PROJET M2i

CAMPUS DU NUMÉRIQUE
by CCI Campus

AP3

LIVRABLE 2

RAPPORT DE CLÔTURE DU PROJET

Date limite de remise : 31 décembre 2022

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l'auteur ou des auteurs et n'engagent aucunement CCI Campus

SOMMAIRE

Date limite de remise : 31 décembre 2022 1

1) RESUME DU PROJET 3
1.1) Définitions des rôles et responsabilités 3
1.2) Rappel des objectifs fixés 3

2) CONDUITE DU PROJET 4
2.1) Planning prévisionnel VS Planning réel 4
2.2) Ressources utilisées 6
2.3) Problèmes rencontrés et solutions apportées ou envisagées 8
2.4) Ancien schéma réseau VS nouveau 8

2.5) Tableau de synthèse 9

3) RESULTATS 10
3.1) Résultats attendus VS Résultats obtenus 10

4) ANALYSE FINALE 10
4.1) Analyse et état finale du projet 10

5) CONCLUSION 10

6) DOCUMENTATION TECHNIQUE 11
6.1) Création du serveur STG-SRV01 11
a) Information du serveur 11
b) Installation de l'Active directory 11
c) l'Arborescence 19
d) DNS 28
e) DHCP 36
f) Mise en place DFS DFS-R 47
g) Ajout d'un serveur d'espace de nom 55
h) Ajout de dossiers partagé 56
i) DFS-R configuration de la réplication 59
6.2) Création du Routeur / Firewall Opensense Strasbourg 62
a) Information du serveur 62
b) Création de la VM 63
c) Configuration réseau 66

d) Configuration général....68
e) Mise en place VPN IPSEC....71
f) Mise en place du portail captif....76
6.3) Création du Routeur / Firewall Opensense Mulhouse.... 92
a) Information du serveur....92
b) Configuration réseau....92
c) Configuration générale....94
d) Mise en place VPN IPSEC....96
6.4) Serveur de Sauvegarde SAN et cliché instantané Shadow copy 103
a) Installation du serveur TrueNas....103
b) Configuration de TrueNas....107
c) Activation des clichés instantanés....112
d) Utilisation des versions précédentes....116

1) RESUME DU PROJET

1.1) Définitions des rôles et responsabilités

	Tom HOERMANN	Matteo ADDARIO
Responsabilité	Chef de projet	Technicien
Rôles	Routeur /Firewall VPN IpSec Portail captif ADDS, DNS, DHCP	SAN Truenas Shadowcopy DFS réplication GPO

1.2) Rappel des objectifs fixés

La nouvelle CCI Grand Est a remplacé depuis le 1er janvier 2017 les 3 anciennes CCI régionales d'Alsace. En 2022, CCI Campus inaugure un nouveau campus du numérique avec 9 formations de Bac+2 à Bac+5. Pour ces nouvelles formations, la DSI a décidé de lancer un appel d'offres pour la création d'un réseau informatique indépendant, la création et l'équipement de nouvelles salles informatiques.

Pour ce faire, nous allons devoir améliorer le service aux utilisateurs et faciliter d'administration par la DSI en faisant un système d'information indépendant, un système informatique uniformisé, des liaisons inter-sites entre les établissements et des redondances.

Un retour sur investissement par la réduction des coûts sera à réaliser (possession/exploitation). On réalisera une documentation complète et on facilitera l'administration.

Faciliter le travail collaboratif en termes de partage et d'accessibilité des données inter-sites

Et enfin, la dernière partie que nous traiterons se trouve au niveau de la sécurité des systèmes et des données. Il faudra mettre un accès internet légal à disposition mais aussi faciliter la mise en place d'un PCA (plan de continuité d'activité), la redondance des serveurs, service et données et faire des sauvegardes régulières des serveurs.

Pour ce qui concerne les objectifs attendus pour cet Atelier professionnel, trois règles très importantes sont à respecter :

- Respecter la date de début et de fin de projet
- La solution que nous proposons doit être à moindre coût et nous avons un budget à respecter de maximum 100 000€ HT
- Rendre les livrables et effectuer les soutenances aux dates prévues

Pour ce qui est de la mise en œuvre technique, nous créerons une nouvelle salle informatique à Strasbourg et à Mulhouse en mettant en place des serveurs, des postes de travail, etc.... et faire attention au coût des licences et de la main d'œuvre.

Nous mettrons en place une liaison WAN inter-sites chiffrée mais aussi une harmonisation du plan d'adressage et de nommage sur l'ensemble des sites.

Nous créerons des serveurs et des rôles/services en haute disponibilité (AD/DNS/DHCP/DFS/Partage SMB/etc. ..)

Un portail-captif avec authentification forte sera mise en œuvre et il faudra qu'il soit conforme à la législation Française et Européenne.

Une redondance, des droits et des permissions adaptés devront être possible lors de l'accès aux données stockant les dossiers personnels des enseignants et des élèves sur les deux sites.

Et enfin, il faudra qu'on prenne en considération les recommandations de l'ANSSI.

2) CONDUITE DU PROJET

2.1) Planning prévisionnel VS Planning réel

Planning prévisionnel :

Taches à réaliser	Date de début	date de fin	Durée	Réalisateur
Serveur AD, DNS, DHCP	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Julien GOMES
DFS, Réplication	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Julien GOMES
Routeur OpenSense + Firewall + portail captif	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Tom HOERMANN
VPN IpSec	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Tom HOERMANN
Serveur de sauvergarde trueNas + Shadow copy	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Matteo ADDARIO
GPO	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Matteo ADDARIO
Mise en commun + correcteur erreur	Vendredi 16/12/22	Vendredi 16/12/22	4 Heures	Groupe 2

Le planning prévisionnel nous montre que l'on avait chacun 2 jours pour réaliser nos parties, plus 4 heures de mise en commun et de correction d'erreur.

