Data Sheet

NCP Secure Enterprise Linux Client

Versatile central manageable VPN Client Suite for Linux

- Central Management and Network Access Control
- Compatible with VPN gateways (IPsec Standard)
- Integrated, dynamic personal firewall
- FIPS Inside
- Fallback IPsec/HTTPS (NCP VPN Path Finder Technology)
- Strong Authentication
- Multi Certificate Support
- Integrated support for 3G / 4G hardware
- Integration of all security and communication technologies for universal remote access
- Free of charge 30 day full version

Universality

NCP Secure Enterprise Linux Client is a component of NCP's „Network Access Technology" the holistic NCP Secure Enterprise Solution. The teleworker works transparently and securely at any location (mobile or stationary) in the same manner as he works at his office within his corporate environment. Highly secure data connections to VPN gateways from all well-known suppliers can be established using IPsec standards. Data are transferred independent of media type via stationary networks, public wireless networks, LANs (e.g. in the branch office network), the Internet, as well as wireless networks such as wireless LANs within his corporate environment and at hotspots. Teleworkers can use any end device under Linux 32 or 64 bit-operating systems from any location, to access central data repositories and any application. Even behind firewalls or proxies, whose settings always prevent IPsec data connections, the NCP VPN Path Finder technology allows for remote access.

Security

The NCP Secure Enterprise Client offers extensive security mechanisms that prevent attacks in any remote access environment. Hence, it offers comprehensive security of both, the end device and the corporate network. This is true, even at hotspots during the logon and logoff process to the Wi-Fi network. In addition to data encryption the most important integrated components are: a dynamic personal firewall, support of OTP (One-Time Password tokens), certificates in a PKI (Public Key Infrastructure) and endpoint security*.

Optimized for remote access, the NCP's Network Access Control Solution generally prevents insufficiently protected end devices from accessing the central data network. Use the personal firewall to define policies for: Ports, IP addresses and segments, as well as applications. An additional safety criterion is "Friendly Net Detection"(location awareness), i.e. automatic detection of secure and non-secure networks. The appropriate firewall rules are activated or deactivated depending on whether a friendly net is detected. In contrast to common firewalls, the centrally administrable* NCP firewall is already active at system startup. The Multi Certificate Support feature enables VPN connections to various companies, each which

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

demand a user certificate of its own. All Client configurations can be locked by the administrator which means, the user cannot change the locked configurations. The cryptographic module complies with the requirements of FIPS 140-2 (certificate #1747).

Usability and Profitability

"Easy-to-use" for both, user and administrator - the NCP Secure Enterprise Client offers simple installation and simple operation. A graphical, intuitive user interface provides information on all connection and security states. Detailed log information paves the road for effective assistance from the help desk. The feature “automatic media detection” automatically selects the fastest communication medium available. A configuration wizard enables easy set up of connection profiles. Integrated support of Mobile Connect Cards for WWAN (Wireless Wide Area Network) applies, without restriction, for all operating systems supported. The additional installation of the user interface supplied by the card manufacturers is not necessary. The Client Monitor can be tailored to include your company name or support information.
Usability also means cost reduction through less time spent trainings, less documentation and fewer support cases. VPN tunnels can be configured to be established automatically.

Central management*

The NCP Secure Enterprise Management offers as “single point of administration” all functionalities and automation mechanisms for commissioning and economic operation of remote access VPNs.

*) Option

Data Sheet

NCP Secure Enterprise Linux Client

Operating Systems	32/64 Bit: Ubuntu Desktop 14.04.2, open SUSE 13.2, Fedora 22, Debian 8.1.0, CentOS 7.1, SUSE Linux Enterprise Desktop 12
Security Features	The Secure Enterprise Linux Client supports all major IPsec standards in accordance with RFC
Personal Firewall **Firewall Configuration***	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (FND)** (analysis of: current network address and IP address; automatic FND, secure hotspot logon; differentiated filter rules relative to: protocols, ports and addresses, LAN adapter protection, central administration with Client firewall configuration plug-in*
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-conformant; IPsec proposals can be determined through the IPsec gateway (IKE, IPsec Phase 2); Event log; communication in the tunnel; MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPsec tunnel mode
Encryption	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS); Hash algorithms: SHA-256, SHA-384, SHA-512, MD5, Diffie-Hellman Groups 1,2,5,14
FIPS Inside	The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747). FIPS compatibility is always given if the following algorithms are used for set up and encryption of the IPsec connection: ▪ DH Group: Group 2 or higher (DH starting from a length of 1024 Bit) ▪ Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit ▪ Encryption Algorithms: AES with 128, 192 and 256 Bit or Triple DES
Authentication Processes	IKE (Aggressive mode and Main Mode), Quick Mode; XAUTH for extended user authentication; IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2); support of certificates in a PKI: Soft certificates, smart cards, and USB tokens: Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready
Strong Authentication **- Standards** **PKI Enrollment***	X.509 v.3 Standard; Entrust Ready PKCS#11 interface for encryption tokens (USB and smart cards); smart card operating systems: TCOS 1.2 and 2.0; smart card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys in soft certificates; PIN policy; administrative specification for PIN entry in any level of complexity; revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP. CMP* (Certificate Management

Data Sheet

NCP Secure Enterprise Linux Client

Network Access Control	Endpoint Policy Enforcement*
Networking Features	LAN emulation: virtual Ethernet adapter
Network Protocol	IP
Dialers	NCP Internet Connector
VPN Path Finder	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is no possible (prerequisite: NCP VPN Path Finder Technology on the Gateway is required)
Additional Features	Automatic media detection, UDP encapsulation, Multi certificate support
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server
Transmission Media	Internet, xDSL, LAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, PSTN, ISDN
Line Management	DPD with configurable time interval; channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges)
Data Compression	IPCOMP (lzs), deflate
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3498, RFC 3947: 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 **Intuitive, Graphical User Interface**	Multilingual (English, German); Intuitive operation; configuration, connection management and monitoring, connection statistics, log-files, trace tool for error diagnosis; traffic light icon for display of connection status; integrated support of Mobile Connect Cards (PCMCIA, embedded); password protected configuration management and profile management, configuration parameter lock

*) Prerequisites: NCP Secure Enterprise Management and/or NCP Secure Enterprise Server

**)Download NCP FND server: https://www.ncp-e.com/en/resources/download-vpn-client.html
More information on NCP Secure Enterprise Clients:
https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-clients.html

FIPS 140-2 Inside

NCP PATH FINDER

Next Generation Network Access Technology