



NCP VS GovNet Connector mit neuen Features

Der praxisorientierte und leistungsstarke NCP VS GovNet Connector erhält in Version 2.10 die Features Hotspot-Anmeldung und Friendly Net Detection

Nürnberg, 07. Dezember 2021 – NCP, der führende Spezialist für vollautomatisierte, sichere Datenkommunikation, veröffentlicht als „Qualifizierter Hersteller im Sinne des Bundesamtes für Sicherheit in der Informationstechnik (BSI)“ die Version 2.10 des VS GovNet Connector. Das Release wurde im Rahmen des „Qualifizierten Zulassungsverfahrens“ entwickelt und ist für VS-NfD (Verschlussache – Nur für den Dienstgebrauch), für den Schutz von EU-Informationen bis zum Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ sowie für den Schutz von NATO-Informationen bis zum Geheimhaltungsgrad „NATO RESTRICTED“ zugelassen. Die leistungsstarke Softwarelösung ist das Bindeglied zwischen dem VS-NfD-Daten verarbeitenden Arbeitsplatz und der zugehörigen Gegenstelle (NCP Secure VPN GovNet Server). Anwender profitieren vom großen Funktionsumfang und der einfachen Handhabung bei gleichzeitig höchster Sicherheit. In Version 2.10 wurden die Features Hotspot-Anmeldung sowie Friendly Net Detection implementiert.

Bei der Nutzung eines öffentlichen Hotspots müssen sich Anwender häufig über eine Website des Hotspot-Betreibers anmelden und müssten dafür am VPN-Tunnel vorbei kommunizieren. Dies ist jedoch im Behörden- und meist auch im Business-Umfeld nicht gestattet. Mit der Secure Hotspot-Anmeldung von NCP werden Sicherheitsbedenken ausgeräumt. Klickt der User auf einen von ihm ausgewählten Hotspot, baut der VS GovNet Connector automatisch die Verbindung zum Unternehmensnetz auf, sollte der Internetzugang ohne Anmeldedaten möglich sein. Meist ist dies nicht der Fall und der Client startet aus Sicherheitsgründen einen funktionsreduzierten Webbrowser. Die Client Firewall gestattet hierbei nur diesem gehärteten Browser den Zugriff auf die Hotspot-Anmeldeseite solange bis die Anmeldung abgeschlossen ist. Der Vorteil dieses Verfahrens ist, dass der Nutzer nun auf sichere Weise einen öffentlichen Hotspot nutzen kann, ohne an den Sicherheitseinstellungen etwas ändern zu müssen.

Das Feature Friendly Net Detection (FND) erkennt anhand eines erreichbaren Friendly Net Detection Servers, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet. Diese Erkennung ist Zertifikats-basiert und bietet damit hohe Sicherheit. Je nach Netz





aktiviert die FND-Funktion die entsprechenden Firewall-Regeln und kann im sicheren Netzwerk den VPN-Verbindungsaufbau unterbinden. Dadurch können innerhalb des sicheren Netzes beispielsweise administrative Zugriffe auf das Endgerät gestattet werden, während dies im unsicheren Netz nicht erlaubt ist. Im Gegensatz zu herkömmlichen Firewalls ist die des VS GovNet Connectors bereits beim Systemstart aktiv. Voraussetzung für die Verwendung des FND-Features ist der Einsatz des NCP Friendly Net Detection Servers ab Version 4.0.

Der NCP VS GovNet Connector 2.10 erfüllt alle vom BSI geforderten Sicherheitsstandards und bleibt gleichzeitig eine sehr praxisorientierte und von den Anwendern äußerst leicht zu bedienende VPN-Software. Er wird auf Endgeräten mit Windows 10 (Version 1607 bis 21H1) oder Windows 11 (bis Version 21H2) installiert. Nach erfolgreicher Authentisierung stehen dem Benutzer über LAN, WLAN oder Mobilfunk via Virtual Private Network (VPN) alle Anwendungen und Ressourcen aus dem zentralen Datennetz zur Verfügung. Dabei verfügt der hochsichere und ausgereifte Software-Client über weitere Features wie biometrische Authentisierung, VPN Path Finder Technology, Quality of Service und mehr.

Die rein softwarebasierte Lösung NCP VS GovNet Connector lässt sich ideal mit Standard-Werkzeugen auf die jeweiligen Arbeitsplätze verteilen und arbeitet mit modernsten und stärksten Verschlüsselungsalgorithmen. Abgestimmt ist die Software speziell auf den Einsatz in Ministerien, Behörden und geheimschutzbetreuten Unternehmen. Dabei dient sie der sicheren Bearbeitung und Übertragung von Daten mit der Einstufung u.a. als „VS-NfD“. Der Software-Client garantiert eine besonders einfache Handhabung, ohne an spezielle Hardware gebunden zu sein. Rollout, Inbetriebnahme, Softwareupdate und Administration erfolgen komfortabel über das NCP Secure Enterprise Management (SEM) als „Single Point of Administration“. Flexible Lizenzmodelle wie zum Beispiel „Pay-per-Use“ decken jeden Kundenbedarf ab.

Keywords

NCP, VS-NfD, BSI, NCP VS GovNet Connector, Version 2.10, Secure VPN GovNet Server, hochsicheres VPN, Zulassung des BSI, Verarbeitung von Daten nach VS-NfD, Hotspot-Anmeldung, Friendly Net Detection, biometrische Authentisierung, VPN Path Finder, Quality of Service





Weitere Informationen

- NCP VS GovNet Connector und NCP Secure VPN GovNet Server
www.ncp-e.com/de/produkte/vpn-fuer-vs-nfd
- Wenn Sie mehr über NCP engineering erfahren möchten, dann besuchen Sie
www.ncp-e.com

Über NCP

Die NCP engineering GmbH mit Hauptsitz in Nürnberg ist weltweit führender Software-Hersteller für hochsichere Lösungen in den Bereichen Remote Access, Endpoint Security und Industrie 4.0 / IIoT. Namhafte, global agierende Großkonzerne, mittelständische Unternehmen, Ministerien und Behörden setzen auf die Lösungen "Made in Germany", um ihre IT-Infrastrukturen vor den aktuellen Bedrohungssituationen zu schützen. Zum Portfolio gehören auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Lösungen.

Pressekontakt:

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

