

# SECURETECH

*“vous protéger est notre métier.”*

Réponse appel à projet  
Acquisition, maintenance  
d'une Infrastructure de protection réseau



# SOMMAIRE

## *Objet*

1. Ensemble, Protégeons votre avenir
  - a) Présentation de l'entreprise
  - b) SecureTech en chiffre
  - c) Nos valeurs
  - d) Une expertise certifiée
  - e) Une équipe de spécialiste
  - f) Un réseau de partenaire reconnus
  - g) Ils nous font confiance
2. Présentation du projet
  - a) Etat des lieux de l'existant
  - b) Avantages et inconvénients rencontrés
  - c) Présentation de la solution
  - d) Avantage de la solution
  - e) Déploiement de la solution
3. Élément budgétaire
  - a) Description du budget
  - b) Plan de règlement des paiements
4. Annexes

## Objet :

Dans le cadre du projet d'acquisition, maintenance d'une infrastructure de protection réseau, vous trouverez à travers ce mémoire technique l'offre détaillée de SecureTech.

L'objectif visé est de développer la sécurité des infrastructures existantes, tout en proposant des solutions innovantes et efficaces.

En 2022, 60% des entreprises françaises ont été victimes de cyberattaques, engageant des pertes de 50 000 € HT en moyenne par cible atteinte selon l'ANSSI. Dans un paysage numérique en constante évolution, où les cybermenaces se diversifient et se complexifient, la sécurisation des réseaux informatiques est devenue une priorité absolue pour toutes les entreprises. SecureTech reconnaît que la robustesse des infrastructures de sécurité de nos clients est cruciale pour protéger ses données sensibles, maintenir la continuité des opérations et préserver sa réputation.

Face à cette réalité, nous vous proposons à travers notre offre des mesures stratégiques pour renforcer la défense de votre réseau, venant compléter les dispositifs existants, en apportant une couche de sécurité additionnelle. SecureTech est parfaitement positionnée pour vous accompagner dans cette démarche grâce à notre expertise technique et notre capacité à implémenter des solutions qui répondent aux exigences spécifiques de nos clients.

Au fil de ce mémoire technique, nous détaillerons nos compétences et nos moyens, en présentant la solution envisagée avec nos experts, la planification et les ressources employées et le chiffrage de l'offre proposée.

Nous vous remercions de l'intérêt et du temps que vous consacrerez à la lecture et à l'analyse de ce mémoire.

## 1. Ensemble, protégeons votre avenir

### a) Présentation de l'entreprise

Protéger, Évoluer, Innover : tels sont les mots d'ordre de notre société, leader de la cybersécurité en France. Fondée en 2009 par Redwan Felfel, Hugo Martin et Mourad Amghar, SecureTech s'engage à fournir des solutions de sécurité numérique de pointe, en mettant l'accent sur l'innovation technologique et organisationnelle.

SecureTech se distingue par ses spécialités et son savoir-faire dans le domaine de la cybersécurité. En tant qu'acteur majeur sur le marché, notre entreprise offre une gamme étendue de services et de solutions pour répondre aux besoins spécifiques de nos clients.

SecureTech adopte une approche holistique de la cybersécurité, en intégrant des solutions technologiques, des processus organisationnels et des programmes d'acculturation des employés pour créer une défense robuste contre tout type de menace. Notre approche globale garantit une protection complète des actifs numériques de nos clients, tout en minimisant les risques et en optimisant les performances opérationnelles.

Nous sommes engagés dans une culture d'innovation continue, axée sur la recherche et le développement de nouvelles technologies et de meilleures pratiques en matière de cybersécurité. Cette quête incessante de l'excellence nous permet de rester à la pointe de l'industrie et d'offrir à nos clients des solutions innovantes et adaptées à leurs besoins évolutifs.

Bien que le siège social de l'entreprise soit situé à Paris, notre présence s'étend à travers tout le territoire français, avec des bureaux stratégiquement implantés en Métropole



## **b) SecureTech en chiffres**



Notre entreprise a connu une croissance significative au cours des dernières années, avec des chiffres qui reflètent notre engagement envers l'excellence et la satisfaction client. Au cours de l'exercice précédent, nous avons enregistré une augmentation de 20 % de notre chiffre d'affaires par rapport à l'année précédente, atteignant ainsi un chiffre record de vente de 3 millions d'euros. Cette croissance dynamique témoigne de la confiance continue de nos clients dans nos services et solutions. De plus, notre taux de fidélisation client a augmenté de 15 %, démontrant notre capacité à maintenir des relations solides et durables avec nos clients existants. En parallèle, nous avons également étendu notre portée géographique en ouvrant de nouveaux bureaux dans trois nouvelles régions, renforçant ainsi notre présence sur le marché national et international. Ces réalisations reflètent notre engagement envers l'innovation, la qualité et la satisfaction client, et nous sommes déterminés à continuer à surpasser les attentes et à atteindre de nouveaux sommets de succès dans les années à venir.

### **c) Nos valeurs**

Notre entreprise a établi sa réputation sur la base de valeurs fondamentales, au cœur de notre identité, qui guident nos actions et interactions avec nos clients et partenaires :

- Qualité : nous nous engageons à fournir des solutions de cybersécurité de la plus haute qualité, garantissant la protection et la tranquillité de nos clients,
- Innovation : nous sommes constamment à la recherche de nouvelles technologies et de meilleures pratiques pour offrir des solutions de pointe à nos clients, les aidant ainsi à rester en avance sur les menaces numériques,
- Agilité : nous sommes flexibles et adaptatifs dans notre approche, toujours prêts à repenser nos processus et nos stratégies pour répondre aux besoins changeants de nos clients et de l'environnement numérique en constante évolution.

### **d) Une expertise certifiée**

La crédibilité et l'excellence de SecureTech sont attestées par un ensemble de certifications reconnues dans l'industrie de la cybersécurité. Ces accréditations illustrent notre engagement envers les meilleures pratiques et standards internationaux, assurant à nos clients des services de sécurité de la plus haute qualité.

Nous disposons d'une équipe d'experts hautement qualifiés et certifiés dans divers domaines de la cybersécurité, allant de la protection des réseaux et des données à la gestion des risques et à la conformité réglementaire via les certifications CISSP, CISM, et CEH.

Nous sommes également certifiés PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Informations), PDIS (Prestations de Détection d'Incidents de Sécurité) et PRIS (Prestataire de Réponse aux Incidents de Sécurité) depuis 2016 par l'ANSSI, témoignant de notre expertise dans le domaine.

### **e) Une équipe de spécialistes**

L'équipe de SecureTech est composée de professionnels hautement qualifiés et passionnés, chacun apportant son expertise unique pour offrir des solutions de cybersécurité de pointe à nos clients.

- Mourad Amghar : fondateur et responsable commercial, Mourad joue un rôle essentiel dans le développement des relations avec les clients et la promotion des solutions de SecureTech sur le marché. Son expertise commerciale et sa vision stratégique contribuent à la croissance continue de l'entreprise.

- Hugo Martin : cofondateur et technico-commercial, Hugo est chargé d'assurer la satisfaction client en proposant des solutions technologiques adaptées à leurs besoins spécifiques. Son approche technique et son sens du service client sont des atouts précieux pour SecureTech.

