Produktinformation

VPN Software-Lösung für VS-NfD

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

VPN Software-Lösung für VS-NfD

Insbesondere Behörden, Ämter und geheimschutzbetreute Unternehmen übermitteln sensible Daten mit schützenswerten Informationen von Bürgern oder hochsensiblen Projekten. Die Sicherheit der eingesetzten Kommunikationswege spielt deshalb eine besondere Rolle und muss den Empfehlungen und Vorgaben des **Bundesamtes für Sicherheit in der Informationstechnik (BSI)** entsprechen.

Politiker, Regierungsbeamte und Mitarbeitende benötigen einen schnellen, einfachen und sicheren Zugriff auf die für sie bereitgestellten Netzwerkressourcen und Daten. Hierfür stehen folgende Softwarekomponenten zur Verfügung:

- **NCP VS GovNet Connector:** Verfügt über eine BSI-Zulassung für VS-NfD (BSI-VSA-10907). Darüber hinaus ist die Software für den Schutz von EU-Informationen bis zum Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ für den nationalen Einsatz sowie für NATO-Informationen bis zum Geheimhaltungsgrad „NATO RESTRICTED“ zugelassen.
- **NCP VS GovNet Server:** Verfügt über eine BSI-Zulassung für VS-NfD (BSI-VSA-10711).
- **NCP Secure Enterprise Management:** Dient als zentrale Administrationskomponente.

Die NCP-Softwarekomponenten können zur sicheren Bearbeitung und Übertragung von **Verschlusssachen – nur für den Dienstgebrauch (VS-NfD)** und sensibler Daten eingesetzt werden. NCP verfolgt den Qualitätsanspruch **IT-Security Made in Germany** und setzt auf modernste Technologien und Standards:

- durch das BSI geprüfte Sicherheit
- Elliptische-Kurven-Kryptografie
- Friendly Net Detection
- Hotspot-Anmeldung
- VPN Path Finder Technology (Fallback IPsec/HTTPS)[1]
- starke Authentisierung
- managebare Firewall
- Unterstützung von WLAN und Mobilfunk
- Custom Branding-Optionen

VS-NfD

NATO|OTAN RESTRICTED

EU|UE RESTRICTED

Softwarebasierte Lösung

Der **NCP VS GovNet Connector** ist das Bindeglied zwischen dem VS-NfD-Daten verarbeitenden Arbeitsplatz und der zugehörigen Gegenstelle **(NCP VS GovNet Server)**. Als rein softwarebasierte Lösung lässt er sich ideal und einfach mit jeder Standard-Softwareverteilung auf die jeweiligen Windows-Arbeitsplätze ausrollen und auf mobile Endgeräte wie Laptops installieren. 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 BSI zum NCP VS GovNet Server herstellen.

Aufgrund der Unterstützung von Standard-Schnittstellen ist die Kombination mit weiterer, vom BSI zugelassener Software (z. B. Festplattenverschlüsselung) problemlos möglich. Selbstverständlich unterstützt der NCP VS GovNet Connector die vom BSI geforderte starke Benutzerauthentisierung nach dem Prinzip der elliptischen Kurven (Elliptic Curve Cryptography).

Zudem umfasst die BSI-Zulassung des VS GovNet Connectors auch die Nutzung von SmartCard-Lesern ohne integriertes PIN-Pad. Dadurch können Anwender auch die in ihren Laptops integrierten SmartCard-Leser VS-NfD-konform zur Authentifizierung nutzen.

Der VS GovNet Server darf zum sicheren Betrieb und im Rahmen allgemeiner Vorgaben des BSI ab der aktuellen Version auf einer virtualisierten Plattform verwendet werden. Informationen zur Installation finden sich im Administrationshandbuch des VS GovNet Servers.

VPN Path Finder Technology

Die von NCP patentierte **VPN Path Finder Technology**[1] ermöglicht Remote Access auch hinter 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 Sicherheitsmerkmale bleiben zu 100 % erhalten, so dass das VPN Path Finder-Protokoll sicherheitstechnisch nicht neu bewertet werden muss.

Der integrierte Budget Manager des NCP VS GovNet Connectors ermöglicht einen wirtschaftlichen Betrieb, indem sich Volumen- und Zeitbudgets sowie Provider festlegen und überwachen lassen. So bleiben die Onlinekosten jederzeit im Blick und lassen sich gezielt kontrollieren. Probleme mit gerade im Home-office verbreiteten DS Lite-Anschlüssen gehören so ebenfalls der Vergangenheit an.

