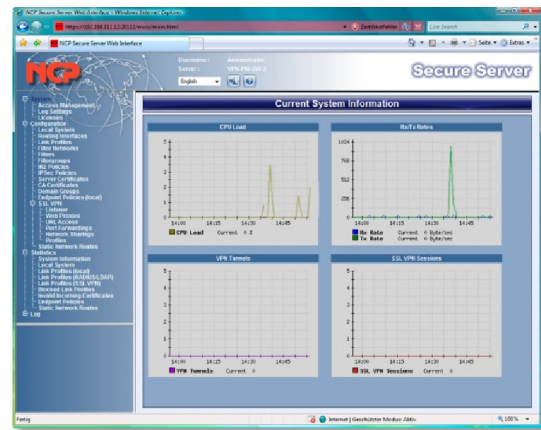


## Next Generation Network Access Technology

### Hybrid IPsec/SSL-VPN gateway software Central component of a holistic Virtual Private Network (VPN)

- ▶ **Universal platform for IPsec VPNs and SSL VPNs**
- ▶ **Compatible with IPsec gateways from all major manufacturers (IPsec standard)**
- ▶ **Integrated IP routing and firewall functionalities**
- ▶ **Fallback IPsec/HTTPS (VPN Path Finder Technology)**
- ▶ **Central and distributed installation**
- ▶ **Bandwidth management**
- ▶ **Network Access Control\***
- ▶ **Multi company support (use by multiple companies)**



### Universality

The NCP Secure Enterprise VPN Server is a component of NCP's "Secure Network Access Technology", the holistic remote access solution. As platform for universal highly secure access to the corporate network the VPN gateway satisfies all communication and security requirements for operation of a professional virtual private network.

Via the NCP Secure Enterprise VPN Server secure data connections can be set up to the corporate network on the basis of an IPsec VPN and/or SSL VPN, as needed.

User management can be executed directly via the VPN gateway or back-end systems, such as RADIUS LDAP or MS Active Directory.

For increased availability it is possible to integrate one or multiple NCP Secure Enterprise VPN Servers in a high availability environment with failsafe or load balancing servers.

In addition to the usual installation on a standard PC (Windows/Linux) behind a firewall in the DMZ (Demilitarized zone) the NCP Secure Enterprise VPN Server can also be used directly on the public network (Wide Area Network). Integrated IP routing and firewall functionalities ensure connectivity and security for networking a branch office for example. Even behind firewalls, whose settings always prevent IPsec data connections, the NCP Path Finder technology allows for remote access.

The VPN Server software is modular and highly scalable. It can be extended as desired to meet the respective demand for remote users and VPN tunnels. Installation of the NCP Secure VPN Server software is possible on dedicated PCs (in larger VPN environments we recommend parallel use of multiple systems for availability reasons) or on an existing server (e.g. in smaller

networks). If multiple VPN systems will be used then the optional High Availability services ensure high availability and uniform capacity utilization of all NCP Secure Enterprise VPN Servers.

Consistent implementation of standards enables universal implementation in existing IT infrastructures and compatibility with VPN gateways provided by other manufacturers in IPsec environments.

### Security

The NCP Secure Enterprise VPN Server supports all the security mechanisms that are required for confidential access to the corporate network. Access and transmission security are ensured through: IPsec and SSL tunneling, data encryption, firewalling, strong authentication, support of OTP (One-Time Password) tokens, and certificates in a PKI (Public Key Infrastructure).

Validity of certificates can be verified relative to the Certification Authority offline or online at each dial-in based on revocation lists. Within the framework of Endpoint Security\* every external device is checked for specified, security relevant parameters prior to accessing the productive network. If there is deviation from target values then the system can trigger various pre-defined activities. In an IPsec VPN the options are: Disconnect, continue in the quarantine zone, or starting external applications on the remote PC. For an SSP VPN access authorizations to certain applications will be granted on the basis of pre-defined security levels. After concluding a SSL session all data on the end device are deleted automatically. Compliance with the security policies is mandatory and cannot be bypassed or manipulated by the remote user.



Protocols and extensive messages of the central VPN management system meets all compliance requirements and provide the requisite overview for network administrators - at any time.

New security technologies as well as supplemental features can be added at anytime through simple updates.

## Performance and convenience

With the NCP Secure Communications solution the Intranet is extended with remote workstations. Mobile and stationary teleworkers become integrated participants in a cross company data network. The manner in which and the extent to which the remote users are allowed to access the central corporate network is specified from the central location or determined by the tunneling technology used.

Using NCP's IPsec VPN solution via the NCP Secure Client Software, the user can transparently access all network applications and other network functions - among others Voice over IP. It does not matter if the user seeks access from his office or from his tele-work place. The NCP Secure Client Software is based on LAN emulations.