- Redwan Felfel : cofondateur et chef de projet, il supervise la gestion des projets de cybersécurité de bout en bout, en veillant à ce que les solutions livrées répondent aux exigences et aux normes de qualité les plus élevées. Son leadership et son expertise technique garantissent le succès des projets de SecureTech.

Autres membres clés de l'équipe : ingénieurs en cybersécurité, pentesters, juristes, support clients, développeurs ... notre équipe agile travaille en étroite collaboration pour offrir des

solutions de cybersécurité de qualité supérieure, aidant ainsi nos clients à protéger leurs actifs numériques et à prospérer dans un environnement numérique en constante évolution.

#### **f) Un réseau de partenaires reconnus**

SecureTech est également partenaire de leaders technologiques reconnus, ce qui nous permet de rester à la pointe de l'innovation et de la technologie en matière de sécurité numérique.

Ces certifications et partenariats sont la preuve de notre capacité à répondre aux exigences les plus strictes en matière de cybersécurité et témoignent de la confiance que nos clients peuvent placer en SecureTech pour la protection de leurs actifs numériques.

En tant que partenaire certifié de fabricants renommés tels que Fortinet et Clavister, SecureTech bénéficie d'un accès privilégié aux dernières technologies et aux ressources les plus récentes. Ces partenariats stratégiques nous permettent de proposer à nos clients des solutions de pointe et des conseils avisés pour renforcer leur posture de sécurité numérique. Nous sommes également spécialisés dans la configuration de matériel Fortinet et Clavister, offrant ainsi une expertise supplémentaire dans l'intégration et la gestion de ces solutions de sécurité de premier plan.

#### **g) Ils nous font confiance ...**

SecureTech intervient auprès de donneurs d'ordres très variés, tels que des exploitants de réseaux de communication, de fibre optique ou d'électricité, d'éclairage, d'eau, d'assainissement, de gaz, des entreprises de travaux publics, des collectivités locales, des entreprises de géotechnique, de géomètres-experts, etc.



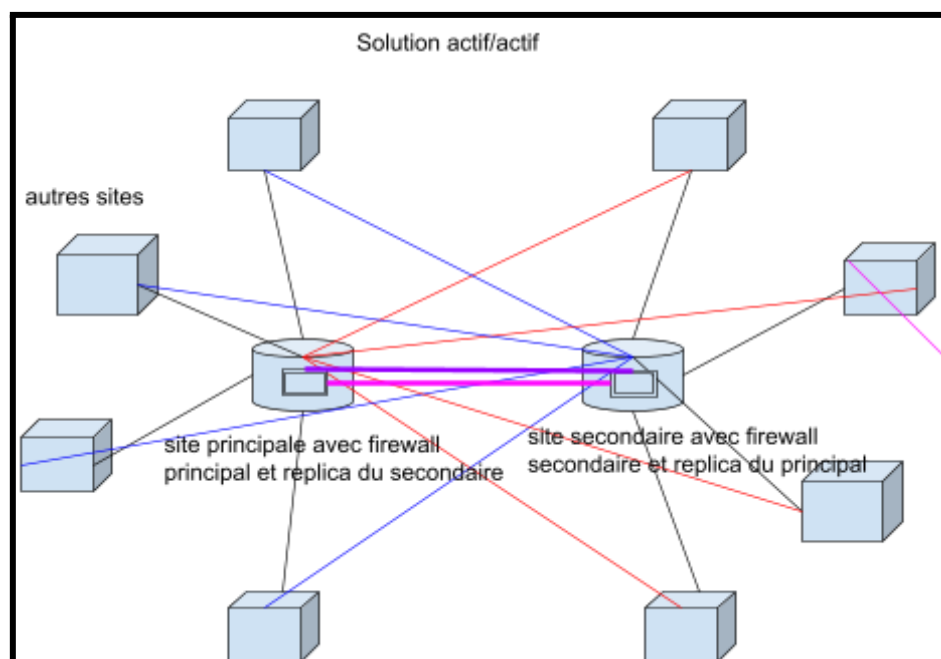
L'un des témoignages les plus marquants de l'expertise de SecureTech en matière de cybersécurité est notre collaboration réussie avec BolouCorp, une société opérant dans le monde du bâtiment, de structure similaire à celle de votre entreprise.

Confrontée à une série d'attaques de phishing sophistiquées qui ont compromis des données, cette entreprise nous a sélectionné pour trouver une solution.

Nous avons rapidement déployé une équipe d'experts qui a conçu et mis en œuvre une stratégie de défense, en intégrant des solutions avancées de détection et de prévention des intrusions. Nous avons non seulement stoppé les attaques en cours, mais aussi considérablement renforcé la posture de sécurité de notre client.

En effet, dans les six mois suivant notre intervention, BolouCorp a enregistré une réduction de 70% des tentatives d'intrusion et une amélioration notable de la détection des menaces. Cette collaboration a non seulement sauvé notre client de pertes potentielles estimées à plusieurs milliers d'euros, mais a également renforcé son image vis-à-vis de ses clients.

Voici l'exemple d'une installation complexe réalisée par nos équipe :





Cette solution active/active est beaucoup moins répandue et nécessite une intervention plus longue mais elle assure une réactivité en cas de perte de nœuds ou du firewall, l'autre firewall ou les autres nœuds disponible prendront automatiquement en charge le trafic qui est tombé sur les nœuds libres et actifs.

## **2. Présentation du projet**

### **a) Etat des lieux de l'existant**

- La Direction comprend les dirigeants et les cadres supérieurs de l'entreprise,
- Les Services RH, Finance et IT représentent les différents départements fonctionnels,
- Chaque service est composé de plusieurs équipes spécifiques à leurs domaines (recrutement, comptabilité, développement, etc.),
- Chaque équipe compte un certain nombre d'employés, en fonction de la taille et des besoins du service ou de l'équipe ; on dénombre pas moins de 500 postes utilisateurs sur un site principal, et plusieurs sites annexes répartis en Bourgogne - Franche-Comté,
- Le réseau actuel est protégé par un seul pare-feu TP-Link Archer X10, et n'a pas de solution VPN.

### **b) Avantages et inconvénients rencontrés**

#### **Avantages :**

**Simplicité de gestion :** Avec un seul pare-feu, la gestion des règles de sécurité est plus simple et centralisée. Il est plus facile de maintenir et de mettre à jour les politiques de sécurité.

**Coût réduit :** La mise en place et la gestion d'un seul pare-feu peuvent être moins coûteuses en termes d'investissement initial, de licences et de maintenance par rapport à la gestion de plusieurs pare-feu.

**Facilité de surveillance :** La surveillance du trafic réseau et des activités malveillantes est simplifiée car toutes les données passent par un seul point de contrôle.

#### **Inconvénients :**

**Point de défaillance unique (SPOF) :** En cas de panne ou de compromission du pare-feu unique, tout le réseau est vulnérable. Cela peut entraîner une interruption des activités commerciales et une perte de données.

**Performance :** Un pare-feu unique peut devenir une menace pour le trafic réseau, surtout dans les environnements à fort trafic. Cela peut entraîner des retards et une dégradation des performances du réseau.

**Limite :** Un seul pare-feu peut avoir du mal à gérer un réseau en expansion. À mesure que l'entreprise se développe, le pare-feu unique peut devenir insuffisant pour gérer la charge de trafic croissante.

