Redwan FELFEL
Mourad AMGHAR
Hugo MARTIN

# SAE 401 PilPro

## Entreprise:


Nom de l'entreprise: **SecureTechNet**

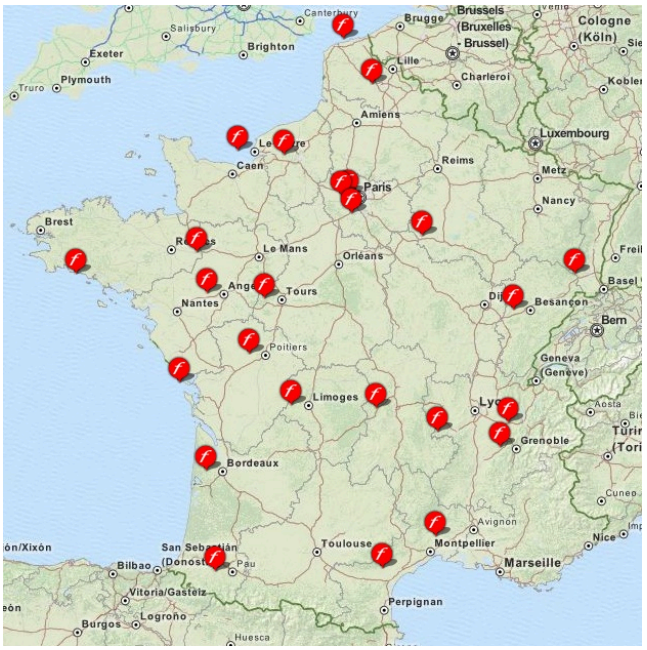
Description de l'entreprise:

SecureTechNet est un leader en matière de cybersécurité, offrant des solutions innovantes et fiables pour protéger les entreprises contre les menaces numériques. Spécialisés dans la configuration de matériel Fortinet et Clavister, nous sommes dédiés à la sécurisation des réseaux, des systèmes et des données, garantissant ainsi la tranquillité d'esprit de nos clients dans un monde numérique en constante évolution.

Départements:

- Développement de solutions de cybersécurité pour les entreprises
- Recherche et développement en cybersécurité
- Ventes et marketing spécialisés dans l'industrie
- Support client et services professionnels

Siège Principal : Basée sur Paris La Défense




Produits et services:

1. Protection des réseaux industriels:
   - Développement de solutions de sécurité pour les réseaux industriels, y compris la protection des systèmes de contrôle et des lignes de production contre les cyberattaques.

2. Sécurité des données et conformité réglementaire:
   - Mise en place de solutions de cryptage, de gestion des identités et des accès, ainsi que de conformité réglementaire pour assurer la confidentialité et l'intégrité des données sensibles des entreprises.

3. Gestion des risques et évaluation de la cybersécurité:
   - Réalisation d'évaluations approfondies de la cybersécurité, d'analyses des risques et de tests de vulnérabilité pour identifier les faiblesses potentielles dans les infrastructures informatiques des entreprises et proposer des mesures correctives.

4. Formation et sensibilisation à la cybersécurité:

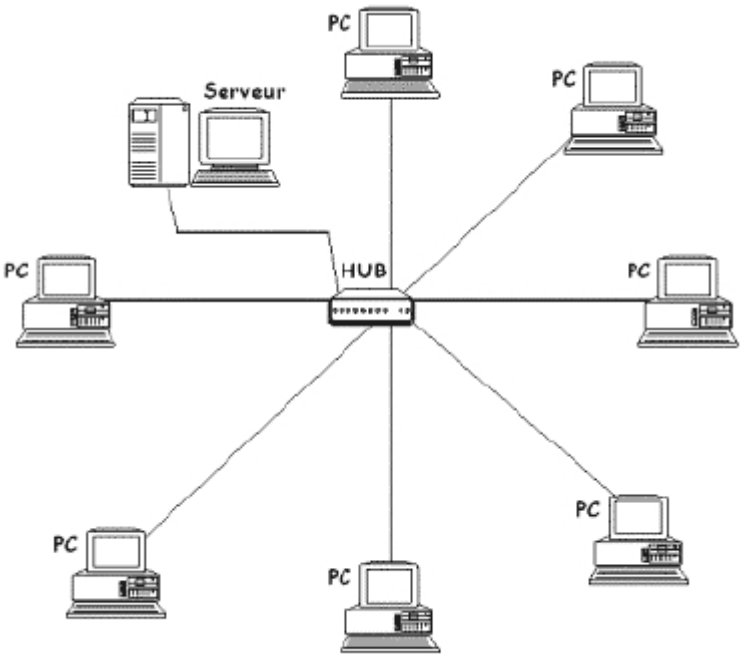
- Offre de programmes de formation sur mesure pour sensibiliser le personnel des entreprises aux meilleures pratiques de cybersécurité et aux menaces actuelles en matière de sécurité informatique.

