Des dÃ©fis de sÃ©curitÃ© apparaissent avec le lancement de lâ□□IPv6
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 22/5/2012 13:00:00

Il ne fait aucun doute que le lancement mondial imminent du**protocole IPv6 le 6 Juin 2012** annonce une nouvelle Ã¨re de lâ□□infrastructure Internet dans le monde entier, Ã la fois en termes dâ□□Ã©volution et dâ□□adoption gÃ©nÃ©ralisÃ©e.

Le monde a dÃ©jÃ eu un avant-goÃ»t du nouveau protocole en Juin dernier, lors de la JournÃ©e Mondiale IPv6. MenÃ© par lâ□□Internet Society, plus de 1 000 sites Internet, entreprises hightech et FAI ont Ã©tÃ© encouragÃ©s Ã passer collectivement Ã lâ□□IPv6 durant une pÃ©riode de 24 heures pour â□□testerâ□□ le protocole et essayer dâ□□anticiper les problÃ¨mes techniques qui pourraient se produire lors du lancement officiel.

Le 6 Juin 2012, les principales organisations high-tech et leaders du Web tels que Google, Facebook et Yahoo!, entre autres, basculeront vers le nouveau protocole Internet lors du lancement mondial officiel.

Et la transition devient de plus en plus nÃ©cessaire.

Le protocole actuel IPv4, qui supporte environ 3,7 milliards dâ□□adresses, a simplement Ã©puisÃ© le stock dâ□□adresses disponibles, en partie du fait de lâ□□explosion des appareils mobiles. Mais lâ□□IPv6, de son cÃ´tÃ©, a une capacitÃ©

illimitÃ©e dâ□□adresses ce qui lui permet de sâ□□adapter Ã une infrastructure mobile et Internet mondiale en pleine croissance.

Cependant, avec le lancement imminent du protocole mondial IPv6, les chercheurs et professionnels de lâ□□IT anticipent certains dÃ©fis, en particulier en matiÃ¨re de sÃ©curitÃ© commente **Christophe Auberger**, Responsable Technique chez Fortinet.

Lâ□□aspect novateur et le manque de connaissances relatifs au protocole IPv6 feront quâ□□il y aura forcÃ©ment des erreurs de configuration, des problÃ¨mes de compatibilitÃ© et autres maladresses dâ□□implÃ©mentation. Il nâ□□existe pas les connaissances institutionnelles sur lâ□□IPv6 que lâ□□on

a sur lâ□□IPv4, qui a Ã©tÃ© utilisÃ© depuis des dÃ©cennies et offre une vaste base de connaissances.

Mais peut Ãªtre que le plus important dÃ©fi en matiÃ¨re de sÃ©curitÃ© est que de nombreux appareils de sÃ©curitÃ© rÃ©seau sont capables de transfÃ©rer le trafic IPv6, mais pas de lâ□□inspecter. Et, comme lâ□□IPv6 est activÃ© par dÃ©faut sur de nombreuses plateformes rÃ©seaux actuelles â□□ tel que Windows 7 â□□ ces systÃ¨mes sont dÃ©jÃ installÃ©s sur le rÃ©seau.

La plupart des systÃ¨mes qui nâ□□ont pas lâ□□IPv6 activÃ© ont la capacitÃ© de contourner ce problÃ¨me en encapsulant les paquets IPv6 dâ□□en-tÃªtes IPv4. Ils lisent lâ□□en-tÃªte, mais ne peuvent pas lire le contenu du paquet en lui-mÃªme. Ils ne peuvent donc pas faire lâ□□inspection approfondie habituelle des paquets, et transfÃ¨rent donc juste les paquets. Câ□□est seulement quand ils ont une implÃ©mentation dual stack, quâ□□ils peuvent autoriser les fonctions de sÃ©curitÃ© rÃ©seau Ã simultanÃ©ment traiter et inspecter les paquets provenant Ã la fois des protocoles IPv4 et IPv6.

Plusieurs constructeurs de sÃ©curitÃ© offrent cette fonctionnalitÃ© â□□ mais pas tous â□□ et câ□□est justement lâ□□un des risques auxquels sont confrontÃ©s les professionnels de la sÃ©curitÃ© rÃ©seau aujourdâ□□hui. Ils doivent sâ□□assurer que leurs produits de sÃ©curitÃ© peuvent inspecter le trafic

IPv6. Sâ□□ils peuvent seulement transfÃ©rer le trafic IPv6, ces produits pourraient Ã©galement transfÃ©rer le contenu malveillant.

MÃªme avec une implÃ©mentation dual stack, les organisations ont nÃ©anmoins besoin de vÃ©rifier si elles ont les mÃªmes fonctionnalitÃ©s de sÃ©curitÃ© activÃ©es pour le protocole IPv4 que pour lâ□□IPv6. Dans le cas contraire, les appareils de sÃ©curitÃ© rÃ©seau sont susceptibles de laisser passer des Ã©lÃ©ments critiques du trafic malveillant qui pourraient potentiellement compromettre le rÃ©seau.

Certaines des politiques et technologies sur lesquelles vous comptez peuvent uniquement fonctionner en IPv4 et non en IPv6, et crÃ©ent ainsi les dÃ©ficits de votre couverture de sÃ©curitÃ©. Cependant, mettre Ã jour lâ□□infrastructure de sÃ©curitÃ© rÃ©seau pour permettre le transfert Ã lâ□□IPv6 nâ□□est pas un projet simple et prendra probablement des annÃ©es pour Ãªtre complÃ¨tement abouti. Câ□□est pourquoi de nombreuses organisations, faisant face Ã des mises Ã jour matÃ©rielles qui sont potentiellement longues et onÃ©reuses, nâ□□ont pas prÃ©vues dâ□□adopterlâ□□IPv6 de si tÃ´t.

Pourtant, les entreprises ne vont pas pouvoir Ã©viter lâ□□IPv6 encore trop longtemps.

Suite au lancement du 5 Juin, beaucoup plus de trafic IPv6 atteindra leurs rÃ©seaux. Lorsque lâ□□IPv6 reprÃ©sentera 5 Ã 10 pourcents de vos donnÃ©es â□□ plutÃ´t quâ□□une fraction de pourcent comme a lâ□□heure actuelle â□□ Ã©viter les mises Ã jour nÃ©cessaires va devenir beaucoup plus difficile Ã justifier. Les DSI vont donc devoir se pencher sur ce problÃ¨me rapidement.