### **c) Présentation de la solution**

La sécurité des réseaux est une préoccupation majeure pour toute entreprise, en particulier lorsque plusieurs sites distants doivent être connectés au siège principal. Actuellement, le réseau utilise un seul pare-feu pour cette architecture. Cependant, pour améliorer la sécurité, la redondance et la capacité de gestion, une migration vers une solution à deux pare-feux est proposée. Cette solution implique l'installation d'un pare-feu au siège principal et un second pare-feu au site distant choisi par le client. Pour effectuer cette migration tout en minimisant les temps d'arrêt et en garantissant une transition en douceur, voici la proposition détaillée :

#### **Etape préalable :**

**Évaluation de l'Architecture Actuelle :** Avant de procéder à la migration, il est crucial de comprendre l'architecture réseau existante, y compris la configuration du pare-feu actuel, les règles de sécurité, les VLAN, les tunnels VPN, etc.

Nous devons réaliser un audit sur la configuration actuelle pour optimiser le changement de firewall et minimiser le délais de changement et les chances d'erreurs lors du changement.

Le plan d'adressage IP de tous les sites devra nous être remis pour une configuration fluide et rapide.

Il faudra pour le deuxième pare-feu sélectionner le Site Distant : Il faudra définir au préalable ce site pour savoir s'il faut intervenir sur site ou virtualiser la configuration pour l'importer dans notre data center.

#### **Configuration du Pare-feu au Site Principal :**

Installation physique du pare-feu au siège principal.

Configuration des interfaces réseau, des adresses IP et des VLAN pour correspondre à l'infrastructure réseau existante.

Transfert des règles de sécurité et des politiques de pare-feu depuis l'ancien pare-feu vers le nouveau, en tenant compte des spécificités de la plate-forme Fortinet.

### **Configuration du Pare-feu au Site Distant :**

Installation physique du deuxième pare-feu Fortinet FG100F au site distant choisi.

Configuration des interfaces réseau, des adresses IP et des VLAN en fonction de l'infrastructure existante au site distant.

Configuration des tunnels VPN si nécessaire pour assurer la connectivité sécurisée avec le siège principal et les autres sites distants.

### **Test de Connectivité et de Sécurité :**

Effectuer des tests de connectivité pour garantir que les deux pare-feu fonctionnent correctement et que les règles de sécurité sont appliquées comme prévu.

Tester la résilience du réseau en simulant des pannes pour vérifier la capacité des pare-feu à basculer en mode de basculement sans perte de connectivité.

### **Migration du Trafic :**

Rediriger le trafic réseau vers le nouveau pare-feu au siège principal et au site distant.

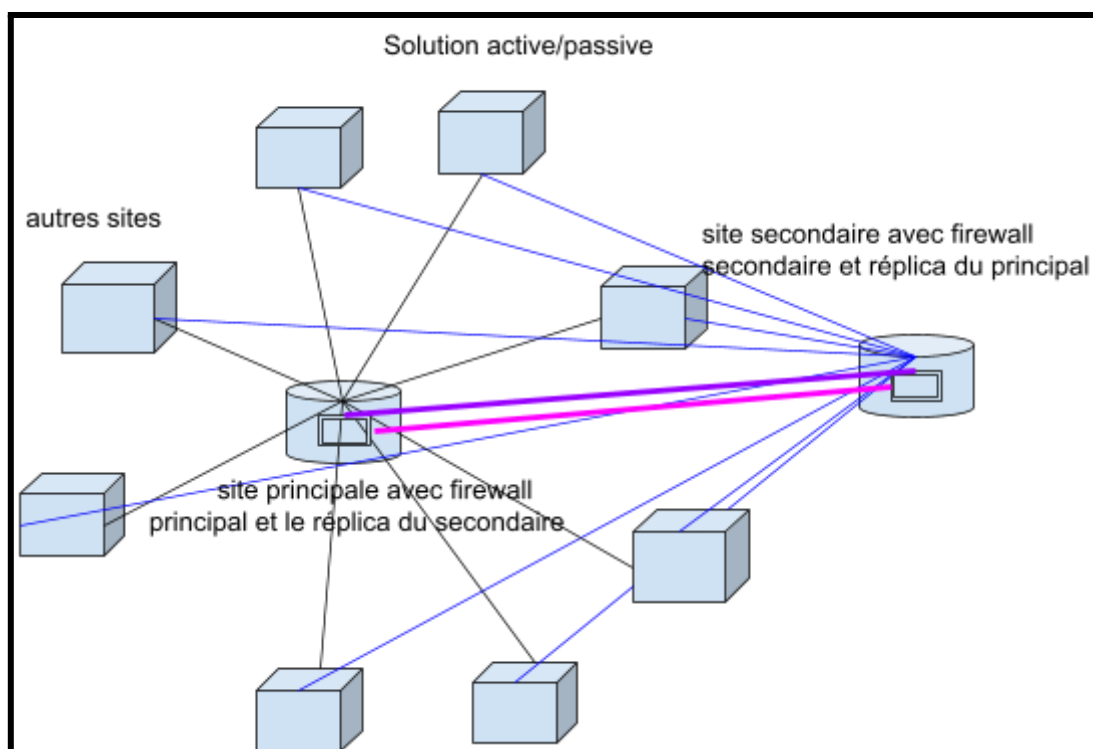
Surveiller attentivement le trafic pendant cette phase pour détecter tout problème de performance ou de compatibilité.

### **Formation du Personnel :**

Former le personnel sur la gestion et la surveillance des pare-feux Fortinet FG100F, en mettant l'accent sur les fonctionnalités spécifiques de la plate-forme et les meilleures pratiques de sécurité.

Ceci était les prérequis pour ce projet, ci dessous les deux solutions de la nouvelle infrastructure et architecture pour l'entreprise PILPRO :

La solution demandée est une solution à deux Firewall, on ne propose généralement dans ce cas que la solution soit active/passive, qui consiste à placer un firewall dans vos locaux (là où se situe déjà le Firewall de votre entreprise) et un autre sur un site distant, soit un site qui vous appartient directement (un local secondaire, un autre site) soit dans notre data center. Cette solution permettra d'éviter les pannes et les coupures si un des matériels est défectueux ou tombe en panne.



Ici sur le schéma on voit les deux sites qui sont interconnectés entre eux par la connexion Heartbeat qui informe les deux firewall si l'un d'eux tombe en panne.

En cas de panne la connexion ne sera pas coupée car le firewall qui était passif deviendra actif et reprendra là où en était son prédécesseur, ce qui garantit une fluidité constante au niveau de l'utilisateur.

Cette solution est la plus connue et utilisée, aussi bien pour assurer une maintenance simple et rapide pour le client mais surtout pour assurer la continuité de l'activité, il faut aussi savoir que les 30 sites distants seront directement connectés au firewall principal comme c'est le cas actuellement dans l'entreprise, cependant ils auront une liaison VPN sur les deux firewall pour garder un contact et en cas de panne directement basculer sur le firewall secondaire.

