WIKIPÉDIA

Pare-feu à états

En informatique, un **pare-feu à états** (''stateful firewall", ''stateful inspection firewall" ou ''stateful packet inspection firewall" en anglais) est un pare-feu qui garde en mémoire l'état de connexions réseau (comme les flux TCP, les communications UDP) qui le traversent. Le fait de garder en souvenir les états de connexions précédents permet de mieux détecter et écarter les intrusions et assurer une meilleure sécurité. Le pare-feu est programmé pour distinguer les paquets légitimes pour différents types de connexions. Seuls les paquets qui correspondent à une connexion active connue seront autorisés par le pare-feu, d'autres seront rejetés.

L'inspection d'état (''stateful inspection"), appelée aussi le filtrage dynamique (''Dynamic Packet Filtering") est une fonctionnalité de sécurité qui est souvent implémentée dans des réseaux d'entreprises. Cette fonctionnalité a été inventée par Check Point Software, qui l'a lancée avec leur logiciel FireWall-1 en 1994 [1], et dont le brevet a été déposé le 15 décembre 1993. [2] Cependant, le principe avait déjà été mis au point par une société française du nom d'ACE TIMING pour son produit Système d'Interconnexion Sécurisé (SIS) entre 1992 et 1993. Cette dernière n'a pas déposé de brevet à ce propos.

Sommaire

Origines et principes

Avant l'arrivée des pare-feu à états, un ''pare-feu sans état" (''stateless firewall"), qui traite chaque trame (ou paquet) de manière isolée, était normal. Ce pare-feu « primitif », qui filtre les paquets en opérant au niveau de la couche réseau (couche 3 du modèle OSI) et qui est plus efficace car il ne regarde que l'en-tête de chaque paquet. Mais comme il ne garde pas en mémoire les paquets précédents, donc les états précédents de connexion, il est vulnérable aux attaques d'usurpation (spoofing attack **(en)**). Ce pare-feu n'a aucun moyen de savoir si un paquet donné fait partie d'une connexion existante, ou tente d'établir une nouvelle connexion, ou est juste un paquet voyou.

Les pare-feu à états, eux, sont conscients des états de connexion, et offrent aux administrateurs réseau un contrôle plus fin du trafic réseau. L'exemple classique d'une opération de réseau qui peut échouer avec un pare-feu sans état est le File Transfer Protocol (FTP). De par leur conception, ces protocoles doivent être en mesure d'ouvrir des connexions aux ports élevés arbitraires pour fonctionner correctement. Étant donné qu'un pare-feu sans état n'a aucun moyen de savoir que le paquet destiné au réseau protégé (à destination du port 4970 d'un certain hôte, par exemple) fait partie d'une session FTP légitime, il laissera tomber le paquet. Les pare-feu à états résolvent ce problème en maintenant un tableau des connexions ouvertes et en associant intelligemment les nouvelles demandes de connexion avec des connexions légitimes existantes.

Description

Mémorisation de l'historique

Un pare-feu à états assure le suivi de l'état des connexions de réseau (tels que les flux TCP ou UDP) et est capable de garder en mémoire les attributs significatifs de chaque connexion. Ces attributs sont collectivement connus en tant qu'état de la connexion, et peuvent inclure des détails tels que les adresses IP et les ports impliqués dans la connexion et les numéros de séquence des paquets qui traversent la connexion. L'inspection qui tient compte des états (Stateful Inspection) surveille les paquets entrants et sortants dans le temps, ainsi que l'état de la connexion, et stocke les données dans des tableaux dynamiques des états. Ces données cumulatives sont évaluées, de sorte que les décisions de filtrage ne seraient pas seulement basées sur des règles définies par l'administrateur, mais aussi sur le contexte qui a été construit par les connexions précédentes ainsi que les paquets précédents appartenant à la même connexion.

La vérification la plus intensive de l'unité centrale est effectuée au moment de l'établissement de la connexion. Les entrées sont créées uniquement pour les connexions TCP ou les flux UDP qui répondent à une politique de sécurité définie. Après cela, tous les paquets (pour cette session) sont traités rapidement car il est simple et rapide pour déterminer si elle appartient à une session existante, présélectionnée. Les paquets associés à ces sessions sont autorisés à passer à travers le pare-feu. Les sessions qui ne correspondent pas à une politique sont rejetées, tout comme les paquets qui ne correspondent pas à une entrée de table existante.

Expiration des sessions

Afin d'éviter que la table d'état soit saturée, les sessions vont s'expirer s'il n'y a aucun trafic au bout d'un certain moment. Ces connexions périmées sont retirées de la table d'état. Or, cela introduit des coupures de sessions extrêmement gênantes pour plusieurs applications. Pour éviter ce genre d'inconvénient, de nombreuses applications envoient donc périodiquement des messages *keepalive* pour garder la connexion pendant les périodes de non-activité utilisateur, ce que font également certains pare-feu s'ils y sont paramétrés.

