RFC 7610 : DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 septembre 2015

Date de publication du RFC : Août 2015

https://www.bortzmeyer.org/7610.html

Un peu de sécurité IPv6 sur le réseau local : comment protéger les pauvres machines IPv6 contre un méchant serveur DHCP, qui répond à la place du serveur légitime, et plus rapidement que lui ? Pas de surprise, la solution est la même qu'en IPv4 ("*DHCP snooping*") et est détaillée dans ce RFC : le commutateur bloque les réponses DHCP qui viennent d'un port où aucun serveur DHCP n'est censé être présent.

Le mécanisme porte le doux nom de "*DHCP Shield*". DHCP, normalisé dans le RFC 8415[1], est très proche en IPv6 et en IPv4 et, dans les deux cas, n'offre quasiment aucune sécurité. Sur un réseau sans serveur DHCP officiel, une machine peut prétendre être serveur DHCP et tout le monde va la croire et accepter ses annonces. C'est une des plaies des réseaux locaux, d'autant plus qu'authentifier le serveur DHCP est très difficile puisqu'on utilise justement DHCP pour ne rien avoir à configurer sur les machines clientes. Sur un réseau avec serveur DHCP légitime, un faux serveur peut parfois se faire écouter, par exemple s'il répond plus vite. Et, même quand il n'y a qu'un seul serveur DHCP, rien ne garantit que les machines utiliseront uniquement les adresses IP qui leur ont été allouées officiellement.

Pour "*DHCP Shield*", le mode de fonctionnement normal est que l'administrateur réseaux configure le commutateur en lui disant sur quels ports du commutateur se trouve le serveur DHCP légitime. Le commutateur examine alors tous les messages et rejette les réponses DHCP qui viendraient d'un autre port. Le problème d'un serveur DHCP pirate est très proche de celui d'un routeur IPv6 pirate qui envoie des "*Router Advertisement*" (RFC 4861, section 4.2) trompeurs et la solution est donc très proche (pour les RAcailles, les RA illégitimes, le problème était exposé dans le RFC 6104 et la solution, "*RA Guard*", dans les RFC 6105 et RFC 7113).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8415.txt

Voilà pour le principe, les détails maintenant. Un commutateur ordinaire ne protège pas contre les serveurs DHCP pirates. Il faut un "*DHCPv6 Shield Device*" (section 3 du RFC), commutateur « intelligent » capable de mettre en œuvre la technique décrite dans ce RFC. Demandez à votre vendeur avant d'acheter, s'il y a bien les fonctions de "*DHCP Shield*".

Il faut ensuite le configurer explicitement (le commutateur pourrait apprendre seul, en regardant les réponses mais c'est risqué : si le serveur pirate est déjà en service au moment où le commutateur démarre, ce dernier pourrait prendre le pirate pour le serveur légitime). Cette configuration est faite par l'administrateur réseaux, qui désigne le ou les ports du commutateur qui peuvent légitimement voir arriver des réponses DHCPv6, car un serveur légitime se trouve derrière (section 4 du RFC).

Dit comme cela, ça a l'air simple. Mais, dans les réseaux réels, plein de complications peuvent survenir et la section 5 du RFC, sur les problèmes possibles, est **beaucoup** plus longue que la section 4 qui décrit l'algorithme. Premier gag possible, les en-têtes d'extension IPv6 qui sont très difficiles à analyser <https://www.bortzmeyer.org/analyse-pcap-ipv6.html>. Notre RFC impose donc aux mises en œuvre de "*DHCP shield*" d'analyser **tout** le paquet, de ne pas se limiter arbitrairement aux N premiers octets, car la liste des en-têtes peut être longue. (La section 6 note que cela peut être difficile sur le "*fast path*" - mis en oeuvre dans le matériel - des commutateurs et suggère de jeter le paquet si on ne peut pas l'analyser complètement, mais avec une liste de protocoles de transport qui soit configurable, pour éviter de bloquer les nouveaux protocoles apparus après la vente du commutateur.)

Pour aider un peu les pauvres commutateurs, le RFC 7112 impose que, dans un paquet fragmenté, la **totalité** des en-têtes soit dans le premier fragment (autrement, un serveur DHCPv6 pirate pourrait « tricher » en « cachant » la réponse IPv6 dans le deuxième fragment et en espérant qu'il ne soit pas analysé). Le commutateur doit donc jeter les paquets fragmentés dont le premier fragment ne contient pas toute la chaîne des en-têtes. (Interdire que les réponses DHCP soient fragmentées aurait été encore plus efficace mais pouvait être gênant dans certains cas, où il y a un besoin légitime d'envoyer de grandes réponses.) Cette politique peut sembler violente mais, de toute façon, un paquet fragmenté n'incluant pas la totalité des en-têtes n'a déjà quasiment aucune chance de passer les pare-feux actuels.

Il faut aussi prêter attenion aux fragments qui se recouvrent (RFC 5722). Ils peuvent permettre d'échapper à la détection par le commutateur.

Plus contestable, la décision en cas d'en-têtes dont le champ "*Next Header*" est inconnu. Malheureusement, en IPv6, il n'y a pas de moyen garanti de sauter par dessus un tel en-tête (c'est un peu mieux depuis le RFC 6564). Notre RFC 7610 prend donc une décision radicale : par défaut, les paquets IPv6 ayant un tel en-tête doivent être jetés sans merci. Une option du commutateur doit permettre, si l'administrateur le demande, de les accepter (cf. RFC 7045 pour un point de vue plus général sur la question).

Si le paquet est protégé par IPsec/ESP, le commutateur ne peut évidemment pas savoir si c'est du DHCP ou pas, le but d'ESP (RFC 4303) étant bien d'empêcher les intermédiaires d'être indiscrets. Dans ces conditions, le commutateur doit transmettre le paquet. Les machines clientes qui acceptent des réponses DHCP sur IPsec (ça doit être très rare !) doivent donc les authentifier elles-mêmes, ce qui est dans la logique d'IPsec.

Une fois ces précautions prises, le "*DHCPv6 Shield Device*" peut déterminer si le paquet est une réponses DHCPv6 et, si oui, et si elle ne vient pas par le bon port, la jeter, protégeant ainsi les clients DHCP innocents.

La section 6 résume certains problèmes de sécurité du "*DHCP Shield*". Elle rappelle que celui-ci ne protège pas contre les attaques non-DHCP (évidemment) ni même contre certaines attaques DHCP (comme les dénis de service).

Elle rappelle également que "*DHCP Shield*" devrait être présent sur tous les commutateurs du réseau : autrement, un attaquant relié à un commutateur bête, qui ne filtre pas, verra ses paquets acceptés s'il y a au moins un serveur légitime sur ce commutateur (puisqu'il aura fallu, en aval, autoriser le port où est relié ce commutateur.)

Notez que notre RFC ne propose pas de solution à l'usurpation d'adresses IP (une machine utilisant une adresse qui ne lui a pas été allouée en DHCP, cas mentionné au début de mon article) mais que ces solutions sont dans le RFC 7513.

À l'heure actuelle, au moins certains commutateurs Cisco ont cette fonction de "*DHCP Shield*".