

Rapport de stage

13 mai 2024 - 14 juin 2024

Entreprise : Linkwe

Etablissement : Saint paul bourdon blanc

TABLE DES

Matière

01	Page de garde
02	Sommaire
03	Présentation de l'entreprise
06	Outils utilisés
08	Missions réalisées lors du stage
16	Conclusion
17	Annexe rapport journalier
19	Annexe audit
22	Annexe trunk
31	Annexe VPN

Présentation d'entreprise

Linkwe est une entreprise spécialisée dans le Cloud, le réseau et la télécommunications.

Créeé en 2019, elle s'efforce de fournir des services innovants pour améliorer la connectivité et la téléphonie des entreprises.

Mission

Linkwe veut fournir des solutions de connectivité fiables, rapides et sécurisées, tout en innovant constamment. Leur objectif est de répondre aux besoins croissants de communication numérique en Entreprise

Produits et Services

Linkwe offre une gamme variée de produits et services, notamment :

Solutions de Réseau Haut Débit : Fourniture d'Internet haut débit pour les entreprises et les particuliers de la région.

Technologies de Connectivité : Développement et mise en place de solutions de connectivité avancées pour améliorer la communication.

Services de Sécurité Réseau : Mise en œuvre de services de cybersécurité pour protéger les données et les communications des clients.

Support Technique et Maintenance : Assistance technique et maintenance pour garantir le bon fonctionnement des solutions de connectivité.

Moyens Informatiques de l'Entreprise

Pour soutenir ses activités, Linkwe dispose de plusieurs solution informatiques :

- Infrastructure Réseau :

Serveurs dédiés et virtualisés pour héberger les services internes et clients.

Systèmes de sauvegarde et de récupération pour garantir la continuité des services.

Équipements de réseau modernes (routeurs, switches) pour assurer une connectivité rapide et fiable.

- Sécurité Informatique :

Firewalls et systèmes de détection d'intrusion pour protéger les réseaux.

Logiciels antivirus et anti-malware pour sécuriser les terminaux.

Politiques de sécurité strictes et audits réguliers pour maintenir la sécurité des données.

- Services Cloud :

Utilisation de plateformes cloud pour le stockage et la gestion des données.

Solutions de collaboration en ligne pour faciliter le travail d'équipe et la communication.

- Support et Maintenance :

Équipe de support technique disponible pour assister les clients.

Protocoles de maintenance préventive pour assurer le bon fonctionnement des systèmes.

Linkwe

Direction

Ressource Humaine
Gestion Administrative
ADV

Blandine CHABERT D HIERES
OWNER

Hugues CHABERT D HIERES
OWNER

Commerce

Eymeric PEROUSE
Commerce

Jérôme Spée
Agent

Méryl DELON
CdP

Fabrice Boffy
Support

Jérémy MESTRE
Support

Kevin REBILLARD
Support

Raymond Flandin
CdP

Hyacinthe F.R
Alternant

Mathéo B
Alternant

Aymen BATROOZI
Alternant

Support

ORGANIGRAMME

Outils utilisés

1. Sofia par Sewan

Sofia est un outil développé par Sewan, un fournisseur de services télécom et cloud. Cet outil est généralement utilisé pour la gestion des services de télécommunication, incluant la gestion des lignes téléphoniques, la configuration des équipements réseau, et le suivi des incidents.

Fonctionnalités principales :

- Gestion des abonnements et des services télécom : Configuration et suivi des services téléphoniques et internet pour les clients.
- Supervision réseau : Suivi en temps réel des performances du réseau et identification des incidents.
- Support client : Interface pour gérer les tickets d'incidents et les demandes des clients.

2. Nebula de Zyxel

Nebula est une plateforme de gestion réseau basée sur le cloud, développée par Zyxel. Cet outil permet de gérer et de superviser à distance une infrastructure réseau, incluant des points d'accès Wi-Fi, des switches, et des routeurs.

Fonctionnalités principales :

- **Gestion centralisée des équipements réseau :** Permet de configurer et de superviser tous les équipements connectés à un réseau via une interface web.
- **Surveillance en temps réel :** Offre des informations en temps réel sur les performances du réseau et les états des équipements.
- **Maintenance à distance :** Mise à jour des firmwares et résolution des problèmes sans besoin d'une intervention sur site.

3. Winbox

Winbox est un outil de configuration pour les routeurs MikroTik. Il offre une interface graphique permettant de configurer de manière intuitive les routeurs et de gérer les paramètres réseau avancés.

Fonctionnalités principales :

- **Configuration des routeurs MikroTik :** Permet de configurer les paramètres de base et avancés des routeurs, y compris les règles de firewall, les configurations de VPN, et la gestion des utilisateurs.
- **Gestion des réseaux :** Surveillance et optimisation des performances des réseaux gérés par les routeurs MikroTik.
- **Outils de diagnostic :** Inclut des outils pour diagnostiquer les problèmes de réseau, comme les tests de ping, les traces de route, et les analyses de trafic.

Missions Réalisées

Mission 1 : Audit de Sécurité Informatique pour une Entreprise Métallurgique

Problématique : L'entreprise métallurgique utilise une trentaine de postes de travail pour contrôler ses machines-outils pour le travail des métaux. Elle souhaite optimiser l'utilisation de ses ressources informatiques et renforcer sa sécurité face aux cybermenaces croissantes. L'objectif de l'audit est d'identifier les ordinateurs, leurs fonctions respectives, et de proposer des améliorations que Linkwe peut apporter.

Étude de l'Existant

1. Identification des Postes de Travail :

- Inventaire complet des postes de travail (ordinateurs de bureau, laptops) utilisés dans l'entreprise.
- Recensement des logiciels et systèmes d'exploitation installés sur chaque poste.
- Analyse des rôles et des responsabilités des utilisateurs de chaque poste de travail.

2. Fonctions des ordinateurs :

- Identification des fonctions spécifiques de chaque poste de travail, notamment les postes utilisés pour le contrôle des machines métallurgiques.
- Évaluation des logiciels critiques pour les opérations de fabrication, tels que les logiciels de contrôle de machines CNC (Commande Numérique par Calculateur), les systèmes de gestion de production et les logiciels de conception assistée par ordinateur (CAO).

3. Pratiques Actuelles de Sécurité :

- Analyse des mesures de sécurité en place, telles que les politiques de gestion des mots de passe, les protocoles de sauvegarde des données, et les solutions antivirus.
- Identification des vulnérabilités potentielles, y compris les failles dans la protection des données et les risques liés à l'accès non autorisé.

Cahier des Charges

1. Fonctions Attendues :

- Renforcer la sécurité des postes de travail pour protéger les données sensibles et les processus de fabrication.
- Optimiser l'utilisation des ressources informatiques pour améliorer la productivité et l'efficacité opérationnelle.
- Assurer la conformité avec les normes de sécurité de l'industrie métallurgique et les régulations en matière de protection des données.

2. Contraintes :

- Minimiser les interruptions des opérations de fabrication pendant la mise en œuvre des améliorations.
- Garantir la compatibilité des nouvelles solutions de sécurité avec les systèmes existants et les logiciels critiques utilisés pour le contrôle des machines métallurgiques.
- Respecter le budget alloué et les délais définis pour la réalisation des améliorations.

Résultats Obtenus

1. Identification des Vulnérabilités :

- Les failles de sécurité ont été identifiées, y compris l'absence de politiques de gestion des mots de passe robustes, des solutions antivirus obsolètes, et des protocoles de sauvegarde insuffisants.
- Des postes de travail non protégés contre l'accès non autorisé ont été repérés, ainsi que des logiciels non mis à jour présentant des risques de sécurité.

2. Recommandations d'Améliorations :

- Mise en place de politiques de gestion des mots de passe plus strictes, incluant des exigences de complexité et des changements réguliers.
- Installation et configuration de solutions antivirus et de logiciels de sécurité à jour sur tous les postes de travail.
- Établissement de protocoles de sauvegarde réguliers et sécurisés pour protéger les données critiques.
- Renforcement des contrôles d'accès, y compris l'utilisation de pare-feux et de VPN pour sécuriser les communications internes et externes.

3. Optimisation des Ressources :

- Recommandations pour la mise à jour des logiciels critiques et des systèmes d'exploitation pour garantir la compatibilité et la performance optimale des postes de travail.
- Proposition de solutions de gestion centralisée des ressources informatiques pour améliorer l'efficacité et la réactivité en cas d'incident.

4. Conclusion :

- L'audit a permis de dresser un état des lieux précis des ressources informatiques de l'entreprise métallurgique et de proposer des recommandations pertinentes pour renforcer sa sécurité et son efficacité opérationnelle.
- En identifiant les ordinateurs, leurs fonctions et les améliorations potentielles, Linkwe a apporté des solutions adaptées aux besoins spécifiques de l'entreprise métallurgique, contribuant ainsi à son développement et à sa pérennité sur le marché. Les mesures de sécurité renforcées et l'optimisation des ressources informatiques permettent à l'entreprise de se prémunir contre les cybermenaces tout en améliorant sa productivité.