Approche client:
Nous collaborons étroitement avec nos clients pour comprendre leurs besoins spécifiques en matière de cybersécurité et leur fournir des solutions personnalisées qui répondent à leurs exigences uniques. Notre objectif est d'établir des partenariats à long terme avec nos clients et de les aider à renforcer leur résilience face aux cybermenaces émergentes.

# Matériel existant :

-Infra VMware sur châssis HP DL380
-Stockage MSA 2060
-globalement tout en HP

architecture réseaux entre les différents sites :




VPN (tunnel IP sec ) / ADSL géré en interne

Le vpn opérateur interconnecte environ 30 sites distants par liaisons FTTH 1000M et 4 sites en FTTO 100M/100M. Le débit de l’usine est de 300M/300M (300Mo/s) sur technologie fibre optique

## Firewall : Fortinet FG200E

4 interfaces distinctes : Inside, Outside, DMZ 1 (service wan).
En DMZ1 sont installés :
- Le serveur WEB
- Le serveur DNS publique
- La passerelle de mail
- Le serveur VPN des administrateurs

Demande du client :

-Doublement de firewall :

Pour faire un doublement de firewall une solution souvent utilisée est la méthode actif/passif qui en cas de panne d’un des deux firewall l’autre prend le relais sans interruption.

### 3.6 Administration de la solution

Dans le cadre de ce projet, l'accent est mis sur la gestion efficace et sécurisée de la solution technique. Pour répondre à cet impératif, une approche méthodique a été élaborée afin de satisfaire aux exigences particulières de votre entreprise tout en assurant une expérience d'administration optimale.

#### 3.6.1 Management

Nous nous engageons à fournir une interface d'administration complète et conviviale, permettant une gestion centralisée et simplifiée de l'ensemble des équipements. Voici un aperçu détaillé des fonctionnalités clés de notre approche :

- Interface d'administration sécurisée: Notre priorité est d'assurer la sécurité des échanges entre les administrateurs et l'interface d'administration. Nous mettrons en place des mesures de sécurité robustes, telles que l'authentification à deux facteurs et le cryptage des données, pour protéger l'accès aux informations sensibles.

- Configuration en mode objet: Nous adopterons une approche de configuration en mode "objet" pour faciliter la gestion des politiques de sécurité. Cela permettra aux administrateurs de définir des règles basées sur des éléments spécifiques tels que les machines, les réseaux, les services et les protocoles, simplifiant ainsi la gestion et la maintenance de l'infrastructure.

- Administration centralisée : Notre solution permettra d'administrer plusieurs équipements à partir d'une seule interface, offrant ainsi une gestion centralisée et unifiée de l'ensemble du parc d'équipements. Cette approche réduit la complexité opérationnelle et permet d'économiser du temps et des ressources.

- Représentation graphique de l'architecture : Nous fournirons une représentation visuelle de l'architecture réseau, permettant aux administrateurs de visualiser clairement la topologie du réseau, y compris les équipements tels que les pare-feu, les commutateurs et les routeurs. Cette cartographie facilitera la compréhension de l'infrastructure et aidera à identifier rapidement les éventuels problèmes de configuration.

- Supervision et suivi des niveaux d'alarmes : L'interface d'administration offrira des fonctionnalités de supervision en temps réel, permettant aux administrateurs de surveiller les performances des équipements et de recevoir des alertes en cas de dépassement des seuils prédéfinis. Des indicateurs visuels clairs, tels que des indicateurs de couleur rouge/vert, seront utilisés pour signaler les niveaux d'alarmes et assurer une réactivité rapide en cas de problème.

- Gestion centralisée des opérations : Nous mettrons en place des fonctionnalités permettant la réalisation centralisée de tâches courantes telles que la sauvegarde, la mise à jour et le déploiement de politiques. Cela permettra de simplifier les opérations d'administration et de garantir la cohérence des configurations à travers l'ensemble de l'infrastructure.

