Dans le cadre de ma formation, je suis chargé de mettre en place une veille technologique afin de suivre les évolutions des dispositifs technique de l'infrastructure, connaître l'état du marché, proposer des évolutions, et anticiper les besoins de formation des utilisateurs.

thème de la veille : **les pare-feux**

Phase A – Initialisation

1. Introduction au patrimoine technologique de GSB

La société GSB possède une infrastructure informatique déployée sur divers emplacements reliés entre eux. Le patrimoine informatique se compose de serveurs, qu'ils soient physique ou virtuel, de postes de travail, d'équipements réseau (commutateurs, routeurs, points d'accès Wi-Fi) ainsi que des logiciels qui assurent la gestion et la protection du système d'information. Chaque site possède un système de pare-feu, assurant la protection des données en transit entrant et sortant. Un Active Directory centralisé facilite la gestion des utilisateurs et des ressources. Les solutions de sauvegarde garantissent la continuité des opérations, tandis que les outils de monitoring offrent une surveillance en temps réel de l'état du réseau et des serveurs.

2. Moyens techniques

GSB emploie diverses technologies pour garantir le fonctionnement correct de son infrastructure. Au niveau matériel, on utilise des serveurs, des switchs pour administrer le réseau local, des points d'accès Wi-Fi pour la connexion sans fil, des routeurs pour gérer les connexions externe, et des NAS pour le stockage de données. En ce qui concerne le logiciel et GSB se sert de Windows Server pour gérer le réseau.

3. Éléments techniques à mettre sous veille

Parmis l'ensemble des technologies utilisées, quatre ont été identifiées comme prioritaire pour une veille technologique :

1. **Les pare-feux**, élément central de la cybersécurité
2. **Les systèmes de sauvegarde**, essentiels pour la continuité d'activité
3. **La virtualisation**, qui permet de réduire les coûts et optimiser les ressources
4. **La supervision**, nécessaire pour assurer la disponibilité des services informatiques

4. Choix argumenté : les pare-feux

Les pare-feux sont des outils indispensables pour la sécurité informatique. Ils permettent de gérer les flux de données, de prévenir des intrusions et de protéger les ressources internes. Dans un contexte où les cybermenaces sont en constante évolution, il est primordial d'assurer une veille active sur ces dispositifs. Par ailleurs, la conformité avec les réglementations (comme le RGPD) impose un haut niveau de sécurité des systèmes. Enfin, la diversité des solutions (open source comme pfSense ou commerciales comme FortiGate) nécessite une veille constante pour suivre leurs évolutions.

Phase B – Choix des sujets de veille

5. Technologies retenues

Deux technologies de pare-feu ont été choisies :

- **pfSense** : solution open source connue pour sa flexibilité, ses fonctionnalités diverses (NAT, VPN, filtrage, détection intrusions) et sa communauté active. pfSense est idéal pour les PME et les environnements techniques limités en budget.

- **Fortinet FortiGate** : solution commerciale haut de gamme, reconnue pour son efficacité, son intégration avec d'autres produits Fortinet, et ses fonctionnalités UTM (filtrage web, antivirus, IPS). Elle est très présente dans les grandes entreprises.

6. Risques à surveiller

Si aucune veille n'est effectuée, plusieurs risques apparaissent :

- Non-mise à jour des signatures de menaces
- Exposition à des failles de sécurité non corrigées
- Diminution de la performance du pare-feu
- Incompatibilités avec de nouveaux systèmes

Pour les autres technologies non retenues, les risques sont aussi réels :

- **Supervision** : mauvaise détection d'incidents
- **Sauvegarde** : perte de données critiques
- **Virtualisation** : exploitation inefficace des ressources serveur

Phase C – Mise en place de la veille

7. Veille active

La veille active repose sur une recherche volontaire et planifiée d'informations. Elle inclut :

- La consultation des sites officiels des éditeurs (pfSense.org, fortinet.com)
- L'inscription à des newsletters spécialisées (Fortinet Security Fabric, Netgate News)
- La lecture de flux RSS de sites comme LeMagIT, ZDNet ou 01net Pro
- Le visionnage de chaînes YouTube techniques sur les pare-feux
- La participation à des forums (Reddit, Spiceworks)

8. Veille passive

La veille passive consiste à recevoir des informations automatiquement. Elle comprend :

- Les Google Alertes sur des mots-clés ciblés
- Les publications LinkedIn de spécialistes de la cybersécurité
- Les actualités partagées sur Twitter/X par les éditeurs et chercheurs

9. Stratégie

La stratégie de veille mise en place s'appuie sur un rythme hebdomadaire pour la veille active, complété par des alertes quotidiennes via la veille passive. Cette approche garantit une couverture large et régulière durant toute l'année scolaire.

Phase D – Exploitation de la veille

10. Crédibilité des sources

On connaît les sources utilisées dans le domaine de l'informatique. Les sites des éditeurs offrent des renseignements fiables et actualisés. Plusieurs sites effectuent une validation croisée et l'analyse des documents CERT contribuent à renforcer la pertinence des données recueillies.

11. Coûts / Bénéfices

Le coût de la surveillance technologique est restreint (principalement du temps humain), mais il permet de diminuer les dangers informatiques, de prévoir les besoins en équipement ou en formation, et d'améliorer la réactivité de l'entreprise face aux risques.

