Datenblatt

NCP VS GovNet Connector für Windows

Zentral administrierbare, softwarebasierte Lösung für Arbeitsplätze mit Verarbeitung von VS-NfD-Daten zum Remote Zugriff

- BSI-Zulassung (VS-NfD)
- NATO RESTRICTED und EU RESTRICTED
- zentrales Management
- Self Check zur Überwachung der korrekten Funktion
- Network Access Control (Endpoint Policy)
- managebare Firewall
- Friendly Net Detection
- Hotspot-Anmeldung
- VPN Path Finder Technology
- (Fallback IPsec/HTTPS)
- starke Authentisierung
- Unterstützung von WLAN und Mobilfunk
- Custom Branding Option

Softwarebasierte Lösung

Der NCP VS GovNet Connector ist das Bindeglied zwischen dem VS-NfD-Daten verarbeitenden Arbeitsplatz und der zugehörigen Gegenstelle. Er erfüllt zudem die Richtlinien für NATO RESTRICTED und EU RESTRICTED. Als eine rein softwarebasierte Lösung lässt er sich ideal mit Standard-Werkzeugen auf die jeweiligen Arbeitsplätze verteilen. Der Anwender profitiert vom großen Funktionsumfang und der einfachen Handhabung bei gleichzeitig hoher Sicherheit.

Auf Basis des IPsec-Standards lassen sich hochsichere Datenverbindungen nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum NCP Secure VPN GovNet Server herstellen.

Aufgrund der Unterstützung von Standard-Schnittstellen ist die Kombination mit weiterer vom BSI zugelassener Authentisierungshardware (z.B. SmartCard-Leser) oder Software (z.B. Festplatten-verschlüsselung) problemlos möglich.

Selbst-verständlich unterstützt der NCP VS GovNet Connector die vom BSI geforderte Verifizierung der Signatur nach dem Prinzip der elliptischen Kurven (Elliptic Curve Cryptography).

Anwender können mit Windows-Rechnern von jedem Standort weltweit auf das zentrale Datennetz zugreifen. Der NCP VS GovNet Connector unterstützt mit Seamless Roaming den automatischen Wechsel auf das beste zur Verfügung stehende Verbindungs¬medium – ideal für den Always On-Betrieb. Zusammen mit dem NCP Secure VPN GovNet Server als Gegenstelle bleibt eine Anwendungssession auch während eines Medien-wechsels oder einer kurzzeitigen Unterbrechung erhalten.

Self Check

Der im VS GovNet Connector vorhandene Integritätsdienst führt eine kontinuierliche Überwachung der korrekten Funktionalität im Betriebssystem durch. Eine etwaige Kompromittierung des VS GovNet Connectors resultiert in der Überführung des Endgerätes in einen sicheren Zustand, der eine weitere Kommunikation jeglicher Art unterbindet.

Des Weiteren dient der Integritätsdienst der

Durchführung eines, zu jedem Zeitpunkt, sicheren Remote-Updateprozesses des VS GovNet Connectors durch das zentrale Management.

VPN Path Finder Technology

Firewalls bzw. Proxies, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert. Hierbei wird automatisch in einen modifizierten IPsec-Protokoll-Modus gewechselt, der den zur Verfügung stehenden HTTPS-Port für den VPN-Tunnel nutzt. Alle in IPsec enthaltenen Sicherheits-merkmale bleiben zu 100 % erhalten, so dass das VPN Path Finder Protokoll sicherheitstechnisch nicht neu bewertet werden muss.

Einen wirtschaftlichen Betrieb ermöglicht der im NCP VS GovNet Connector enthaltene Budget Manager. Über ihn lassen sich Volumen/Zeit-Budgets oder Provider bestimmen und über-wachen, damit die Onlinekosten nicht „aus dem Ruder laufen“.

Authentisierung

Neben der Unterstützung von Zertifikaten bzw. SmartCards in einer PKI (Public Key Infrastructure) bietet der NCP VS GovNet Connector auch die optionale Unterstützung von OTP-Lösungen [3] (One Time Passwort) oder eine biometrische Authentisierung vor der VPN-Einwahl, zum Beispiel über Fingerabdruck- oder Gesichtserkennung. Die Authentisierung erfolgt hierbei direkt nach dem Klick auf den Verbinden-Button in der Connector-GUI, wobei der Verbindungsaufbau erst gestartet wird, wenn die biometrische Authentisierung erfolgreich abgeschlossen ist. Besitzt der Rechner keine Hardware zur biometrischen Authentisierung oder ist diese nicht aktiviert, kann sich der Anwender auch wahlweise über sein Passwort authentisieren.

