Pressemitteilung

VPN Client mit biometrischer Authentisierung und optimiertes VPN Management System für Juniper SRX Series

Die Version 11.1 des NCP Exclusive Remote Access Clients ermöglicht Authentisierung mittels biometrischer Merkmale wie z.B. Fingerabdruck- oder Gesichtserkennung. Administriert wird er über das NCP Exclusive Remote Access Management, welches jetzt in Version 5.0 verfügbar ist.

Nürnberg, 29. Mai 2018 – Mit dem NCP Exclusive Remote Access Windows Client bietet NCP einen Windows VPN Client, der für Juniper Networks® SRX Series Firewalls optimiert ist und sich ausschließlich gegen ein Juniper SRX Gateway verbindet. Zentral administriert werden die VPN Clients mit dem NCP Exclusive Remote Access Management. Die Version 11.1 des NCP Exclusive Remote Access Clients bietet neue Funktionen wie die biometrische Authentisierung (z.B. via Fingerabdruck), eine an Windows 10 angepasste GUI sowie einen neuen Credential Provider mit HotSpot-Anmeldung. Mit dem NCP Exclusive Remote Access Management Server in der neuen Version 5.0 profitieren Administratoren unter anderem von mehr Performance, Verbesserungen bei der Inbetriebnahme sowie eines zusätzlichen weltweiten Providers für 2-Faktor Authentifizierung.

Im NCP Exclusive Remote Access Windows Client wurde eine biometrische Authentisierung vor der VPN-Einwahl, zum Beispiel über Fingerabdruck- oder Gesichtserkennung, hinzugefügt. Die Authentisierung erfolgt direkt nach dem Klick auf den Verbinden-Button in der Client GUI, wobei der Verbindungsaufbau erst gestartet wird, wenn diese erfolgreich abgeschlossen ist. Besitzt der Rechner keine Hardware zur biometrischen Authentisierung oder ist diese nicht aktiviert, kann sich der Benutzer auch wahlweise über sein Passwort authentisieren. NCP speichert dabei keine biometrischen Daten.

Ein weiteres Highlight des NCP Exclusive Remote Access Windows Client ist der neue Credential Provider mit HotSpot-Login vor Benutzeranmeldung mit anschließendem VPN-Tunnelaufbau. Nutzt der Anwender die VPN Client-Funktion Windows Pre-Logon kann er bereits VOR der Anmeldung am Windows System einen VPN-Tunnel in die Firmenzentrale aufbauen. Die Benutzeranmeldung am lokalen Windows System geschieht daraufhin durch diesen VPN-Tunnel, so dass er an der zentralen Windows Domäne / Active Directory authentifiziert wird. Ab dieser Clientversion ist bereits in der Pre-Logon-Phase die sichere Anmeldung auch an einem WLAN-HotSpot möglich, d.h. der Client ist durch die integrierte dynamische Firewall zu jedem Zeitpunkt der Anmeldung am HotSpot optimal geschützt. Für den Anwender macht es also keinen Unterschied, ob er sich im Büro oder an einem HotSpot

seiner Wahl befindet.

Das NCP Exclusive Remote Access Management ist perfekt auf die Juniper SRX Series abgestimmt. In der Version 5.0 können durch die Performance-Optimierung Lastspitzen z.B. durch annähernd gleichzeitiges Anmelden mehrere tausend Benutzer wirksam abgefangen werden.

Ab dem Exclusive Remote Access Management 5.0 und der Konsole 5.0 wird die Inbetriebnahme durch vorinstallierte Plug-ins erleichtert. Außerdem erhält der Administrator Benachrichtigungen in der Konsole über aktuell anliegende Ereignisse. Es werden z.B. Fehler und Warnungen sowie Infos zur Lizenz oder dem Ablauf des CA-Zertifikats markant und unübersehbar angezeigt. Ein Klick auf diese Benachrichtigung zeigt weitere Details.

Darüber hinaus wird ab der Version 5.0 die 2-Faktor Authentifizierung des SMS Providers Sophos MCS unterstützt. Der Vorteil von SMS-Kommunikation besteht darin, dass eine SMS ihren Empfänger auch bei schlechter Netzqualität oder abgeschaltetem Datenempfang des Empfängers weltweit erreicht.

Keywords

NCP, Juniper SRX, biometrische Authentisierung, Gesichtserkennung, Fingerabdruck, Pre-Logon, Credential Provider, GUI, HotSpot-Anmeldung, IPsec, VPN Client, Remote Access, Software, Remote Access Management, VPN Management, Performance-Optimierung, 2-Faktor Authentifizierung

Weitere Informationen

- NCP Exclusive Remote Access Clients
  https://www.ncp-e.com/de/exclusive-remote-access-solution/vpn-client/
- NCP Exclusive Remote Access Management
  https://www.ncp-e.com/de/exclusive-remote-access-solution/sem/
- Wenn Sie mehr über NCP engineering erfahren möchten, dann besuchen Sie www.ncp-e.com
- Kontaktieren Sie NCP auch über unseren Blog VPN Haus, über Twitter, Linkedin, Facebook, Xing oder YouTube

Pressemitteilung

Über NCP
Die NCP engineering GmbH mit Hauptsitz in Nürnberg vereinfacht den sicheren Zugriff auf zentrale Datennetze via Internet. NCP Produkte und Lösungen erfüllen alle Anforderungen hinsichtlich Benutzerfreundlichkeit, Sicherheit und Wirtschaftlichkeit.
Die Kernkompetenzen liegen auf den Gebieten IP-Routing, zentrales Management von remote Systemen sowie Verschlüsselungs-, VPN- und Firewall-Technologien.
Das Unternehmen entwickelt Software in den Bereichen Mobile Computing, Teleworking, Filialvernetzung, M2M sowie Industrie 4.0 (IIoT). Zum Portfolio gehören auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Lösungen. Die Technologie der NCP Produkte garantiert die Integration und Kompatibilität mit den Produkten anderer Hersteller. Für die nationale und internationale Vermarktung der Produkte und Lösungen setzt NCP sowohl auf die Zusammenarbeit mit Technologie- und OEM-Partnern als auch auf den Vertrieb über Distributoren und zertifizierte Systemhäuser. Zu den Kunden zählen Unternehmen, Behörden und Organisationen.

Pressekontakt:
NCP engineering GmbH
Oliver Bezold
Telefon: +49 911/99 68 - 124
Fax: +49 911/99 68 - 299
E-Mail: oliver.bezold@ncp-e.com
Twitter: @NCP_engineering