Les firewall qu'on propose pour votre entreprise et vos besoins est le FORTINET FG100F qui correspond parfaitement à une installation comme la vôtre, il répond aux critères cités ci-dessous:

*IPS = 2.6 Gbps*

*VPN SSL = 1Gbps*

*56 000 nouvelles sessions par seconde pour 1.5M de connexion simultanée.*

*Voir le rets en annexe page 32.*

Une architecture comme celle-ci peut être réalisée rapidement grâce à nos ingénieurs qualifiés sur ce type de matériel car nous sommes en partenariat depuis maintenant 5 ans avec FORTINET et nos ingénieurs sont formés chaque année directement chez fortinet qui les formes sur les nouveautés et s'assure qu'ils soit toujours capable d'intervenir sur n'importe quel matériel de chez eux.

En effet la marque Fortinet est une société renommée dans le domaine de la cybersécurité, offrant une gamme complète de solutions de sécurité, dont leurs firewalls sont la technologie qu'ils maîtrisent le plus. La qualité de ses firewalls est largement reconnue dans l'industrie pour plusieurs raisons:

Tout d'abord, les firewall Fortinet sont réputés pour leur robustesse et leur fiabilité. Ils sont conçus pour détecter et bloquer efficacement une large gamme de menaces, des attaques sophistiquées aux tentatives de piratage plus basiques. Cette fiabilité est cruciale dans un paysage de menaces en constante évolution où la sécurité des données est une priorité absolue pour les entreprises.

De plus, les firewalls Fortinet offrent une performance élevée sans compromettre la sécurité. Ils sont capables de gérer un volume important de trafic réseau tout en maintenant des temps de réponse rapides, ce qui est essentiel pour les environnements réseau à haute vitesse où la latence peut avoir un impact significatif sur les performances globales.

Un autre avantage majeur des pare-feu Fortinet est leur architecture intégrée et leur approche de sécurité unifiée. Cette approche permet de consolider plusieurs fonctions de sécurité, telles que la prévention des intrusions, la détection des malwares, la protection contre les menaces avancées persistantes (APT), et bien d'autres, au sein d'une seule plateforme. Cela simplifie la gestion et réduit la complexité des infrastructures de sécurité, tout en améliorant la visibilité et le contrôle sur les activités réseau.

Enfin, Fortinet investit continuellement dans la recherche et le développement pour améliorer ses firewalls et anticiper les nouvelles menaces émergentes. Leur engagement envers

l'innovation et la sécurité en fait un choix de confiance pour les entreprises de toutes tailles à la recherche de solutions de sécurité réseau hautement performantes et évolutives.

Nous faisons confiance à Fortinet depuis maintenant 5 ans et nous vous garantissons la sécurité des produits que nous vous proposons, puisque nous même nous utilisons fortinet dans nos locaux.

Les firewall de chez fortinet sont certifiés EAL (Evaluation Assurance Level), ICSA et FIPS (Federal Information Processing Standard)

#### d) Avantages de notre solution

**Redondance Améliorée :** Avec deux pare-feu Fortinet FG100F en place, le réseau bénéficie d'une redondance accrue, réduisant ainsi le risque de temps d'arrêt en cas de défaillance matérielle ou de panne.

**Sécurité Renforcée :** Les fonctionnalités avancées de sécurité offertes par les pare-feu, telles que l'inspection des paquets SSL, l'analyse comportementale et la prévention des intrusions, renforcent la posture de sécurité du réseau.

**Meilleure Gestion :** La console de gestion unifiée de Fortinet permet une gestion centralisée des deux pare-feu, simplifiant ainsi les tâches d'administration et de surveillance du réseau.

**Évolutivité :** La solution à deux pare-feu offre une évolutivité pour répondre aux besoins futurs de l'entreprise, que ce soit en termes de capacité de traitement, de bande passante ou de fonctionnalités de sécurité supplémentaires.

#### e) Déploiement de la solution

Planning du projet	T0	septembre 2024	octobre 2024	novembre 2024	décembre 2024
Audit initial					
Réajustement de la configuration suite audit					
Commande et réception matériel					
Tests préliminaires					
Installation des pare-feux dans l'infrastructure réseau					
Configuration du matériel selon les spécifications					
Tests post-déploiement					
Formation du personnel du client					
Période de garantie					

Le déploiement de la solution de pare-feu est scindée en plusieurs phases distinctes. Dans la première phase, nous commanderons et recevrons le matériel nécessaire suite à l’audit et aux réajustements apportés. Ensuite, nous procéderons au déploiement des pare-feux par lots dans la deuxième phase, suivie de la configuration technique dans la troisième phase. La quatrième phase comprendra des tests rigoureux pour garantir la performance et la sécurité de la

[illegible]

solution, et une période de formation des utilisateurs. Enfin, une période de garantie de six mois assurera un support continu après l'implémentation.

Tout au long du projet, nous mettrons en place un suivi rigoureux des indicateurs clés de performance (KPI) que nous avons identifiés. Cela nous permettra d'évaluer en temps réel la progression du projet et de garantir que chaque phase est menée à bien de manière efficace et efficiente. En surveillant de près ces KPI, tels que le délai de déploiement, la satisfaction du client, la conformité aux exigences, le nombre d'incidents post-déploiement et le taux d'adoption, nous serons en mesure d'identifier rapidement les éventuels écarts par rapport aux objectifs définis et de prendre des mesures correctives appropriées.

Ce suivi continu des KPI nous permettra également de garantir que les résultats du projet répondent pleinement aux attentes du client et aux normes de qualité élevées que nous nous sommes fixées.

### 3. Elements budgétaires

La section "Éléments Budgétaires" fournit une ventilation détaillée des coûts associés à la mise en œuvre du projet de migration vers une solution à deux pare-feu Fortinet FG100F. Cette partie du plan budgétaire offre une compréhension approfondie des dépenses nécessaires pour l'acquisition de matériel, de licences logicielles, de services professionnels, ainsi que d'autres frais associés à la réalisation du projet. Chaque élément budgétaire est présenté avec son coût unitaire, sa quantité, et son total, permettant ainsi une évaluation précise des dépenses engagées pour atteindre les objectifs de sécurité et de redondance du réseau.

## **a) Description du budget**

- **Matériel :**

1. Pare-feu Fortinet FG100F (Site Principal) :

- Coût unitaire : 4000 € HT
- Quantité : 1
- Total : 4000 € HT

2. Pare-feu Fortinet FG100F (Site Distant) :

- Coût unitaire : 4000 € HT
- Quantité : 1
- Total : 4000 € HT

3. Pare-feu Fortinet FG40F (Sites secondaires)

- Coût unitaire : 565 € HT
- Quantité : 29
- Total 16385 € HT

Dans le cadre de notre infrastructure réseau, nous avons choisi les pare-feux Fortinet FG100F pour nos sites principaux et distant, évalués à 4000 € HT chacun. Pour les sites secondaires, nous avons opté pour les pare-feux Fortinet FG40F, au coût unitaire de 565 € HT. Avec 29 unités nécessaires, le coût total s'élève à 16385 € HT. Cette configuration assure une protection efficace tout en maintenant la continuité de nos opérations.

- **Licences Logicielles :**

1. Licence de Sécurité Avancée pour les Pare-feu :

- Coût unitaire : 2000 € HT par pare-feu
- Quantité : 2
- Total : 4000 € HT

2. Licence de Sécurité pour les Pare-feu :

- Coût unitaire : 138 € HT par pare-feu
- Quantité : 29
- Total : 4000 € HT

L'acquisition de la Licence de Sécurité Avancée pour les Pare-feu est essentielle pour garantir la protection optimale de notre réseau. Chaque pare-feu Fortinet FG100F et FG40F requiert une licence individuelle, évaluée à 2000 € HT par pare-feu.