En résumé, notre approche vise à fournir une interface d'administration complète et sécurisée, répondant aux exigences spécifiques de votre entreprise et facilitant la gestion efficace de votre infrastructure réseau. Nous sommes déterminés à garantir la sécurité et la disponibilité des services tout en offrant une expérience utilisateur optimale à vos administrateurs.

## 3.7. Prestations

Dans le cadre de la mise en œuvre de la solution technique proposée, notre entreprise s'engage à fournir un ensemble complet de prestations pour garantir le déploiement efficace et sécurisé de l'architecture proposée. Nos services seront réalisés par une équipe d'experts expérimentés et qualifiés, sous la supervision directe du responsable de la sécurité des systèmes d'information (RSSI), afin d'assurer la conformité avec les exigences et les normes de sécurité établies.

### Phase d'analyse

Nous débuterons par une phase d'analyse approfondie visant à recueillir tous les éléments nécessaires à la validation de l'architecture proposée. Cette étape cruciale nous permettra de comprendre en détail votre infrastructure existante, vos besoins spécifiques ainsi que les contraintes éventuelles. Nous travaillerons en étroite collaboration avec vos équipes pour garantir une compréhension exhaustive de votre environnement technique.

### Phase de réalisation

Une fois l'analyse terminée et l'architecture validée, notre équipe technique passera à la phase de réalisation. Sous la supervision du RSSI, nous procéderons à la mise en place de l'architecture proposée en respectant les bonnes pratiques de déploiement et de sécurité. Nous veillerons à ce que chaque composant soit installé de manière optimale et configuré selon les spécifications convenues.

### Phase de paramétrage

La phase de paramétrage revêt une importance capitale dans le processus de déploiement. Sous la responsabilité du RSSI, nous nous assurerons que tous les matériels et logiciels sont configurés de manière adéquate, en tenant compte de vos besoins spécifiques en termes de sécurité et de performance. Chaque paramètre sera minutieusement ajusté pour garantir un fonctionnement optimal du système.

### Phase de test

Avant de passer à la mise en production, nous procéderons à une batterie de tests exhaustifs. Ces tests permettront d'identifier et de corriger toute anomalie éventuelle, garantissant ainsi la fiabilité et la robustesse de la solution. Nous nous assurerons également que la solution répond à toutes les exigences fonctionnelles et de sécurité définies au préalable.

### Phase de transfert de compétence

Nous attachons une grande importance au transfert de compétences à vos équipes. Notre équipe vous accompagnera dans la prise en main de la solution, en

fournissant une formation approfondie sur son utilisation, son administration et sa maintenance. Nous veillerons à ce que vos équipes soient parfaitement autonomes dans la gestion quotidienne de votre infrastructure.

Phase de validation
Enfin, une fois toutes les étapes précédentes complétées, nous procéderons à une validation complète de la solution en production. Cette validation, prononcée par le RSSI, confirmera le bon fonctionnement de l'ensemble de l'architecture et sa conformité aux exigences spécifiées. Nous nous assurerons également que la mise en production se déroule de manière transparente, minimisant ainsi toute interruption de service pour vos utilisateurs finaux.

Nous nous engageons à fournir un service de qualité, respectant les délais convenus et répondant pleinement à vos attentes. Votre satisfaction et la sécurité de vos systèmes d'information sont notre priorité absolue.

Adaptation des règles de sécurité existantes

En accord avec vos besoins spécifiques, notre équipe s'engage à fournir une adaptation soigneuse des règles de sécurité existantes à votre infrastructure. Après avoir récupéré les règles constitutives du pare-feu actuel, comprenant les règles de protocoles et les tables de translation, nous proposerons une analyse approfondie pour déterminer les ajustements nécessaires afin d'améliorer la sécurité des différentes zones de votre réseau.

