

**Internet : Spirent, l'IPV6, Le Chiffre de La Bête pour les PME !.**

**Internet**

Posté par : JPilo

Publié le : 5/5/2011 11:30:00

Tandis que les fournisseurs de services s'inquiètent au sujet de la fin des adresses IPV4, comment les équipes en charge des services informatiques dans **les entreprises doivent-elles se préparer pour l'IPV6 ?**

Directeur du service International Business Development chez Spirent Communications, **Alan Way** nous explique tout.

**L'IPV6 fait soudain la une de l'actualité**. Le fait que nous allons bientôt nous trouver à court d'adresses IP a comme un goût d'Armageddon, un goût suffisamment prononcé pour entraîner une forte augmentation des gros titres abordant ce sujet dans les nouvelles. Nous sommes tous si dépendants d'internet que nous frissonnons à l'idée d'en être dépossédés.

On pourrait penser que l'IPV6 a surgit de nulle part, telle une bête en maraude, mais on est bien loin de la vérité. En effet, spécialiste des tests et des contrôles, Spirent Communications aide les organisations à tester leurs supports pour ce nouveau protocole et la fonctionnalité double pile depuis 2004.



« Il y a 5 ans nous aidions déjà certaines organisations, notamment le US Department of Defense, à se préparer pour l'IPV6 », nous informe **Alan**. « Le problème était bien compris, mais n'apparaissait pas comme une menace imminente, les gens s'en sont donc un peu lassés. Aujourd'hui l'IPV6 fait à nouveau la une de l'actualité et on nous demande une nouvelle fois notre aide. Durant le laps de temps séparant ces deux événements, il semblerait que les difficultés économiques aient relayé l'IPV6 au second plan et qu'elle ait été oubliée, jusqu'à la peur récente suscitée par la fin de l'IPv4 ».

Il est temps de poser un regard calme sur ce problème, en adoptant le point de vue des entreprises. A quel point est ce grave ? Quelle est la menace réelle pour l'entreprise ? Quelle est la meilleure stratégie à adopter et pour quelle(s) raison(s) ?

***Est-ce que le problème ne va pas tout simplement disparaître ?***

Si le sujet est resté au second plan pendant des années, pourquoi ne pas attendre que ça se passe pour le moment ? A court terme, il n'y a apparemment pas grand intérêt à se

préparer pour l'IPv6 si vos partenaires et vos clients sont tous en IPv4, ce qui est très probablement le cas en Europe et aux USA. C'est dans l'Est et dans les pays en voie de développement que l'IPv6 se développe rapidement : de nombreux utilisateurs apparaissent et la pénurie de nouvelles adresses y représente une menace imminente.

**Même lorsque nous allons manquer des adresses IP**, un peu plus tard cette année, cela ne signifiera pas pour autant la fin des services internet ; en effet, les fournisseurs de services possèdent désormais et déjà plusieurs façons de contourner le problème. Le NAT (à Traduction d'adresse réseau) fait en sorte que des adresses IPv4 déjà utilisées ailleurs puissent être attribuées à l'intérieur d'un réseau tout en étant dotées d'une étiquette IPv6 unique en dehors de celui-ci. Ainsi, lorsqu'un message arrive dans le réseau, le serveur NAT traduit cette adresse IPv6 unique en une adresse IPv4 interne, et vice versa lorsqu'un message quitte le réseau. Une seconde approche consiste à encapsuler des paquets IPv6 dans des paquets IPv4, de sorte que vos contacts IPv6 puissent communiquer avec votre système IPv4 d'origine, et de la même manière, que vos messages puissent leur être renvoyés encapsulés à l'intérieur de paquets IPv6 si cela s'avérait nécessaire. La solution 6RD (Développement rapide de l'IPv6) utilise cette approche d'encapsulation.

**Alors, pourquoi s'ennuyer à mettre à jour ?** La réponse est simple : les solutions apportées par le NAT et l'encapsulation ne sont que des moyens pour contourner le problème. Elles nécessitent un traitement en temps réel des messages, ajoutant à la latence du système. L'organisation qui s'accrochera obstinément à son vieil héritage IPv4 ne sera évidemment pas coupée du monde extérieur mais elle souffrira d'une dégradation croissante de ses performances tandis que de plus en plus de communications passeront par l'IPv6. Pour les services financiers et toutes autres transactions similaires à grande vitesse, cela serait désastreux. Pour les autres secteurs, cela émussera leur côté compétitif.

### **Les risques.**

D'autres problèmes apparaîtront si vous ne faites rien à propos de l'IPv6. Ainsi, les pare-feux ne reconnaîtront pas le trafic IPv6 à moins d'être programmés pour le faire. Un système d'origine pourra donc permettre librement le passage de paquets IPv6, sans qu'aucun contrôle ne soit effectué. A ce jour, l'unique raison empêchant la communauté criminelle de s'engouffrer plus avant dans cette voie est que, jusqu'ici, la plupart des cibles sont encore en IPv4. Mais il existe déjà des botnets IPv6 et des paquets de contrôle malveillants en circulation, et le danger ne fera que grandir. Si votre organisation n'a absolument pas besoin de l'IPv6, la solution la plus sûre est alors de bloquer tout trafic IPv6 jusqu'à ce que vos clients vous le réclame.

