Documentation de la Mise en place d’un pare-feu

FALLA Anthony, Mathis Jacquet, Ibrahim Charpentier, Youssef Idouchbareg, Olivier Cogne, Walid Heddadj, Axel Boutot

Table des matières

Introduction : 2

Définition : 2

Sélection du type de pare-feu : 2

Configurer le pare-feu : 2

Tests et validation 3

Maintenance du pare-feu 3

Conclusion 3

Introduction :

Afin de fournir un environnement sécurisé sur la machine, il est nécessaire de mettre en place un pare-feu. Il existe plusieurs méthodes pour le mettre en place. Mais avant tout, il est indispensable de déterminer les objectifs de sécurité que l'on souhaite atteindre. Cela peut aller d'une limitation de la navigation sur internet à une protection contre les attaques externes.

Attention, il est important de noter qu'aucune méthode ne garantit à 100 % une protection infaillible.

Définition :

Un pare-feu ou firewall en anglais est un logiciel ou matériel ayant pour objectif de filtrer les interactions sur le réseau. Le firewall protège un réseau particulier ou professionnel du réseau public à savoir internet.

Sélection du type de pare-feu :

Il existe 2 types de pare-feu. Tout d'abord, il existe les pare-feu logiciel, c'est-à-dire qu'il s'agit d'une application présente sur la machine. Le deuxième type de pare-feu est le pare-feu matériel ou physique, ce qui signifie que le pare-feu est connecté au réseau à l'aide de câbles. Chacun de ces 2 types ont leurs avantages et inconvénients.

En effet, les pare-feu logiciel sont plus flexibles et abordables mais une puissance de calcul limité. Il existe des logiciels tel que Windows Defender Firewall, pfSense ou encore IPTables. A l'inverse, les pares-feux matériels sont plus performants mais moins flexibles et plus coûteux. Il existe des pares-feux de périphérie, pour entreprise, pour des datacenters, nouvelle génération ainsi que des pare-feu UTM.

Il est donc important de prendre en compte les caractéristiques des 2 types de pare-feu afin de configurer celui répondant à nos objectifs de sécurité.

Configurer le pare-feu :

Lorsque vous êtes certain du pare-feu utilisé, il faut à présent le configurer. Tout d'abord, il est conseillé de noter les autorisations et les interdictions des services et applications transitant sur le réseau. Ensuite, il faut configurer les ports ouverts ainsi que les protocoles de communication. Cela permet de restreindre le nombre d'accès. Une fois toutes les mesures mis en place, il est recommandé de vérifier le fonctionnement du pare-feu en faisant des tests. Si des erreurs se produisent, les erreurs apparaitront dans le dossier log du pare-feu. De ce fait, il est important d'activer le système de logs puisqu'en plus erreurs, il est possible de repérer des comportements suspects tel que des entrées illicites ainsi que l'envoi de données sur le réseau. Notons également qu'il faut ajouter des alertes en cas de problème ou d'évènement inhabituel.

Tests et validation

Afin de s’assurer que le pare-feu est correctement configuré, il est indispensable de faire des tests avant sa mise en marche définitive. Pour ce faire, il suffit de tester des adresses ip qui doivent être bloqués et que chaque utilisateur et service (s’il s’agit dune entreprise) puissent accéder à ce qu’ils peuvent normalement accéder sans interruption. Ces tests permettent de valider le bon fonctionnement du pare-feu.

Maintenance du pare-feu

Afin de bloquer les nouvelles menaces, il est important d’effectuer des mises à jour régulières des règles mises en place. De plus, il est recommandé de toujours surveiller les logs ainsi que les alertes afin de réagir le plus rapidement possible en cas d’attaque.

Conclusion

En suivant toutes ces étapes, vous serez capable du point de vue théorique de mettre en place un pare-feu fonctionnel et efficace.