Firewall

Un Firewall (pare-feu en français) est un appareil de protection de réseaux. Il surveille le trafic entrant/sortant, et autorise ou bloque le trafic basé sur un ensemble de règles définies au préalable.

Il existe plusieurs types de pare-feu : le pare-feu sans état, avec état, applicatif, et de nouvelle génération.

- Les pare-feu sans-état utilisent des informations concernant la destination d'un paquet de données, sa provenance et d'autres paramètres pour déterminer si les données présentent une menace. Ces paramètres doivent être saisis par un administrateur ou par le fabricant au moyen de règles qu'ils ont définies au préalable. Si un paquet de données sort des paramètres considérés comme acceptables, le pare-feu sans état peut identifier la menace et restreindre ou bloquer les données qui l'hébergent.
- Un pare-feu avec état inspecte tout ce qui se trouve dans les paquets de données, les caractéristiques des données et leurs canaux de communication. Les pare-feu avec état examinent le comportement des paquets de données et, si quelque chose semble anormal, ils peuvent filtrer les données suspectes. En outre, un pare-feu peut apprendre comment les données se comportent, en cataloguant les modèles de comportement.
  Si l'examen d'un paquet de données révèle un comportement suspect - même si ce type de comportement n'a pas été saisi manuellement par un administrateur - le pare-feu peut le reconnaître et traiter la menace. Il peut être utilisé à la périphérie d'un réseau ou à

l'intérieur, comme c'est le cas d'un pare-feu à segmentation interne (ISFW), qui protège des segments spécifiques du réseau au cas où un code malveillant s'y introduirait.

- Un pare-feu d'application Web aide à protéger les applications Web en filtrant et en surveillant le trafic HTTP entre une application Web et Internet. Il protège généralement les applications Web contre les attaques telles que la falsification intersites, le cross-site-scripting (XSS), l'inclusion de fichiers et l'injection SQL, entre autres. C'est une défense de la couche 7 du protocole (dans le modèle OSI), et n'est pas conçu pour se défendre contre tous les types d'attaques. Cette méthode d'atténuation des attaques fait généralement partie d'une suite d'outils qui, ensemble, créent une défense globale contre une série de vecteurs d'attaque.
- Les NGFW (Next Generation Firewall) sont la dernière génération de pare-feu.
  Ils vérifient non seulement la conformité complète d'un paquet, mais aussi qu'il correspond au protocole attendu. Ainsi, un paquet qui veut passer par le port TCP 80 devra utiliser le protocole HTTP. De même, ils permettent la gestion de la qualité de service (QOS : Quality Of Service), le blocage d'URL, l'inspection approfondie des paquets (DPI : Deep packet inspection), SSL / SSH ou la détection de malwares. Les options sont si nombreuses que la configuration d'un tel dispositif peut devenir très complexe et nécessiter l'intervention de spécialistes.
  En bref, les NGFW ont la capacité de comprendre et de prendre des décisions en analysant les détails du trafic. Ceci a deux implications majeures : tout d'abord, un traitement gourmand en temps de calcul (en fonction du débit binaire). Deux éléments, un besoin de mises à jour régulières afin de pouvoir contrôler les dernières menaces.

Revision #4
Created 12 April 2021 15:48:22 by Khroners
Updated 13 April 2021 10:52:12 by Khroners