NCP's PortableLAN Client (Fat Client) offers transparent network access if an SSL VPN is in place. Compared to the NCP Enterprise Client Suite, this solution, however, does not offer all features and has some restrictions in respect to usability, administration and performance.

Apart from the normal range of functions, NCP's SSL VPN solution offers two additional, application-based options for access to the company network:

- Web Proxy - clientless operation for Web applications. You can use NCP's SSL Web Proxy on all web browsers that come as standard with the operating system of the end-device.

- Port Forwarding - Thin Client for Client-/Server Applications (TCP/IP). The data of the configured application(s) (e.g. Remote Desktop, Telnet, SSH-Sessions) is (are) re-directed by a Thin Client that has been downloaded automatically. The Thin Client is a prerequisite for the use of all security mechanisms mentioned above: e.g. cache protection and endpoint security.

NCP's SSL VPN strictly supports strong user authentication via OTP and certificates. In case of Web Proxy or Port Forwarding, the use of certificates depends on the browser. In an IPsec VPN the same network address (IP address) can be assigned to the NCP Secure Client after each dial-in. This facilitates remote administration and central user support. This is a private IP address from the enterprise's address pool. The remote participant can always be uniquely identified based on his IP address - regardless of the location from which he dials into the corporate network. With dynamic assignment of an IP address from a pool the address can be reserved for a certain user within a defined period (lease time).

NCP Secure Enterprise VPN Server is optimised for remote access, i.e. the support and management of a large number of teleworkers or VPN tunnels. Management functions are used to

control and monitor all data connections between teleworkstations and corporate headquarters. These integrated automation mechanisms ensure transparency, and optimize performance, security, and the profitability of the holistic VPN solution.

The NCP Secure Enterprise VPN Server supports Dynamic DNS (DynDNS) for reachability of the VPN gateway. In an IPsec VPN the remote client (teleworker) is reachable from the central location over ISDN via "trigger call" (i.e. "D-channel knocking").

Multi Company Support enables concurrent utilization of a system by multiple companies (resource sharing). Convenient access management enables reliable administration of each company's respective NCP Secure Enterprise Clients through its own system administrators.