Diagramme de Gantt prévisionnel :

Diagramme de Gantt	Vendredi 21/10/22	Vendredi 04/11/22	Vendredi 18/11/22	Vendredi 02/12/22
Serveur AD, DNS, DHCP				
DFS, Réplication				
Routeur OpenSense + Firewall + portail captif				
VPN IpSec				
Serveur de sauvergarde trueNas + Shadow copy				
GPO				
Mise en commun + correction erreur				

Planning réel :

Taches à réaliser	Date de début	date de fin	Débug	Durée	Réalisateur
Serveur AD, DNS, DHCP	Mercredi 14/12/22	Jeudi 15/12/22	Rien	8 Heures	Tom HOERMANN
DFS, Réplication	Mercredi 14/12/22	Jeudi 15/12/22	2 heures jeudi 15/12/2022	8 Heures	Matteo ADDARIO
Routeur OpenSense + Firewall + portail captif	Vendredi 21/10/22	Vendredi 04/11/22	Rien	8 Heures	Tom HOERMANN
VPN IpSec	Vendredi 18/11/22	Vendredi 02/12/22	2 heures mercredi 14/12/2022	7 Heures	Tom HOERMANN
Serveur de sauvergarde trueNas + Shadow copy	Vendredi 21/10/22	Vendredi 04/11/22	2 heures mercredi 14/12/2022	8 Heures	Matteo ADDARIO
GPO	Vendredi 18/11/22	Vendredi 02/12/22	Rien	8 Heures	Matteo ADDARIO
Mise en commun + correcteur erreur	Vendredi 16/12/22	Vendredi 16/12/22	6 heures mercredi 14/12/2022	6 Heures	Matteo ADDARIO Tom HOERMANN

Le planning réel montre la partie serveur AD et serveur Core à était réalisé très tard au vu de l'abandon du technicien Julien Gomes dans le projet. Cette partie a donc était repartie entre les 2 autres opérateurs ce qui à créer du retard. Des heures de mise en commun et debug ont aussi était ajouté.

Diagramme de Gantt réel :

Diagramme de Gantt	Vendredi 21/10/22	Vendredi 04/11/22	Vendredi 18/11/22	Vendredi 02/12/22	mercredi 14/12/2022	Jeudi 15/12/2022
Serveur AD, DNS, DHCP						
DFS, Réplication						
Routeur OpenSense + Firewall + portail captif						
VPN IpSec						
Serveur de sauvergarde trueNas + Shadow copy						
GPO						
Mise en commun + correction erreur						

2.2) Ressources utilisées

Devis interne :

Description	Quantité	Prix unitaire HT	Prix total HT
PC Office Intel i7 Business	60	399,00 €	23 940,00 €
kit clavier + souris	60	38,40 €	2 304,00 €
Dell SE2222H Écran	60	129,00 €	7 740,00 €
NAS 4baies Synology RackStation RS822RP+	2	1 238,00 €	2 476,00 €
DD NAS 1 To WD Red Plus	6	76,29 €	457,74 €
Switch Cisco SB CBS250-48P-4G	2	999,99 €	1 999,98 €
Serveurs HPE ProLiant DL20 Gen10 Plus	6	1 176,99 €	7 061,94 €
HPE Midline - Disque dur - 2 To	12	201,60 €	2 419,20 €
Routeur industriel compact	2	219,00 €	438,00 €
License Windows servers 2016	6	882,00 €	5 292,00 €
License Windows 10 family	60	129,00 €	7 740,00 €

Total HT	61 868,86 €
TVA (20,00 %)	12 373,77 €
Total TTC	**74 242,63 €**

Devis externe :

Description	Quantité	Prix unitaire HT	Prix total HT
INFRASTRUCTURE - chef de projet	8	699,00 €	5592,00 €
INFRASTRUCTURE - Techniciens	8	399,00 €	3192,00 €

Total HT	8784,00 €
TVA (20,00 %)	1756,80 €
Total TTC	**10540,80 €**

2.3) Problèmes rencontrés et solutions apportées ou envisagées

Technicien en moins → répartitions des taches et augmentation du temps de travail

VPN IPSec qui n'arrive plus à faire la connexion tunnel → problème lié aux IP données par l'opérateur internet → résolue avec un changement de réseau et de configuration VirtualBox

2.4) Ancien schéma réseau VS nouveau

<u>Ancien shéma réseau :</u>

Nouveau schéma réseau :

2.5) Tableau de synthèse

Name	**Ip address**	**Netmask**	**Passerelle**	**DNS**
		STRASBOURG		
RTE-STG01 LAN	192.168.100.1	255.255.255.0		192.168.100.2
RTE-STG01 WAN	172.20.10.4	255.255.255.0		192.168.100.2
STG-SRVW01	192.168.100.2	255.255.255.0	192.168.100.1	192.168.100.2
STG-SRVW02	192.168.100.3	255.255.255.0	192.168.100.1	192.168.100.2
STG-NAS01	192.168.100.4	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P01	192.168.100.5	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P02	192.168.100.6	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P03	192.168.100.7	255.255.255.0	192.168.100.1	192.168.100.2
		MULHOUSE		
RTE-MUL01 LAN	192.168.200.1	255.255.255.0		192.168.200.2
RTE-MUL01 WAN	172.20.10.3	255.255.255.0		192.168.200.2
MUL-SRVW01	192.168.200.2	255.255.255.0	192.168.200.1	192.168.200.2
MUL-SRVW02	192.168.200.3	255.255.255.0	192.168.200.1	192.168.200.2
MUL-NAS01	192.168.200.4	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P01	192.168.200.5	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P02	192.168.200.6	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P03	192.168.200.7	255.255.255.0	192.168.200.1	192.168.200.2