**Si au contraire vous décidez de supporter le trafic IPv6**, gardez à l'esprit que l'encapsulation peut fournir un chemin accablant à un code IPv6 malveillant caché à l'intérieur de paquets IPv4 a priori inoffensifs. Il ne suffit pas que votre pare-feu supporte l'IPv6, vous devez également ajouter une technologie de vérification des paquets en profondeur pour vous assurer un trafic sain, sans pour autant compromettre les performances de votre réseau.

**D'autres risques sont inhérents au protocole en lui-même.** Par exemple, l'IPv6 permet un trafic multicast qui peut être bloqué en IPv4 et il est possible de définir des équipements virtuels rogués qui se comportent comme des routeurs et kidnappent le trafic IPv6

légitime. Mais tout ceci allant au-delà du propos de cet article, il est suffisant de savoir que de tels risques existent.

Point positif, l'IPv6 au sein du réseau entreprise rend beaucoup plus facile l'encryptage du trafic. Si on prend en compte le fait que plus des deux tiers des attaques qui réussissent viennent de l'intérieur du réseau plutôt que de l'extérieur, la capacité à concevoir l'encryptage depuis le bureau plutôt que depuis le bord du réseau a des conséquences importantes sur la sécurité : des conséquences qui justifient l'adoption rapide de l'IPv6 parmi les gouvernements et les organisations de défense.

### **Une stratégie optimisée.**



Il est évident que, pour de nombreux SMO au moins, il y a quelque chose à dire contre. Si vous ne dépendez pas actuellement d'utilisateurs IPv6, alors bloquez ce type de trafic pour le moment. Cela vous laissera le temps de prévoir de meilleures décisions pour l'avenir. Laissez d'autres être les pionniers, laissez le temps aux problèmes de sécurité à voquer d'être résolus et ne mettez à jour en passant à l'IPv6 qu'une fois le bon moment venu.

Une mise à jour « correcte » doit inclure un test préalable du réseau. On peut lister tous les changements et réfléchir soigneusement à leurs implications, prendre toutes les précautions nécessaires pour éviter tout accroc et pourtant, et c'est là la complexité des réseaux actuels, la seule façon de savoir que vous avez fait les choses correctement est de tester la structure entière en termes de fonctionnalités et de performances, notamment dans des conditions d'attaques ou de stress. Un réseau peut fonctionner à merveille pendant des mois et s'effondrer lors d'un pic de trafic, au moment même où vous dépendez le plus de lui.

**Passer   l'IPv6 signifie in vitablement l'utilisation des deux protocoles en tandem** : le jour o  plus personne n'aura besoin de l'IPv4 est loin d' tre arriv . Prenez en consid ration ce que cela signifie. En plus de devoir programmer vos pare-feu et vos IDS pour les deux types de trafic, les routeurs vont devoir  tre reconfigur s, les interfaces serveurs et les routeurs relais (border relay routers) fonctionneront en mode double pile. Chacun de ces changements est minime, mais vous ne pouvez  tre certains de leur effet combin  qu'en effectuant des tests complets.

C'est pr cis ment le travail que nous avons commenc    faire en 2004 lorsque quelques grandes organisations tourn es vers l'avenir ont d cid  qu'elles devaient se pr parer   l'IPv6. Le secret est de construire d s le d part des tests faisant partie integrante de la strat gie de mise   jour, plut t que de les rattacher   posteriori.

**Que vous utilisiez les  quipements Spirent ou que vous externalisiez le test vers nos ing nieurs**, le processus reste le m me. Le r seau peut  tre reproduit en laboratoire gr ce   la simulation d'op rations r alistes correspondant exactement au profil d'un trafic quotidien. La charge peut  tre augment e jusqu'  atteindre le point de rupture, fournissant ainsi des donn es importantes sur le potentiel de charge du r seau, puis une gamme compl te de conditions extr mes peut  tre impos e, seules ou en parall le  panne du syst me local, conditions d'attaques, pics de trafic etc. Des rapports d' tailles sont g n r s automatiquement, soulignant les goulets d' tranglement ou les points faibles pr sents dans le r seau.

**Avant que la mise   jour soit  tendue**, vous b n ficiez d'une alerte pr alable vous permettant de savoir de quelle mani re elle peut impacter le r seau. Bien souvent, les r sultats montrent de petites am liorations peu co teuses n cessaires   l'am lioration du r seau et, parfois, des clients s'aper soient qu'ils  taient sur le point d'investir outre mesure dans des mises   jour hors de prix alors qu'une solution bien moins ch re fonctionnerait tout aussi bien. Dans ces cas l , le retour sur investissement pour le test est imm diat.

Puis, une fois que le r seau a  t  mis   jour de fa on optimale, vous pouvez incorporer un programme de test automatis  qui contr lera en continu les performances du syst me et la qualit  de service, fournissant ainsi des alertes pr venant chaque probl me potentiel bien en amont.

Les r seaux actuels sont complexes, ils forment un  cosyst me soigneusement  quilibr  qui peut cependant avoir un comportement surprenant si des changements, m me relativement minimes, sont effectu s. L'IPv6 est un de ces petits changements : ne l'adoptez pas si vous n' tes pas absolument certains que votre syst me peut le supporter. Testez-le, ou pr parez vous    tre test s.