NCP engineering résout le problème des environnements d'accès hostiles aux communications IPsec

Avec la nouvelle technologie de calcul des chemins signée NCP, les utilisateurs nomades vont pouvoir se connecter au réseau de leur entreprise de n'importe quel point distant, tout en respectant les politiques de sécurité en vigueur

Mountain View (Californie, États-Unis), le 15 mars 2010 - NCP engineering, Inc. annonce aujourd'hui le lancement d'une nouvelle technologie permettant de résoudre le problème des pare-feu dont le paramétrage bloque les communications IPsec et empêche les utilisateurs distants de se connecter au réseau de leur entreprise. Baptisée *Pather Finder*, cette technologie de calcul des chemins signée NCP marque une véritable révolution dans l'univers de l'accès distant en donnant aux utilisateurs la garantie de pouvoir établir une connexion sécurisée au réseau de leur entreprise de n'importe quel point distant. Plus précisément, elle permet d'établir une connexion intégrale d'accès VPN IPsec, tout en veillant à la bonne application des politiques en vigueur — sans jamais compromettre la productivité ni la sécurité de l'entreprise. Il suffit à l'utilisateur de se connecter sur le réseau local, comme il le ferait sur n'importe quel autre réseau. Il est ensuite connecté au réseau de son entreprise sans avoir à attendre ou à modifier les paramètres. Autre avantage : la sécurité du réseau local n'est jamais compromise, garantissant ainsi le respect des règles de sécurité de l'entreprise mais aussi des politiques de sécurité publique.

Le problème du paramétrage des pare-feu hostiles aux communications IPsec se pose souvent avec les bornes publiques d'accès Internet. En sécurisant son réseau, le propriétaire de la borne – un hôtel, un aéroport, un café, etc. – pose des restrictions pour n'autoriser que la navigation Internet et l'utilisation des applications de messagerie électronique. Le fait de restreindre les paramètres du pare-feu de cette manière avait, jusqu'à présent, pour conséquence d'interdire les connexions d'accès VPN IPSec. Les utilisateurs perdaient un temps considérable à contacter les techniciens du service d'assistance informatique pour leur demander d'établir un accès réseau à distance et de pouvoir utiliser autre chose que leurs seules applications de messagerie électronique et de navigation sur Internet.

Comment ça marche :

- La technologie de calcul des chemins *(Path Finder)* de NCP est intégrée aux clients VPN de l'entreprise. Grâce à cette fonction, le système identifie la passerelle VPN ne pouvant se connecter via le protocole IPsec standard, l'ajuste automatiquement sur un autre protocole IPsec puis émule le protocole HTTPS pour établir la connexion.
- La connexion assurée grâce à la technologie *Path Finder* est fiable et assurée grâce à un serveur centralisé NCP Secure Enterprise Server. Les collaborateurs distants peuvent utiliser leurs dispositifs habituels d'authentification, tout en

bénéficiant des avantages d'IPsec – utilisation simultanée des certificats à base logicielle et matérielle, par exemple.

- Grâce à cette technologie, les contraintes de performances sont également moins élevées côté passerelle, puisqu'avec IPsec, chaque volet de la sécurité est pris en compte – autrement dit, une sécurité de bout-en-bout s'appuyant sur une politique de sécurité centralisée.

Citation :

- *« Les clients qui ont renouvelé leurs systèmes d'accès distants avec la solution NCP Secure Enterprise Management System vont pouvoir constater une baisse importante du nombre d'appels à traiter par leurs centres d'assistance informatique. Dans le même temps, ceux qui, parmi leurs collaborateurs, sont amenés à travailler à distance – de leur domicile, d'un hôtel, d'un aéroport, etc. – vont pouvoir gagner en productivité : ils ne perdront plus leur temps au téléphone avec les techniciens du service d'assistance informatique »*, explique Jörg Hirschmann, directeur technique de NCP engineering. *« Grâce à notre technologie Path Finder, les problèmes de connexion réseau causés par le paramétrage des pare-feu hostiles aux communications IPsec, appartiennent désormais au passé. »*

Ressources :

- Pour plus d'informations sur la technologie de calcul des chemins *(Path Finder)* de NCP, rendez-vous sur www.ncp-e.com.

- Retrouvez NCP sur son blog, sur VPN Haus ou encore sur Twitter.

- Pour mieux comprendre en quoi NCP engineering révolutionne le marché des solutions d'accès distant, rendez-vous sur http://vpnhaus.ncp-e.com/category/rethink-remote-access/.

A propos de NCP

Créée en 1986 et ayant son siège à Nuremberg en Allemagne, NCP Engineering GmbH, développe des logiciels destinés à sécuriser les communications des entreprises, opérateur et administrations. NCP se concentre sur la connexion des équipements clients fixes et nomades ainsi que des réseaux de filiales, d'agences et de succursales, le tout par le canal d'Internet, des réseaux publics commutés et des réseaux locaux filaires ou sans fil. Son cœur de compétences réside dans le routage IP, la communication au sein des réseaux commutés, la gestion centralisée des PC distants, ainsi que les technologies de cryptage et de VPN (réseaux privés virtuels). La société propose des solutions de sécurisation, indépendantes des applications et des secteurs d'activité, pour tout environnement d'accès distant reposant sur sa gamme de produits Secure Communications. Par ailleurs, la technologie de NCP garantit l'intégration et la compatibilité avec les produits d'autres fabricants. La commercialisation, l'intégration et la maintenance des solutions NCP sont assurées par des partenaires certifiés.