3) RESULTATS

3.1) Résultats attendus VS Résultats obtenus

Résultat Attendu	Résultat obtenus
Serveur ADDS, DNS, DHCP	Mis en place et opérationnel
DFS, réplication	Mis en place et opérationnel
Routeur/Firewall	Mis en place et opérationnel
VPN IPsec	Mis en place et opérationnel
Portail Captif	Mis en place et opérationnel
Serveur de sauvegarde + Shadow copy	Mis en place et opérationnel

4) ANALYSE FINALE

4.1) Analyse et état finale du projet

Le service a donc été amélioré pour les utilisateurs et il permet de faciliter l'administration par la DSI avec ce nouveau système d'information indépendant. Le système informatique est maintenant uniformisé et des liaisons inter-sites entre les établissements sont possibles. La sécurité de pertes des données et amélioré grâce au système de redondances.

Le budget de 100 000€ HT établie par le client a été respecté. Le budget total du projet est donc de 84 783.40€ HT.

Le projet a été finaliser dans les temps et à respecté les demandes du cahier des charges.

5) CONCLUSION

Pour conclure, malgré les difficultés rencontrées avec le VPN IPSEC et la mise en place du DFS, les objectifs imposés dans le cahier des charges ont était remplies dans le temps et avec le budget imposé.

6) DOCUMENTATION TECHNIQUE

6.1) Création du serveur STG-SRV01

a) Information du serveur

Nom du serveur : **STG-SRV01**

Interfaces IP :
- LAN : 192.168.100.2

Taille disque dur : 60 GB

RAM : 2 GO

Version: Microsoft Windows 2019 Standard

b) Installation de l'Active directory

On tout d'abord changer le nom du serveur en se rendant dans le panneau de configuration :

Panneau de configuration › Système et sécurité › Système

Puis modifier les paramètres,

Et on redémarre.

On se rend maintenant dans le Gestionnaire de serveur et on va ajouter le rôle active directory « AD DS »
On clique sur ajouter des rôles et des fonctionnalités :

Puis on clique sur suivant,

On sélectionne notre serveur, puis suivant,

On coche le rôle AD DS et on clique sur ajouter des fonctionnalités :

On va faire suivant jusqu'à l'installation :

Une fois installé, on va cliquez sur le drapeau et ensuite sur « promouvoir cde serveur en contrôleur de domaine »

On choisit l'option « ajouter une nouvelle foret » et on rentre notre nom de domaine :

Suivant,

On garde les paramètres par default et on entre un mot de passe pour notre domaine :

Suivant,

Suivant,

On laisse et suivant,

Suivant,

On clique sur installer,

On voit qu'on est bien dans le domaine :

On peut maintenant connecter nos équipements dans le domaine, par exemple pour les postes Windows 10, on se rend dans les paramètres Windows, changer le nom du pc, et on rentre le nom de domaine.
Après s'être identifier avec le mot de passe du domaine créer précédemment, on arrive à se connecter :

c) l'Arborescence

On va maintenant créer notre arborescence.
On se rend dans l'outils « Utilisateurs et ordinateurs Active directory »,

On va faire une clique droite sur notre nom de domaine et créer une Unité organisationnelle pour Strasbourg et une pour Mulhouse :

CCI-CAMPUS.LAN
Builti
Comp
Doma
Forei
Mana
Users
Délégation de contrôle...
Rechercher...
Changer de domaine...
Changer de contrôleur de domaine...
Augmenter le niveau fonctionnel du domaine...
Maîtres d'opérations...
Nouveau
Toutes les tâches
Affichage
Actualiser
Exporter la liste...
Propriétés
Aide
Ordinateur
Contact
Groupe
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur
Dossier partagé

Nouvel objet - Unité d'organisation
Créer dans : CCI-CAMPUS.LAN/
Nom :
Strasbourg
Protéger le conteneur contre une suppression accidentelle
Nouvel objet - Unité d'organisation
Créer dans : CCI-CAMPUS.LAN/
Nom :
Mulhouse
Protéger le conteneur contre une suppression accidentelle

On va ensuite créer des UO « Groupes » et « users » dans strasbourg et mulhouse, dans l'uo groupes de strasbourg on va créer le groupe « GRP1 » et dans groupes de Mulhous on créer le groupe « GRP2 » :

On va créer les users « Paul » et « Pierre » dans le GRP1 de l'UO Strasbourg et créer les users « Isabelle » et « Nathalie » dans GRP2 de l'UO Mulshouse :

Paul :

Nouvel objet - Utilisateur
Créer dans : CCI-CAMPUS.LAN/Strasbourg
Mot de passe :
Confirmer le mot de passe :
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Le compte est désactivé
< Précédent
Suivant >
Annuler

Nouvel objet - Utilisateur
Créer dans : CCI-CAMPUS.LAN/Strasbourg
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :
Nom complet : Paul A
Nom de connexion de l'utilisateur : Paul A@CCI-CAMPUS.LAN
L'utilisateur ne peut pas changer de mot de passe.
Le mot de passe n'expire jamais.

