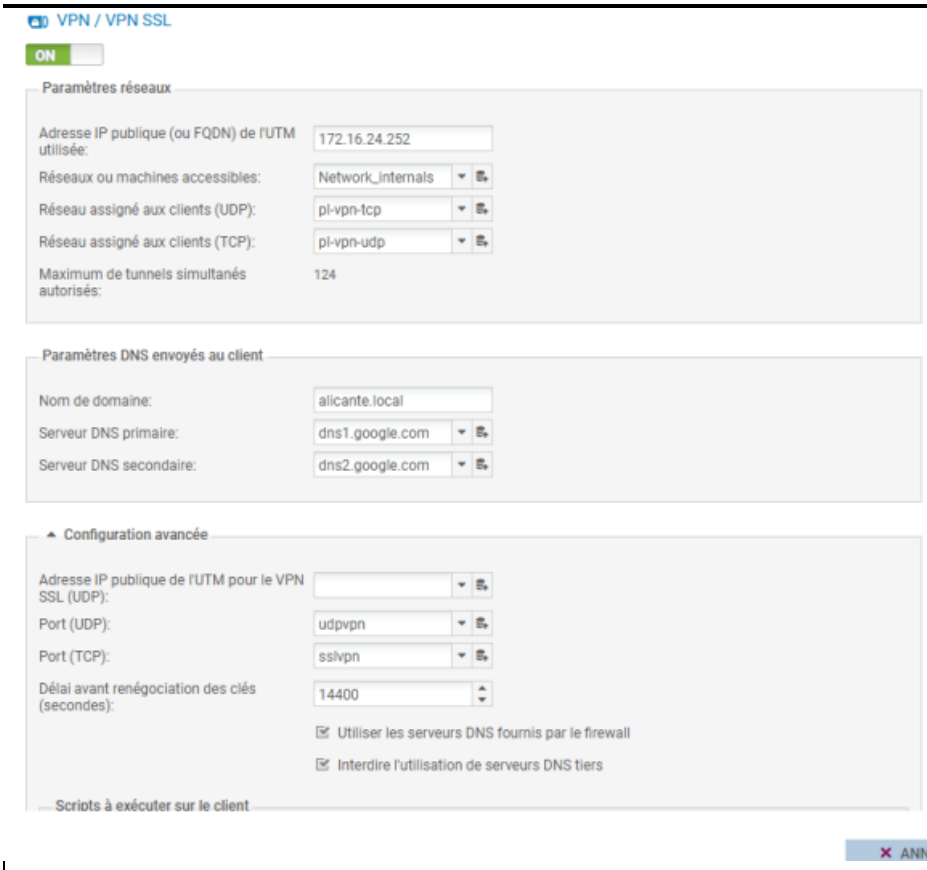


3. 2 Config VPN

Nous configurons le VPN en lui configurant une IP publique ainsi que des plages TCP et UDP pour le tunnel VPN :

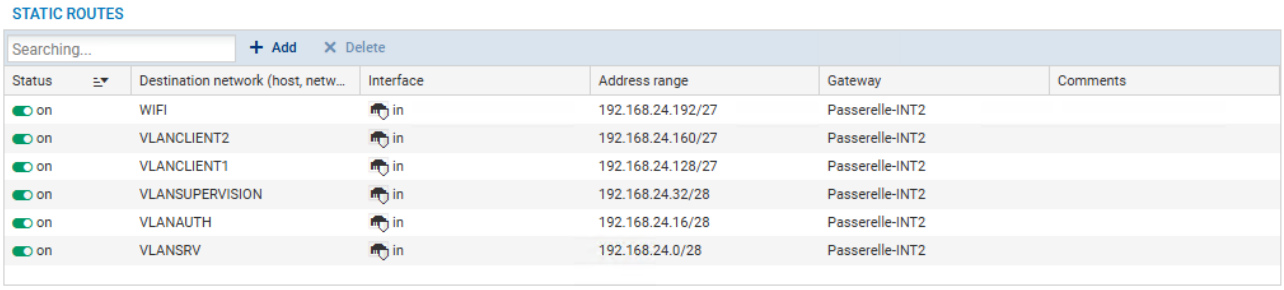


Nous déclarons également le nom de domaine Alicante :

