Brocade, A10 Networks et BlueCat Networks rejoignent le laboratoire d'interopérabilité DNSSEC de VeriSign

Objectif : réussir le déploiement du protocole DNSSEC pour une sécurité accrue sur Internet

Mountain View, Californie (États-Unis), le 5 juillet 2010 – VeriSign, Inc. (indice NASDAQ : VRSN), fournisseur réputé de services d'infrastructure sur Internet pour le monde numérique, annonce aujourd'hui la participation de Brocade, A10 Networks et BlueCat Networks à son laboratoire d'interopérabilité créé pour aider les éditeurs à vérifier la conformité de leurs solutions avec le protocole DNS Security Extensions (DNSSEC).

Grâce à un système de signatures électroniques associées aux données DNS, DNSSEC vérifie l'authenticité et l'intégrité des données circulant sur Internet. Il est essentiel que le travail effectué au sein du laboratoire d'interopérabilité DNSSEC de VeriSign puisse porter sur le plus grand nombre possible de composants d'infrastructure, et ce avant la mise en service des serveurs racine le 15 juillet. Selon le calendrier de déploiement, VeriSign doit introduire le protocole sur le domaine .edu en juillet, sur le domaine .net d'ici le quatrième trimestre 2010 et sur le domaine .com d'ici le premier trimestre 2011.

Par ailleurs, VeriSign travaille en collaboration avec d'autres acteurs du secteur dans le cadre du déploiement DNSSEC au niveau des serveurs racine. VeriSign s'est récemment associé à l'ICANN, au ministère américain du Commerce et à 14 représentants réputés de la communauté pour générer et stocker la première clé électronique cryptographique permettant de sécuriser les serveurs racine – ces partenariats marquant une étape clé du déploiement DNSSEC.

Brocade, A10 Networks et BlueCat Networks travailleront désormais aux côtés de Cisco Systems, Juniper Networks et d'autres sociétés au sein du laboratoire d'interopérabilité DNSSEC de VeriSign afin de tester leurs solutions dans un environnement conforme au protocole DNSSEC – ce dernier étant conçu pour protéger les noms de domaine contre les attaques de type MITM *(Man-in-the-Middle)* et les attaques par empoisonnement du cache DNS.

« Face à la tendance actuelle, qui suppose de pouvoir accéder à des données et applications critiques via Internet, à tout moment et en tout lieu, il est nécessaire de mutualiser les efforts déployés pour diminuer les risques de menace pesant sur les infrastructures réseau », déclare Keith Stewart, directeur en charge de la gestion des produits chez Brocade. *« Nous qui prônons la protection des investissements et la haute disponibilité sur le marché de la gestion réseau, nous nous sommes donné pour mission de simplifier et de sécuriser les communications Internet de bout en bout, y compris au niveau des serveurs DNS. Notre participation au laboratoire d'interopérabilité DNSSEC de VeriSign est la garantie pour nos clients de bénéficier d'une solution éprouvée et sûre pouvant être déployée sur les réseaux de nouvelle génération. »*

« Le système DNS se trouve au cœur même du fonctionnement d'Internet. Grâce au protocole DNSSEC, il est possible de garantir un niveau d'intégrité supérieur lors des requêtes DNS, pour une sérénité accrue des consommateurs, des entreprises et de l'ensemble des internautes lors de leurs transactions en ligne », déclare Lee Chen, fondateur et Président-directeur général de A10 Networks. *« Nous nous réjouissons de pouvoir tester nos solutions AX Series au sein du laboratoire d'interopérabilité DNSSEC de VeriSign. Ce faisant, nous allons garantir l'intégration optimale de notre fonctionnalité de mise à disposition d'applications et d'équilibrage de charge des serveurs dans les environnements DNSSEC. »*

« BlueCat n'a pu construire sa réputation de fournisseur de solutions de gestion des adresses IP (IPAM, IP Address Management) physiques et virtuelles en ignorant les exigences du marché », déclare Luc Roy, vice-président en charge de la gestion des produits et du marketing chez BlueCat Networks. *« L'interopérabilité DNSSEC constitue un impératif, non seulement pour nos clients mais aussi à l'échelle du secteur des communications Internet tout entier. Le laboratoire de VeriSign offre un moyen très simple à l'ensemble des intervenants de jouer un rôle à part entière dans l'introduction de ce protocole. »*

Les équipes de VeriSign affectées au laboratoire d'interopérabilité DNSSEC sont à la disposition des fournisseurs de solutions et de services pour déterminer si les paquets DNS contenant des données DNSSEC – généralement plus volumineux que les paquets DNS standard – sont susceptibles de causer des problèmes au niveau des composants de leur infrastructure d'entreprise et de l'infrastructure Internet. Exemple : pour évaluer la taille et la structure des paquets DNS, certaines solutions peuvent reposer sur des règles non applicables au protocole DNSSEC.

« Les tests d'interopérabilité permettent d'identifier et de résoudre toutes les difficultés techniques pouvant compromettre le déploiement sécurisé, stable et adaptatif du protocole DNSSEC sur les domaines .edu, .net et .com », explique Ken Silva, vice-président et directeur de la technologie chez VeriSign. *« Une fois le protocole DNSSEC déployé, on observe une augmentation du trafic de données au sein du système DNS, causée par le différentiel de taille des paquets DNSSEC et des paquets DNS actuels. Il est donc essentiel qu'un plus grand nombre d'entreprises profite du laboratoire d'interopérabilité DNSSEC d'ici la fin du déploiement du protocole sur les serveurs racine cet été, l'objectif associé étant de garantir la prise en charge sans faille du protocole par les pare-feu, les applications et les autres composants concernés. »*

Outre la gestion du laboratoire d'interopérabilité DNSSEC, VeriSign a mis en place un programme destiné à faciliter le déploiement du protocole DNSSEC pour un large panel d'acteurs opérant sur Internet. Au cours de ces derniers mois, VeriSign a notamment publié des documents techniques, animé des séances de formation, participé à des forums métier et mis au point des outils visant à simplifier la gestion DNSSEC.

La société a également soutenu activement son réseau de registraires dans le cadre du déploiement DNSSEC en mettant notamment à leur disposition un « kit de développement logiciel » (SDK, software development kit) et d'autres outils, documents de formation, services et plates-formes d'assistance. Une fois le déploiement effectué sur les domaines .com et .net, VeriSign prévoit également de proposer des services d'échange de clés aux registraires.

« Sans le soutien de VeriSign, le passage au protocole DNSSEC serait beaucoup plus coûteux, long et difficile », déclare Clint Page, Président-directeur général de Dotster, Inc. *« VeriSign nous accompagne dans l'élaboration de notre stratégie de déploiement. Cette étape figure sur notre feuille de route et nous étudions actuellement les questions de disponibilité. »*

Pour en savoir plus sur le calendrier de déploiement du protocole DNSSEC par VeriSign, rendez-vous sur le site : http://www.verisign.com/dnssec.

À propos de VeriSign

VeriSign, Inc. (NASDAQ : VRSN), exploite des services d'infrastructure numérique qui permettent la réalisation de milliards d'interactions sécurisées chaque jour à travers les réseaux vocaux, vidéo et de transmission de données mondiaux. Pour plus d'actualités et d'informations sur la société VeriSign, rendez-vous à l'adresse www.VeriSign.fr.