Pierre :

Isabelle :

Nouvel objet - Utilisateur
Créer dans : CCI-CAMPUS.LAN/Mulhouse
Prénom :
Isabelle
Initiales :
Nom :
A
Nom complet :
Isabelle A
Nom d'ouverture de session de l'utilisateur :
Isabellle A
@CCI-CAMPUS.LAN
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
CCI-CAMPUS\
Isabellle A
< Précédent
Suivant >
Annuler

Nathalie :

Nouvel objet - Utilisateur
Créer dans : CCI-CAMPUS.LAN/Mulhouse
Prénom :
Nathalie
Initiales :
Nom :
B
Nom complet :
Nathalie B
Nom d'ouverture de session de l'utilisateur :
Nathalie B
@CCI-CAMPUS.LAN
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
CCI-CAMPUS\
Nathalie B

On ajoute maintenant les users dans leurs groupes respectifs :

GRP1 :

GRP2 :

On créer aussi un compte Admin de secours :

On l'ajoute dans le groupe Administrateur :

d) DNS

On va maintenant configurer notre DNS :

On se rend dans l'onglet « outils » et « DNS » :

On fait un clic droit sur notre serveur et on choisit configurer un serveur Dns :

Suivant,

On choisit la zone directe :

Suivant,

Suivant,

On rentre le nom de la zone :

Suivant,

Suivant,

On rentre l'ip de notre serveur DNS :

Suivant,

On peut créer les hôtes de nos serveur et routeurs :

On clique sur nouvel hôte (A ou AAA) :

Pour RTE-STG01 :

Pour SRV-STG02 :

Pour le STG-NAS01 :

Et pour les postes :

On peut retrouver nos hôtes via le cmd avec la commande nslookup :

Exemple sur RTE-STG01 :

```
C:\Users\Administrateur>nslookup
DNS request timed out.
    timeout was 2 seconds.
Serveur par dÚfaut :   UnKnown
Address:  ::1

> RTE-STG01
Serveur :   UnKnown
Address:  ::1

Nom :    RTE-STG01.CCI-CAMPUS.LAN
Address:  192.168.100.1
```

On peut maintenant essayer d'accéder en web à notre routeur RTE-STG01 grâce à son nom :

e) DHCP

On installe d'abord le rôles DHCP :

On se rend dans l'assistant ajout de rôles et fonctionnalités :

On clique sur ajouter des fonctionnalités, puis sur suivant jusqu'à l'installation.
Une fois fait, on peut cliquez sue le drapeau et faire « terminer la configuration DHCP » :

Suivant,

On peut laisser tel quel et valider :

On ferme.

On a maintenant accès à l'outils DHCP que l'on peut ouvrir :

On fait un clic droit sur notre serveur puis sur ipv4 et on choisit l'option créer une nouvelle étendue :

On entre le nom de l'étendu :

On va définir l'étendu de la plage d'adresse IP :
Ici elle sera de 192.168.100.5 à 192.168.100.100 pour les postes clients

On ne va pas mettre d'adresse exclues :

Suivant,

On met ensuite un bail d'une durée de 30 jours :

Suivant,

Suivant,

On précise quel routeur doivent utiliser nos clients :

Assistant Nouvelle étendue
Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.
Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.
Adresse IP
Ajouter
192.168.100.1
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler

Suivant,

Assistant Nouvelle étendue
Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.
Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.
Domaine parent :
CCI-CAMPUS.LAN
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.
Nom du serveur :
Adresse IP :
Ajouter
Résoudre
192.168.1.53
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler

Suivant,

On laisse les paramètres WINS par default,

Suivant,

Suivant,

On constate que notre étendu est bien créée et actif :

On peut maintenant vérifier le bon fonctionnement du DHCP.

On se rend sur notre client Windows 10 STG-POSTE-P01 :

On voit que le DHCP est activé et qu'il a attribué l'IP 192.168.100.5 qui est la première adresse disponible de notre étendu.

f) Mise en place DFS DFS-R

1. Depuis le gestionnaire de serveur, cliquer sur Ajouter des rôles et des fonctionnalités.

2. Au lancement de l'assistant, cliquer sur le bouton Suivant

3. Choisir Installation basée sur un rôle ou une fonctionnalité et cliquer sur Suivant.

4. Sélectionner le serveur puis cliquer sur Suivant.

5. Cocher la case Espace de nom DFS qui se trouve dans Services de fichiers et de stockage / Services de fichiers et iSCSI.

6. Valider en cliquant des fonctionnalités en cliquant sur Ajouter des fonctionnalités.

8. Cliquer sur Suivant

9. Passer la section Fonctionnalités en cliquant sur Suivant

10. Démarrer l'installation en cliquant sur le bouton Installer

L'administration du rôle se fait à l'aide de la console Gestion du système de fichier distribués DFS.

1. Depuis la console « Gestion du système de fichier distribués DFS » cliquer sur Nouvel espace de nom … qui se trouve dans la partie Actions.

2. Entrer le nom du serveur qui hébergera l'espace de nom puis cliquer sur Suivant.

3. Entrer le nom du partage racine puis cliquer sur Suivant.

4. Choisir l'option Espace de nom de domaine puis cliquer sur Suivant.

Un espace de nom de domaine permet l'accès au dossier par une adresse de type : \\nom-de-domaine\partage-racine\dossier-partagé.

5. Cliquer sur le bouton Créer

6. Une fois créé, cliquer sur Fermer pour quitter l'assistant.

7. Le namespace est disponible dans la console d'administration. Vous pouvez dès maintenant accéder au partage \\domaine-ad\partage.

