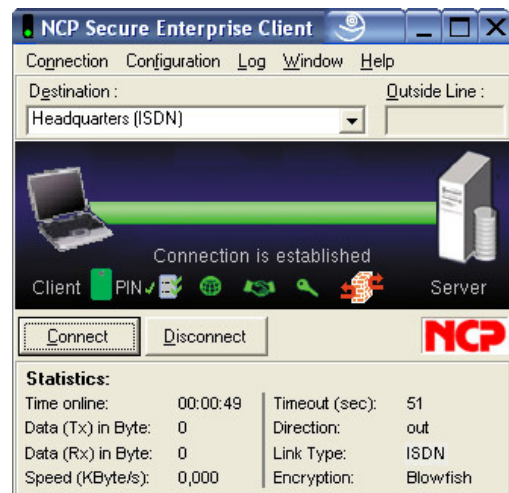


Universal, centrally manageable IPSec client software for Linux

- ▶ **Highly secure access to the central data network**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Worldwide dial-in to the corporate network**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Strong authentication with certificates - software and hardware**
- ▶ **Endpoint security and central management**



Universality

The NCP Secure Enterprise Linux Client is a component of the holistic NCP Secure Enterprise Solution. The communication software is used for universal teleworking in any remote access VPN environment. Highly secure data connections can also be established to NCP Secure Enterprise Servers as well as to VPN gateways from all well-known suppliers on the basis of the IPSec standard. 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 on corporate campuses and at hotspots. Teleworkers can use any end device under Linux (for example desktops, laptops, notebooks, Pocket PCs, handhelds, mobile phones) from any location, to access central data repositories and any application.

Security

Universal implementation possibilities require security mechanisms that repel attacks in any remote access environment. Even at hotspots during the logon and logoff process. In addition to VPN tunneling the most important integrated components are: data encryption, a dynamic personal firewall, support of OTP (One-Time Password tokens) and certificates in a PKI (Public Key Infrastructure). 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", i.e. automatic detection of secure and non-secure networks. Depending on

whether a friendly net is detected the appropriate firewall rules will be activated or deactivated. All configurations can be entered centrally by the administrator and parameters can be set so that configurations cannot be changed by the user. Central management mechanisms (see below) enable automatic transfer of all configuration parameters to the Client. The NCP Dialer also offers protection against cost-intensive outside dialers.

Convenience

"Easy-to-use" – simple installation and operation of the client software. A graphic, intuitive user interface provides information on all connection states. The teleworker works in the same manner as he/she would work at the office workstation. Domain logon is also appropriately convenient. Automatic updates ensure current versions of software and configurations.

Central management*

The NCP Secure Enterprise Management Software offers all functionalities and automation mechanisms for commissioning and operation of remote access VPNs. As part of endpoint security all safety-relevant parameters are checked before access is granted to the corporate network. The safety policies are mandatory and cannot be bypassed or manipulated by the user.

*) optional

Technical data

Operating systems	As of Linux kernel version 2.4.10 (including SuSE 9.3 kernel version 2.6.11.4-20a, SuSE 10.0 kernel version 2.6.13-15, Fedora Core3 kernel version 2.6.9-1.667)
Security features	The Enterprise Client supports all major IPSec standards in accordance with RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (FND) (analysis of: current network address, IP address and MAC address of the DHCP server); 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*
Firewall configuration*	
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 modes: tunnel mode, transport 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; Diffie-Hellman Groups 1,2,5 seamless rekeying (PFS); hash algorithms: SHA1, MD5
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	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 <i>CRL</i>), CARL (Certification Authority Revocation List, formerly <i>ARL</i>), OCSP. CMP* (Certificate Management Protocol),
PKI enrollment*	
Endpoint Security	Endpoint Policy Enforcement*
Networking features	LAN emulation: Ethernet adapter with NDIS interface
Network protocols	IP
Dialers	NCP Secure Dialer
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	Stationary networks: analog telephone network, ISDN, xDSL, LAN wireless networks: WLAN, GSM, GPRS, UMTS (depending on the hardware used), Internet
Line management	DPD with configurable time interval; Short Hold Mode; WLAN roaming (handover); channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges); budget manager
Data compression	Stac (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 graphic user interface	Multilingual (German, English, Polish); 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); password protected configuration management and profile management, configuration parameter lock

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

More information on NCP Secure Communication products is available on the Internet at: www.ncp.de

You can test a full version of the Secure Enterprise Linux Client for 30 days, free of charge here:

<http://www.ncp.de/english/download/testsoftware/index.html>