
NCP
SECURE COMMUNICATIONS

# Datenblatt

# NCP Secure Enterprise Linux Client

## Universelle, zentral managebare VPN Client Suite für Linux

- Zentrales Management und Network Access Control
- Kompatibilität zu VPN Gateways (IPsec Standard)
- Dynamische Personal Firewall
- VPN Path Finder Technology (Fallback IPsec / HTTPS)
- Starke Authentisierung
- Multi-Zertifikatsunterstützung
- FIPS Inside
- Unterstützung von 3G/4GHardware (LTE)
- Kostenlose 30-Tage-Vollversion


## Universalität und Kommunikation

Der NCP Secure Enterprise Linux Client ist ein Baustein der NCP Next Generation Network Access Technology – der ganzheitlichen Remote Access VPN-Lösung.

Auf Basis des IPsec-Standards lassen sich hochsichere Datenverbindungen auch zu VPN Gateways anderer Anbieter herstellen. Teleworker können mit Linux-Endgeräten von jedem Standort weltweit auf das zentrale Datennetz zugreifen.

Die von NCP entwickelte „VPN Path Finder Technology“ 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.

## Sicherheit

Der NCP Secure Enterprise Linux Client verfügt über zusätzliche Sicherheitsmechanismen wie eine integrierte dynamische Personal Firewall. Das Feature „Friendly Net Detection“ erkennt anhand der im Client vorgegebenen Sicherheitsregeln, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet. Es aktiviert je nach Netz die entsprechenden Firewall-Regeln. Dies gilt auch im Umfeld von Hotspots, hier insbesondere während des An- und Abmeldevorgangs am WLAN. Die NCP Personal Firewall ist zentral administrierbar*.

Weitere Security Features sind die Unterstützung von OTP-Lösungen (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Ein ebenso verfügbarer Endpoint Policy-Check verhindert den Zugriff ungenügend geschützter Endgeräte auf das zentrale Datennetz.

Die „Multi-Zertifikatsunterstützung“ ermöglicht VPN-Verbindungen mit unterschiedlichen Firmen, die jeweils ein eigenes Benutzerzertifikat erfordern. Es lassen sich mehrere Zertifikats-einstellungen festlegen und diese pro Profil zuordnen. Das Kryptografiemodul, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).

## Usability und Wirtschaftlichkeit

Die einfache Bedienung und die zentrale Administrierbarkeit des NCP Secure Enterprise Linux Clients sind einzigartig am Markt. Die grafische, intuitive Benutzeroberfläche informiert den Anwender über alle Verbindungs- und Sicherheitsstati vor und während einer Daten-verbindung. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Ein Konfigurationsassistent ermöglicht das ein-fache Anlegen von Profilen.

Ein frei gestaltbares Banner in der Client GUI steht für Firmenlogo oder Supporthinweise zur Verfügung.

## Zentrales Management

Das NCP Secure Enterprise Management bietet unter dem Anspruch „Single Point of Administration“ alle Funktionalitäten und Automatismen für den wirtschaftlichen Betrieb eines ganzheitlichen Remote Access VPN. Rollout, Inbetriebnahme und den wirtschaftlichen Betrieb eines ganzheitlichen Remote Access VPN.

*) Installation eines NCP Secure Enterprise Managements erforderlich

| | |
|---|---|
| **Betriebssysteme** | 32/64 Bit: Ubuntu Desktop 10.04.3 LTS, open SUSE 11.3, 11.4, 12.1, Fedora 16, Debian 5.0.8 |
| **Security Features** | Der NCP Secure Client unterstützt alle IPsec Standards nach RFC |
| Personal Firewall<br>Firewall Konfiguraton* | Stateful Packet Inspection;<br>IP-NAT (Network Address Translation);<br>Friendly Net Detection (FND)**,<br>Auswertung von aktueller Netzwerkadresse und IP-Adresse;<br>Automatische FND,<br>Secure Hotspot Logon;<br>Differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen, zentrale Administration mit Client Firewall Configuration Plug In* |
| Virtual Private Networking | IPsec (Layer 3 Tunneling), RFC-konform;<br>IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKE, IPsec Phase 2);<br>Event log;<br>Kommunikation im Tunnel;<br>MTU Size Fragmentation und Reassembly;<br>DPD;<br>NAT-Traversal (NAT-T);<br>IPsec Tunnel Mode |
| Verschlüsselung (Encryption) | Symmetrische Verfahren: AES 128,192,256 Bits;<br>Blowfish 128, 448 Bits; Triple-DES 112,168 Bits;<br>Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits;<br>Seamless Rekeying (PFS);<br>Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1,2,5,14 |
| FIPS Inside | Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).<br>Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:<br>▪ Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit)<br>▪ Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit<br>▪ Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES |
| Authentisierungsverfahren | IKE (Aggressive und Main Mode), Quick Mode;<br>XAUTH für erweiterte User-Authentisierung;<br>IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP);<br>PFS;<br>PAP, CHAP, MS CHAP V.2;<br>IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2);<br>EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2);<br>Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens;<br>Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready |

| | |
|---|---|
| Starke Authentisierung – Standards<br>PKI Enrollment* | X.509 v.3 Standard<br>PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2 und 2.0;<br>Smart Card ReaderInterfaces: PC/SC, CT-API;<br>PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten;<br>PIN-Richtlinie;<br>Administrative Vorgabe für die Eingabe beliebig komplexer PINs;<br>Revocation: EPRL (End-entity Public-key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL), OCSP. CMP* (Certificate Management Protocol) |
| Network Access Control | Endpoint Policy Enforcement* |
| Networking Features | LAN Emulation: Virtual Ethernet-Adapter |
| Netzwerkprotokoll | IP |
| VPN Path Finder | NCP VPN Path Finder Technology* mit Proxy-Unterstützung, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP Secure Enterprise Server 8.0) |
| Weitere Features | UDP-Encapsulation, Multi-Zertifikatsunterstützung |
| IP Address Allocation | DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server |
| Übertragungsmedien | Festnetze: analoges Fernsprechnetz, ISDN, xDSL, LAN<br>Funknetze: GSM, GPRS, UMTS, LTE (abhängig von eingesetzter Hardware), Internet |
| Line Management | DPD mit konfigurierbarem Zeitintervall;<br>Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert;<br>Timeout (zeit- und gebührengesteuert) |
| Datenkompression | IPCOMP (lzs), Deflate |
| Point-to-Point Protokolle | PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet;<br>LCP, IPCP, MLP, CCP, PAP, CHAP, ECP |
| Internet Society RFCs und Drafts | RFC 2401 –2409 (IPsec), RFC 3498, RFC 3947:<br>IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP |

| | |
|---|---|
| Client Monitor<br>Intuitive, grafische Benutzeroberfläche | Mehrsprachig (Deutsch, Englisch);<br>Intuitive Bedienung;<br>Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose;<br>Ampelsymbol für Anzeige des Verbindungsstatus;<br>Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre |

*) Voraussetzungen: NCP Secure Enterprise Management und / oder NCP Secure Enterprise Server
**) Download des NCP FND Servers: https://www.ncp-e.com/de/service/download-vpn-client/

Weitere Informationen zu NCP Secure Enterprise Linux Clients:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-clients/

FIPS 140-2 Inside


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