**Rapport de Projet : Étape 2 - Déploiement**

L'implémentation du déploiement de la solution IDS/IPS a été une étape cruciale dans le renforcement de la sécurité du réseau hospitalier. Initialement, le choix était envisagé, mais au cours des tests et de la mise en place de l'architecture, une transition vers *Security Onion* a été préférée en raison de sa gestion de la sécurité, en effet *OSSEC* est un “Host Intrusion Detection Systems“ (HIDS) or *Security Onion* est un “Network Intrusion Detection Systems” (NIDS).

1. *Architecture Réseau* :

Dans le cadre des directives spécifiques de l'hôpital, nous avons pris la décision stratégique d'utiliser le routeur existant comme pare-feu, écartant ainsi des solutions tierces telles que StormShield ou pfSense. Cette orientation résulte de la nécessité d'adhérer à une politique d'utilisation de services gratuits et faciles à manipuler, tout en assurant une sécurité adéquate du réseau. De plus, le cloisonnement via des VLANs isolé judicieusement les différents services du réseau, réduisant ainsi la surface d'attaque.

2. *Positionnement de l'IDS/IPS* :

L'IDS Security Onion est délibérément positionné entre le routeur et le réseau externe, utilisant une approche de détection inline. Cela signifie que le trafic réseau traverse physiquement l'IDS/IPS sur son chemin vers sa destination, permettant ainsi à l'IDS/IPS d'analyser et de prendre des mesures en temps réel. .

3. *Gestion du Cloisonnemen*t :

La gestion du cloisonnement est cruciale pour limiter la propagation d'attaques à l'intérieur du réseau. Des règles de pare-feu ont été déployées pour délimiter les parties du réseau, et l'utilisation de VLANs isole des services spécifiques. Par exemple, les serveurs ADDS, de messagerie, de base de données, les terminaux, et les postes de contrôle sont isolés dans des VLANs distincts, renforçant ainsi la protection du réseau contre les mouvements latéraux d'attaques.

4. *Règles de Pare-feu :*

L'un des aspects cruciaux de l'architecture réseau est la mise en place de règles de pare-feu pour renforcer la sécurité à chaque niveau de la structure. Les règles de pare-feu sont élaborées avec une approche stratégique pour maximiser la protection des services et des données médicales sensibles.

4.1 *Pare-feu au Niveau de l'IDS Security Onion :*

L'IDS Security Onion, positionné en amont du routeur, joue un rôle essentiel dans la première ligne de défense contre les menaces potentielles. Les règles de pare-feu à ce niveau visent à :

* Autoriser sélectivement le trafic entrant basé sur des adresses IP spécifiques.
* Bloquer tout trafic suspect ou malveillant dès son entrée dans le réseau.

Cela assure une détection précoce et une prévention proactive des intrusions, minimisant ainsi les risques dès le début du parcours du trafic.

4.2 *Pare-feu au Niveau du Routeur :*

Le routeur, agissant comme pare-feu entre les différentes parties du réseau, est configuré avec des règles précises pour garantir un cloisonnement sécurisé. Ces règles de pare-feu se concentrent sur :

* Limiter l'accès entre les VLANs pour éviter tout mouvement non autorisé d'un réseau à un autre.
* Autoriser sélectivement le trafic entre les segments qui nécessitent une communication. Tel que les postes qui devront interagir avec le serveur Web

Ainsi, le routeur fonctionne comme un point de contrôle central, régulant le flux de données entre les services spécifiques et renforçant la protection du réseau.

4.3 *Pare-feu au Niveau des Serveurs et Services :*

À chaque niveau de service, des règles de pare-feu sont mises en œuvre pour personnaliser la protection en fonction des exigences spécifiques. Par exemple :

* Les serveurs ADDS et de messagerie (VLAN 40) ont des règles restreignant l'accès à des plages d'adresses IP autorisées.
* La base de données (VLAN 30) a des règles strictes pour contrôler l'accès, limitant la communication aux seuls services nécessaires.

Cette approche garantit que chaque service est protégé individuellement et que seules les communications autorisées sont permises.

5. *Installation et Configuration* :

L'installation de l'infrastructure matérielle a été réalisée avec une attention particulière à la connectivité entre les composants. La solution IDS/IPS, Security Onion, a été installée et configurée selon les exigences du projet. Des ajustements ont été apportés pour optimiser la détection tout en minimisant l'impact opérationnel, assurant ainsi une intégration fluide dans l'environnement existant du réseau hospitalier.

6. *Performances Générales* :

Les tests ont confirmé que la plupart des services fonctionnaient de manière optimale. Cependant, il est important de noter que nous avons identifié quelques problèmes avec certaines règles du pare-feu. Malgré ces challenges, le pare-feu a démontré une efficacité notable dans son rôle de protection, filtrant le trafic conformément aux règles définies dans la mesure du possible. Ces problèmes identifiés seront rapidement résolus dans le cadre de la phase d'optimisation continue du projet.

**Conclusion**

Les résultats obtenus à l'issue de ces tests confirment la réussite de la mise en œuvre de notre infrastructure, offrant ainsi une protection solide et adaptée aux besoins du réseau du centre hospitalier. En conclusion, cette étape de déploiement établit une infrastructure solide pour le bon fonctionnement des différents services mis en place dans le réseau hospitalier. La supervision continue, la démonstration des capacités de la solution, et l'optimisation constante face aux menaces constituent la prochaine phase du projet.