

NCP engineering Launches End-to-End VPN Solution in North American Market

*Greater Flexibility and Transparency for Network Administrators,
A True One-Click VPN for Users*

Boston—March 23, 2009—[NCP engineering GmbH](#) today launched the industry's most comprehensive, easy-to-manage VPN solution for the North American market. Built from the ground up to provide complete network transparency and seamless interoperability with existing infrastructure, the modular solution combines both SSL and IPSec management with strong policy enforcement. End-users can connect from any device to the network through a secure VPN tunnel with one click, regardless of if they are on a WLAN, LAN or cellular network.

The solution consists of the [NCP Secure Enterprise Management System](#), [NCP Secure Enterprise Server](#) (or gateway) and the IPSec [NCP Secure Enterprise Client](#). Each component integrates fully with all Cisco, Juniper, Check Point, SonicWall and other major vendor equipment, preserving existing technology investments for customers. Full NAC support and management is also provided with the installation of the complete enterprise system.

"Today more than ever, companies are looking to increase their network security, boost employee productivity while away from the office and preserve as much of their current IT systems as possible," said Peter Söll, CEO, NCP engineering GmbH. "Flexible, transparent VPN technology is no longer a pipe dream; we have removed the [management headaches](#) associated with secure remote network access. Enterprises can now truly capitalize on the ease-of-use, modularity and scalability of our secure communications technology."

The complete NCP enterprise VPN solution consists of:

- **The NCP Secure Enterprise Management System**

A centrally-controlled software solution that provides network administrators with a single point of administration for a company's entire IPSec and SSL VPN network, as well as full NAC management. All status information is made graphically available on the system monitor in real time, and plug-in updates and configuration settings can be easily controlled and distributed. User data can be imported via standardized interfaces from existing directory services and identity and access management systems (IAM). Built-in transition software ensures redundancy systems guarantee high availability of the management system, avoiding costly downtime and loss of policy settings.

- **The NCP Secure Enterprise Server**

A hybrid IPSec and SSL gateway that controls and monitors all VPN connections to and from the central data network. It offers high availability clustering to maintain network performance speeds and allows administrators to run up to 10,000 concurrent SSL sessions. Unique to NCP, the gateway provides one plug-in for full network access. The NCP Secure Enterprise Server supports the industry's widest variety of end-point platforms and any IPSec-based device, including the iPhone.

- **The NCP Secure Enterprise Client**

A bundled client, personal firewall and dialer provide the most secure end-point connection for the industry's widest array of platforms, including Windows-based (Mobile 5/6x, CE, XP/Vista 32/64-bit, 7 beta), Symbian (S60 3rd Edition) and Linux-based operating systems. The universally-adaptable IPSec client is seamlessly compatible with any gateway on the market. The user-friendly GUI and intelligent policy enforcement provide even non-technical users with a one-click VPN. The client's latest features include Wireless Service Provider Roaming (WISPr) and streamlined Universal Mobile Telecommunications System (UMTS) Card support, and a budget manager for wireless minutes.

NCP engineering will be providing a full demo of its enterprise product portfolio during the RSA Conference in San Francisco, April 20-24, booth #1356-1, and at Infosecurity Europe in London, April 28-30, booth #M 90.

For additional information about NCP, please visit the company's blog, [VPN Haus](#) or follow it on Twitter at [@vpnhaus](#).

About NCP engineering GmbH

Headquartered in Nuremberg, Germany, NCP engineering helps IT network managers secure data transmission in public networks and across the Internet. Organizations that employ remote access, mobile computing, teleworking and e-commerce throughout the world rely on NCP for key secure communications technology including Remote Access, IP-Routing, VPN and Firewall solutions, Identity and Access Management (IAM) and Network Access Control (NAC). The firm is devoted to avoiding vendor-lock for customers through regular compatibility testing and full integration with PKI-Infrastructures, as well as support for two-factor authentication on end-devices. NCP serves North American customers through a network of technology, reseller and VAR, and OEM partners, including WatchGuard and Astaro.

Press Contacts:

NCP engineering GmbH
Juergen Hoenic
+49 911 99 68 151
juergen.hoenig@ncp-e.com

March Communications
Eric Seymour / Beth Brenner
+1 617 960 9856 / 9873
eric@marchpr.com / beth@marchpr.com