Trust Seal
www.teletrust.de/itsmig

SECURE COMMUNICATIONS

Produktinformation

VPN Software-Lösung für VS-NfD

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 VPN-Lösung spielt deshalb eine besondere Rolle und muss den Empfehlungen und Vorgaben des **Bundesamtes für Sicherheit in der Informationstechnik (BSI)** entsprechen.

Politiker, Regierungsbeamte und Mitarbeiter müssen in der Lage sein, auf die für sie bereitgestellten Netzwerkressourcen und Daten schnell, einfach und sicher zuzugreifen. Folgende Softwarekomponenten können hierfür genutzt werden:

- der **NCP VS GovNet Connector 2.x** verfügt über eine Zulassung des BSI für VS-NfD (BSI-VSA-10599). Zudem ist er für den Schutz von EU-Informationen bis zum Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED" für den nationalen Einsatz und für den Schutz von NATO-Informationen bis zum Geheimhaltungsgrad „NATO RESTRICTED" zugelassen.
- der **NCP Secure VPN GovNet Server** verfügt über eine Zulassung des BSI für VS-NfD (BSI-VSA-10427)
- das N**CP Secure Enterprise Management** als zentrale Administrationskomponente (Einsatz nach VS-NfD in Abstimmung mit dem BSI)

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
- VPN Path Finder Technology (Fallback IPsec/HTTPS)[2]
- Friendly Net Detection
- Hotspot-Anmeldung
- Network Access Control (Endpoint Policy)[1]
- starke Authentisierung
- managebare Firewall
- Unterstützung von WLAN und Mobilfunk
- Custom Branding Optionen

Softwarebasierte Lösung

Der **NCP VS GovNet Connector** ist das Bindeglied zwischen dem VS-NfD-Daten verarbeitenden Arbeitsplatz und der zugehörigen Gegenstelle (NCP Secure VPN GovNet Server). Als rein softwarebasierte Lösung lässt er sich ideal und einfach mit jeder Standard-Softwareverteilung auf die jeweiligen Arbeitsplätze ausspielen 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 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. 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).

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

VPN Path Finder Technology

Die von NCP patentierte **VPN Path Finder Technology**[2] 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.

Einen wirtschaftlichen Betrieb ermöglicht der im NCP VS GovNet Connector enthaltene Budget Manager, über den sich Volumen/Zeit-Budgets oder Provider bestimmen und überwachen lassen, damit die Onlinekosten nicht „aus dem Ruder laufen". Probleme mit gerade im Homeoffice verbreiteten DS-Lite-Anschlüssen gehören so ebenfalls der Vergangenheit an.

Authentisierung

Neben der Unterstützung von Zertifikaten bzw. Smart-Cards in einer PKI (Public Key Infrastructure) bietet der NCP VS GovNet Connector auch die optionale Unterstützung von **OTP-Lösungen** (One Time Password)[3] 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**[1] verhindert den Zugriff ungenügend geschützter Endgeräte auf das zentrale Datennetz. Hierbei werden sicherheitsrelevante Parameter des Endgerätes und dessen Software (z.B. Status des Virenscanners, Domainzugehörigkeit, Stand des Betriebssystems ...) überprüft. Diese Parameter sind zudem beliebig anpassbar, wodurch auch eine technisch automatisierte Compliance-Prüfung möglich ist.

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.

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 einer Management Konsole mit grafischer Oberfläche. Der Management Server dient der Konfiguration und Administration aller daran angebundener 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 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.

Installation und Konfiguration

Die Konfigurationseinstellungen werden mit dem zugehörigen NCP Secure VPN GovNet Manager erstellt und die Konfigurationsdaten via USB-Stick oder über einen speziellen Administrator-VPN-Tunnel übertragen.
Der NCP Secure VPN GovNet Server ist 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 Connectivity 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 Secure VPN GovNet Server, NCP Secure Enterprise Management

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

[3] OTP ist nicht Teil der Zulassung

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

NCP
SECURE COMMUNICATIONS

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

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968-0
vertrieb@ncp-e.com
www.ncp-e.com

Wir freuen uns auf ein Gespräch mit Ihnen!