Trust Seal
www.teletrust.de/itsmig

SecurITy made in Germany

Datenblatt

NCP VS GovNet Server

IPsec VPN Gateway Software

Sicherer Fernzugriff auf das Behörden-/ Firmennetz gemäß VS-NfD-Richtlinien

- BSI-Zulassung (VS-NfD); In Vorbereitung: 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
- Load Balancing
- Mandantenfähigkeit
- Multi-Prozessor-Unterstützung, beliebig skalierbar
- Gehärtetes Linux-System – kompatibel zu Standard-Serverhardware

Einsatzbereich

Der NCP VS 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. Es eignet sich ideal als Gegenstelle für den NCP VS GovNet Connector, der für die Verarbeitung von Daten gemäß VS-NfD am Anwender-Arbeitsplatz ebenfalls vom BSI zugelassen wurde. Ebenso kann der NCP VS GovNet Server als Gegenstelle für Apple iOS- und iPadOS-Geräte fungieren, die gemäß den Vorgaben für INDIGO (**i**OS **N**ative **D**evices **I**n **G**overnment **O**peration) konfiguriert sind.

Installation und Konfiguration

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

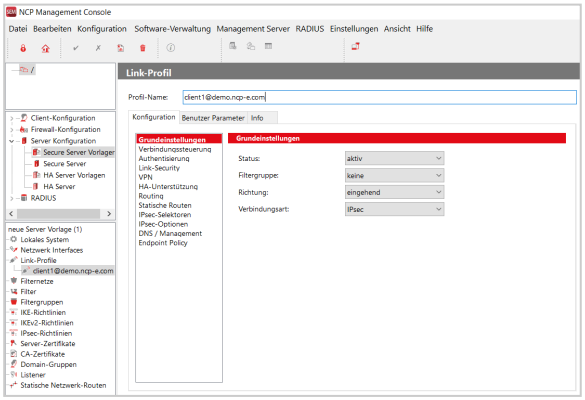


Image installiert. Die Konfiguration geschieht mittels des NCP Secure Enterprise Managements Servers. Mit dieser zentralen Instanz werden ebenso die für den zugelassenen Betrieb notwendigen NCP VS GovNet Connectoren zentral verwaltet.

Der NCP VS 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.

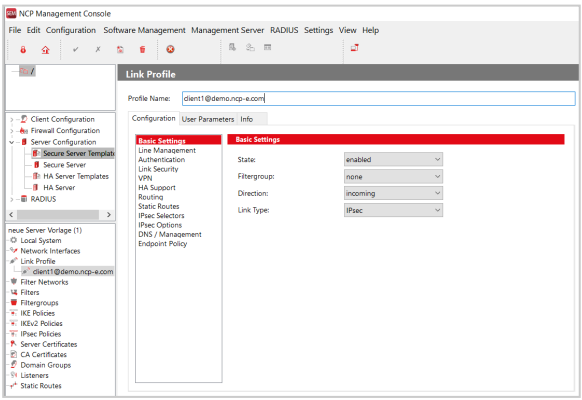
NCP VPN Path Finder

Mit dem NCP VPN Path Finder stellt NCP eine einzigartige Technologie bereit, die Remote Access auch hinter Proxys/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 VS GovNet Servers stand Sicherheit an erster Stelle. Um das Risiko durch Angriffe auf das Server-System selbst zu minimieren, wird ein gehärtetes Linux Basisbetriebssystem

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 Zufallszahlengenerator der Klasse DRG.4 unter Einbindung einer SmartCard.



Allgemeines

Zugelassene Hardware	Standard-Server mit x86-64 Hardware und Kompatibilität zu Debian 11.7; UEFI/BIOS Konfiguration: Legacy BIOS Mode (UEFI im CSM-Modus) 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;
Konfiguration	Konfiguration mit dem zentralen NCP Secure Enterprise Management Server
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 eine PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten bereitgestellt werden.
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), RFC 7427 (IKEv2 Signature Authentication, Padding-Verfahren), XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, RFC 3527 (DHCPv4), RFC 5685 (IKEv2 Redirect)
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 (NIST, Brainpool) oder RSA bis 4096 Bits; Pre-Shared Keys; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready
VPN Path Finder NCP 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
Empfohlene VPN Clients Kompatibilitäten	NCP VS GovNet Connector, NCP Secure Client, Standardkonforme IPsec Clients
BSI-Zulassung	Zulassung NCP VS GovNet Server BSI-VSA-10711

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