

Contact:

Caroline Smith
Springboard Public Relations
732-863-1900
caroline.smith@springboardpr.com

For Immediate Release:**NCP engineering Releases Virtual Secure Enterprise VPN Server**

New Virtual VPN Appliance is Ideal for Enterprises and Service Providers

Sunnyvale, CA (April 8, 2019) – [NCP engineering](#) today released the Virtual Secure Enterprise VPN Server as a fully virtualized VPN solution for enterprises, service providers and SaaS providers. As a virtual VPN appliance, the NCP Virtual Secure Enterprise VPN Server connects mobile and stationary users in a cross-company data network. The VPN appliance is also predestined for Industrial Internet of Things (IIoT) projects. Special features of the NCP Virtual Secure Enterprise VPN Server include an advanced multi-tenancy capability, NCP's patented VPN Path Finder Technology, easy updates, and high availability.

NCP's Virtual Secure Enterprise VPN Server licensing model is subscription-based and consists of the VPN gateway, high availability services, and a hardened operation system. It is designed to meet the needs of businesses or service providers looking for a virtualized and resource-efficient alternative to traditional solutions. The multi-tenancy capability of the NCP Virtual Secure Enterprise VPN Server allows service providers to combine several companies on one VPN gateway simultaneously with resource sharing. With convenient access management, the NCP VPN clients can be managed by administrators of the connected companies. The number of remote users and VPN tunnels can also be scaled as needed.

“As a virtual VPN appliance, our new Virtual Secure Enterprise VPN Server is scalable, easy to install, and simple to configure,” said Patrick Oliver Graf, CEO of NCP engineering. “Another big advantage of this virtual appliance is that all security patches are provided exclusively by NCP and, therefore, the responsible administrator does not need any prior special knowledge to update the operating system.”

Additional security features of the NCP Virtual Secure Enterprise VPN Server include the support of one-time password (OTP) solutions and certificates in a public key infrastructure (PKI). The validity of certificates is checked each time a connection is established by means of blacklists offline or online to the Certification Authority (CA).

Resources

- To learn more about the NCP Virtual Secure Enterprise VPN Server, please see the corresponding product page: <https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/gateway/>.
- Reach NCP engineering on its blog, [VPN Haus](#), or [LinkedIn](#), [Twitter](#), [Facebook](#), [Google+](#) or [YouTube](#).

About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their remote access, and overcome the complexities of creating, managing and maintaining secure network access for staff.

NCP's award-winning product line spans the spectrum of remote access, from IPsec/SSL VPNs to endpoint firewalls and network access control (NAC) functions. The company's products support organizations with complex remote user needs, and that want to leverage the latest end-devices to increase staff productivity, reduce network administration and adapt policy changes on-the-fly. Each solution is interoperable with existing third-party software or hardware.

With global headquarters in Nuremberg, Germany and North American headquarters in the San Francisco Bay Area, the company serves 35,000-plus customers worldwide throughout the healthcare, financial, education and government markets, as well as many Fortune 500 companies. NCP has established a network of national and regional technology, channel and OEM partners to serve its customers. For more information, visit www.ncp-e.com.

###