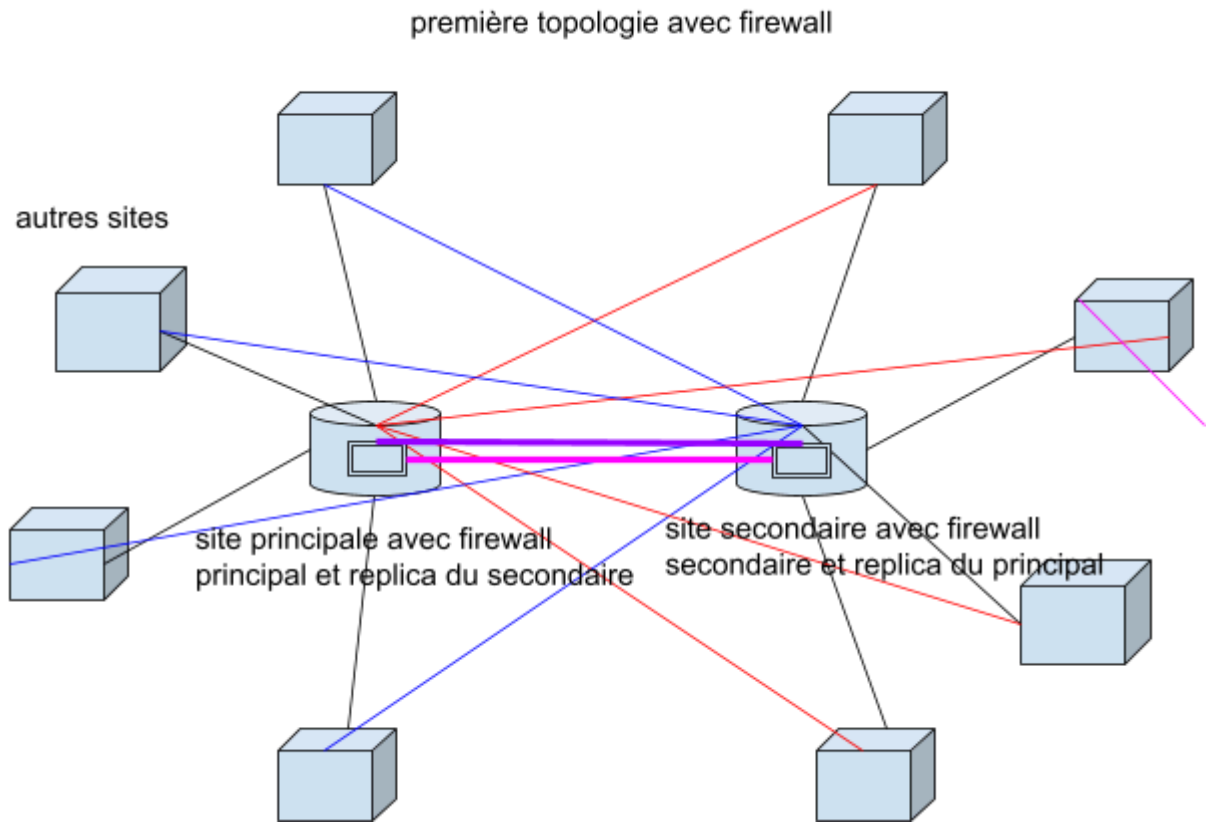
Nous élaborerons une nouvelle liste de règles à implémenter, en prenant en considération les exigences spécifiques de votre entreprise et en nous assurant que chaque règle est en adéquation avec les normes de sécurité les plus strictes.

Implémentation et test des configurations de sécurité
Une fois les nouvelles règles de sécurité définies et validées par votre équipe, nous procéderons à l'implémentation et au test des configurations de pare-feu et de VPN. Notre objectif est de minimiser tout impact sur vos opérations en assurant une transition fluide vers la nouvelle infrastructure.

Nous planifierons la mise en production de manière stratégique, en la programmant un vendredi après-midi pour limiter l'interruption des échanges et l'impact sur les utilisateurs internes et externes de votre entreprise. Cette approche garantira une transition en douceur vers la nouvelle infrastructure, tout en maintenant un niveau élevé de disponibilité des services.