Network Access Control

Ein ebenso verfügbarer Endpoint Policy-Check verhindert den Zugriff ungenügend geschützter Endgeräte auf das zentrale Datennetz. Hierbei können Informationen zum Status eines Viren-scanners, der Domänenzugehörigkeit, dem Stand des Betriebssystems und andere Faktoren abgefragt werden.

Firewall

Der NCP VS GovNet Connector verfügt über eine integrierte dynamische Personal Firewall. Diese ist zentral administrierbar, so dass Regelwerke für Ports, IP-Adressen, Segmente und Applikationen vom Administrator zentral definiert werden können. Ebenso lassen sich Firewallregeln für innerhalb und außerhalb des VPN-Tunnels konfigurieren. Die Firewall des NCP VS GovNet Connectors ist bereits beim Systemstart des Rechners aktiv.

Friendly Net Detection

Die „Friendly Net Detection“ erkennt anhand einer zertifikatsbasierten Authentisierung des Friendly Net Detection Servers im sicheren Firmen- bzw. Behördennetz die sichere Netzwerkumgebung (Friendly Net). Daraus resultierend können im VS GovNet Connector für das Friendly Net konfigurierte Firewallregeln automatisch aktiviert werden um beispielsweise den Datenaustausch ohne einen notwendigen VPN-Tunnel zuzulassen oder administrative Zugriffe auf das Gerät zu ermöglichen. Darüber hinaus kann dem Anwender der manuelle Aufbau des VPN-Tunnels im Friendly Net verwehrt werden.

Hotspot-Anmeldung

Die Vorgabe in unsicheren Netzwerkumgebungen ausschließlich durch den VPN-Tunnel zu kommunizieren, schließt zunächst eine Anmeldung an einem WLAN-Hotspot aus, da hierfür zunächst ohne VPN-Tunnel mit einem Webbrowser auf eine Anmeldeseite zugegriffen werden muss.

Dieses Problem wird durch die im VS GovNet Connector integrierte Hotspot-Anmeldung gelöst, die

mit einem dedizierten, abgesicherten Webbrowser im Zusammenspiel mit dynamisch zu- und abgeschalteten Firewallregeln ein höchstes Maß an Sicherheit zu jedem Zeitpunkt der Hotspot-Anmeldung vor dem VPN-Tunnelaufbau bietet. War die Anmeldung erfolgreich so wird dies vom VS GovNet Connector selbsttätig erkannt und automatisch der VPN-Tunnel aufgebaut.

Zentrales Management

Rollout, Inbetriebnahme, Softwareupdate und Administration des NCP VS GovNet Connectors erfolgen über das NCP Secure Enterprise Management (SEM) und das zugehörige VS GovNet Connector-Plug-in als „Single Point of Administration“ (Voraussetzung für den Einsatz des NCP VS GovNet Connectors). Grundsätzlich lassen sich alle Einstellungen im NCP VS GovNet Connector durch den Administrator sperren. Somit werden Veränderungen seitens der Anwender verhindert.

Am VS GovNet Connector erzeugte Log-Dateien, sowie das neue Audit-Log mit allen sicherheitsrelevanten Ereignissen, werden periodisch an das zentrale Management zur Auswertung übertragen.

Quality of Service

Durch die Quality of Service-Funktion wird Bandbreite für konfigurierte Applikationen, wie beispielsweise VoIP, reserviert. Die Priorisierung ausgewählter Datenquellen am Anwender-PC geschieht für den Datentransport im VPN-Tunnel in Senderichtung. Für den Anwender im Home-Office ergibt sich daraus eine ungestörte VoIP-Kommunikation durch den VPN-Tunnel auch bei hohem Datenaufkommen.

Custom Branding Option

Ein frei gestaltbares Banner in der Client GUI steht für Firmenlogo oder Supporthinweise (Custom Branding Option) zur Verfügung. Zudem ist die Client-GUI an ein barrierefreies Arbeiten angepasst und unterstützt u.a. den Betrieb von Screen-Readern.

Betriebssysteme [1]	Microsoft Windows 10 (64 Bit) Version 1607 oder neuer auf x86-64 Prozessorarchitektur Microsoft Windows 11 (64 Bit) auf x86-64 Prozessorarchitektur
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall Firewall Configuration	Stateful Packet Inspection; IP-NAT (Network Address Translation); differenzierte Filterregeln bezüglich: Protokolle, Ports, Applikationen und Adressen, Schutz des LAN-Adapters; IPv4- und IPv6-Unterstützung; zentrale Administration Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand eines NCP FND-Servers [4]); Secure Hotspot Login; Home Zone [2];
VPN Bypass [2]	Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Virtual Private Networking [3]	IPsec (Layer 3 Tunneling), RFC-konform; IKEv1/IKEv2; Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption) [3]	Symmetrische Verfahren: AES 128, 192, 256 Bits; Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 8192 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-21, 25-30
Authentisierungsverfahren [3]	IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKEv2 IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards, USB Tokens und Zertifikate mit ECC-Technologie Multi-Zertifikatskonfiguration; One-Time Passwords und Challenge Response Systeme (u.a.RSA SecurID Ready)