Information supplémentaire en annexe page 19

Mission 2 : Cr éation d'un Trunk Multisite en Utilisant l'Outil Sofia de Sewan

Un Trunk en t élophonie est une connexion qui permet à un s ystème t élphonique d'entreprise (PBX) de transmettre des appels vocaux via un r éseau IP, en utilisant le protocole SIP. Remplaçant les lignes t élphoniques par des connexions Internet.

Problématique : L'entreprise souhaite centraliser et optimiser sa gestion des communications t élphoniques en mettant en place un trunk multisite unique au lieu d'avoir des trunks s éparés pour chaque site. Cela vise à r éduire les coûts, simplifier la gestion et améliorer la qualit é et la s écurit é des communications inter-sites.

Étude de l'Existant :

Pour comprendre la situation actuelle et les besoins de l'entreprise, une étude approfondie de l'infrastructure t élphonique et r éseau a été menée :

1. Analyse de l'Infrastructure R éseau :

- Cartographie des Sites G éographiques : Recensement des diff érents sites de l'entreprise et de leur r épartition g éographique.
- Équipements R éseau Existants : Identification des routeurs, switches, pare-feux et autres équipements r éseau pr ésents sur chaque site.

2. Évaluation des Systèmes T élphoniques Actuels :

- PBX et T él phones : Identification des systèmes PBX (Private Branch Exchange) en place, qu'ils soient traditionnels ou IP, ainsi que des types de t él phonies utilisés (analogiques, IP).
- Usage et Capacités : Analyse des volumes d'appels, des heures de pointe et des capacités actuelles en termes de lignes et de canaux de communication.

Cahier des Charges :

Pour la mise en place d'un trunk multisite avec l'outil Sofia de Sewan, le cahier des charges a été défini pour répondre aux besoins de centralisation des communications et surmonter les contraintes techniques et opérationnelles.

Les principales exigences sont :

1.Fonctions Attendues :

- **Trunk Multisite Unique** : Mettre en place un trunk SIP unique qui dessert tous les sites de l'entreprise, au lieu de trunks séparés pour chaque site.
- **Connectivité Sécurisée et Fiable** : Assurer une connexion trunk SIP sécurisée pour garantir une communication fluide et fiable entre les différents sites.
- **Gestion Centralisée** : Utilisation de l'outil Sofia de Sewan pour une gestion centralisée des lignes SIP, permettant une configuration et une maintenance simplifiées.

2.Contraintes :

- **Compatibilité Matérielle** : Assurer que les équipements réseau et téléphoniques existants sont compatibles avec le trunk SIP.
- **Sécurité** : Implémentation de mesures de sécurité robustes pour protéger les communications vocales contre les interceptions et les attaques.
- **Qualité de Service (QoS)**: Garantir une qualité de service élevée pour les appels vocaux, en minimisant la latence, la gigue et la perte de paquets.

Résultats Obtenus :

La mise en place du trunk multisite avec l'outil Sofia de Sewan a permis d'atteindre les objectifs définis dans le cahier des charges. Les principaux résultats obtenus sont :

1. Amélioration de la Connectivité :

- **Communication Fluide** : Les différents sites de l'entreprise peuvent désormais communiquer de manière fluide et sécurisée via un trunk SIP unique.
- **Réduction des Coûts** : Les coûts de communication inter-sites ont été significativement réduits grâce à la centralisation du trunk SIP.

2. Gestion Simplifiée :

- **Interface Centrale** : La gestion des lignes SIP est centralisée via l'outil Sofia de Sewan, simplifiant les opérations de configuration et de maintenance.
- **Scalabilité Facile** : La scalabilité des canaux SIP a permis d'ajuster rapidement la capacité en fonction des besoins, sans nécessiter d'investissements matériels supplémentaires.

3. Sécurité Renforcée :

- **Protocole Sécurisé** : Les communications sont sécurisées grâce à l'utilisation de protocoles robustes et de mesures de sécurité avancées.
- **Surveillance et Maintenance** : Les mécanismes de surveillance intégrés permettent de détecter et de résoudre rapidement les problèmes potentiels, assurant une disponibilité continue des services.

4. Conclusion :

La création d'un trunk multisite avec l'outil Sofia de Sewan a permis de moderniser et de centraliser l'infrastructure téléphonique de l'entreprise, offrant une solution de communication plus efficace, sécurisée et économiquement avantageuse. En passant d'une configuration avec des trunks séparés pour chaque site à un trunk multisite unique, l'entreprise a pu réduire ses coûts, simplifier la gestion et améliorer la qualité de ses communications.

Information supplémentaire en annexe page 22

Conclusion de Stage chez Linkwe

Mon expérience de stage chez Linkwe a été une période enrichissante et formatrice. Au cours de ces 5 semaines passés au sein de l'entreprise, j'ai eu l'opportunité de découvrir de nouveaux domaines, d'acquérir des compétences précieuses et de travailler au sein d'une équipe dynamique et professionnelle.

Ce stage m'a permis de mettre en pratique les connaissances théoriques acquises au cours de mes études et de les enrichir grâce à des projets concrets.

Je tiens à exprimer ma gratitude envers toute l'équipe de linkwe pour son accueil chaleureux, son soutien constant et les précieux enseignements dispensés tout au long de mon stage.

Je repars de ce stage avec une vision plus claire de mes objectifs professionnels, une meilleure compréhension du fonctionnement d'une entreprise dans le domaine de la téléphonie, du réseau, et du cloud.

Je suis reconnaissant pour cette opportunité qui m'a été offerte et je suis convaincu que les compétences et les connaissances acquises lors de ce stage me seront précieuses dans mes projets futurs.

Je tiens également à remercier Madame Chabert d'Hières pour son encadrement attentif et ses conseils avisés tout au long de mon stage.

Enfin, je souhaite adresser mes meilleurs vœux de succès à Linkwe pour ses projets futurs.