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** (One-Time Password) oder eine **biometrische Authentisierung** vor der VPN-Einwahl, zum Beispiel über Fingerabdruck- oder Gesichtserkennung. Die Authentisierung erfolgt hierbei direkt nach dem Klick auf die Schaltfläche „Verbinden“ 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.

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).

Auf dieser Grundlage können die für das Friendly Net konfigurierten Firewallregeln im VS GovNet Connector automatisch aktiviert werden. So lässt sich beispielsweise der Datenaustausch ohne VPN Tunnel zulassen oder ein administrativer Zugriff auf das Gerät 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 Höchstmaß 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.

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 Firewall-Regeln für innerhalb und außerhalb des VPN Tunnels konfigurieren. Die Firewall des NCP VS GovNet Connectors ist bereits beim Systemstart des Rechners aktiv.

Zentrales Management

Rollout, Inbetriebnahme, Softwareupdate und Administration des NCP VS GovNet Connectors erfolgen über das **NCP Secure Enterprise Management** (SEM) 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.

Das **NCP Secure Enterprise Management** besteht aus einem Management Server und einem Dashboard zur Statusüberwachung. Der Management Server dient der Konfiguration und Administration aller daran angebundenen NCP-Komponenten. Das betrifft sowohl die Clients als auch die Server. Es handelt sich um ein datenbankbasiertes System, das mit nahezu jeder Datenbank korrespondiert. Für die Hochverfügbarkeit des Management Servers sorgt optional der Backup Management Server, der durch einen integrierten Replikationsdienst immer über den aktuellen Datenbestand verfügt.

Custom Branding Option

Ein frei gestaltbares Banner in der Client GUI steht für das Firmenlogo und Supporthinweise (Custom Branding Option) zur Verfügung.

„Die Stärkung der Cyber-Resilienz von Bundesbehörden [....] duldet ebenso wie die Modernisierung der Cybersicherheitsarchitektur [...] keinen Aufschub.“

Bundesministerium des Innern und für Heimat

Windows Pre-Logon

Die NCP Pre-Logon-Funktionalität ermöglicht dem Nutzer eine sichere Anmeldung an Windows-Systemen durch eine direkte Authentifizierung über Active Directory – auch über das Internet. Noch vor der eigentlichen Windows-Anmeldung wird dem Nutzer nach dem Systemstart die Option angeboten, eine VPN-Verbindung zum Unternehmensnetzwerk herzustellen.

Dieser Vorgang erfolgt über den sogenannten NCP Pre-Logon Access Provider (PLAP). Nach Auswahl dieser Option authentisiert sich der Anwender mit einem persönlichen Benutzerzertifikat sowie der dazugehörigen PIN. Sobald der VPN Tunnel erfolgreich aufgebaut ist, besteht eine direkte Verbindung zum zentralen Netzwerk.

Dadurch wird der Rechner nicht nur zentral administrierbar, auch die anschließende Anmeldung am Windows-System erfolgt sicher und direkt über die Authentisierung via Active Directory – unabhängig vom Standort des Endgeräts.

Installation und Konfiguration

Der NCP VS GovNet Server ist eine Software Appliance, die auf jeder Standard-Serverhardware installiert werden kann. Die Verwaltung erfolgt über das zentrale Management.

Zudem ist der VS GovNet Server zu IPsec VPN-Gateways und -Clients anderer Hersteller kompatibel.

Benutzerverwaltung

Die Benutzerverwaltung erfolgt flexibel über Backend-Systeme wie z. B. RADIUS, LDAP oder MS Active Directory oder direkt am VPN-Gateway. Integrierte IP-Routing- und Firewall-Funktionalitäten sorgen für die erforderliche Konnektivität und Sicherheit.

Wichtige Hinweise

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

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

[2] OTP ist nicht Teil der Zulassung

Testen Sie die Vollversion für 30 Tage: vertrieb@ncp-e.com

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann kontaktieren Sie uns!

NCP engineering GmbH

Dombühler Str. 2
90449 Nürnberg

Tel.: +49 911 9968 222
vertrieb@ncp-e.com

www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen.

Weitere Infos auf unserer Webseite!

mey-agentur_23-03-2