Authentification par poignée de main à trois voies

Le pare-feu à états dépend de l'établissement de connexion en « poignée de main à trois voies » (''three-way handshake'') parfois décrit comme "SYN, SYN-ACK, ACK" (montrant l'ordre de l'utilisation des bits SYN (synchronisation) et ACK (acknowledgement : accusé de réception)) du protocole TCP lorsque le protocole utilisé est TCP; si le protocole est UDP, le pare-feu à états ne dépend pas de tout ce qui touche à TCP.

Quand un client ouvre une nouvelle connexion, elle envoie un paquet avec le bit SYN dans le header du paquet. Tous les paquets avec le bit SYN sont considérés par le pare-feu comme de nouvelles connexions. Si le service auquel le client a demandé est disponible sur le serveur, ce service répondra au paquet SYN avec un paquet dans lequel à la fois le bit SYN et le bit ACK sont fixés. Le client répondra alors avec un paquet dans lequel seul le bit ACK est fixé, et la connexion entrera dans l'état ESTABLISHED (établi). Un tel pare-feu va laisser passer tous les paquets sortants, mais permettra seulement des paquets entrants faisant partie d'une connexion établie (ESTABLISHED), protégeant ainsi les machines contre les tentatives d'intrusion de la part des hackers.

Sessions avec des protocoles sans connexion

De nombreux pare-feu à états sont en mesure de pister l'état des flux avec les protocoles sans connexion. UDP, le protocole de type « sans connexion » le plus courant, utilise la technique UDP hole punching qui consiste à envoyer des paquets avec un contenu minimal pour garder la session.

Ces sessions obtiennent habituellement l'état ESTABLISHED immédiatement après que le premier paquet est vu par le pare-feu.

Avec les protocoles sans connexion, les sessions ne peuvent terminer que par time-out.

Limites du concept

Il y a des modèles de pare-feu à états qui peuvent avoir plusieurs fonctionnalités. Par contre, la notion de « pare-feu à états » est simple, et limitée à garder un suivi de l'état de connexion. Pour les connexions existantes, le pare-feu à états ne fait que consulter le tableau des états. Son rôle n'est même pas de vérifier le paquet contre l'ensemble des règles du pare-feu, qui peut être étendu. Aussi, le concept d'inspection approfondie des paquets (deep packet inspection) n'est pas lié à celui du pare-feu à états. Son rôle est seulement de vérifier le trafic entrant contre sa table d'états et d'établir la correspondance ou pas. Il n'a pas besoin de faire de l'inspection approfondie des paquets.

Imperfections

Vulnérabilités

Il existe un risque que les vulnérabilités dans les décodeurs de protocole individuels pourraient permettre à une personne malveillante de prendre le contrôle du pare-feu. Cette préoccupation souligne la nécessité de maintenir un logiciel de pare-feu à jour[3]

Certains pare-feu à états soulèvent également la possibilité que les hôtes individuels peuvent être trompés en sollicitant les connexions externes. Cette possibilité ne peut être complètement éliminée par l'audit du logiciel hôte. Certains pare-feu peuvent être vaincus de cette manière par la simple visualisation d'une page web (soit avec Javascript activé, ou après avoir cliqué sur un bouton)[4].

Références

1. Check Point Introduces Revolutionary Internet Firewall Product Providing Full Internet Connectivity with Security – consulté le 20 novembre 2013 (http://www.checkpoint.com/press/1994/interop_press.html) « Copie archivée » (https://web.archive.org/web/20180723052937/http://www.checkpoint.com/press/1994/interop_press.html) (*version du 23 juillet 2018 sur l'Internet Archive*)
2. System for securing inbound and outbound data packet flow in a computer network – Gil Shwed - Checkpoint Software Technologies Ltd. (Jerusalem, IL) – consulté le 20 novembre 2013 (http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=5,606,668.PN.&OS=PN/5,606,668&RS=PN/5,606,668)
3. The Grumpy Editor's Tomato review – Jonathan Corbet – 11 janvier 2010 – consulté le 16 décembre 2013 - "...both L7-Filter and IPP2P are explicitly unmaintained. Given the steady stream of security updates for protocol dissectors in WireShark, your editor has a hard time believing that these other classifiers can be completely free of security issues." (http://lwn.net/Articles/369367/)
4. Hacker pierces hardware firewalls with web page - No interaction required – Dan Goodin – 6 janvier 2010 – consulté le 16 décembre 2013 (https://www.theregister.co.uk/2010/01/06/web_based_firewall_attack/)

Voir aussi

- Bastion (informatique)
- IPCop
- Juniper Networks
- Liste de pare-feu
- M0n0wall
- Packet Filter
- Pare-feu
- Sécurité informatique