Annexe

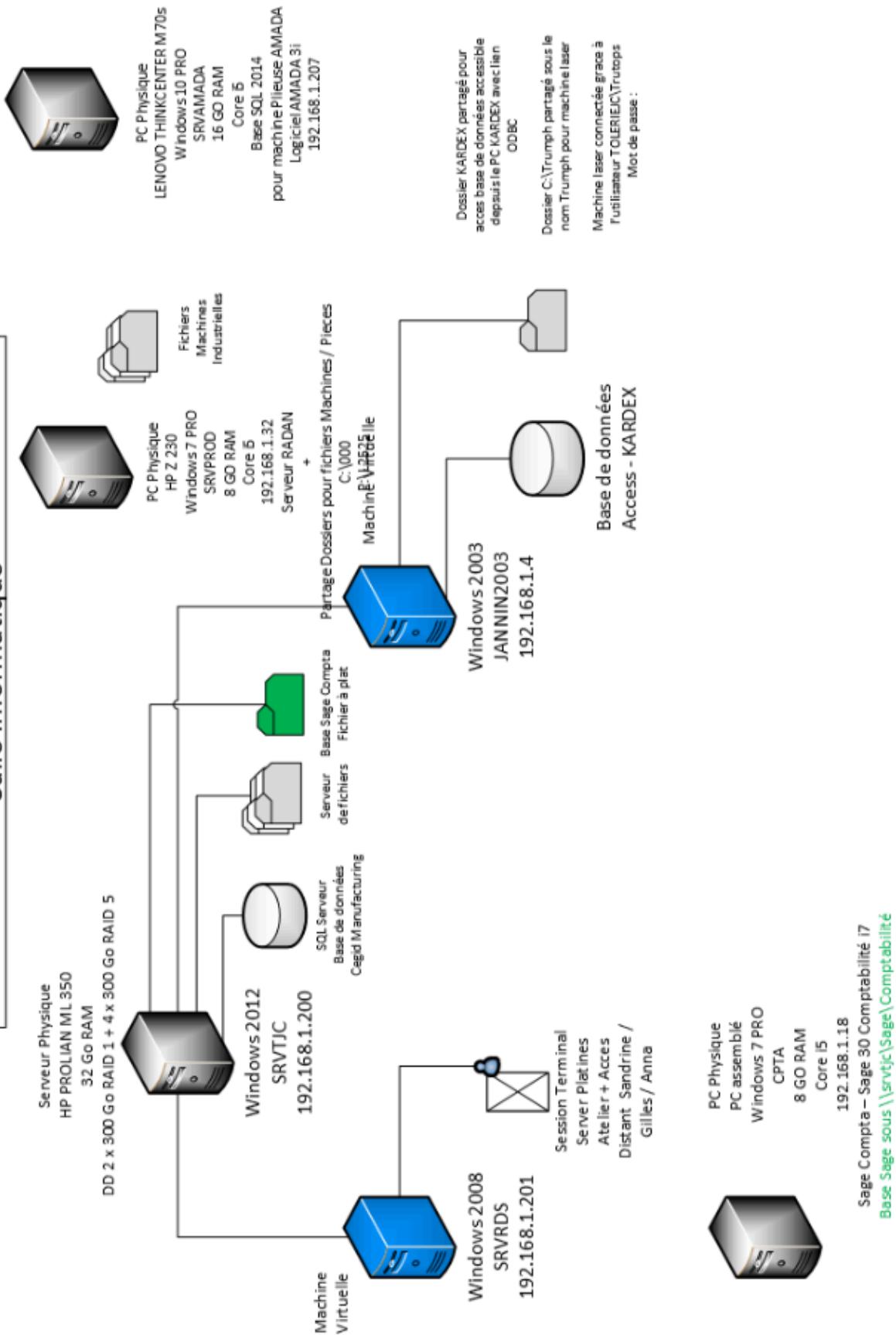
Rapport journalier

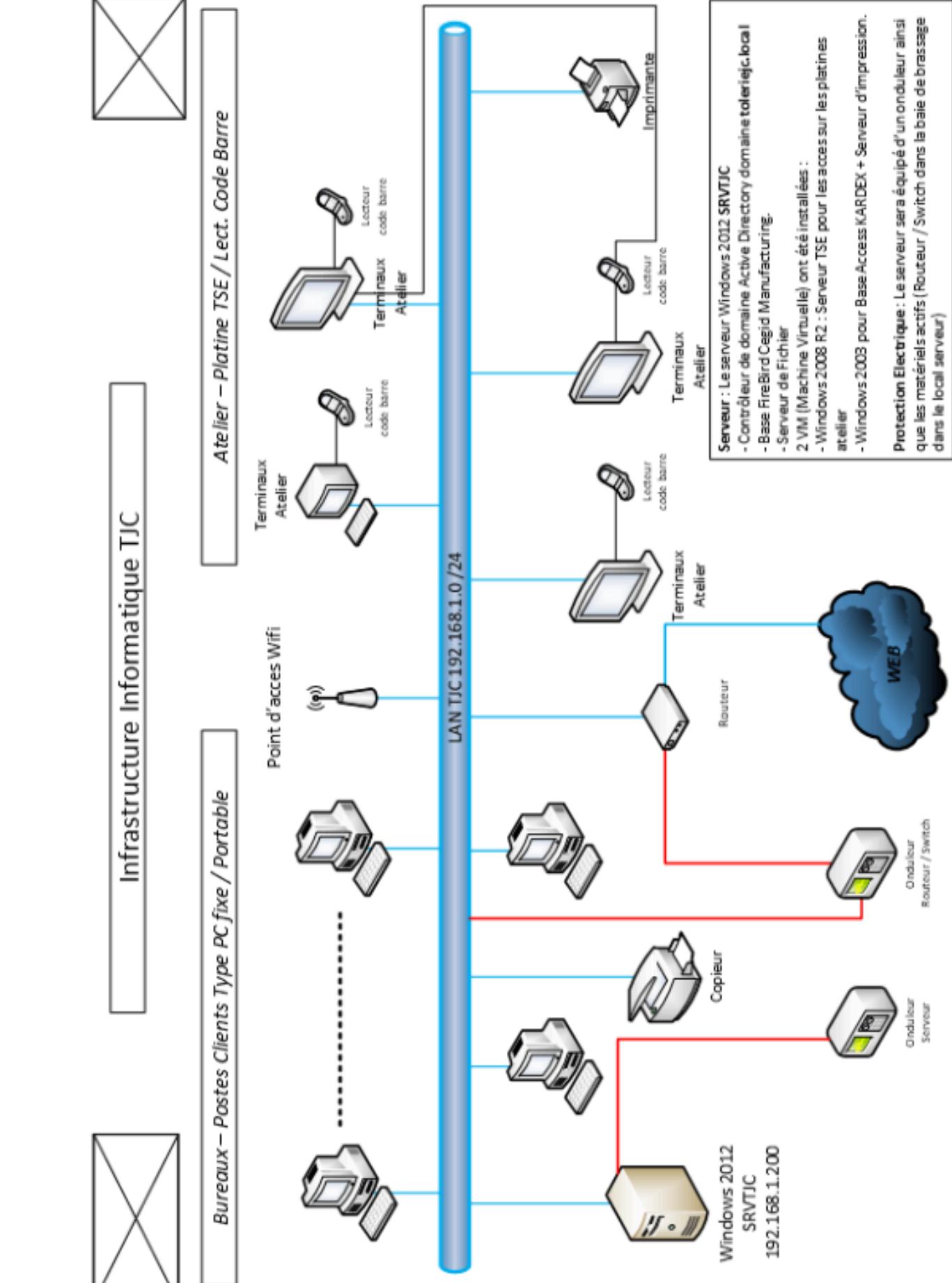
13/05/24	présentation de l'entreprise et des outil utiliser
14/05/24	Préparer des Téléphone avec Sophia(un outil de gestion), pour une entreprise, affecter chaque téléphone a une personne.
15/05/24	Création d'un VPN de supervision entre un lien client et LINKWE et lien Client et Centreon
16/05/24	installation de pc et équipement chez un client
17/05/24	installation de pc et équipement chez un client
21/05/24	reset de pare-feu (ZyXEL usg 300, ZyXEL usg 50) test d'équipement défectueux (yealink WH62) Test DECT Yealink, contrôle pour vérifier qu'il n'y a aucun bug sur l'outil SOFIA avec les appareils
22/05/24	Déplacement chez un client pour faire une audit de tous les poste existant, puis une explication au client au problématique, au solution et a l'amélioration possible sur le réseau.
23/05/24	reprise du test DECT Yealink début d'écriture du rapport et de l'oral de stage
27/05/24	mise en place d'un Trunk multisite
28/05/24	mise en place d'un routeur pour une entreprise avec Sofia
29/05/24	Ajout de lien Sofia ou Destiny sur Centreon pour superviser tous les liens

30/05/24	teste de la couverture wifi d'une borne paramétrage d'un routeur
31/05/24	reset de pare feu et mise a jour pour une future installation
03/06/24	reset de fortigate et mise a jour pour une future installation
04/06/24	Nouveaux testes sur le DECT Affectation de ligne téléphonique a un client
05/06/24	Migration de pc d'un réseau local sur azure chez le client
06/06/24	Migration de pc d'un réseau local sur azure a distance
07/06/24	Nouveaux testes sur le DECT
10/06/24	Configuration de pc pour une futur mise en place
11/06/24	Intervention chez le client pour la mise en place de pc
12/06/24	Paramétrage et teste sur un Wireless Bridge
13/06/24	Intervention chez un client en vue d'une futur installation Paramétrage de pc
14/06/24	

Audit de Sécurité

Configuration Serveur + Machines Virtuelles Salle Informatique





Nom PC	Nom utilisateur	OS 32 BIT / 64	Version Office	RAM	Processeur	DD / Free	Type de pc
KARDEX-TJC	kardex	WIN10 PRO	365 Business	8	i3	265 / 161	PC PROD
WCAT17	SALVA	WIN10 PRO	Non	16	XEON	256 / 75	PC PROD
HPZ230-1	TRUBENDMASTER	WIN 7 PRO	2007	8	i5	917 / 822	PC PROD
HPZ230-2	TRU2525	WIN 7 PRO	2007	8	i5	838 / 797	PC PROD
HPZ230-3	TRUCELL7000	WIN 7 PRO	2007	4	i5	917 / 797	PC PROD
HPZ640-1	soudaser	WIN10 PRO	Non	16	XEON	930 / 856	PC PROD
TRUETOPSRV	TRUTOPS	WIN 7 PRO	Non	8	i7		PC PROD
TJC-EXPEDITION	expedition	WIN10 PRO	365 Business	8	i3	256 / 91	PC BUREAU
HPZ22G4-1	BE	WIN10 PRO	2007	8	i5	915 / 838	PC BUREAU
HPZ230-4	BE	WIN 7 PRO	2007	8	i5	512 / 362	PC BUREAU
HPSU2IE	logistique	WIN10 PRO	2019	4	i3	256 / 124	PC BUREAU
PC-PROJET-TJC	logistique	WIN10 PRO	Non	8	i5	512 / 322	PC BUREAU
TJC-LANCEMENT	lancement-tjc	WIN10 PRO	365 Business	8	i3	256 / 79	PC BUREAU
PC-METHODE	metodes	WIN10 PRO	365 Business	16	i7	512 / 296	PC BUREAU
HP-280-3	qualite2	WIN 7 PRO	2007	4	i3	512 / 371	PC BUREAU
NOMADEGJC	controle	WIN 7 PRO	2007	8	i3	512 / 450	PC BUREAU
METHODE-LAPTOP	metodes	WIN10 PRO	365 Business	8	i5	512 / 121	PC BUREAU
CPTA	comptabilite	WIN 7 PRO	2007	8	i3	931 / 882	PC BUREAU
PC-SECRETAIRAT	secretariat	WIN10 PRO	365 Business	8	i3	256 / 116	PC BUREAU
JANNIN8	BE	WIN10 PRO	2007	8	i5	265 / 113	PC BUREAU
PCPRD2	BE	WIN 7 PRO 32 Bits	2007	2	i3	750 / 392	PC BUREAU
Z240-1	invite1	WIN 7 PRO	2007	8	i7	917 / 772	PC BUREAU
HPZBOOK-1	qualite2	WIN 7 PRO	2007	16	i7	512 / 308	PC BUREAU
PC-JFRIGEARD	respond	WIN10 PRO	365 Business	8	i5	256 / 115	PC BUREAU
NATHALIE-PC	RH	WIN 7 PRO	2007	6	i3	465 / 275	PC BUREAU