8.En cliquant sur l'espace de nom et en allant sur l'onglet Serveurs d'espace de noms, il est possible de voir le chemin d'accès au serveur.

g) Ajout d'un serveur d'espace de nom

1. Depuis la console d'administration Gestion du système de fichier distribués, faire un clic droit sur l'espace de nom et cliquer sur Ajouter un serveur d'espace de nom …

2. Entrer le nom du serveur puis cliquer sur OK

h) Ajout de dossiers partagé

Dans cette partie nous allons voir comment ajouter un dossier partagé.

Le dossier sera accessible à l'adresse suivante : \\domaine-ad\namespace\dossier.

Prérequis :

- Le dossier doit déjà être partagé.

Pour illustrer le tutoriel, nous allons ajouter dans un dossier Informatique qui est partagé sur le serveur LAB-FIC1.

1. Depuis la console, faire un clic droit sur l'espace de nom et cliquer sur Nouveau dossier…

2. Entrer le nom du dossier dans le namespace puis cliquer sur Ajouter.

3. Saisir le nom du serveur, cliquer sur le bouton Afficher les dossiers partagés, sélectionner le dossier et appuyer sur OK.

4. Cliquer sur OK

5. Cliquer sur OK

6. Le dossier est ajouté

i) DFS-R configuration de la réplication

1. Depuis la console, faire un clic droit sur Réplication puis cliquer sur Nouveau groupe de réplication

2. Choisir Groupe de réplication multi-usage et cliquer sur Suivant.

3. Entrer le nom du groupe de réplication, sélectionner le domaine puis cliquer sur Suivant.

4. Ajouter les serveurs membres du groupe de réplication et cliquer sur Suivant.

5. Choisir la topologie en maille pleine et cliquer sur Suivant.

6. Sélectionner réplication en continu et cliquer sur le bouton Suivant.

7. Choisir le membre principal pour la réplication puis cliquer sur Suivant.

6.2) Création du Routeur / Firewall Opensense Strasbourg

a) Information du serveur

Nom du serveur : **RTE-STG01**

Interfaces IP :

- LAN : 192.168.100.1
- WAN : dhcp

Taille disque dur : 20 GB

RAM : 512 MO

Version : OpenSense : 22.1.2

b) Création de la VM

On commence la création de la Vm :

Dès la phase de démarrage finis, on arrive sur cette interface :

On se connecte avec le compte « installer » pour débuter l'installation.

Login : installer
MDP : opnsense

On va cliquer sur la barre espace à la ligne « France » et ensuite faire entrer pour continuer

On fait entrée sur la ligne « install (UFS) »

On choisit « proceed anyway »

On choisit notre disque virtuel

Yes

Une fois l'installation terminé, on peut changer le mot de passe de root et ensuite choisir l'option « complete install » :

On arrive ensuite sur l'interface principale du serveur :

Et on se connecte avec le compte par default :

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

 LAN (em0)       -> v4: 192.168.1.1/24
 WAN (em1)       -> v4/DHCP4: 0.0.0.0/8

 HTTPS: SHA256 67 10 C2 39 5F 1A BE E6 14 C0 D9 23 2E 6F 06 8C
               42 F6 5F 46 DD 5C 32 77 6E 9D 9E 90 34 E9 F5 86
 SSH:   SHA256 toShFTJN0oREDPi0W7LFje5iu5mJoLa8ip4rtunHMH0 (ECDSA)
 SSH:   SHA256 mywi60vxiu17xcNnSiPSoct5Ruqn9imHvF4vFrcAqUI (ED25519)
 SSH:   SHA256 uglG4nYNXHbLwOb85F4GNKQPY2B+I34CfqiLP1vesR8 (RSA)

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

Login : root
Mdp : opnsense

c) Configuration réseau

On va maintenant assigner les interfaces et changer l'ip de nos cartes réseaux.

Pour ce faire on va entrer l'option « 1 » :

```
Do you want to configure LAGGs now? [y/N]: n
```

```
Do you want to configure VLANs now? [y/N]: n
```

On va choisir la carte « em0 » pour l'interface WAN

```
Enter the WAN interface name or 'a' for auto-detection: em0
```

Et la carte « em1 » pour l'interface LAN

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1
```

Ensuite on confirme avec « y »

```
The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed? [y/N]: y
```

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

LAN (em1)       -> v4: 192.168.1.1/24
WAN (em0)       -> v4/DHCP4: 172.20.10.3/28
```

On change maintenant l'ip du LAN :

On choisit l'option « 2 »,

```
Enter an option: 2

Available interfaces:

1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

On choisit le LAN,
On refuse le DHCP et on rentre l'ip statique et le masque :

```
Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

On refuse ensuite le reste :

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
```

La configuration est maintenant terminée :

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

 LAN (em1)       -> v4: 192.168.100.1/24
 WAN (em0)       -> v4/DHCP4: 172.20.10.3/28
```

snapshot prise

d) Configuration général

On peut maintenant accéder à notre routeur via un accès web avec notre client Windows

On peut commencer la configuration générale du serveur en cliquant sur le bouton « next » :

On va rentrez les informations suivantes :

Next,

Next,

On laisse tout par default sauf le serveur dhcp :

On laisse par default et next

On peut maintenant sauvegarder les changements et quitter.

snapshot prise

e) Mise en place VPN IPSEC

On va tout d'abord créer les règles firewall, pour ce faire, on va se rendre dans l'onglet « pare-feu → règles → WAN ».

On autorise le Protocol ESP, le port 500 et le port 4500 sur l'interface WAN :

Ensuite, on se rend dans l'onglet « VPN → IPSec → Paramètre du Tunnel » :

Et on coche la case « activer IPSec » tout en bas :

On va maintenant configurer notre tunnel en cliquant sur le « + » à droite.