Ainsi, pour les deux pare-feux FG100F et les pare-feux FG40F, le coût total des licences s'élève à 8000 € HT. Ces licences activent des fonctionnalités avancées telles que l'inspection SSL et la prévention des intrusions, renforçant ainsi la sécurité de notre infrastructure réseau.

- Services Professionnels :

1. Consultation et Expertise :

- Coût horaire du consultant : 150 € HT/heure
- Nombre d'heures estimées : 20 heures
- Total : 3000 € HT

La catégorie "Consultation et Expertise" couvre les frais pour les conseils spécialisés nécessaires à la planification et à l'exécution du projet. Avec un tarif de consultation de 150 € HT par heure et une estimation de 20 heures de travail, le coût total s'élève à 3000 € HT. Ces heures seront utilisées pour évaluer l'infrastructure existante, concevoir une stratégie de migration adaptée, et fournir des recommandations essentielles pour assurer le succès du projet. Cette expertise externe garantit une planification précise et une transition fluide vers la nouvelle infrastructure.

2. Changement et installation des nouveaux pare-feu :

- Coût horaire du technicien : 80€ HT/heure
- Nombre d'heures estimées : 20 heures
- Total : 1600 € HT

Dans le cadre du projet, le remplacement et l'installation de nouveaux pare-feu ont été envisagés pour renforcer la sécurité du système. Le coût horaire du technicien chargé de cette tâche est évalué à 80€ HT par heure, avec une estimation de 20 heures de travail nécessaires. Ainsi, le coût total pour cette phase s'élève à 1600€ HT.

3. Configuration et rédaction d'audit des pare-feus :

- Coût horaire de l'ingénieur : 125€ HT /heure
- Nombre d'heures estimées : 25 heures
- Total : 3125 € HT

De plus, la configuration et la rédaction d'audit des pare-feux requièrent l'intervention d'un ingénieur dont le tarif horaire est de 125€ HT. Pour cette étape, une estimation de 25 heures est établie, portant le coût total à 3125€ HT. Ces dépenses sont prévues dans le cadre du budget alloué au projet afin d'assurer une mise en place efficace et sécurisée des pare-feu.

#### 4. Migration des données :

- Coût horaire de l'ingénieur en migration de données : 150 € HT/heure
- Nombre d'heures estimées : 25 heures
- Total : 3750 € HT

Dans la phase de migration des données, un ingénieur spécialisé est requis pour garantir la transition en douceur vers la nouvelle infrastructure. Avec un tarif horaire de 150 € HT et une estimation de 25 heures de travail, le coût total pour cette phase s'élève à 3750 € HT. Ces heures seront consacrées à la planification et à l'exécution de la migration, garantissant ainsi l'intégrité et la sécurité des données pendant tout le processus. Ce professionnel assure que les opérations réseau se déroulent sans heurts et en conformité avec les normes de sécurité établies.

#### 5. Formation du Personnel :

- Coût par session de formation : 1250 € HT
- Nombre de sessions : 3
- Total : 3750 € HT

Dans le cadre de la formation du personnel, un budget de 3750 € HT est alloué pour trois sessions de formation, chacune coûtant 1250 € HT. Outre l'apprentissage des compétences techniques nécessaires à la gestion des nouveaux pare-feu Fortinet FG100F.

Ces sessions visent également à sensibiliser le personnel aux menaces potentielles telles que le phishing et autres formes d'arnaques en ligne. En comprenant les techniques d'attaque et en apprenant à reconnaître les signaux d'alerte, le personnel sera mieux équipé pour détecter et prévenir les tentatives de cybercriminalité, renforçant ainsi la sécurité globale du réseau de l'entreprise.

- Frais de Déplacement et d'Installation :

##### 1. Frais de Déplacement vers le Site Distant :

- Coût par déplacement : 800 € HT
- Nombre de déplacements : 6
- Total : 4800 € HT

Un budget de 4800 € HT est réservé pour les déplacements vers le site distant. Ces déplacements, facturés à 800 € HT chacun, sont nécessaires pour l'installation, la configuration des pare-feu et la migration des données vers les nouveaux pare-feu Fortinet FG100F. Ils garantissent une transition efficace vers la nouvelle infrastructure, minimisant les temps d'arrêt et assurant la continuité des opérations réseau.

- **Frais Récurrents :**

1. **Frais de Connectivité pour le Site Distant (Location de Ligne) :**

- Coût mensuel : 300 € HT
- Durée : 12 mois
- Total Annuel : 3600 € HT

Un budget annuel de 3600 € HT est alloué pour les frais de connectivité du site distant, représentant une location de ligne mensuelle de 300 € HT sur une période de 12 mois. Ces frais garantissent une connectivité continue et fiable avec le site distant, essentielle pour maintenir les opérations réseau de manière optimale. En assurant une connexion stable, ces frais contribuent à la performance globale du réseau et à la réussite du projet de migration vers les nouveaux pare-feu Fortinet FG100F.

- **Coûts Additionnels (Frais Administratifs, Taxes, etc.) :**

- Estimation : 5% du coût total (61010 € HT)
- Total : 3050 € HT

- **Coût Total du Projet :**

- Total des Éléments Budgétaires : 61010 € HT
- Coûts Additionnels (G) : 3050 € HT
- Coût Total Estimé : 64060 € HT

En résumé, le détail des coûts montre que l'entreprise est sérieusement engagée envers la sécurité et la redondance de son infrastructure réseau.

Les investissements dans les pare-feu Fortinet FG100F, les licences logicielles avancées, les services professionnels et la formation du personnel démontrent une approche holistique pour garantir le succès du projet de migration.

En allouant des ressources financières adéquates à chaque aspect du projet, l'entreprise s'assure une transition en douceur vers une infrastructure plus sécurisée et fiable.

La différence entre le coût total estimé et le coût final représente non seulement le bénéfice financier, mais aussi la valeur ajoutée en termes de sécurité et de continuité des opérations. Ce rapport financier met en évidence l'importance d'une planification budgétaire précise et d'une gestion rigoureuse des ressources pour atteindre les objectifs stratégiques de l'entreprise en matière de sécurité informatique.