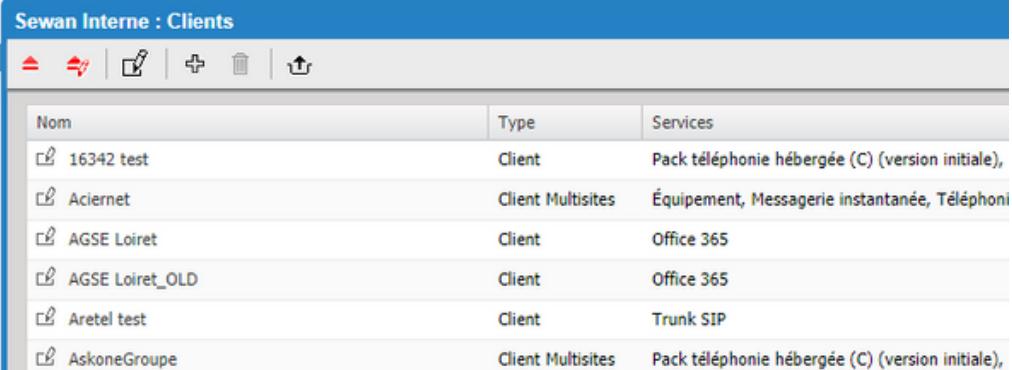
Trunk multiliste

Création d'un client Trunk Multisite

Création du client 

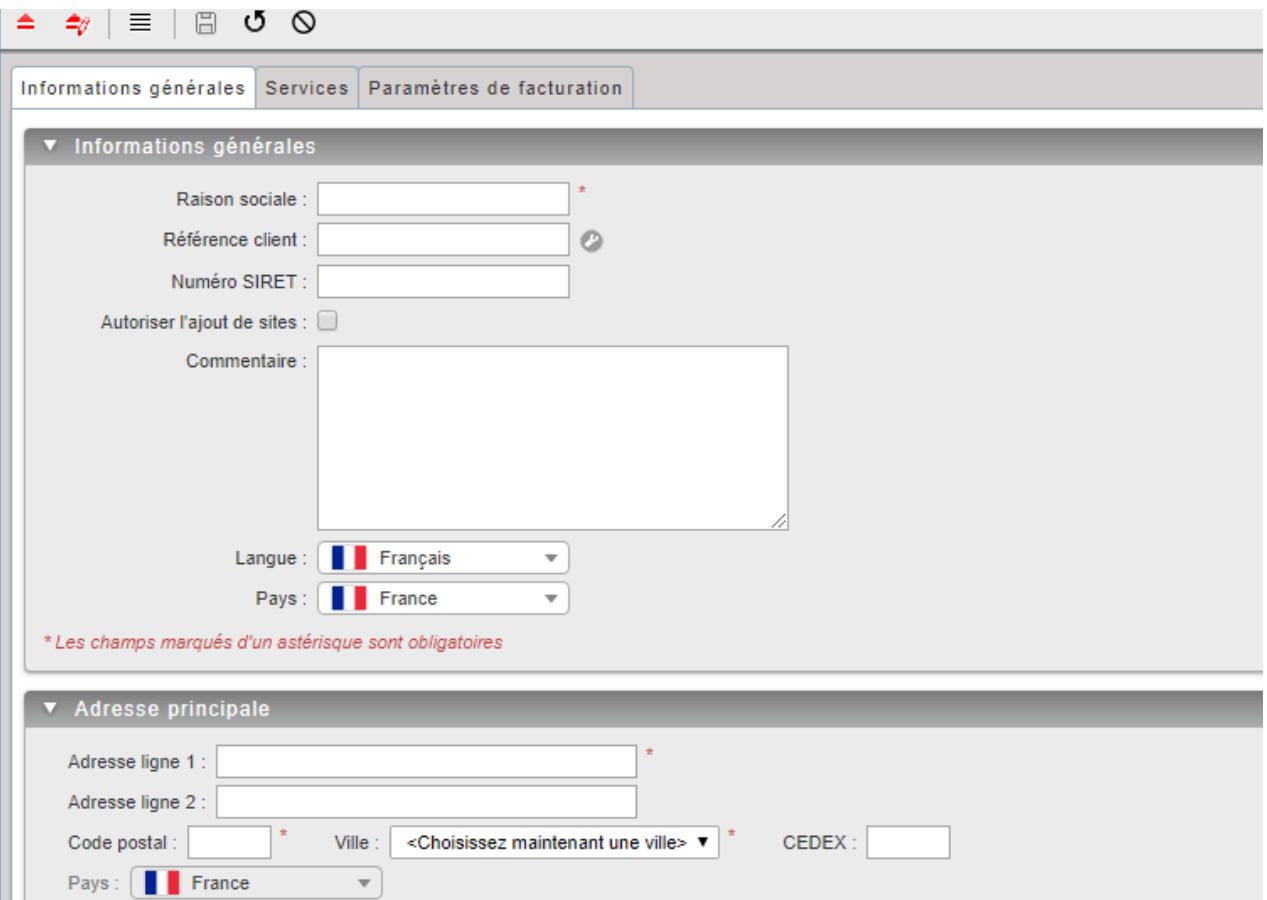
Aller dans Sophia et via le panneau de navigation cliquer sur « Clients »

Appuyer sur pour créer une entrée



Nom	Type	Services
16342 test	Client	Pack téléphonie hébergée (C) (version initiale),
Aciernet	Client Multisites	Équipement, Messagerie instantanée, Téléphonie
AGSE Loiret	Client	Office 365
AGSE Loiret_OLD	Client	Office 365
Aretel test	Client	Trunk SIP
AskoneGroupe	Client Multisites	Pack téléphonie hébergée (C) (version initiale),

La vue ci-dessous s'affiche



Informations générales Services Paramètres de facturation

Informations générales

Raison sociale : *
Référence client : 
Numéro SIRET :
Autoriser l'ajout de sites :
Commentaire :

Langue :  Français
Pays :  France

* Les champs marqués d'un astérisque sont obligatoires

Adresse principale

Adresse ligne 1 : *
Adresse ligne 2 :
Code postal : * Ville : <Choisissez maintenant une ville> * CEDEX :
Pays :  France

Remplir les champs obligatoires (marqués d'une étoile)

- Raison Sociale
- Adresse (important pour le routage des appels d'urgence)

Passer à l'onglet service

Sewan Interne : Clients [Partner guide]

Informations générales Services Prix d'achat Voix Trunk SIP illimité Paramètres de facturation

Liste des services disponibles

Trunk SIP
 Trunk Multisites illimité

Cocher les services nécessaires à l'installation du client, dans notre cas « Trunk Multisites Illimité »

Enregistrer à l'aide de la disquette

Création de l'utilisateur sous le compte client

Une fois le client créé, il faut aller créer les utilisateurs qui seront les Trunks en question.

Au niveau de la fiche client, accéder à la liste des utilisateurs en cliquant sur la flèche pointant vers le bas

Descendre au niveau du client Partner guide

Informations générales Services Prix d'achat Voix Trunk Multisites illimité Paramètres de facturation

Liste des services disponibles

Trunk SIP
 Trunk SIP illimité

La vue ci-dessous s'affiche :

Il s'agit de la liste des utilisateurs du client (vide pour le moment)

Cliquer sur 

Partner guide : Utilisateurs

Nom	Prénom	Numéro(s)	Equipement(s)

Page 1 / 0 25

La vue ci-dessous s'affiche

Informations générales Services

▼ Informations utilisateur

Civilité : Aucune	Fonction :
Nom : Partner	E-mail :
Prénom : Guide	Langue : Français
Description :	Téléphone fixe :
	Mobile :
	Numéro abrégé mobile :
	Profil : Utilisateur

* Les champs marqués d'un astérisque sont obligatoires

▼ Informations d'identification

Login : gpartner	@partnerguide.services-mobile.fr *
------------------	------------------------------------

▼ Adresse principale

<input checked="" type="radio"/> Utiliser l'adresse du compte client
<input type="radio"/> Spécifier l'adresse :
Adresse ligne 1 : 2 cité Paradis
Adresse ligne 2 :
Code postal : 75010 Ville : Paris CEDEX :

Renseigner les champs obligatoires

- Nom
- Adresse (par défaut figure l'adresse renseignée sur la fiche du client, pour la changer, cliquer sur « spécifier l'adresse »)

Passer à l'onglet service
Cocher le service « Téléphonie Fixe »

▼ Sélection des services



Téléphonie fixe

Un pop-up s'ouvre afin de rappeler l'information importante suivante.