On rentre notre passerelle distante qui est le WAN du routeur de Mulhouse,

ID du correspondant	Adresse IP du correspondant
Clé Pré-Partagée (PSK)	12345
Proposition Phase 1 (Algorithmes)	
Algorithme de chiffrement	256 bit AES-GCM with 128 bit ICV
Algorithme de hachage	SHA256
Groupe de clé DH	14 (2048 bits)
Durée de vie	28800
Options avancées	
Installe les politiques	☑
Désactiver le Renouvellement de clé	☐
Désactiver Réauthentification	☐
Isolation de tunnel	☐
SHA256 96 Bit Truncation	☐
NAT Traversant	Activer
Désactiver MOBIKE	☐

On rentre notre clé de cryptage qui est ici « 12345 », puis on Save.

Phase 1

Recherche 7

Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
☑	IPv4 IKEv2	172.20.10.3		256 bit AES-GCM with 128 bit ICV + SHA256 +...	

« ‹ 1 › »

Affichage des entrées 1 à 1 sur 1

On clique sur « ajouter une phase 2 »,

On entre l'adresse réseau de l'interface LAN du site de Mulhouse :

On change l'algorithmes de chiffrement en AES256 et l'algorithmes de hachage en SHA256 :

On Save.

Ce qui nous donne ça :

On va maintenant se rendre dans l'onglet « vue globale des statuts » et cliquez sur le bouton « start » à droite sur les 2 serveurs :

Une fois fait, on aperçoit que nos 2 serveurs sont bien reliés :

f) Mise en place du portail captif

On va tout d'abord ajouter un interface réseau à notre sur notre serveur qui hébergera le portail captif (ici RTE-STG01) :

On se rend dans l'onglet : Interface → assignations

On clique sur le + ce qui va nous créer l'interface OPT1 :

On save.

On clique sur « OPT1 », on arrive sur son interface :

On coche « activer l'interface ».

On choisit ensuite un type de configuration ipv4

Et on rentre l'adresse de la carte :

On va ensuite activer le dhcp notre interface GuestNet. On se rend dans l'onglet Services → DHCPv4 → GuestNet :

On rentre les informations suivantes :

Et on sauvegarde.

On peut maintenant configurer nos règles firewall sur notre interface :

On créer une règle qui laisse passer le DNS :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description
								Automatically generated rules
	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS

On ajoute une règle qui ouvre tous les ports de 8000 à 10000 pour l'authentification du portail captif :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description
								Automatically generated rules
	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS
	IPv4 TCP	GuestNet net	*	GuestNet adresse	8000 - 10000	*	*	Allow Captive Portal Login

On ajoute une règle qui bloque l'accès au réseau LAN depuis le GuestNet

	IPv4 *	GuestNet net	*	LAN net	*	*	*	Block Local Networks

Ce qui nous donne les règles suivantes :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description
								Automatically generated rules
	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS
	IPv4 TCP	GuestNet net	*	GuestNet adresse	8000 - 10000	*	*	Allow Captive Portal Login
	IPv4 *	GuestNet net	*	LAN net	*	*	*	Block Local Networks
	IPv4 *	GuestNet net	*	*	*	*	*	

autoriser	bloquer	rejeter	tracer	entrant	première correspondance
passer (désactivé)	bloquer (désactivé)	rejeter (désactivé)	tracer (désactivé)	sortant	dernière correspondance

Une fois les règles FW créée, on peut se rendre dans l'onglet : Services → Portail Captif → Administration

On clique sur le + pour créer notre portail captif,

On rentre les informations suivantes et on save.

On va maintenant créer un modèle pour l'interface d'authentification du portail captif, on se rend dans l'onglet « Modèles » :

On clique sur « download default template »

On import ensuite le modèle télécharger en cliquant sur le +.

On va maintenant limiter la bande passante utilisable par les potes clients.

On se rend dans l'onglet « pare-feu → Shaper → Tuyaux » :

On clique sur le +,

On créer un « Tuyau » de 10 Mbit/S pour la bande passante des téléchargements :

Et un autre de 1 Mbit/S pour l'upload :

On créer ensuite des règles :

On clique sur +.

On a donc la règles pour la cible « Download »,

Et la règles pour la cible « upload ».

On save et on applique.

On créer maintenant le « Bon d'échange », on se rend dans « Système → Accès → Serveurs :

On clique sur le +.

On rentre les informations suivantes :

On save.

Ensuite on se rend dans :

On clique sur « créer des bons d’échange »,

On créer un bon d'échange d'une validité de 1 jour qui n'expire jamais.

Une fois qu'on a cliqué sur générer, on arrive sur cette page et un fichier CSV se télécharge :

On retrouve dans notre CSV les Informations des comptes :