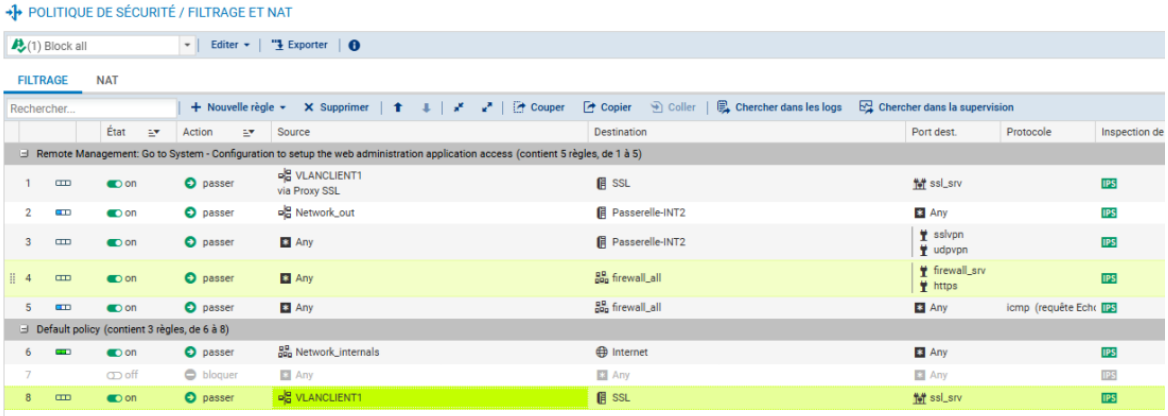


é

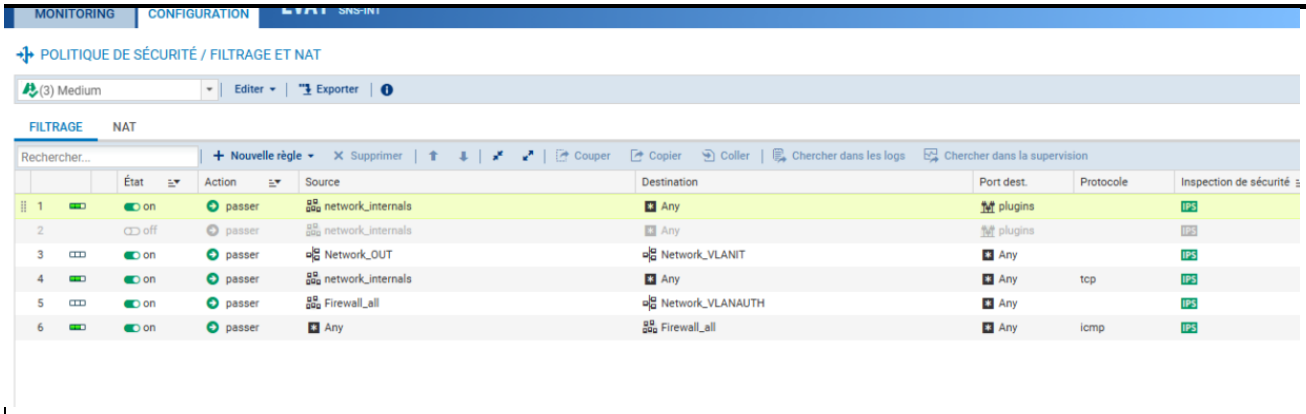
Nous déclarons les routes sur le SNS Externe :



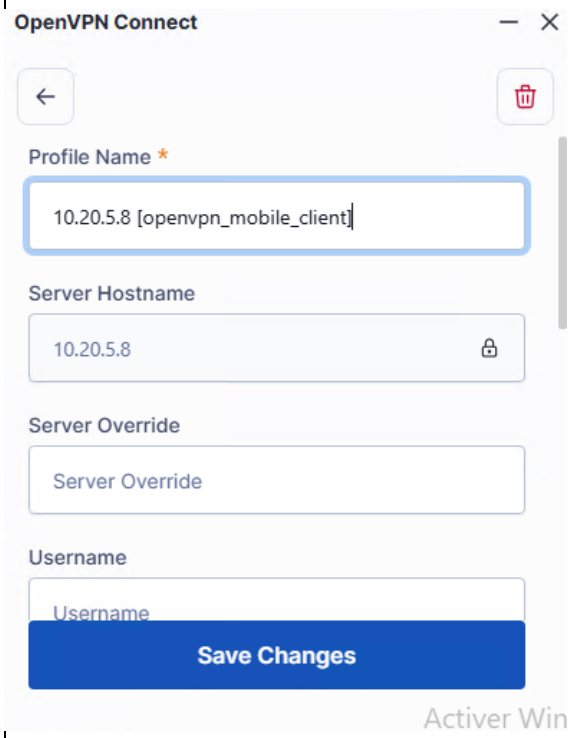
Une fois notre VPN créé sur notre SNS Interne, nous devons le déclarer sur notre Stormshield externe et ont créé des règles de filtrage par protocole :



Nous déclarons les politiques de sécurités et de filtrage et NAT sur le stormshield interne :

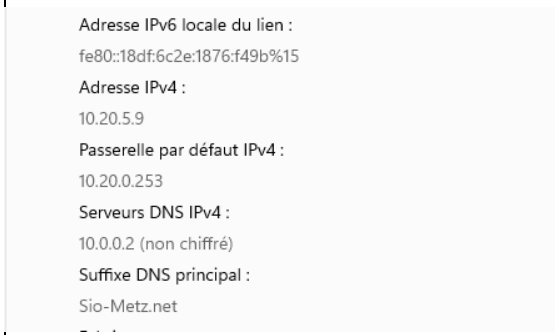


Une fois toutes ces règles créent, nous pouvons télécharger le profil VPN utilisateur.