Par défaut, le nombre maximum d'appels simultanés d'un trunk est de 8. Avant de sauvegarder la configuration du trunk, sélectionner une valeur dans l'onglet « Téléphonie fixe » sous l'encart « Type ». En cas de sauvegarde avant la sélection d'une valeur, le nombre maximum d'appels simultanés prendra la valeur par défaut.

Cliquer sur « OK » pour fermer le message d'information.

Création du Trunk Multisite

Création du Trunk Général

Le Trunk Général est le Trunk qui portera l'offre et qui devra être configuré sur l'équipement client afin que le service de Multisite fonctionne.

Une fois l'utilisateur créé il faut :

- Aller dans l'onglet « Téléphonie Fixe »
- Par défaut le Compte sera configuré en « Trunk Site » (nous nous y attarderons après)
- Choisir un Trunk Général avec le forfait désiré

Partner guide : Utilisateurs [Partner Guide] *

Informations générales Services Téléphonie fixe Statut Forfaits

Type

Type de compte : Trunk Multisites
Trunk Général - illimité national

Nombre maximum d'appels simultanés : Limité à : 2 appels

Sécurité

Authentification : Par mot de passe : Identifiant : gpartner@partnerguide.testdomainesewan.fr
Générer un nouveau mot de passe

Afficher le mot de passe après génération

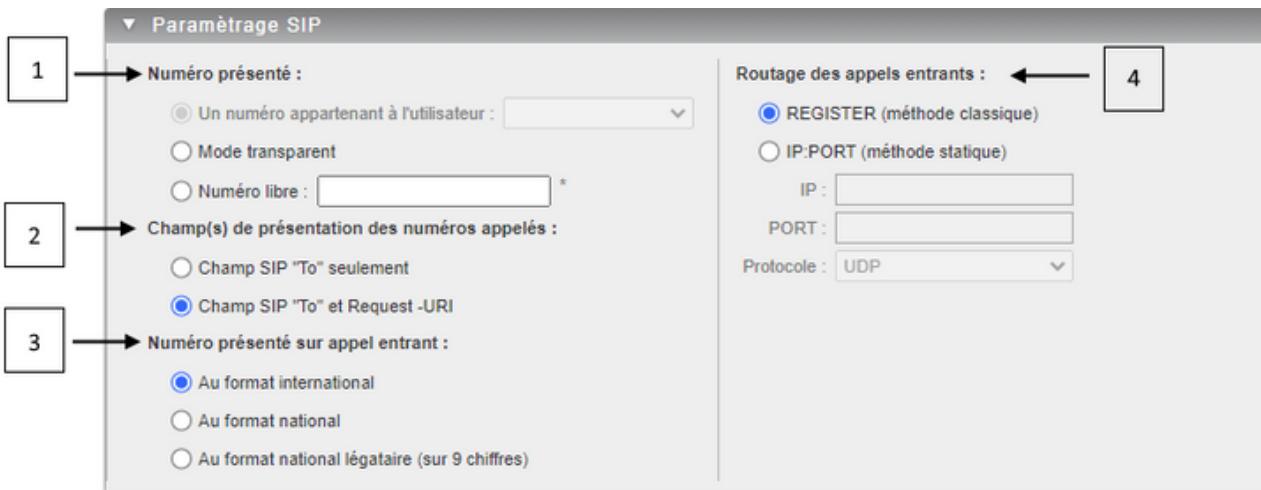
Par adresse IP :

Restrictions d'appels : Profil de restriction : --Aucun--

Paramétrage SIP

Numéro présenté : Un numéro appartenant à l'utilisateur : Mode transparent Numéro libre : *
Champ(s) de présentation des numéros appelés : Champ SIP "To" seulement Champ SIP "To" et Request-URI
Numéro présenté sur appel entrant : Au format international Au format national Au format national légataire (sur 9 chiffres)
Routage des appels entrants : REGISTER (méthode classique) IP : PORT : Protocole : UDP

1. Permet de choisir le forfait appliqué au trunk.
2. Permet de choisir le nombre de canaux désirés.
3. Il s'agit de l'onglet qui permet de choisir la méthode d'enregistrement du Trunk : Login/mdp ou par adresse IP.
4. Permet de générer un nouveau mot de passe (lorsque l'authentification par login/mdp est choisie).
5. Permet d'afficher le nouveau mot de passe généré (cocher cette case avant de générer le nouveau mot de passe)
6. Permet d'appliquer un profil de restriction (si besoin)
7. La fenêtre « Paramétrage SIP » est détaillée dans le point suivant du document.



1. Permet de gérer la présentation des numéros lors des appels sortant, soit :

- présenter un numéro faisant partie de la liste du stock (sélection via le menu déroulant)
- présenter uniquement le numéro envoyé par l'équipement du client (mode transparent)
- présenter un numéro librement défini (renseigner le champ libre prévu à cet effet)

2. Permet de gérer le champ de présentation des numéros appelés

3. Permet de gérer le format des numéros présentés

- International : +33xxxx
- National : 0xxxx

4. Méthode de routage pour les appels entrants :

- REGISTER : méthode d'authentification classique, l'équipement client vient s'enregistrer auprès de notre plateforme
- IP PORT : Méthode par routage manuel, tous les appels sont envoyés vers l'IP et le port définis

Enregistrer avec la disquette

L'utilisateur Trunk est créé.

Création de Trunk Site

Le Trunk Site est le Trunk qui sera créé pour chacun des sites et qui configurera le nombre de communications simultanées desdits sites. Ces Trunks n'auront pas à être enregistrés sur les équipements client.

Affectation du numéro au compte client

Pour obtenir des numéros, il faut au préalable passer une commande chez Sewan.

Une fois cela fait, les numéros sont disponibles dans le stock (Ressources/Numéros) du client créé.

Il est préférable de créer le client dans Sophia avant de commander les numéros.

Au niveau du client (vue sur la liste de ses utilisateurs), aller dans le menu de navigation de gauche et sélectionner : « ressources », puis « Numéros internes »

	Numéro	Service	Type	Utilisateur	Commentaire Partenaire	Routage	Date de commande
<input type="checkbox"/>	+33130050881	VoIP	- Aucun -			Routé	

Pour les affecter au compte utilisateur, aller sur la fiche de ce dernier :

Via le menu de navigation, développer « Configuration » puis cliquer sur « Utilisateurs ».

La vue sur la liste des utilisateurs du client apparaît.

Selectionner l'utilisateur cible en cliquant sur le crayon précédent son nom.

La fiche de l'utilisateur apparaît.

Via l'onglet « Téléphonie fixe », sélectionner le ou les numéros désirés parmi ceux disponibles dans le menu déroulant (numéros précédemment vus dans les ressources du client).

Attribuer le ou les numéros, et enregistrer à l'aide de la disquette

Il est possible d'attribuer tous les numéros disponibles en une seule fois avant d'enregistrer.

Partner guide : Utilisateurs [Partner Guide]

L'utilisateur a été modifié.

Informations générales Services Téléphonie fixe Statut Forfaits

Type

Type de compte : Trunk SIP Nombre maximum d'appels simultanés :

Fixe et mobile + 70 destinations Limité à : 2 appels

Numéros et équipements

Numéro(s) : Équipement(s) :

+33130050881 Stock vide

Stock vide

Partner guide : Utilisateurs [Partner Guide] *

Informations générales Services Téléphonie fixe Statut Forfaits

Type

Type de compte : Trunk Multisites Trunk Général associé : Nombre maximum d'appels simultanés :

Trunk Site Aucun Limité à : 2 appels

Numéros et équipements

Numéro(s) : Assigner :

