

Versatile IPSec client software for Linux operating systems

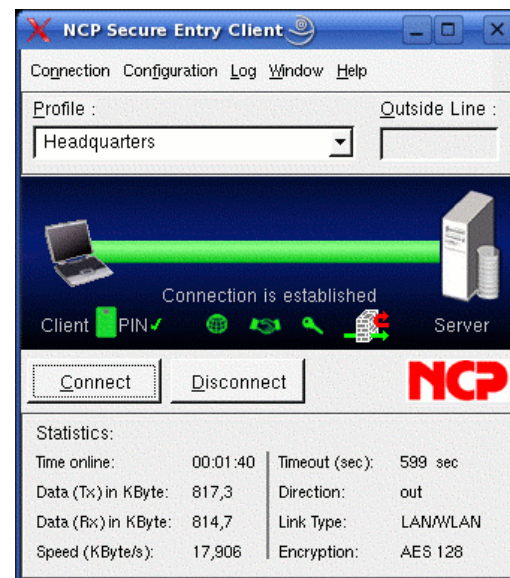
- ▶ **Highly secure, encrypted access to the central data network**
- ▶ **Worldwide dial-in via all public cable networks and wireless networks**
- ▶ **Compatible with VPN gateways from different manufacturers**
- ▶ **Support of all IPSec protocol extensions**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Strong authentication with certificates**

Versatility

The NCP Secure Entry Linux Client is an intelligent client software that can be implemented in any Virtual Private Network and terminate against any IP-Sec gateway (e.g., concentrator, router, firewall). The connection can be established over any wired or wireless networks, be it public or private. Data are transferred independent of the media type via stationary networks, public wireless networks, LANs (e.g. in the branch office network), the Internet, as well as wireless LANs (WiFi) on corporate campuses and at hotspots. Teleworkers can use any end device to access central data repositories and applications from any location.

Security

Universal implementation possibilities require security mechanisms to repel attacks in any remote access environment. Even at hotspots during the login and logoff process. The Entry Client supports all IPSec standards as set in the RFCs. The product meets the highest security requirements. Strong user authentication is provided by the support of OTP tokens (RSA SecurID Ready) as well as digital certificates in a PKI. An integrated personal firewall shields against attacks from local networks and the Internet. The latest encryption algorithms protect sensitive data in transit.



Convenience

"Easy-to-use" - the NCP Secure Entry Client offers simple installation and simple operation. The integrated installation wizard and an intuitive graphic user-interface ensure convenient operation. The user works from any location, just like he does on his/her office workstation. Detailed loggings are also provided by the software.

The user doesn't "notice" the Client software at all during his remote access session. The Client software monitors and secures every data connection of the respective application, automatically in background.

*IPSec Compatibility

Compatible IPSec gateways: Astaro, Bintec, Check Point, Cisco, Concept04, Cosine, D-Link, F-Secure, Fortinet, FreeSwan, Genua, Intermate, Lancom, Linksys, NCP, Netgear, Netscreen, OpenBSD, OpenSwan, Pyramid, Smoothwall, SonicWall, Symantec, TelcoTech, WatchGuard.

For further information see:

www.ncp.de/english/services/ipseckompat

Technical Data

System Requirements	Linux kernel version 2.4.10 or higher (SuSE 9.3 kernel versions 2.611.4-20a, NOVELL SuSE 10.0 kernel versions 2.6.13-15, Fedora Core 3 kernel versions 2.6.9-1.667); 64 MB RAM, min. 10 MB free on HD; WAN and/or LAN adapter
Security Features	The Entry Client supports all IPSec standards as set in the RFCs. The product meets the highest security requirements.
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (check of current network address against IP address and MAC address of DHCP server); Secure Hotspot Logon; differentiated filter rules for protocols, ports, addresses and links; LAN adapter protection
Virtual Private Networking	Native IPSec (Layer 3 tunneling), RFC conform; IPSec proposals can be determined by IPSec gateway (IKE, IPSec Phase 2); event log; block and central tunneling; MTU size fragmentation and reassembly
Encryption	Supported Symmetric Ciphers: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; Dynamic key exchange protocols: RSA up to 2048 bits; Diffie-Hellman groups 1,2,5; Seamless rekeying (PFS); Hash process: SHA1, MD5
Authentication Methods	IKE (aggressive and main mode), XAUTH for extended user authentication; IKE config mode for dynamic allocation of a virtual address from the internal address range (private); MS CHAP V.2; EAP-MD5 (Extensible Authentication Protocol): extended authentication against switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): extended, certificate based authentication against switches and access points (Layer 2); Support of certificates in a PKI: Soft Certificates, Smart Cards & USB Tokens; Pre-shared secrets; One-Time Passwords & Challenge Response systems; RSA SecurID Ready.
Strong Authentication Standards	X.509 v.3 certificate format, also Entrust Ready; PKCS#11 interface for cryptographic tokens (USB and Smart Cards); Smart Card OS: TCOS 1.2 and 2.0; Smart Card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys stored in Soft Certificates; PIN policy; administrative rule for any complex PIN entry; Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>formerly CRL</i>), CARL (Certification Authority Revocation List, <i>formerly ARL</i>), OCSP.
Networking Features	LAN Emulation: virtual Ethernet adapter with NDIS interface
Network Protocol	IP, NAT traversal (NAT-T)
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: dial into the central gateway with changing public IP addresses through IP address query via a DNS server
Communications Media	Wired: PSTN, ISDN, xDSL, Cable, LAN; Wireless: WLAN, GSM, GPRS, UMTS; Internet.
Line Management	DPD for connection monitoring; Shorthold mode, User configurable time intervals in the event of DPD incidents for restoration of VPN tunnels; DPD Timeout; WLAN Roaming (handover); Channel bundling (dynamic in ISDN) with freely configurable threshold value, short hold, timeout (controlled by time and charges);
Compression	Stac & Stac with history (lzs), Deflate (zlib)
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 Graphical 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 displays the connection states. Configuration and profile management with password protection, authorizations adjustable per function, display and show parameter fields.

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