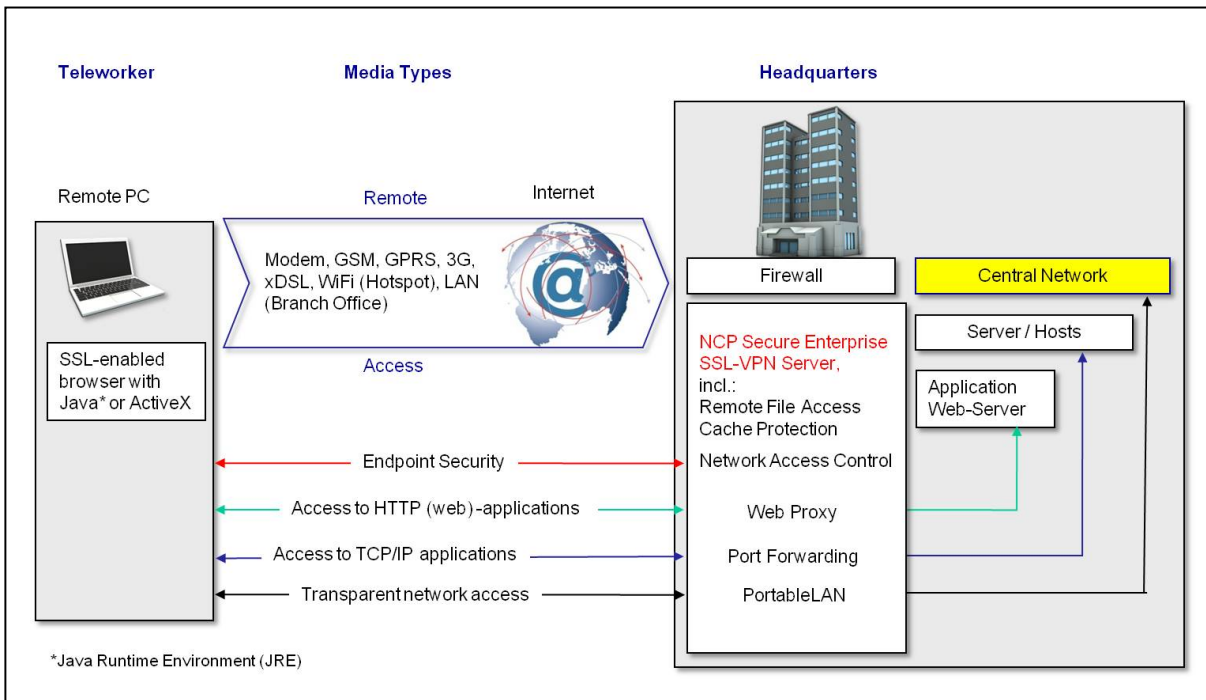
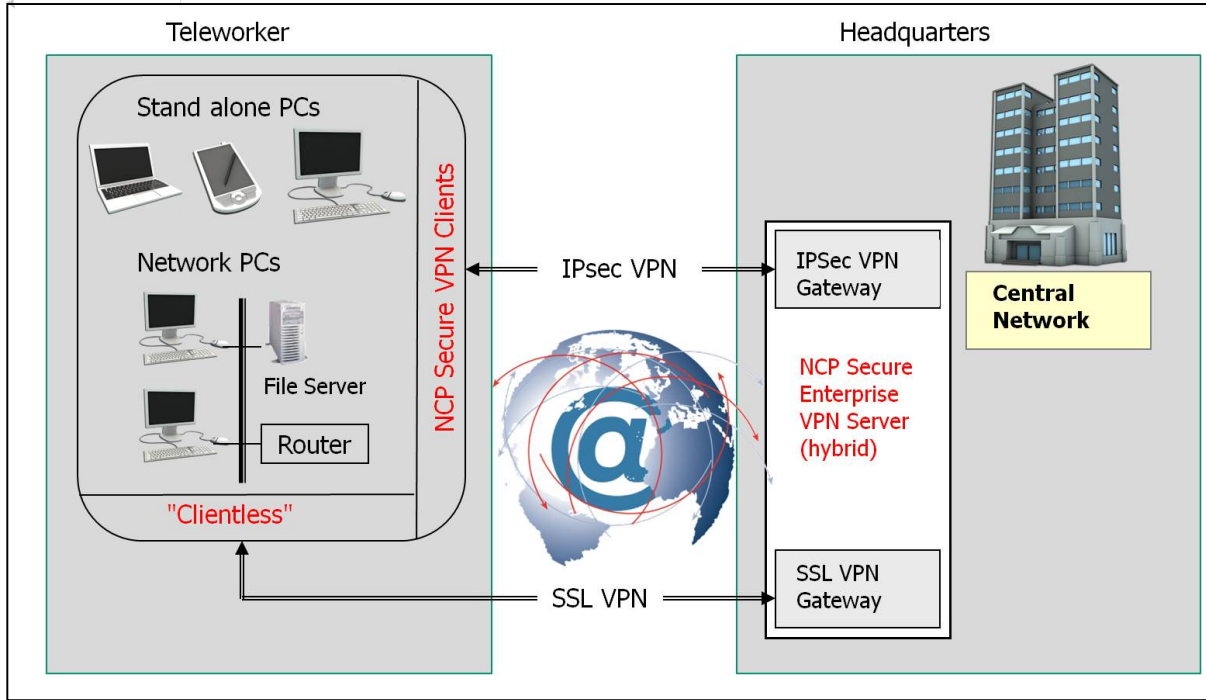
The modular software architecture of the NCP Secure Enterprise VPN Server allows an extension of the system as needed.

## Management

The NCP Secure Enterprise VPN Server is configured and managed via the NCP Secure Enterprise Management by use of plug-in or by use of a webinterface.

\*) Network Access Control is an integrated part of the NCP SSL VPN Gateway. In case of an IPsec VPN, the NCP Secure Enterprise Management is needed

Function and configuration overviews



\*Java Runtime Environment (JRE)

Technical data

IPsec VPN and SSL VPN – general

<b>Operating Systems</b>	32-Bit: Windows 2003 Server, Windows 2003 R2, Windows Server 2008 Linux Kernel 2.6 as of version 2.6.12 (distributions on request). 64-bit: Windows Server 2008, Windows Server 2008 R2
<b>Management</b>	The NCP Secure Enterprise VPN Server is configured and managed via the NCP Secure Enterprise Management by use of server plug-in or by use of a webinterface.
<b>Network Access Control (Endpoint Security)</b>	Endpoint Policy Enforcement for incoming data connections. Verification of predefined, security-relevant client parameters in this regard. Measures in the event of target/actual deviations: - IPsec VPN: Disconnect or continue in the quarantine zone with instructions for action (Messagebox) or start of external applications (e.g. virus scanner update), logging in Logfiles (see the Secure Enterprise Management data sheet for more information). - SSL VPN: Access authorization to certain applications in accordance with defined security levels.
<b>Dynamic DNS (DynDNS)</b>	Connection set up via Internet with dynamic IP addresses. Registration of each current IP address with an external Dynamic DNS provider. In this case the VPN tunnel is established via name assignment (prerequisite: The VPN client must support DNS resolution - as do NCP Secure Clients)
<b>DDNS</b>	Extension of the Domain Name Server (DNS), reachability of the VPN client under a (permanent) name in spite of changing IP address
<b>Network Protocols</b>	IP, VLAN support
<b>Multi Company Support</b>	Group capability, support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth limitation, etc.)
<b>User Administration</b>	Local user administration (up to 750 users), OPT server, RADIUS, LDP, Novell NDS, MS Active Directory Services
<b>Statistics and Logging</b>	Detailed statistics, logging functionality, sending SYSLOG messages
<b>Client/User Authentication Processes</b>	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), user name and password (XAUTH)
<b>Certificates (X.509 v.3)</b>	
<b>Server Certificates</b>	Certificates can be used that are provided via the following interfaces: PKCS#11 interface for encryption tokens (USB and smart cards); PKCS#12 interface for private keys in soft certificates
<b>Revocation Lists:</b>	Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>formerly CRL</i> ), CARL (Certification Authority Revocation List, <i>formerly ARL</i> ),
<b>Online check</b>	Automatic downloads of revocation lists from the CA at certain intervals; Online check: Checking certificates via OCSP or OCSP relative to the CA over http