Sécurité

Restrictions d'appels : Profil de restriction : --Aucun--

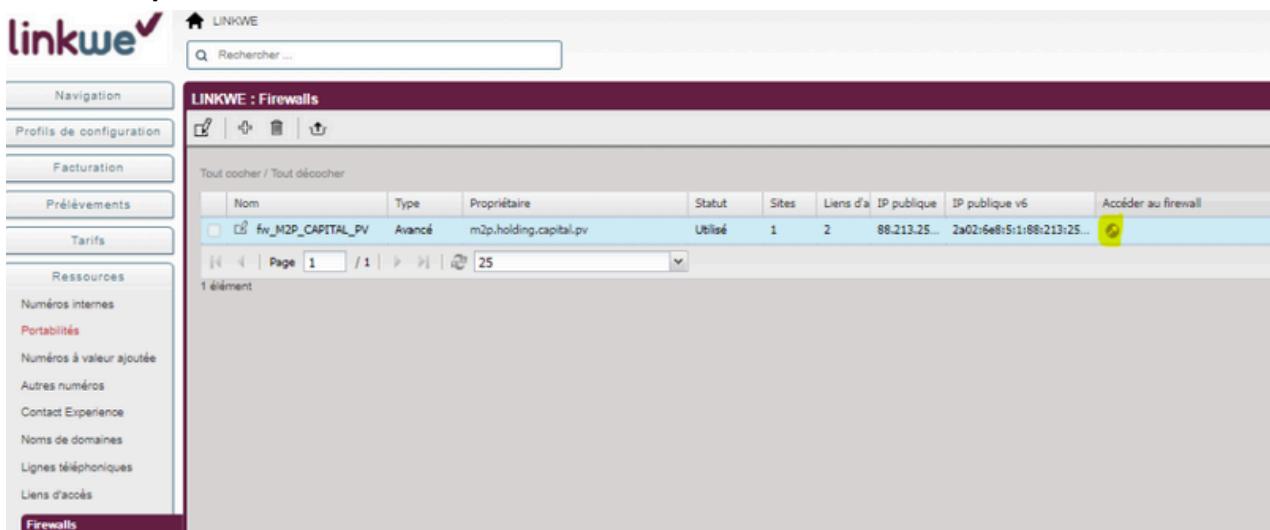
1. Choisir le Trunk Site
2. Permet de choisir le Trunk Général (précédemment créé) associé
3. Permet de choisir le nombre de canaux désirés.
4. Permet, via la liste déroulante, d'affecter des numéros sur le compte (le stock de numéro doit être alimenté au préalable en commandant des numéros chez Sewan).
5. Permet d'appliquer un profil de restriction (si besoin)

Annexe d'autre activité réalisé

PROCEDURE CREATION VPN DE SUPERVISION entre un lien client et LINKWE et lien Client et Centreon

1. SUR LE FIREWALL DU CLIENT

Via Sophia, se connecter au firewall du client



Nom	Type	Propriétaire	Statut	Sites	Liens d'accès	IP publique	IP publique v6	Accéder au firewall
frv_M2P_CAPITAL_PV	Avancé	m2p.holding.capital.pv	Utilisé	1	2	88.213.25...	2a02:6e8:51:88:213:25...	

a. Cr éation du Tunnel VPN :

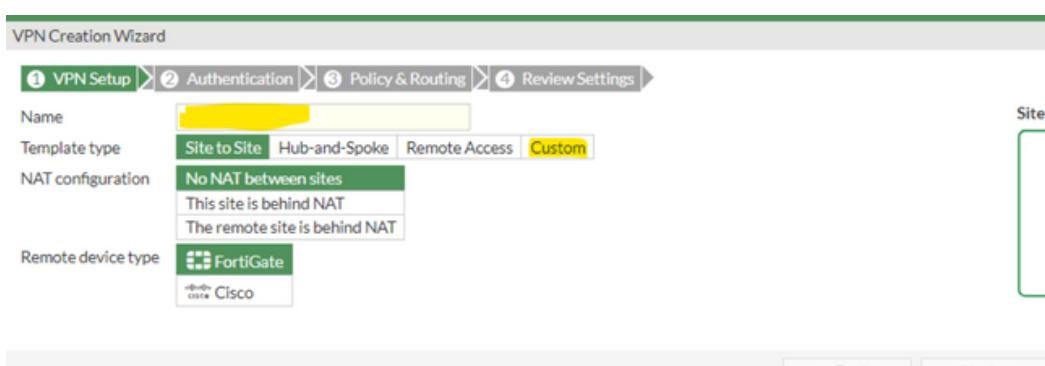
Se rendre dans le menu « VPN » et « IPsec Tunnels »



Tunnel #	Interface Binding #	Status
VPN_SUP_CAPITAL	INET_002044 (INET_002044)	Up

Cliquer sur « Create New » puis « IPsec Tunnel »

Sélectionner « CUSTOM » :



Puis remplir les champs dessous :

Name : ss

Comments : 0/255

Network

IP Version : IPv4

Remote Gateway : Static IP Address

IP Address : 0.0.0.0

Interface : (dropdown menu)

Local Gateway : (checkbox)

Mode Config : (checkbox)

NAT Traversal : Enable

Keepalive Frequency : 10

Dead Peer Detection : On Demand

DPD retry count : 3

DPD retry interval : 20 s

Forward Error Correction : Egress (checkbox) Ingress (checkbox)

Advanced...

Authentication

Method : Pre-shared Key

Pre-shared Key : (dropdown menu)

IP ADRESSE : 195.135.0.178 (qui correspond à l'IP de notre firewall)

INTERFACE : INET (dans le menu déroulant – correspond à l'interface internet du firewall)

Pre-shared Key : définir une clé partagée (au besoin utiliser un générateur de mot de passe. Cette preshared key sera utilisée dans le paramétrage du firewall linkwe donc à conserver pour la suite du paramétrage)

Définition des paramètres de la phase 1 du VPN :

Supprimer les encryption AES128 et Authentification SHA256

Supprimer les encryption AES128 et Authentification SHA1

Supprimer les encryption AES256 et Authentification SHA1

Décocher le Diffie-Hellman Groups « 5 »

Phase 1 Proposal		Add					
Encryption	AES128	Authentication	SHA256	X			
Encryption	AES256	Authentication	SHA256	X			
Encryption	AES128	Authentication	SHA1	X			
Encryption	AES256	Authentication	SHA1	X			
		32	31	30	29	28	27
		21	20	19	18	17	16
		15	14	5	2	1	
Diffie-Hellman Groups							
Key Lifetime (seconds)		86400					
Local ID							
XAUTH							
Type	Disabled						

Définition des paramètres de la phase 2 du VPN :

Il y aura 2 PHASE 2 à créer par lien.

Name : nommer la phase

- Lien_to_Centreon (personnaliser Lien par le type et la localisation : FTTH_LYON par exemple)
- Lien_to_Linkwe (personnaliser Lien par le type et la localisation : FTTH_LYON par exemple)

Local adress : mettre l'adresse local du firewall que vous trouverez dans Sophia

Nom	Type	Propriétaire	Statut	Sites	Liens d'a	IP publique	IP publique v6
fw_M2P_CAPITAL_PV	Avancé	m2p.holding.capital.pv	Utilisé	1	2	88.213.255.44	2a02:6e8:5:1:88:213:25...

Remote address :

Pour la phase 2 liée à linkwe : mettre l'adresse du firewall linkwe : 195.135.0.178/255.255.255.255

Pour la phase 2 liée à centreon : mettre l'adresse du firewall linkwe : 195.135.120.6/255.255.255.255

Supprimer toutes les encryption/ authentification sauf Encryption AES256 et Authentification SHA256

Supprimer le Diffie-Hellman Group « 5 »

Cliquer sur « Auto-negotiate »

The screenshot shows the 'New Phase 2' configuration dialog. It includes fields for Name (xx), Comments (Comments), Local Address (Subnet 0.0.0/0.0.0.0), Remote Address (Subnet 0.0.0/0.0.0.0), and an Advanced... button. The Phase 2 Proposal section contains a table of encryption and authentication pairs:

Encryption	Authentication	X
AES128	SHA1	X
AES256	SHA1	X
AES128	SHA256	X
AES256	SHA256	X
AES128GCM	X	
AES256GCM	X	
CHACHA20POLY1305	X	

Below the table are checkboxes for Enable Replay Detection (checked) and Enable Perfect Forward Secrecy (PFS) (checked). The Diffie-Hellman Group section lists numbers 32, 31, 30, 29, 28, 27, 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1, with 14 checked. At the bottom are Local Port (All checked), Remote Port (All checked), Protocol (All checked), and Auto-negotiate (checkbox).