20221230142437 - Bloc-notes

Fichier Edition Format Affichage Aide

```
username,password,vouchergroup,expirytime,validity
"mY2XXfQn","sZHhYVAu","20221230142437","0","86400"
"vgVqN4Zn","brbKqYkc","20221230142437","0","86400"
"snMhWPCf","JDAmbfJ3","20221230142437","0","86400"
"nF2nbDgY","HYWL4KWJ","20221230142437","0","86400"
"AnK7fMGp","waTLVAUV","20221230142437","0","86400"
"6nVGBJt8","ihM7nFdQ","20221230142437","0","86400"
"FsW8NABd","BYmH2SYn","20221230142437","0","86400"
"uQzLbtiU","M6J3fjyG","20221230142437","0","86400"
"mdgcTUhg","Ym998JRn","20221230142437","0","86400"
"QJQDCbGd","RKwSRfCZ","20221230142437","0","86400"
"AXQQFX4R","4DJXLJnE","20221230142437","0","86400"
"H4LkfhsF","D2yB897V","20221230142437","0","86400"
"iUBFbeui","cuSQHm3j","20221230142437","0","86400"
"H24sfh3D","uCnnBDJY","20221230142437","0","86400"
"VmChW99k","hz2upQSw","20221230142437","0","86400"
"SnCLL7sK","G7BCJNnw","20221230142437","0","86400"
"vVfwiGmm","b8MTzDYb","20221230142437","0","86400"
"JxhbbAEi","AYMMJZMh","20221230142437","0","86400"
"6FrBMsiC","frTHHm8r","20221230142437","0","86400"
"WUWedBMS","FQtcTbi4","20221230142437","0","86400"
"2WBM4irL","9Qh2HTM2","20221230142437","0","86400"
"ViFG4mQq","qyJShmbQ","20221230142437","0","86400"
"JJ3bQLsb","pAsXAhm7","20221230142437","0","86400"
"4g2qtWnL","3inWTS7z","20221230142437","0","86400"
"tW7DWMYL","DhSSYB7f","20221230142437","0","86400"
```

On peut retourner dans l'onglet administration du portail captif et le modifier :

On peut maintenant mettre notre bon d'échange comme méthode d'authentifications :

et choisir notre modèle précédemment créer :

Nous pouvons à présent essayer d'ouvrir une page web avec notre client Windows :

L'accès au web nous demande bien une authentification.

Le portail captif est bien mis en place.

6.3) Création du Routeur / Firewall Opensense Mulhouse

a) Information du serveur

Nom du serveur : **RTE-MUL01**

Interfaces IP :
- LAN : 192.168.200.1
- WAN : dhcp

Taille disque dur : 20 GB

RAM : 512 MO

Version d'OpenSense : 22.1.2

b) Configuration réseau

On va maintenant assigner les interfaces et changer l'ip de nos cartes réseaux.
Pour ce faire on va entrer l'option « 1 » :

```
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

On va choisir la carte « em0 » pour l'interface WAN

```
Enter the WAN interface name or 'a' for auto-detection: em0
```

Et la carte « em1 » pour l'interface LAN

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1
```

Ensuite on confirme avec « y »

```
The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed? [y/N]: y
```

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

LAN (em1)       -> v4: 192.168.1.1/24
WAN (em0)       -> v4/DHCP4: 172.20.10.3/28
```

On change maintenant l'ip du LAN :

On choisit l'option « 2 »,

```
Enter an option: 2

Available interfaces:

1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

On choisit le LAN,

On refuse le DHCP et on rentre l'ip statique et le masque :

```
1 - LAN (em1 - static)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.200.1

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

On refuse ensuite le reste :

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
```

La configuration est maintenant terminée :

```
LAN (em1)       -> v4: 192.168.200.1/24
WAN (em0)       -> v4/DHCP4: 0.0.0.0/8
```

snapshot prise

c) Configuration générale

On peut maintenant accéder à notre routeur via un accès web avec notre client Windows

On peut commencer la configuration générale du serveur en cliquant sur le bouton « next » :

On va rentrez les informations suivantes :

Next,

Next,

On rentre nos serveurs DNS :

On change le mot de passe du compte root :

On peut maintenant sauvegarder les changements et quitter.
snapshot prise

d) Mise en place VPN IPSEC

On va tout d'abord créer les règles firewall, pour ce faire, on va se rendre dans l'onglet « pare-feu → règles → WAN ».

On va autoriser le Protocol ESP, le port 500 et le port 4500 sur l'interface WAN :

Ensuite, on se rend dans l'onglet « VPN → IPSec → Paramètre du Tunnel » :

Et on coche la case « activer IPSec » tout en bas :

On va maintenant configurer notre tunnel en cliquant sur le « + » à droite.

On rentre notre passerelle distante qui est le WAN du routeur de Strasbourg,

ID du correspondant	Adresse IP du correspondant
Clé Pré-Partagée (PSK)	12345
Proposition Phase 1 (Algorithmes)	
Algorithme de chiffrement	256 bit AES-GCM with 128 bit ICV
Algorithme de hachage	SHA256
Groupe de clé DH	14 (2048 bits)
Durée de vie	28800
Options avancées	
Installe les politiques	☑
Désactiver le Renouvellement de clé	☐
Désactiver Réauthentification	☐
Isolation de tunnel	☐
SHA256 96 Bit Truncation	☐
NAT Traversant	Activer
Désactiver MOBIKE	☐

On rentre notre clé de cryptage qui est ici « 12345 », puis on Save.

VPN: IPsec: Paramètres du Tunnel

Phase 1

Recherche 7

Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
☑ ☑	IPv4 IKEv2	172.20.10.4		256 bit AES-GCM with 128 bit ICV + SHA256 +...	

« ‹ 1 › »

Affichage des entrées 1 à 1 sur 1

On clique sur « ajouter une phase 2 »,

On entre l'adresse réseau de l'interface LAN du site de Mulhouse :

On change l'algorithmes de chiffrement en AES256 et l'algorithmes de hachage en SHA256 :

Protocole	ESP
Algorithmes de chiffrement	AES256
Algorithmes de hachage	SHA256 Note: For security reasons avoid the use of the SHA1 algorithm.
Groupe de clés PFS	off
Durée de vie	3600 secondes
Options avancées	
Ping automatiquement l'hôte	
Entrées SPD manuelles	
	Sauvegarder

On peut save.

