NCP
SECURE COMMUNICATIONS

Datenblatt

NCP Secure VPN GovNet Server

IPsec VPN Gateway Software

Sicherer Fernzugriff auf das Firmennetz gemäß VS-NfD-Richtlinien

- BSI-Zulassung (VS-NfD)
- NATO RESTRICTED und EU RESTRICTED
- Unterstützt elliptische Kurven (ECC)
- BSI geprüfter Zufallszahlengenerator der Klasse DRG.4
- Integrierte IP-Routing- und Firewall-Funktionalitäten
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Automatische Tunnelweiterleitung
- Mandantenfähigkeit
- Multi-Prozessor-Unterstützung, beliebig skalierbar
- Gehärtetes Linux-System; Server-Anwendung verwendet „Privilege Separation“

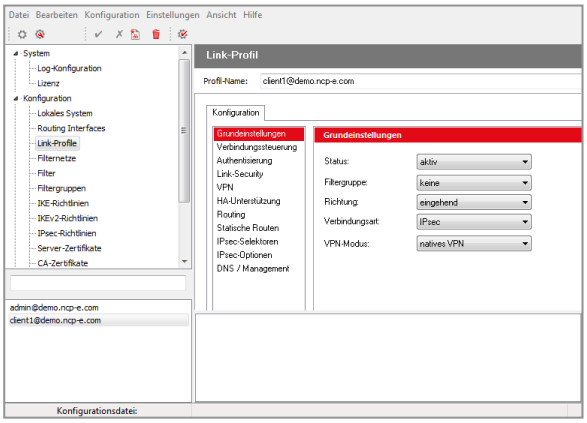
Einsatzbereich

Der NCP Secure VPN GovNet Server erweitert das Portfolio der NCP Next Generation Network Access Technology um eine hochsichere Variante des NCP Secure Enterprise VPN Servers für den Einsatz im Behördenumfeld oder für geheimschutzbetreute Unternehmen.

Das Gateway wurde für die Verarbeitung von Daten der Geheimhaltungsstufe Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen und erfüllt die Kriterien für NATO RESTRICTED und EU RESTRICTED. Es eignet sich ideal als Gegenstelle für den NCP VS GovNet Connector oder die NCP Secure VPN GovNet Box, die für die Verarbeitung von Daten gemäß VS-NfD am Anwender-Arbeitsplatz ebenfalls vom BSI zugelassen wurde.

Installation und Konfiguration

Die Software wird auf einem Standard-Server (Typ: siehe „zugelassene Hardware“) mittels Komplett-Image installiert. 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.

NCP VPN Path Finder

Mit dem NCP VPN Path Finder stellt NCP eine einzigartige Technologie bereit, die Remote Access auch hinter Proxies/Firewalls ermöglicht, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert (z.B. in Hotels). Mit NCP VPN Path Finder bleiben alle Sicherheitsmerkmale der IPsec/IKE-Kommunikation erhalten, es wird jedoch über den HTTPS-Port kommuniziert.

Sicherheit/Starke Authentisierung

Bei der Entwicklung des NCP Secure VPN GovNet Servers stand Sicherheit an erster Stelle. Um das Risiko durch Angriffe auf das Server-System selbst zu minimieren, wird ein gehärtetes Linux Basisbetriebs-system als auch „Privilege Sepa-ration“ der Server-Anwendung verwendet. Für die Kommunikation

kommt im BSI-zugelassenen Fall die Verwendung von Zertifikaten mit elliptischen Kurven zum Tragen. Die Erzeugung hoch-qualitativer Zufallszahlen übernimmt ein von BSI zugelassener Zufallszahlengenerator der Klasse DRG.4 unter Einbindung einer SmartCard.