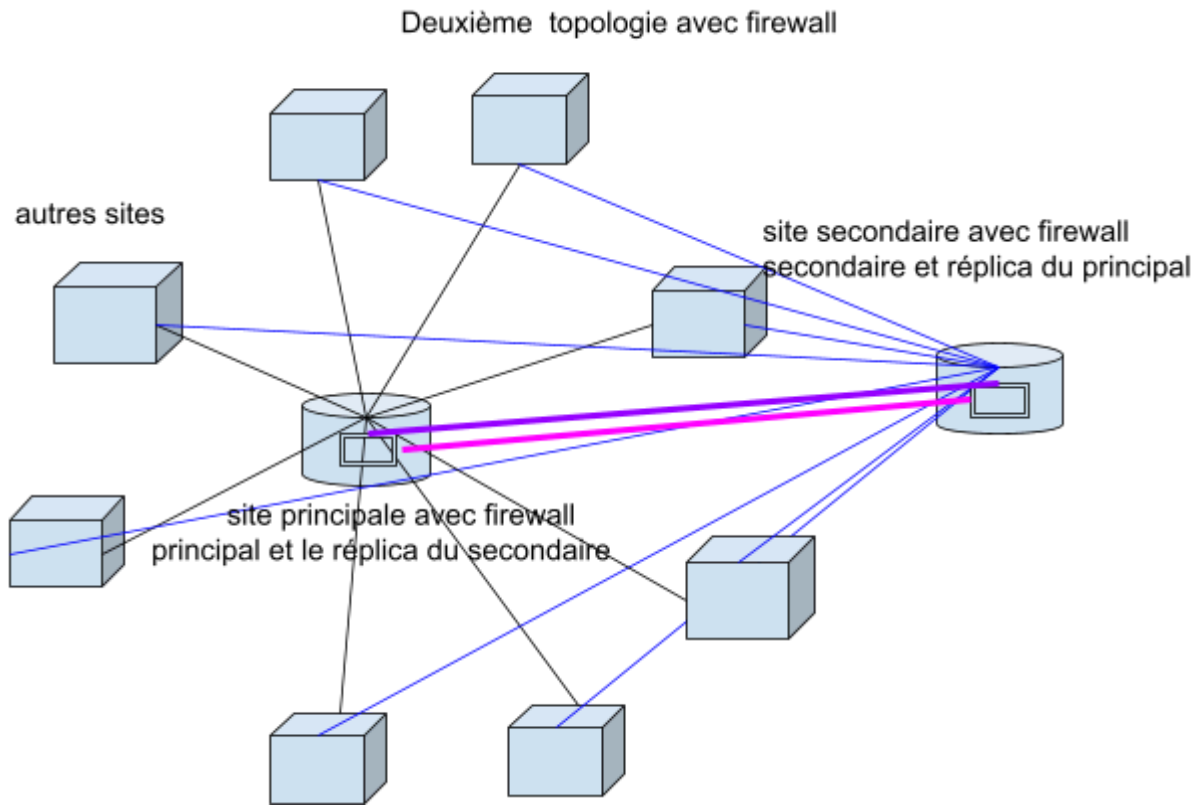
Proposition des solutions :

Une nouvelle infrastructure en double étoile, deux sites seront à prévoir , le site principal et un autre site à définir pour cette solution.
Comme demandé on installera deux firewalls un comme existant dans vos locaux principaux et l'autre dans l'autre structure à définir (soit un autre local à vous soit notre data-center.




Sur cette proposition on propose de garder le site principal mais de rajouter un deuxième site qui pourra être un de vos sites ou notre data-center en topologie de double étoile, mais en divisant par deux les sites que chaque firewall devra gérer.

Aujourd'hui vous avez 30 sites distant soit 15 sites par firewall. Pour assurer la sécurité de chaques sites en cas de pannes ou de dégâts, je propose une solution de réplica c'est à dire que chaques site aura une connexion et une sauvegarde sur le firewall auquel il n'est pas directement relié (connexion rouge et bleu sur le schéma).
Solution peu utilisée car compliqué à mettre en place et spécifique




Sur ce schéma je propose de garder la solution qui est déjà mise en place c'est à dire de mettre 1 firewall sur le site principale et d'y connecter tous les sites distants puis de les connecter à une deuxième Firewall dans un site choisi ( vos sites ou nos sites ) pour pallier à tous problèmes de matériels. Pour chaque site il y aura le firewall dédié et aussi le réplica du firewall distant au cas ou un des deux tombe il pourra reprendre la ou le premier se sera arrêté grâce à une conf qui sauvegarde toutes les données sur les deux (l'actif et le passif ).
Les deux firewalls seront connectés comme ci-dessus (connexion violette et rose), ces deux connexion sont utilisées pour le transfert de données et l'autre pour pinger le firewall distant pour s'assurer de son bon fonctionnement .

intervention

FireWall Fortinet FG 100F 7000€ pour les deux sites Principaux. 3500€ par firewall.

750€ par jour pour configurer le firewall pendant 5-6 jour

800 € d'intervention par jour pendant 3-4 jour pour les deux sites principaux