Starke Authentisierung [3]	X.509 v.3 Standard; biometrische Authentisierung PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TeleSec TCOS 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, V1.0; Smart Card ReaderInterfaces: PC/SC, CT-API; Microsoft CSP; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher; CSP zur Verwendung von SmartCards via API des Herstellers [7] PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL), OCSP
PKI Enrollment [2]	CMP (Certificate Management Protocol)
Network Access Control [5]	Endpoint Policy: Überprüfung Aktualität des Virenscanners, vorhandene Hotfixes/Service Packs, gestartete Dienste, etc.
Networking Features	LAN Emulation: Virtual Ethernet-Adapter, vollständiger WWAN-Support (Wireless Wide Area Network, Mobile Broadband)
Netzwerkprotokolle	IPv4 / IPv6 Dual Stack
Dialer [2]	NCP Internet Connector oder Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script)
Seamless Roaming [2, 6]	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird
VPN Path Finder [6]	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS [2]: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Internet, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, 5G
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; Timeout (zeit- und gebührengesteuert); Budget Manager (Verwaltung von Verbindungszeit und/oder -volumen für GPRS/UMTS und WLAN, bei GPRS/UMTS getrennte Verwaltung für Roaming im Ausland) Verbindungsmodi: automatisch, manuell, wechselnd (Der Verbindungsaufbau ist davon abhängig wie die Trennung zuvor stattgefunden hat)
APN von SIM-Karte	Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen

Datenkompression	IPCOMP (lzs), Deflate (nur für IKEv1)
Quality of Service	Priorisierung konfigurierter Datenströme innerhalb des VPN-Tunnels in Senderichtung
Weitere Features [3]	Automatische Mediatyp-Erkennung, UDP-Encapsulation, WISPr-Support (T-Mobile Hotspots), IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP (Virtual) Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server)
Point-to-Point Protokolle	PPP over GSM, PPP over Ethernet, MLP, CCP, CHAP
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2-Authentisierung nach RFC 7427 (Padding-Verfahren)
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch); Client Info Center; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Test-Werkzeug für Internet-Verfügbarkeit; Trace-Werkzeug für Fehlerdiagnose; Anzeige des Verbindungsstatus; Integrierte Unterstützung von Mobile Connect Cards; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre
Zentrales Management	Voraussetzung für den Betrieb und das zentrale Management des NCP VS GovNet Connectors sind folgende Softwareversionen oder neuer: NCP Secure Enterprise Management Server — Version 6.10 oder neuer NCP Management Console: — Version 6.10 oder neuer VS GovNet Connector Configuration Plugin: — Version 2.20 oder neuer License Plugin: — Version 12.30 oder neuer Firewall Plug-in: — Version 12.30 oder neuer PKI Enrollment Plug-in: — Version 4.05 oder neuer Endpoint Policy Plug-in: — Version 4.00 oder neuer

[1] Für den zugelassenen Betrieb gemäß VS-NfD sind die Vorgaben des BSI bzgl. des verwendeten Betriebssystems zu beachten.

[2] Diese Funktionalität ist nicht Bestandteil der VS-NfD-Zulassung.

[3] Für den zugelassenen Betrieb gemäß VS-NfD dürfen nur die dafür vorgesehenen Algorithmen und vom BSI zugelassenen Lösungen zur starken Authentisierung für VS-NfD verwendet werden. Dies kann beispielsweise mittels eines geeigneten, im Endgerät integrierten SmartCard-Lesers oder einem externen SmartCard-Leser mit integriertem PIN-Pad, wie dem REINER SCT cyberJack® RFID standard, geschehen.

[4] Der NCP Friendly Net Detection Server kann kostenlos als Add-On hier heruntergeladen werden: https://www.ncp-e.com/de/service/download-vpn-client/

[5] Voraussetzung:
NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server, NCP Secure Enterprise Management

[6] Voraussetzung:
NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server oder NCP Secure VPN GovNet Server

[7] Für die korrekte Funktion ist die Installation einer SmartCard API des jew. Herstellers notwendig (Telesec TCOS Read Only Cardmodul zum Microsoft SmartCard BaseCSP mit ECC-Unterstützung V1.1.0.0; Atos CardOS API V5.5)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dem NCP VS GovNet Connector 2.20 am 12. Mai 2023 die Zulassung (BSI-VSA-10710) erteilt.

Eine kostenlose 30-Tage Vollversion können Sie hier anfordern: vertrieb@ncp-e.com

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com