

Juniper protège le datacenter des attaques

DDoS

Les attaques par déni de service DDoS (*Distributed Denial of Service*) et les attaques Web constituent selon les responsables informatiques (60 % pour les premières et 65 % pour les secondes) les pires menaces auxquelles sont confrontées leurs entreprises (étude Ponemon – février 2013).

Rappelons que ces attaques sont presque aussi anciennes que la micro informatique. Elles consistent à perturber les connexions et à empêcher d'accéder à un service réseau ou web en inondant le réseau afin de le saturer.

Le datacenter, qui est au centre de ces services et au cœur du système d'information comme du cloud computing, est la cible privilégiée de ces attaques. La saturation est l'objectif de leurs auteurs, car elle vient grandement perturber le fonctionnement de l'entreprise, voire créer des défaillances qui pourraient entraîner l'ouverture de failles de sécurité.

Junos adopte les mesures pour se protéger

Spécialiste des réseaux, Juniper est bien évidemment un témoin privilégié de ces attaques, et probablement le plus à même d'intégrer dans ses solutions, qui équipent les opérateurs et les systèmes de datacenter, des outils pour s'en protéger.

L'annonce de **Junos DDoS Secure**, la solution de protection des datacenters contre les attaques par déni de service DDoS, est donc stratégique pour Juniper Networks. Grâce à la visibilité détaillée qui lui est offerte sur le réseau et son trafic, accompagnée d'une analyse comportementale, la solution offre une protection évolutive contre les attaques DDoS les plus répandues.

Détection des comportements

Junos DDoS Secure est doté d'un algorithme spécifique nommé CHARM qui analyse le comportement des utilisateurs afin de détecter les activités inhabituelles. D'un côté, le trafic est analysé en continu, ce qui permet d'alimenter une base d'adresses IP dites 'de confiance'. De l'autre, la détection d'un trafic suspect ou non conforme via la dégradation des performances de ressources critiques entraîne une réaction en temps réel. Enfin, des techniques de renseignement distribué dynamique (DDTI) permettent la mise à jour des appliances du réseau dès la détection d'une menace.

Autre fonctionnalité importante de Junos DDoS Secure, la prévention des attaques 'low-and-slow'. Au sein du datacenter, celles-ci visent la couche applicative, mais ne s'engagent qu'une fois entrées dans le datacenter. La solution offre la granularité nécessaire pour réagir tant sur les faux positifs que sur les attaques en volumes.

Protéger les environnements virtualisés

Egalement offre virtuelle, Junos DDoS Secure opère dans les environnements virtualisés, présents sur les infrastructures de cloud computing, avec une compatibilité IPv6. VMware et KVM sont supportés. Cette solution présente deux avantages : elle peut être déployée et configurée rapidement ; et elle peut faire l'objet de services managés proposés par les opérateurs. Dans tous les cas, elle augmente les capacités de bouclier défensif offertes par Junos.

Côté tarification, la licence logicielle 1Gbps (Junos DDoS Secure a la capacité d'aller jusqu'aux 40Gbps) sera proposée au tarif de 18 950 dollars (services de support en supplément) ou 8 950 dollars (services de support inclus) pour une licence annuelle.

Image © nicolasjoseschirado - Fotolia.com

Voir aussi

[Silicon.fr étend son site dédié à l'emploi IT](#)

[Silicon.fr en direct sur les smartphones et tablettes](#)