12. Sous-traitance de la veille ?

La sous-traitance peut s'avérer bénéfique pour les sociétés qui manquent de compétences internes. Toutefois, cela conduit à une diminution de la maîtrise des informations stratégiques et à un coût supplémentaire. Il est préférable pour GSB, qui possède un service informatique, de maintenir cette compétence en interne.

13. Recommandations

La mise à jour des pare-feux, les audits de sécurité réguliers et la formation des techniciens aux nouvelles fonctionnalités (IPS ou filtrage applicatif) sont recommandés. Il est également nécessaire de mettre en œuvre une documentation interne et une politique de mise à jour continue.

14. Évolution des pare-feux sur les deux années

Durant les deux années de BTS SIO SISR, j'ai pu mené une veille portant sur les pare-feux, sur les évolutions technologiques des routeurs, des tendances du marché, et des pratiques en entreprise.

(Première année) découverte

Au début de ma veille, j'ai concentré mes recherches sur les solutions utilisées à l'époque chez GSB, à savoir des **routeurs classiques** avec quelques fonctions de sécurité intégrées. Ces équipements permettaient de faire du NAT, de gérer les ports, et de mettre en place un filtrage très basique par adresse IP. Ils répondaient aux besoins initiaux, mais ne suffisaient plus pour une sécurité efficace face aux menaces modernes.

En parallèle, je me suis intéressé aux bases des pare-feux :

- Fonctionnement des **pare-feux à états**
- Différences entre **filtrage réseau** et **filtrage applicatif**
- Introduction aux concepts de **NAT, DMZ, VPN, proxy, IDS/IPS**

(Deuxième année) Approfondissement et nouvelles orientations

En deuxième année, la veille s'est intensifiée, notamment avec l'arrivée de **pFsense** dans certains sites de GSB. Cela m'a permis de comparer deux approches :

- **pfSense** : flexible, économique, hautement personnalisable, mais nécessitant des compétences techniques solides.
- **FortiGate** : prêt à l'emploi, très sécurisé, doté de fonctionnalités avancées (UTM, antivirus, filtrage applicatif, IPS/IDS, SD-WAN, etc.), mais payant.

Au fil du temps, j'ai aussi suivi l'évolution des fonctionnalités proposées par les pare-feux nouvelle génération, telles que :

- L'intégration de **l'intelligence artificielle pour la détection comportementale**
- Le **filtrage HTTPS avec inspection SSL/TLS**
- La **gestion centralisée** via des consoles cloud (FortiManager, pfSense Plus)

- L’apparition d’offres **Firewall-as-a-Service** (FWaaS), dans un contexte de télétravail et de cloud croissant

J’ai remarqué que les pare-feux sont maintenant considérés comme des plateformes de sécurité complètes, dépassant largement leur fonction historique de filtrage réseau. De nos jours, les fonctions de base de la sécurité applicative, de la prévention des fuites de données (DLP) et de la conformité réglementaire sont intégrées.

15. Concurrence et comparaison avec d’autres solutions

Tout au long de ma veille, j’ai observé l’évolution du marché des pare-feux et la diversité des solutions proposées. Cela m’a permis de comparer régulièrement les solutions en fonction des besoins de GSB, mais aussi des tendances du secteur.

Évolution du marché

- **Cisco** est resté une valeur sûre pour les grandes entreprises déjà équipées de matériels Cisco, mais reste complexe à administrer.

- **OPNsense** a gagné en visibilité en tant qu’alternative sérieuse à pfSense, avec une interface moderne et des mises à jour fréquentes.

- **Palo Alto Networks** a renforcé sa position dans les grands comptes, notamment grâce à sa plateforme cloud Prisma Access et ses outils d’analytique basés sur l’IA.

- **SonicWall** a étoffé sa gamme de pare-feux pour PME avec des interfaces simplifiées et une bonne prise en charge des VPN.

Comparatif avec les routeurs

Les recherches m'ont permis de constater que de nombreux réseaux utilisent encore des routeurs avec quelques fonctions de filtrage. Cependant, ces solutions, bien qu'intéressantes dans des environnements simples, sont insuffisantes pour garantir une sécurité réseau plus robuste :

Équipement	Type	Sécurité	Adapté à GSB ?
Routeurs classiques (TP-Link, Netgear)	Grand public	Très limitée	❌
Ubiquiti UniFi Security Gateway	PME	Moyenne (VLAN, QoS)	❌
MikroTik RouterOS	Avancé	Bonne avec configuration poussée	❌
pfSense	Open Source NGFW	Très bonne	✅
Fortigate	NGFW commercial	Excellente	✅✅

16. Conclusion

Au cours de ces deux dernières années de veille technologique, j'ai pu enrichir mes compétences au niveau des firewall, comprenant leur importance stratégique au sein d'une infrastructure et les différentes manières dont ils peuvent être mis en œuvre en fonction des besoins spécifiques de l'entreprise.

J'ai pu constater la progression de la sécurité réseau chez GSB, qui est passée d'une simple protection via des routeurs à une approche de cybersécurité solide avec des pare-feux professionnels (pfSense et FortiGate). Cela m'a également donné l'opportunité de juxtaposer différentes options, d'analyser leurs avantages et inconvénients, et de réaliser que la sélection d'un pare-feu est principalement conditionnée par le contexte, les ressources humaines et le niveau de risque tolérable.

Cette expérience m'a sensibilisé à l'importance d'une vigilance constante dans le secteur de la cybersécurité, où des technologies telles que les technologies comme les menaces évoluent très rapidement. Elle constitue un véritable atout pour mes futures fonctions en entreprise.