## **b) Plan de règlement des paiements**

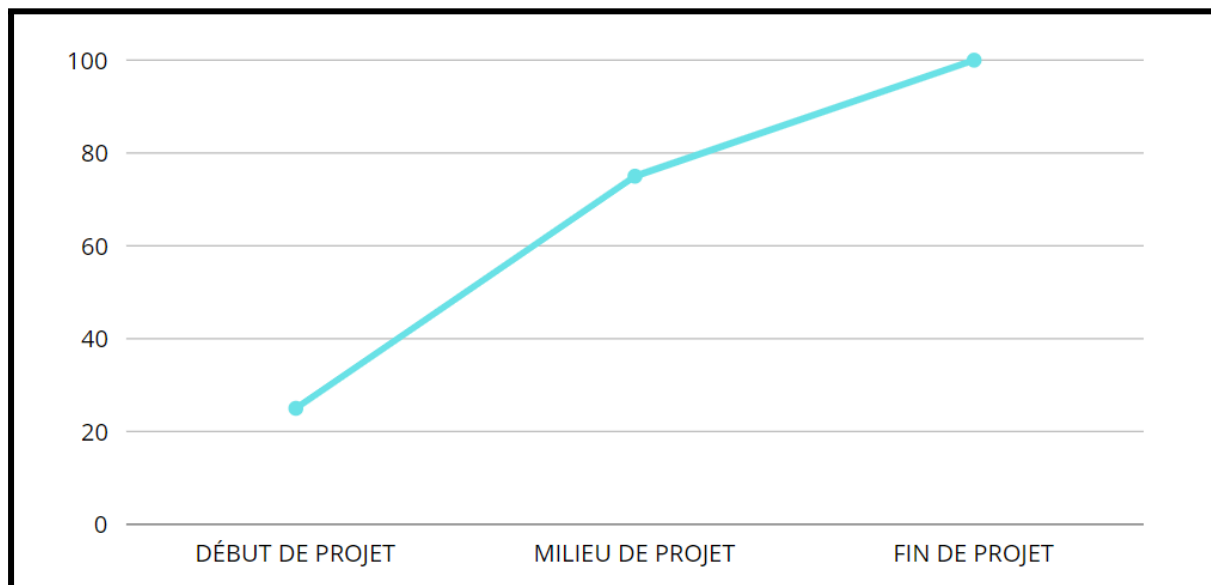
En ce qui concerne les échéances de paiement, nous avons convenu d'un plan en trois parties pour assurer une gestion financière équilibrée et efficace du projet. Tout d'abord, un premier versement correspondant à 25% du prix total du projet sera exigé avant le lancement, agissant à la fois comme une garantie et une aide pour l'acquisition initiale du matériel nécessaire.

Par la suite, le deuxième versement sera effectué au milieu de l'exécution du projet, représentant 50% du coût total. Cette étape intermédiaire est considérée comme cruciale dans le déroulement du projet, et le paiement à ce stade reflète l'importance et les progrès accomplis jusqu'à ce point.

Enfin, le solde restant, soit 25% du montant total, sera réglé à la conclusion du projet. Ce dernier versement conclura les engagements financiers et sera effectué une fois que toutes les livraisons auront été satisfaisantes et que toutes les exigences du projet auront été remplies conformément aux attentes convenues.

Ce plan d'échéancier de paiement vise à assurer une répartition équilibrée des coûts tout au long du projet, offrant une sécurité financière à la fois au client et au prestataire de services, tout en garantissant que chaque partie du projet soit achevée de manière satisfaisante avant le versement des fonds correspondants.

Pour une visualisation claire des échéances de paiement convenues, veuillez consulter le graphique ci-dessous :



En ce qui concerne la méthode de paiement, nous avons opté pour le règlement sur facture via virement bancaire, car cette méthode offre plusieurs avantages tant pour notre entreprise que pour nos partenaires.

Le choix du virement bancaire assure un processus de paiement sécurisé, réduisant les risques liés aux transactions financières. Chaque paiement sera accompagné d'une facture détaillée, présentant tous les éléments facturés de manière transparente, ce qui facilite la traçabilité des dépenses et contribue à une gestion financière précise du projet.

De plus, cette méthode est reconnue pour son efficacité, permettant des transactions rapides et fluides entre les parties impliquées, ce qui favorise une collaboration harmonieuse et efficace tout au long du projet.

Politique en cas de retard de paiement :

En cas de retard de paiement, des frais supplémentaires seront appliqués. Pour chaque jour de retard, une majoration de 5% sera ajoutée au montant initial de la facture. Cette mesure vise à souligner l'importance de respecter les délais de paiement convenus.

Nous comprenons que des imprévus peuvent survenir, mais nous encourageons vivement nos partenaires à honorer leurs engagements financiers dans les délais impartis. Non seulement

cela permet de maintenir une bonne relation professionnelle, mais cela évite également des coûts supplémentaires inattendus.

Notre objectif est de favoriser une collaboration fluide et transparente, où les paiements sont effectués en temps voulu pour assurer la stabilité financière du projet.

Politique pour les paiements anticipés :

En reconnaissance des efforts de gestion financière proactive, nous offrons une remise de 2% pour tout paiement anticipé effectué avant la date prévue. Cette remise est un moyen de récompenser nos partenaires commerciaux qui contribuent à accélérer le processus de paiement.

En effectuant des paiements anticipés, nos partenaires démontrent leur engagement envers une gestion efficace des finances et contribuent à renforcer la stabilité financière du projet. Nous encourageons nos partenaires à profiter de cette opportunité de réduction pour maximiser leurs économies tout en maintenant une gestion financière responsable.

Gestion des finances du projet :


La gestion des finances du projet sera effectuée de manière rigoureuse et transparente tout au long de sa réalisation. Les paiements seront suivis et documentés à chaque étape du processus. Pour ce faire, nous utiliserons des outils et des systèmes spécialisés conçus pour gérer efficacement les finances du projet. Ces outils permettront non seulement de suivre les paiements entrants et sortants, mais aussi de documenter chaque transaction de manière précise et détaillée.


Des rapports réguliers seront générés pour fournir une vue d'ensemble de l'état financier du projet. Ces rapports permettront de surveiller les dépenses, d'identifier les tendances éventuelles et de prendre des décisions éclairées en matière de gestion financière. De plus, des audits périodiques sont prévus pour garantir la conformité aux politiques financières établies et assurer la transparence dans toutes les transactions.


Communication sur les paiements :


Pour assurer une communication fluide et efficace concernant les paiements, nous avons établi plusieurs canaux de contact pour répondre à vos questions et résoudre vos préoccupations. Vous pouvez nous contacter par e-mail à l'adresse [securetech.depannage@outlook.com](mailto:securetech.depannage@outlook.com) ou par téléphone au 01 23 45 67 89.

Notre équipe dédiée est là pour vous fournir toute l'assistance nécessaire et vous guider à travers le processus de paiement. Que vous ayez besoin de clarifications sur une facture, des détails sur les méthodes de paiement acceptées, ou toute autre question financière, n'hésitez pas à nous contacter. Votre satisfaction est notre priorité, et nous nous engageons à vous offrir un service clientèle de qualité pour garantir une expérience de paiement transparente et sans souci.

 01 23 45 67 89

 <https://SecureTech.com>

 SecureTech.depannage@outlook.com

 123 Anywhere St., Any City

## 4. Annexes

CONTRAT DE MAINTENANCE LOGICIEL & SYSTÈME

CONTRAT N°001

Nom de l'entreprise PRESTATAIRE : SecureTech

Et,

Nom de l'entreprise CLIENT : PILPRO

Le présent contrat est constitué de pages comprenant six annexes :

ANNEXE - 1 - Tarifs des prestations : AVEC CONTRAT DE TÉLÉMAINTENANCE

ANNEXE - 2 - Tarifs des prestations : PACKS DE MINUTES D'INTERVENTION

ANNEXE - 3 - Tarifs des prestations : CONTRAT D'INTERVENTION ONE SHOT

ANNEXE - 4 - Contrat intervention one shot

ANNEXE - 5 - Choix du type de contrat de télémaintenance

ANNEXE - 6 - Pack de minutes

Est convenu ce qui suit :

## ARTICLE 1 — Objet du contrat

Ce document définit les modalités du présent contrat de télémaintenance, qui a pour objet, le suivi, l'entretien, le dépannage à distance et le maintien en bon état de fonctionnement, des équipements et des ordinateurs décrits en annexe. Les appareils qui font l'objet du contrat doivent avoir été vendus par le Prestataire ou avoir été approuvés comme étant en bon état de fonctionnement par le Prestataire à la date de départ du présent contrat.