Ce qui nous donne ça :

VPN: IPsec: Paramètres du Tunnel

Phase 1

Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
☑	IPv4 IKEv2	172.20.10.4		256 bit AES-GCM with 128 bit ICV + SHA256 +...	

Affichage des entrées 1 à 1 sur 1

Phase 2

Activé	Type	Sous-réseau local	Sous-réseau distant	Phase 2 Proposal	Co
☑	ESP IPv4 tunnel	LAN	192.168.100.0/24	AES256 + SHA256	

Affichage des entrées 1 à 1 sur 1

On va maintenant se rendre dans l'onglet « vue globale des statuts » et cliquez sur le bouton « start » à droite sur les 2 serveurs :

Une fois fait, on aperçoit que nos 2 serveurs sont bien reliés :

Notre VPN IPSec est maintenant opérationnel et en place.

6.4) Serveur de Sauvegarde SAN et cliché instantané Shadow copy

a) Installation du serveur TrueNas

Appuyer sur Entrée

Appuyer sur tab pour sélectionner Yes et appuyer sur entrée

Appuyer sur espace pour sélectionner et appuyer sur Entrée

Appuyer sur Entrée et garder par défaut

Entrer un mot de passe pour le root

Garder par défaut et appuyer sur Entrée

Appuyer sur entrée

Sélectionner 3 et appuyer sur Entrée pour redémarrer le système.

Cliquer sur Périphérique et aller dans lecteurs optiques pour éjecter le disque du lecteur
Ensuite reboot

b) Configuration de TrueNas

Pour créer une « POOL » aller dans « Storage » puis cliquer sur « ADD ».

Dans le panneau latéral, cliquer sur **« Storage »** puis **« Pools »**.

Cliquer ensuite sur le bouton **« ADD »** en haut à droite.

1- Renseigner le nom du Pool dans le champ **« Name »**.
2- Faire basculer le ou les disques de gauche **Available Disks** à droite **Data VDevs**.
3- TrueNAS vous propose un **type de vDev** en fonction du nombre de disques.
4- Une estimation de la taille finale (après construction du RAID) est également affichée.
5- Cliquer sur **« CREATE »**.

Cocher la case **« Confirm »**.
Cliquer sur **« CREATE POOL »**.

Création des Datasets dans TrueNAS

Création du Dataset « PUBLIC » (Qui sera accessible par tous les utilisateurs) :
Cliquer sur les **« … »** à droite du Dataset.
Cliquer sur **« Add Dataset »**.

Name : Renseigner le nom du Dataset.
Comments : Renseigner une description pour ce Dataset.
Share Type : Choisir le type de partage. Il faudra choisir **« SMB »** pour un partage **Windows**.
Cliquer sur **« SUBMIT »** pour valider.

Configuration des permissions :
Cliquer sur les **« … »**.
Cliquer sur **« Edit ACL »**.

Cliquer sur **« ADD ACL ITEM »**.

Se rendre dans **« Accounts »**, **« Groups »** et cliquer sur **« ADD »** :

Name : ADMIN**.**
Cliquer sur **« SAVE »**.

Se rendre dans **« Accounts »**, **« Users »** et cliquer sur **« ADD »** :

Auxiliary Groups : Sélectionner les groupes d'appartenances :
– **builtin_administrators** uniquement pour les **Admnistrateurs** (Paul).
– Les utilisateurs seront automatiquement ajoutés au groupe **builtin_users**.

Sélectionner le répertoire d'accueil de l'utilisateur.
Cocher la case **« Microsoft Account »** si l'utilisateur se connectera principalement depuis une machine Windows.
Cocher la case **« Permit Sudo »** uniquement pour les administrateurs.
Cocher la case **« Permit Sudo »** uniquement pour les administrateurs.
Un conseil : Ne pas toucher à la partie **« Home Directory Permissions »**.
Répéter l'opération pour les autres utilisateurs.

Cliquer sur **« SUBMIT »**

c) Activation des clichés instantanés

1. Ouvrir l'explorateur Windows, faire un clic droit sur la partition où les clichés instantanés sont à activer

Et cliquer sur Configurer les clichés instantanés.

2. Avant d'activer les clichés instantanés, cliquer sur Paramètres

3. D'ici, il est possible de configurer l'espace alloué aux clichés instantanés (plus l'espace est grand, plus il y aura de point de restauration). Il est aussi possible de gérer la planification, cliquer sur le bouton Planifier

4. Par défaut, il y a deux clichés de configurer à 7H et 12H, le LMMJV

6. Maintenant que les clichés sont paramétrés, cliquer sur Activer

7. Confirmer l'activation en cliquant sur Oui

8. Les clichés instantanés sont maintenant activés, un premier cliché est fait lors de l'activation.

d) Utilisation des versions précédentes

L'accès aux versions précédentes est disponible à l'aide de l'Explorateur Windows sur les clients (W7/8/10) et sur les Serveur (2008/2012/2016/2019…). Elles sont disponibles aussi bien locale que par les partages réseaux et par défaut sont accessibles à tout le monde.

1. Depuis l'explorateur Windows, aller sur le dossier où l'on souhaite restaurer le fichier et faire un clic droit dessus. En fonction de l'emplacement et du système deux options sont disponibles, cliquer sur :

- Restaurer les versions précédentes
- Propriétés

2. Si l'on passe par Propriétés, aller sur l'onglet Versions précédentes. Choisir le point de restauration à explorer et cliquer sur Ouvrir.

Nos clichés instantanés sont maintenant en place et opérationnelle.

Fin de Procédure