3.3 Test de connexion

Voici l'adresse IP du client qui n'est pas connecté au VPN :



Adresse IP client après la connexion VPN :

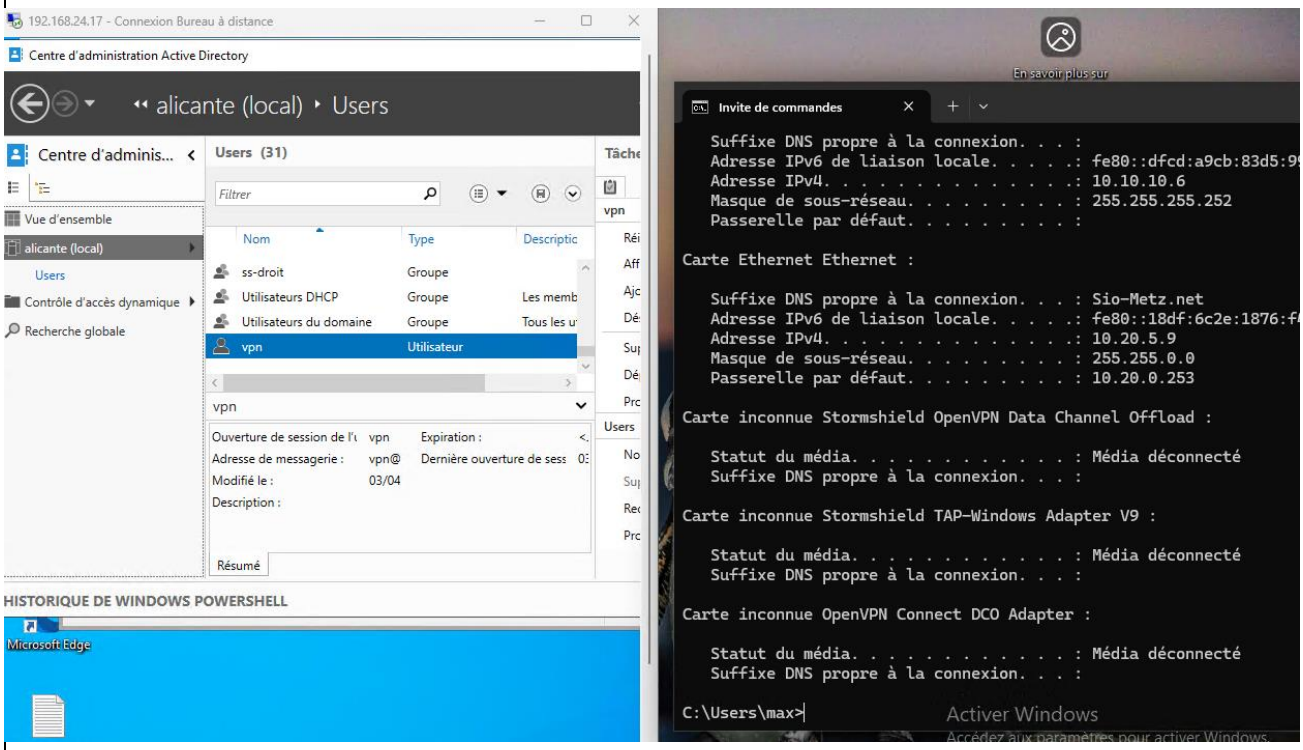
```
Carte inconnue Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dfcd:a9cb:83d5:9931%16
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.10.6
   Masque de sous-réseau. . . . . . . . . : 255.255.255.252
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : Sio-Metz.net
   Adresse IPv6 de liaison locale. . . . .: fe80::18df:6c2e:1876:f49b%15
   Adresse IPv4. . . . . . . . . . . . . .: 10.20.5.9
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.20.0.253
```

Le client peut bien se connecter au réseau une fois le VPN activer :



3.4 RESULTAT ET CONCLUSION

Les résultats attendus de cette solution d'authentification sont :

Un tunnel VPN SSL à bien été mis en place et il est bien fonctionnel. Le VPN est bien relié à l'AD est l'authentification des utilisateurs se fait correctement. Les utilisateurs peuvent bien accéder aux ressources disponibles dans le réseau en étant connecter au VPN.