Valider la phase 2 en cliquant sur le « v »

Créer la deuxième phase 2 de la même manière puis valider sur OK en bas de page.

b. Cr éation des routes statiques :

Cliquer sur le menu « Network » puis « Static routes »

Static Routes		
Destination	Gateway IP	Interface
195.135.120.6/32		VPN_SUP_CAPITAL
195.135.0.178/32		VPN_SUP_CAPITAL
0.0.0.0/0	88.213.255.254	INET_002044 (INET_002044)

Cliquer sur « create new » « IPv4 Static Route :

Static Routes		
Destination	Gateway IP	Interface
195.135.120.6/32		VPN_SUP_CAPITAL
195.135.0.178/32		VPN_SUP_CAPITAL
0.0.0.0/0	88.213.255.254	INET_002044 (INET_002044)

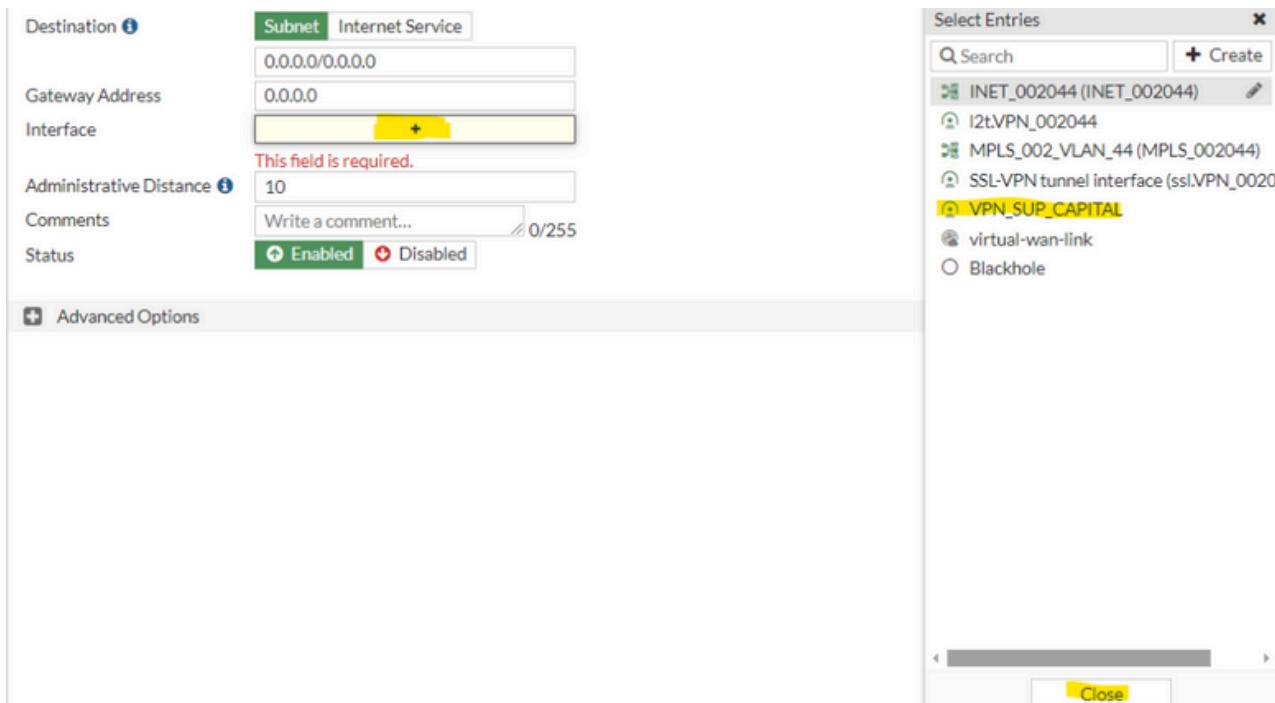
Il faudra cr éer deux routes static vers LINKWE et vers CENTREON

Destination	<input type="text" value="0.0.0.0/0.0.0.0"/>
Gateway Address	<input type="text" value="0.0.0.0"/>
Interface	<input type="text" value=""/>
Administrative Distance	<input type="text" value="10"/>
Comments	<input type="text" value="Write a comment..."/> / 0/255
Status	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>

Dans destination, saisir l'IP linkwe :

195.135.0.178/255.255.255.255 (pour la route linkwe) et
195.135.120.6/255.255.255.255 pour la route Centreon)

Cliquer ensuite sur le + dans le champ interface et sélectionner le nom de l'interface VPN que vous avez cr éé :

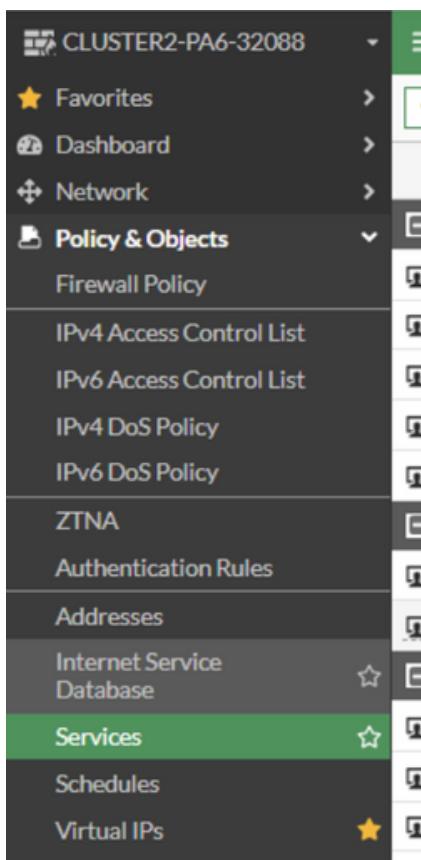


Cliquer sur « close » puis sur « ok » en bas de page pour valider la création.

Recommencer l'opération pour la deuxième route statique.

c. Création des services autorisés

Se rendre dans « Policy & Objects » puis « Services » :



Cliquer sur « Create New » et « Service » :

Créer le service Mikrotik_8291 :

Name	Mikrotik_8291
Comments	Write a comment... 0/255
Color	Change
Show in Service List	<input checked="" type="checkbox"/>
Category	Uncategorized
Protocol Options	
Protocol Type	TCP/UDP/SCTP
Address	IP Range FQDN 0.0.0.0
Destination Port	TCP ▾ 8291 - High + <input type="checkbox"/>
Specify Source Ports	<input checked="" type="checkbox"/>

Name : Mikrotik_8291

Category : Uncategorized

Destination port : 8291

Valider en cliquant sur OK

Création d'un groupe de service :

Cliquer sur « Create New » et « Service Group »

Service		
Service Name	Details	IP/FQDN
Service Group	TCP/80	0.0.0.0
HTTPS	TCP/443	0.0.0.0
File Access		
SAMBA	TCP/139	0.0.0.0
SMB	TCP/445	0.0.0.0
FTP	TCP/21	0.0.0.0

Nommer le groupe de Service : « Service_Linkwe_Admin »
Cliquer sur le « + » pour sélectionner les services :

- HTTP
- HTTPS
- Mikrotik_8291
- PING
- SSH
- TELNET

The screenshot shows the 'Edit Service Group' window. On the left, there's a form with fields for 'Name' (Service_Linkwe_Admin), 'Comments' (Write a comment...), 'Color' (Change), and 'Members'. A list box contains six services: HTTP, HTTPS, Mikrotik_8291, PING, SSH, and TELNET. To the right is a 'Select Entries' dialog box with a search bar and a tree view. The tree shows categories like 'SERVICE (89)', 'General (5)', 'Web Access (2)', and 'File Access (8)'. Under 'Web Access', 'HTTP' and 'HTTPS' are selected, highlighted with a yellow background.

d. Cr éation des r ègles de Pare-feu :

Se rendre dans « Policy & Objects » puis « Firewall policy »

Il faut cr éer deux r ègles de firewall :

MPLS_to_VPN et VPN_to_MPLS (pour autoriser les flux à entrer et sortir du firewall)

Cliquer sur « Create New »

The screenshot shows the 'Create New' rule configuration window. It includes fields for 'Name' (with a question mark icon), 'Incoming Interface' (dropdown menu), 'Outgoing Interface' (dropdown menu), 'Source' (button with a plus sign), 'IP/MAC Based Access Control' (button with a question mark icon), 'Destination' (button with a plus sign), 'Schedule' (dropdown menu set to 'always'), 'Service' (button with a plus sign), and 'Action' (radio buttons for 'ACCEPT' and 'DENY', with 'ACCEPT' selected). Below this is an 'Inspection Mode' section with 'Flow-based' and 'Proxy-based' options ('Flow-based' is selected). At the bottom are tabs for 'Firewall / Network Options' and 'NAT' (with 'NAT' selected).

Donner un nom à la règle du type `to_Sup_Linkwe` ou `From_Sup_Linkwe` (selon la règle que vous créez) ;

Pour la règle « `to_Sup_Linkwe` » :

- **Incoming interface** : choisir « MPLS »
- **Outgoing interface** : choisir le VPN créé
- **Source** : choisir « all »
- **Destination** : choisir « all »
- **Service** : choisir « Service_Linkwe_Admin »
- **Nat** : décocher

Valider sur OK en bas de page.

Pour la règle « `From_Sup_Linkwe` »

- **Incoming interface** : choisir le VPN créé
- **Outgoing interface** : choisir « MPLS »
- **Source** : choisir « all »
- **Destination** : choisir « all »
- **Service** : choisir « Service_Linkwe_Admin »
- **Nat** : décocher

Valider sur OK en bas de page.

