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

For Immediate Release:

NCP engineering Releases Version 12.0 of the Secure Enterprise Client, Secure Entry Client, and Exclusive Remote Access Client for Windows

New VPN Clients Feature IPv4/IPv6 dual stack support and Quality of Service Module

Sunnyvale, CA (August 13, 2019) – NCP engineering today released version 12.0 of the NCP Secure Enterprise and Entry Clients, and NCP Exclusive Remote Access Client optimized for Juniper Networks® SRX Series firewalls. All three clients feature biometric authentication, seamless roaming, friendly net detection, and VPN Path Finder Technology. In version 12.0, NCP has optimized the Home Zone, Connection Management, and the Support Wizard. Brand new features include IPv4/IPv6 dual stack support and the introduction of a Quality of Service (QoS) module, ensuring that specific applications can get the outgoing bandwidth they need in the VPN tunnel.

Transferring large files, sending email, and using VoIP services over the same data connection can quickly use up all available bandwidth. By prioritizing outgoing data, the VPN client ensures that specific user-defined applications like VoIP, which demand high-quality bandwidth management, can maintain a clear and stable connection.

"The new QoS module ensures that active applications can access the maximum outgoing bandwidth allocated to them and that inactive applications do not hog resources," said Patrick Oliver Graf, CEO of NCP engineering.

NCP has also extended IPv6 support in its VPN client, enabling the use of both IPv4 and IPv6 protocols within the VPN tunnel. Split tunneling can be configured separately for IPv4 and Ipv6 protocols.

The Home Zone feature is a special user profile for home office scenarios. Clicking the Home Zone button automatically enables special firewall rules which have been set up by the administrator and only apply while the device is connected to the home office network. This means that the user can conveniently access other devices such as printers or scanners on their home office network. When the user leaves the Home Zone network, the previous firewall rules are reactivated.

In version 12.0, NCP has extended this feature with a new option to temporarily set the Home Zone. Previously, the NCP Secure Client recognized the Home Zone automatically after it had been set once. If the new option is enabled, the Home Zone is forgotten after restart, standby, or change of connection, and must be enabled again by the user.

NCP has improved the handling of different connection media by adding two new options to the Connection Management feature of its Windows clients including "Disable mobile network if LAN cable is plugged in" and "Disable mobile network when Wi-Fi connection is established". Now, instead of the client connecting automatically to all available data networks, users have more granular control over which connection medium is used.

The NCP Secure Enterprise Client is part of the NCP Secure Enterprise Solution, which also includes the NCP Secure Enterprise VPN Server and NCP Secure Enterprise Management. The NCP solution can be purchased through its network of certified partners.

The NCP Secure Entry Windows Client is designed for smaller VPN projects with up to 50 mobile workstations without a central management solution and is compatible with all common IPsec VPN gateways.

With the NCP Exclusive Remote Access Windows Client, NCP offers a Windows VPN Client which is optimized for Juniper Networks® SRX Series firewalls and connects exclusively to a Juniper SRX gateway. The NCP Exclusive Remote Access Clients are managed centrally via the NCP Exclusive Remote Access Management and are only available through the NCP distribution channel.

All NCP Windows clients above version 12.0 are compatible with Microsoft Windows from Windows 7 up to Windows 10 version 1903.

Resources

To learn more, please see the corresponding product pages:

- NCP Secure Enterprise Clients: https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-clients/

- NCP Secure Enterprise Solution: https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/

- NCP Secure Entry Clients: https://www.ncp-e.com/en/products/ipsec-vpn-client-suite/vpn-clients-for-windows-10-8-7-macos/

- NCP Exclusive Remote Access Clients: https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

- NCP Exclusive Remote Access Management: https://www.ncp-e.com/en/exclusive-remote-access-solution/sem/

- 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.

# # #