Allgemeines

Zugelassene Hardware	Fujitsu Primergy RX2540 M1/2/4/5 Server-Familie; Hardware mit RAID-Controller EP400i (LSI Logic / Symbios Logic MegaRAID SAS-3 3108); zwei Ethernet-Interfaces (PLAN CP 2 x 1 Gbit Cu Intel® I350-T2 oder PLAN CP 4 x 1Gbit Cu Intel® I350-T4); zwei SmartCard-Leser Omnikey 3121 (Revision A oder B) und mindestens ein weiterer, baugleicher SmartCard-Leser zum Personalisieren der SmartCards am Administrations-PC; zwei SmartCards TeleSec TCOS 3.0 Signature Card 2.0; UEFI/BIOS Konfiguration: Legacy BIOS Mode
Konfiguration	Konfiguration mit dem NCP Secure VPN GovNet Server Manager; Übertragung der Konfigurationsdaten mittels VPN-Tunnel zum NCP Secure VPN GovNet Server oder manuell via USB-Stick
DDNS	Registrierung der verbundenen VPN Clients am Domain Name Server via DDNS, Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse
Mandantenfähigkeit	Gruppenfähigkeit; Unterstützung von max. 1024 Domänen-Gruppen (d.h. Konfiguration von: Authentisierung, Weiterleitung via GRE, VLAN oder VPN-Tunnel, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.)
Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN-Adapterschutz
Benutzerverwaltung	Lokale Benutzerverwaltung; OTP-Server; RADIUS; LDAP, MS Active Directory Services
Statistik und Logging	Detaillierte Statistik, Logging-Funktionalität, Versenden von SYSLOG-Meldungen (über UDP oder TCP)
Client/Benutzer Authentifizierungsverfahren	OTP-Token, Benutzer- und Hardwarezertifikate (X.509 v.3, mit RSA oder ECC-Schlüssel), Benutzername und Password (XAUTH), EAP
Server-Zertifikate	Es können Zertifikate verwendet werden, die über folgende Schnittstellen bereitgestellt werden: PKCS#12-Schnittstellefür private Schlüssel in Soft-Zertifikaten
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL)
Online-Check	automatische Downloads der Sperrlisten einer CA in bestimmten Zeitintervallen; Online-Check: Überprüfung der Zertifikate mittels OCSP oder OCSP over http

IPsec-VPN

Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; Automatische Behandlung der MTU Size, Fragmentierung und Reassemblierung; DPD; NAT-Traversal (NAT-T); IPsec Modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS
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, IKEv2 (inkl. MOBIKE), XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation

Verschlüsselung	Symmetrische Verfahren: AES 128, 192, 256 Bits (IKEv1: AES-CBC, AES-CTR; IKEv2: AES-CBC, AES-CTR, AES-GCM); Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits; Dynamische Verfahren für den Schlüsselaustausch: Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30 Hash Algorithmen: (MD5), SHA1, SHA 256, SHA 384, SHA 512 PFS
Authentisierungsverfahren	IKEv1 (Aggressive und Main Mode); XAUTH für erweiterte User-Authentisierung; PAP, CHAP, MS CHAP V.2 IKEv2 (Pre-shared Key, Zertifikate, EAP (EAP-MS CHAPv2, EAP-TLS) Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards, USB Tokens, Zertifikate mit ECC-Technologie oder RSA bis 4096 Bits; Pre-Shared Keys; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready
VPN Path Finder	NCP VPN Path Finder Technology (Fallback IPsec /HTTPS-Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist
IP-Adresszuweisung	DHCP (Dynamic Host Control Protocol) over IPsec; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse an die Clients aus einem internen Pool/Adressbereich oder einem zentralseitigen DHCP-Server oder RADIUS
Datenkompression	Deflate
NCP Secure VPN GovNet Server Manager	Konfigurations-Tool für Windows 7, 8.x, 10 Benutzeroberfläche: Deutsch, Englisch
Empfohlene VPN Clients Kompatibilitäten	NCP VS GovNet Connector, NCP Secure VPN GovNet Box, NCP Secure Client, Standardkonforme IPsec Clients
BSI-Zulassung	Zulassung NCP Secure VPN GovNet Server, Version 10.10/10.11/10.12/10.13/10.14 BSI-VSA-10427

NCP PATH FINDER

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