

RFC 3682 : The Generalized TTL Security Mechanism (GTSM)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juillet 2006. Dernière mise à jour le 1 novembre 2007

Date de publication du RFC : Février 2004

<https://www.bortzmeyer.org/3682.html>

Ce RFC présente un mécanisme de sécurité applicable aux protocoles de routage mais aussi à bien d'autres protocoles : il consiste à tester le TTL des paquets entrants. Il a été remplacé par le RFC 5082¹,

Dans un protocole comme BGP, authentifier le routeur en face et s'assurer que ce n'est pas un méchant, peut être difficile. Comme deux routeurs BGP sont en général adjacents (situés sur le même lien physique), la technique GTSM que propose notre RFC est simplement de vérifier le TTL des paquets BGP entrants. Qu'est-ce que le TTL ? C'est simplement un compteur dans le paquet IP qui est décrémenté par chaque routeur traversé. Si le TTL à l'arrivée est de 255 (la valeur maximale possible), c'est qu'aucun routeur n'a été traversé, donc que le paquet provient bien du réseau local.

Notre RFC recommande donc aux routeurs BGP de ne plus envoyer des paquets avec un TTL de zéro (l'ancien comportement, qui permettait de s'assurer que les paquets ne sortent pas du réseau local, les routeurs jettant les paquets de TTL nul) mais avec un TTL de 255, permettant de détecter les attaques venues de l'extérieur.

Le RFC fournit également une spécification de l'usage de GTSM dans le cas où les deux routeurs ne sont pas adjacents. Il note que cette technique est nettement moins sûre et il est prévu de la retirer de la spécification dans le futur, ce qui a été fait dans le RFC 5082, qui l'a remplacé.

On notera que le TTL se nomme "*Hop Limit*" en IPv6 mais qu'il a la même sémantique (c'est bien un nombre de sauts, pas une durée et c'est le terme de TTL en IPv4 qui est erroné).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5082.txt>