## ARTICLE 2 — Télémaintenance préventive

Ce contrat prévoit un diagnostic régulier, fait à distance, afin de contrôler l'évolution et l'intégrité du système. Ce type d'intervention peut uniquement se faire si le CLIENT possède une ligne Internet fonctionnelle et correctement configurée, afin de donner au PRESTATAIRE l'accès à l'ensemble du matériel couvert par le présent contrat. Ces interventions (mensuelle pour les contrats GOLD 8H, trimestrielle pour les contrats PREMIUM et semestrielle pour les contrats STANDARD) seront fixées par le PRESTATAIRE et communiquées au CLIENT afin qu'il valide les dates proposées par le PRESTATAIRE.

Diagnostic à effectuer :

- Vérification des erreurs du système d'exploitation et corrections ;
- Vérification de l'intégrité de la base de registre (systèmes Microsoft) ;
- Vérification des erreurs réseau et correction ;
- Vérification de l'état des disques et maintenance ;
- Mise à jour des pilotes matériels ;
- Mise à jour du système d'exploitation ;
- Mise à jour antivirus ;
- Analyse du système de fichiers par scan antiviral et anti-malware, trojan etc. ;
- Monitoring du Site Internet (si le client en dispose) ;
- Monitoring de la connexion Internet (pour les CLIENTS possédant des adresses IP fixes) ;

## ARTICLE 3 — Dépannage



Ce contrat donne l'accès à une assistance téléphonique et un support par courriel ou via un système d'ouverture de ticket disponible sur la plateforme prévue à cet effet à savoir le site Web de SecureTech dans la rubrique /support/tickets dans les heures d'ouverture des bureaux du PRESTATAIRE définies en annexe. L'ouverture des tickets peut se faire également en envoyant un email à l'adresse [SecureTech.depannage@outlook.com](mailto:SecureTech.depannage@outlook.com).

Le PRESTATAIRE chargera un technicien d'effectuer un diagnostic à distance sur toute demande motivée du CLIENT signalant une anomalie de fonctionnement ou une panne (une confirmation par courriel avec un descriptif succinct du problème doit être envoyée au PRESTATAIRE). Le CLIENT devra afin de permettre la prise de contrôle à distance des équipements à l'origine de la demande d'intervention, se rendre sur la plateforme de SecureTech dans la rubrique /support/assistance pour y télécharger l'application "Teamviewer". Un devis sera proposé au CLIENT qui grâce à ce contrat de télémaintenance bénéficiera de prix avantageux. Les interventions démarreront endéans les 8 H, 24 H ou 48 H à partir de la demande du CLIENT selon les délais contractuels définis en annexe.

#### ARTICLE 4 — Engagement du PRESTATAIRE

Le PRESTATAIRE s'engage à :

1. Mettre à disposition du CLIENT les moyens nécessaires pour assurer une assistance à distance efficace et de qualité ;
2. Mettre en œuvre tous les moyens raisonnables pour répondre aux demandes d'assistance dans les délais contractuels ;
3. Fournir au CLIENT des informations claires et précises concernant les interventions effectuées ;
4. Respecter la confidentialité des données et informations du CLIENT auxquelles il aura accès dans le cadre de ce contrat ;
5. Maintenir un niveau de compétence et de qualification de son personnel technique suffisant pour garantir la qualité des prestations fournies.

#### ARTICLE 5 — Engagement du CLIENT

Le CLIENT s'engage à :

1. Permettre au PRESTATAIRE d'accéder aux équipements couverts par le contrat de télémaintenance, en fournissant les autorisations et les informations nécessaires ;

2. Informer le PRESTATAIRE de toute modification apportée aux équipements couverts par le contrat, susceptibles d'impact sur la télémaintenance ;
3. Signaler au PRESTATAIRE toute anomalie de fonctionnement ou panne dès leur constatation, en fournissant un descriptif précis du problème ;
4. Payer les sommes dues dans les délais convenus.

#### ARTICLE 6 — Durée du contrat

Le présent contrat entre en vigueur à compter de la date de signature par les deux parties et est conclu pour une durée de 2 ans, renouvelable par tacite reconduction pour des périodes successives d'un an, sauf dénonciation par l'une ou l'autre partie, moyennant un préavis de 5 jours par lettre recommandée avec accusé de réception.

#### ARTICLE 7 — Résiliation du contrat

En cas de manquement grave de l'une ou l'autre des parties à ses obligations contractuelles, le présent contrat pourra être résilié de plein droit par l'autre partie, sans préjudice de tous dommages et intérêts.

#### ARTICLE 8 — Prix et modalités de paiement

Le prix des prestations est fixé conformément aux tarifs en vigueur au jour de la signature du contrat, tels que définis en annexe. Les paiements seront effectués par le CLIENT selon les modalités convenues en annexe.

#### ARTICLE 9 — Litiges

En cas de litige relatif à l'exécution ou à l'interprétation du présent contrat, les parties s'efforceront de trouver une solution à l'amiable. À défaut, les tribunaux compétents seront ceux du ressort du siège social du PRESTATAIRE.

#### ARTICLE 10 — Communication entre les parties

Toute correspondance entre les parties concernant l'exécution du présent contrat sera effectuée par courrier recommandé avec accusé de réception ou par voie électronique, aux adresses mentionnées en tête du contrat.

#### ARTICLE 11 — Loi applicable

Le présent contrat est régi par le droit [Préciser le droit applicable].

Fait en deux exemplaires originaux à Montbéliard , le 10 Avril 2024.

Pour le CLIENT, Pour le PRESTATAIRE,

[Signature du CLIENT]

[Signature du représentant du PRESTATAIRE]



## Annexe 1 - Tarifs des prestations

Descriptions	Tarifs horaires HTVA		
	STANDARD 48H	PREMIUM 24H	GOLD 8H
Du lundi au vendredi de 8h00 à 18h00	39 €	49 €	59 €
De 18h00 à 21h00 hors WE et jours fériés	49 €	59 €	69 €
WE et jours fériés	69 €	79 €	89 €

Prix du contrat de télémaintenance (HTVA / par mois / par pc)			
	STANDARD 48H	PREMIUM 24H	GOLD 8H
Par périphérique	14 €	26 €	39 €

## Annexe 2 - PACKS DE MINUTES D'INTERVENTION

Les modalités de paiement convenues entre les parties sont les suivantes :

Prix total HTVA des packs de minutes			
	Du lundi au vendredi de 8h00 à 18h00	De 18h00 à 21h00 hors WE et jours fériés	WE et jours fériés
20 minutes	20 €	+20%	+40%
60 minutes (1 heure)	59 €	+20%	+40%
120 minutes (2 heures)	114 €	+20%	+40%
240 minutes (4 heures)	226 €	+20%	+40%
480 minutes (8 heures)	443 €	+20%	+40%
600 minutes (10 heures)	540 €	+20%	+40%
1200 minutes (20 heures)	980 €	+20%	+40%
3000 minutes (50 heures)	2.350 €	+20%	+40%
+ Sur devis			

