

Data Sheet

NCP Secure Remote
Access Technology

www.ncp.de

NCP

SECURE COMMUNICATIONS

Technical Description of the NCP Secure Remote Access Solution NCP Secure Client and NCP Secure Gateway

NCP Secure Client

System Requirements

Platform for Windows Clients: Windows 98se, NT, 2000, ME, XP and CE
Platform for Linux Clients: Linux kernel version 2.4.x (SuSE or RedHat)
32 MB RAM, min. 10 MB free on HD,
WAN and/or LAN adapter

Dialer

NCP Secure Dialer, Microsoft RAS Dialer

Personal Firewall

IP-NAT, Stateful Inspection, LAN adapter protection and Filtering

Deployment & Administration

NCP Secure Client Manager (optional)
NCP Secure Update Server (optional)
NCP Secure PKI Manager (optional)

NCP Secure Gateway

System Requirements

Platform: Windows NT 4.0 SP5, 2000 (Workstation & Server), Linux kernel v.2.4.x, SUN Solaris 7, 8
CPU: Pentium III
64 MB RAM for each 250 concurrent tunnels, min. 128 MB
Clock: 2 Mbps for each 150 MHz
HD: minimum 50 MB free disk space
Public IP address is required
LAN adapter

When Gateway is used as network access server: ISDN BRI or PRI (max. 120 B-channels), digital modems

Firewall Functionalities

IP-NAT, Stateful Inspection, LAN adapter protection
Filtering: protocols, ports, addresses
SPX Spoofing, SNA and NetBIOS Local Termination

NCP Secure Server Manager

Management software for NCP Gateway.
Platform: Windows 98, ME, NT4.0 SP5, XP and 2000
SNMP and SNMP over SSL

High Availability Services

NCP Load Balancing Server (optional)
NCP Failsafe Server (optional)

Networking Features

LAN Emulation

Ethernet, Token Ring (optional)

Network Protocols

IP, IPX, optionally SNA and NetBIOS

Address Management

WINS, DNS, DHCP, DynDNS

Communications Media

Wired: PSTN, ISDN, xDSL, LAN
Wireless: Internet, WLAN, HSCSD, GSM, GPRS, UMTS

Line Management

Low Level Call Back (COSO)
Shorthand mode, DPD Timeout
WLAN Roaming
Channel bundling with ISDN
Dial-out triggered via ISDN D-Channel

Compression

Stac & Stac with history

Point-to-Point Protocols

PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet
LCP, IPCP, IPXCP, MLP, Call Back, CCP, PAP, CHAP, ECP

Security Features

Virtual Private Networking

Tunneling process definable per link

Layer 2 tunneling modes:
GRE, L2TP, L2sec, IPsec over L2TP

L2sec: SSL handshake in PPP negotiation (TLS/EAP, RFC 2716), SSLCP with/without certificates)

Layer 3 tunneling: (native) IPsec
IPsec proposals are determined by NCP Secure Gateway.

Encryption

Supported Symmetric Ciphers:
AES 128, 192, 256 bit
Blowfish 128, 448 bit
Triple-DES 112, 168 bit
IDEA and CAST (optional)

Dynamic key exchange protocols:
RSA 1024, 2048 bits
Diffie-Hellman groups 1,2,5
Hash process: SHA1, MD5

Authentication Methods

Support of strong authentication with certificates in a PKI:
Soft Certificates,
Smart Cards & USB Tokens
Pre-shared secrets
One-Time Passwords & Challenge Response systems
EAP-MD5

Strong Authentication Standards

X.509 v.3 certificate format (also Entrust Ready)
PKCS#11 interface for cryptographic tokens (USB and Smart Cards)
Smart Card reader interfaces:
PC/SC, CT-API
PKCS#12 interface for private keys stored in Soft Certificates
PIN policy
Revocation: EPRL (CRL), CARL, OCSP

User Administration

Local user configuration on NCP Gateway, OTP Server, RADIUS, LDAP -including Novell NDS, MS Active Directory Services

Internet Society RFCs & Drafts

RFC 2401-2409 (IPsec):
IP Security Architecture, ESP
HMAC-MD5-96, HMAC-SHA-1-96
ISAKMP, IKE, XAUTH, IKECFG, DPD, NAT traversal, UDP encapsulation