2. SUR LE FIREWALL LINKWE

Via Sophia, se connecter au firewall LINKWE

LINKWE : Firewalls								
<input type="checkbox"/> Tout cocher / <input type="checkbox"/> Tout décocher								
Nom	Type	Propriétaire	Statut	Sites	Liens d'a	IP publique	IP publique v6	Accéder au firewall
<input type="checkbox"/> fw_LINKWE_1	Avancé	LINKWE Dardilly	Utilisé	1	2	195.135.0...	2a02:6e8:5:2:195:135:0...	
<input type="checkbox"/> fw_LINKWE_CLOUD_...	Standard	linkwe.cloud.production	Utilisé	0	0	195.135.4...	2a02:6e8:5:5:195:135:4...	

e. Cr éation du Tunnel VPN :

Se rendre dans le menu « VPN » et « IPsec Tunnels »

CLUSTER2-PA6-32088			VPN_002044		
Favorites			IPsec Tunnels		
Dashboard			Create New		
Network			Edit		
Policy & Objects			Delete		
VPN			Search		
IPsec Tunnels			Tunnel		
IPsec Wizard			Interface Binding		
(New, Tunnel, Terminal)			Status		
VPN_SiUP_CAPITAL			INET_002044 (INET_002044)		
			Up		

Cliquer sur « Create New » puis « IPsec Tunnel »

Sélectionner « CUSTOM » :

VPN Creation Wizard

① VPN Setup ② Authentication ③ Policy & Routing ④ Review Settings

Name: [REDACTED]

Template type: Site to Site Hub-and-Spoke Remote Access Custom **Custom**

NAT configuration: No NAT between sites This site is behind NAT The remote site is behind NAT

Remote device type: FortiGate **Cisco**

Site to Site

< Back Next >

Puis remplir les champs dessous :

Name: SS

Comments: 0/255

Network

IP Version: IPv4 **IPv6**

Remote Gateway: Static IP Address

IP Address: 0.0.0.0

Interface: [REDACTED]

Local Gateway:

Mode Config:

NAT Traversal: Enable **Disable** Forced

Keepalive Frequency: 10

Dead Peer Detection: Disable **On Idle** On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress Ingress

Advanced...

Authentication

Method: Pre-shared Key

Pre-shared Key: [REDACTED]

IP ADRESSE : l'adresse IP du firewall client (que vous trouvez dans Sophia)

Nom	Type	Propriétaire	Statut	Sites	Liens d'a	IP publique	IP publique v6
fw_M2P_CAPITAL_PV	Avancé	m2p.holding.capital.pv	Utilisé	1 2		88.213.255.44	2a02:6e8:5:1:88:213:25...

INTERFACE : INET (dans le menu déroulant – correspond à l'interface internet du firewall)

Pre-shared Key : Reprendre la pre share Key utilisé précédemment

Définition des paramètres de la phase 1 du VPN :

Supprimer les encription AES128 et Authentification SHA256

Supprimer les encription AES128 et Authentification SHA1

Supprimer les encription AES256 et Authentification SHA1

Décocher le Diffie-Hellman Groups « 5 »

Phase 1 Proposal	Add					
Encryption	AES128	Authentication	SHA256	X		
Encryption	AES256	Authentication	SHA256	X		
Encryption	AES128	Authentication	SHA1	X		
Encryption	AES256	Authentication	SHA1	X		
Diffie-Hellman Groups	32 21 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	31 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	30 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	29 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	28 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1	27 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
Key Lifetime (seconds)	86400					
Local ID						

Définition des paramètres de la phase 2 du VPN :

Il y aura 2 PHASE 2 à créer par lien.

Name : nommer la phase

- Centreon-to_lien (personnaliser Lien par le type et la localisation : FTTH_LYON par exemple)
- Linkwe_to_Lien (personnaliser Lien par le type et la localisation : FTTH_LYON par exemple)

Local address :

- Pour la phase 2 liée à linkwe : mettre l'adresse du firewall linkwe : 195.135.0.178/255.255.255.255
- Pour la phase 2 liée à centreon : mettre l'adresse du firewall linkwe : 195.135.120.6/255.255.255.255

Remote address : mettre l'adresse du firewall client que vous trouverez dans Sophia

Nom	Type	Propriétaire	Statut	Sites	Liens d'a	IP publique	IP publique v6
fw_M2P_CAPITAL_PV	Avancé	m2p.holding.capital.pv	Utilisé	1 2		88.213.255.44	2a02:6e8:5:1:88:213:25...

Supprimer toutes les encryption/ authentification sauf Encryption AES256 et Authentification SHA256

Supprimer le Diffie-Hellman Group « 5 »

Cliquer sur « Auto-negotiate »

New Phase 2

Name	xx
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0
<input type="checkbox"/> Advanced...	
Phase 2 Proposal	<input type="button" value="Add"/>
Encryption	AES128 Authentication SHA1
Encryption	AES256 Authentication SHA1
Encryption	AES128 Authentication SHA256
Encryption	AES256 Authentication SHA256
Encryption	AES128GCM
Encryption	AES256GCM
Encryption	CHACHA20POLY1305
<input checked="" type="checkbox"/> Enable Replay Detection	
<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy (PFS)	
Diffie-Hellman Group	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1
Local Port	All <input checked="" type="checkbox"/>
Remote Port	All <input checked="" type="checkbox"/>
Protocol	All <input checked="" type="checkbox"/>
Auto-negotiate	<input type="checkbox"/>

Valider la phase 2 en cliquant sur le « v »

Créer la deuxième phase 2 de la même manière puis valider sur OK en bas de page.

f. Création des routes statiques :

Cliquer sur le menu « Network » puis « Static routes »

Cliquer sur « create new » « IPv4 Static Route :

Il faudra créer une route static

Destination <i>i</i>	<input type="button" value="Subnet"/> <input type="button" value="Internet Service"/>
	<input type="text" value="0.0.0.0/0.0.0.0"/>
Gateway Address	<input type="text" value="0.0.0.0"/>
Interface	<input type="text" value="+"/> <i>This field is required.</i>
Administrative Distance <i>i</i>	<input type="text" value="10"/>
Comments	<input type="text" value="Write a comment..."/> <i>0/255</i>
Status	<input type="button" value="Enabled"/> <input type="button" value="Disabled"/>

Destination : saisir l'IP du firewall client :

Cliquer ensuite sur le + dans le champ interface et sélectionner le nom de l'interface VPN que vous avez créé :

Cliquer sur « close » puis sur « ok » en bas de page pour valider la création.

g. Cr éation des r ègles de Pare-feu :

Se rendre dans « Policy & Objects » puis « Firewall policy »

Il faut cr éer 3 r ègles de firewall :

CLOUD_to_VPN et SSL_to_SUP et VPN_to_CLOUD (pour autoriser les flux à entrer et sortir du firewall)

Cliquer sur « Create New »

Name	To_SUP_CAPITAL PV
Incoming Interface	CLOUD_CENTREON_1456 (CLO
Outgoing Interface	SUP_CAPITAL PV
Source	all
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	SUP_Services_clients_Linkwe
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT

Donner un nom à la r ègle du type CLOUD_to_VPN et SSL_to_SUP et VPN_to_CLOUD et SUP_to_SSL (selon la r ègle que vous cr éez) ;

Pour la r ègle « CLOUD_to_VPN » :

- **Incoming interface** : choisir « cloud »
- **Outgoing interface** : choisir le VPN cr éé
- **Source** : choisir « all »
- **Destination** : choisir « all »
- **Service** : choisir « Sup_Service_clients_Linkwe »
- **Nat** : d écocher

Valider sur OK en bas de page.

Pour la règle « VPN_to_CLOUD »

- Incoming interface** : choisir le VPN créé
- Outgoing interface** : choisir « CLOUD »
- Source** : choisir « all »
- Destination** : choisir « all »
- Service** : choisir « Sup_Service_clients_Linkwe »
- Nat** : cocher

Valider sur OK en bas de page.

Pour la règle « SSL_to_SUP »

- Incoming interface** : choisir SSL_VPN
- Outgoing interface** : choisir le VPN créé
- Source** : choisir « all » puis cliquer sur « + » et USER et choisir LINKWE-GROUP

Name	Value
Incoming Interface	SSL-VPN tunnel interface (sslVPN)
Outgoing Interface	SUP_CAPITAL PV
Source	all LINKWE-GROUP
Destination	all
Schedule	always
Service	SUP_Services_clients_Linkwe
Action	✓ ACCEPT ✘ DENY

Inspection Mode: Flow-based

Select Entries

Address	User	Internet Service
Search		
+ Create		
USER (7)		
Local (7)		
Aymen		
Blandine		
Fabrice		
Hugues		
Hyacinthe		
Meryl		
Raymond		
USER GROUP (3)		
AAD-GRP_VPN_SSL_FORTIGATE		
LINKWE-GROUP		
SSO_Guest_Users		

- Destination** : choisir « all »
- Service** : choisir « Sup_Service_clients_Linkwe »
- Nat** : cocher