### Annexe 3 - Tarif contrat one shot

Descriptions	CONTRAT ONE SHOT	
	Tarifs horaires HTVA	
	1 <sup>ère</sup> tranche de 20 minutes	20 minutes supplémentaires
Du lundi au vendredi de 8h00 à 18h00	25 €	25 €
De 18h00 à 21h00 hors WE et jours fériés	35 €	30 €
WE et jours fériés	45 €	35 €

### Annexe 4 - Contrat intervention one shot

☐ Je souscris à un "CONTRAT D'INTERVENTION ONE SHOT"

J'ai pris connaissance de tarifs d'intervention et conditions d'interventions

Date souhaitée pour la première intervention de télémaintenance préventive : \_\_\_\_/\_\_\_\_/\_\_\_\_

Pour l'Entreprise SecureTech

Pour le PRESTATAIRE

### Annexe 5 - Contrat de Télémaintenance

☐ Je souscris à un "Contrat de Télémaintenance Standard".

☐ Je souscris à un "Contrat de Télémaintenance Premium".



☐ Je souscris à un "Contrat de Télémaintenance Gold".

Les mensualités seront de \_\_\_\_\_ pour \_\_\_\_\_ avec un délai d'assistance garanti endéans les \_\_\_\_\_ [Nombre d'heures] heures.

Date souhaitée pour la première intervention de télémaintenance préventive : \_\_\_\_/\_\_\_\_/\_\_\_\_

Pour l'Entreprise SecureTech

Pour le PRESTATAIRE



#### Annexe 6 -Contrat minute intervention

- ☐ J'achète un pack de 20 minutes.
- ☐ J'achète un pack de 60 minutes (1 heure).
- ☐ J'achète un pack de 120 minutes (2 heures).
- ☐ J'achète un pack de 240 minutes (4 heures).
- ☐ J'achète un pack de 480 minutes (8 heures).
- ☐ J'achète un pack de 600 minutes (10 heures).
- ☐ J'achète un pack de 1200 minutes (20 heures).
- ☐ J'achète un pack de 3000 minutes (50 heures).

Le prix du pack sera de \_\_\_\_\_ [Montant en devise] avec un délai d'assistance garanti endéans les 24 heures à partir de la prise d'appel.

Pour l'Entreprise SecureTech

Pour le PRESTATAIRE







## SECURETECH

123 Anywhere St.,  
Any City, ST 12345  
Tél : 01 23 45 67 89  
Mail : securetech.depannage@outlook.com

## DEVIS N° 0123456

Date : 01/02/2030  
Code client : 012345  
Devis valable 2 semaines

## DESCRIPTION :

Renouvellement des équipements de sécurité et configuration de ces mêmes équipements chez l'entreprise PILPRO.

Désignation	Unité	Quantité	Prix Unitaire HT	Total HT
Désinstallation des éléments existants	jour	1	534€	1600€
Commande des nouveaux fire-walls		2	4000€	8000€
licence fortinet avancé		2	2000€	4000€
licence fortinet classique		29	138€	4000€
Ingénieur configuration firewall et rédaction audit	jour	4	3125€	3125€
Frais de déplacement		6	800€	4600€

**Total HT : 25325€**  
**TVA 10% : 2532,5€**  
**Total TTC : 27857,5€**

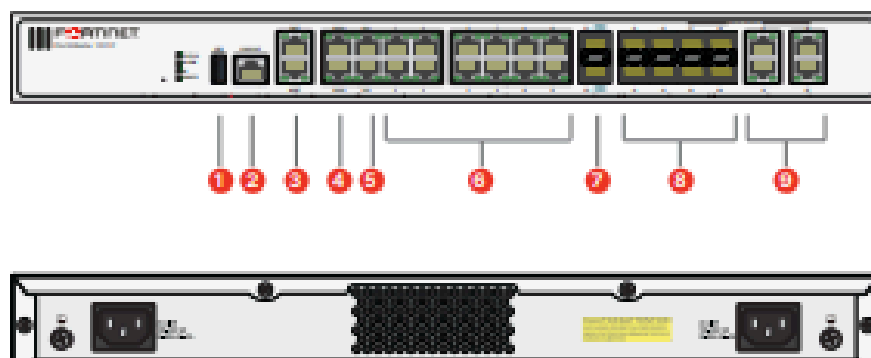
SECURETECH s'engage à réaliser les travaux dans les 15 jours à compter de la signature du devis et du versement de l'acompte pour la somme totale TTC de 27857,5€.

En cas d'acceptation, merci de nous renvoyer ce document avec la date et votre signature précédées de "Bon pour accord".

SIGNATURE

## Hardware

### FortiGate 100F Series



### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/DMZ Ports
4. 2 x GE RJ45 WAN Ports
5. 2 x GE RJ45 HA Ports
6. 12 x GE RJ45 Ports
7. 2 x 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

### Hardware Features



### Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

### Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.



## FortiGate 100F Series

## Data Sheet

### Specifications

	FORTIGATE 100F	FORTIGATE 101F
<b>Interfaces and Modules</b>		
Hardware Accelerated GE RJ45 Ports	12	
Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports	1 / 2 / 1	
Hardware Accelerated GE SFP Slots	4	
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)	2	
GE RJ45 WAN Ports	2	
GE RJ45 or SFP Shared Ports *	4	
USB Port	1	
Console Port	1	
Onboard Storage	0	1x 480 GB SSD
Included Transceivers		0
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		2.6 Gbps
NGFW Throughput <sup>2, 4</sup>		1.6 Gbps
Threat Protection Throughput <sup>2, 4</sup>		1 Gbps
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		20 / 18 / 10 Gbps
Firewall Latency (64 byte, UDP)		4.97 µs
Firewall Throughput (Packet per Second)		15 Mpps
Concurrent Sessions (TCP)		1.5 Million
New Sessions/Second (TCP)		58 000
Firewall Policies		10 000
IPsec VPN Throughput (512 byte) <sup>1</sup>		11.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2000
Client-to-Gateway IPsec VPN Tunnels		16 000
SSL-VPN Throughput		1 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		500
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		1 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		1800
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		135 000
Application Control Throughput (HTTP 64K) <sup>3</sup>		2.2 Gbps
CAPWAP Throughput (HTTP 64K)		15 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		32
Maximum Number of FortiAPs (Total / Tunnel)		128 / 64
Maximum Number of FortiTokens		5000
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 100F	FORTIGATE 101F
Dimensions and Power		
Height x Width x Length (inches)	1.73 x 17 x 10	
Height x Width x Length (mm)	44 x 432 x 254	
Weight	7.25 lbs (3.29 kg)	7.58 lbs (3.43 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Supply	100-240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	26.5 W / 29.5 W	35.3 W / 39.1 W
Current (Maximum)	100V / 1A, 240V / 0.5A	
Heat Dissipation	100.6 BTU/h	121.13 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 90% non-condensing	
Noise Level	40.4 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	USQv6/IPv6	

\* Latency based on Ultra Low Latency (ULL) ports

Caractéristiques du firewall FG100F