IPsec VPN and SSL VPN - dial in

<b>Transmission media</b>	LAN; direct operation on the WAN: Support of max. 120 ISDN B-channels (So, S)
<b>Line management</b>	DPD with configurable time interval; Short Hold Mode; channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges)
<b>Point-to-Point protocols</b>	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
<b>Pool address management</b>	Reservation of an IP address from a pool within a defined period (lease time)
<b>Trigger call</b>	Direct dial of the distributed VPN gateway via ISDN, "knocking in the D-channel"

## IPsec VPN

<b>Virtual Private Networking</b>	IPsec (Layer 3 tunneling), RFC-conformant; MTU size fragmentation and reassembly; DPD; NAT-Traversal (NAT-T); IPsec modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS.
<b>Internet Society RFCs and Drafts</b>	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
<b>Encryption</b>	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; dynamic processes for key exchange: RSA to 4096 bits; Diffie-Hellman Groups 1,2,5,14; hash algorithm: MD5, SHA1, SHA 256, SHA 384, SHA 512
<b>VPN Path Finder</b>	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible
<b>Firewall</b>	Stateful Packet Inspection; IP-NAT (Network Address Translation); port filtering; LAN adapter protection
<b>Authentication Processes</b>	IKE (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; support of certificates in a PKI: Soft certificates, smart cards, and USB tokens: Pre-shared keys, one-time passwords, and challenge response systems; RSA SecurID ready.
<b>IP Address Allocation</b>	DHCP (Dynamic Host Control Protocol) over IPsec; DNS: Selection of the central gateway with changing public IP address by querying the IP address via a DNS server; IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP).
<b>Data Compression</b>	IPCOMP (Izs), Deflate
<b>Recommended System Requirements</b>	
<b>Computer</b>	CPU: Pentium III (or higher) 150 MHz or comparable x86 processor, 512 MB RAM (minimum), per 250 concurrently useable tunnels 64 MB RAM. Clock speed: Data throughput of app. 4,5 mbit/s can be realized for each 150 MHz with a Single Core CPU (including encryption), Data throughput of app. 9 mbit/s can be realized for each 150 MHz with a Dual/Quad Core CPU (including encryption).

## SSL VPN

<b>Protocols</b>	SSLv1, SSLv2, TLSv1 (Application Layer Tunneling)
<b>Web Proxy</b>	Access to internal web applications and Microsoft network drives via a web interface. Prerequisites for the end device: SSL-capable web browser with Java Script functionality
<b>Secure Remote File Access</b>	Upload and download, creating and deleting directories, approximately corresponds to the functionalities of the File Explorer under Windows. Prerequisites for the end device: See Web Proxy
<b>Port Forwarding</b>	Access to client/server applications (TCP/IP), Prerequisites for the end device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0) or ActiveX, SSL Thin Client for Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)
<b>PortableLAN</b>	Transparency access to corporate network Prerequisites for the end device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0) or ActiveX control, PortableLAN Client for Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)
<b>Cache Protection</b>	Required when using Internet Explorers. All transmitted data on the end device will be deleted automatically after the connection is disconnected. Prerequisites for the end device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0), SSL Thin Client for Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)

### Recommended System Requirements\*\*

Number of Concurrent Users	Computer
<b>10 Concurrent Users (CU)</b>	CPU: Intel Pentium III 700 MHz or comparable x86 processor, 512 MB RAM
<b>50 Concurrent Users</b>	CPU: Intel Pentium III 1.5 MHz or comparable x86 processor, 512 MB RAM
<b>100 Concurrent Users</b>	CPU: Intel Dual Core 1.83 GHz or comparable x86 processor, 1024 MB RAM
<b>200 Concurrent Users</b>	CPU: Intel Dual Core 2.66 GHz or comparable x86 processor, 1024 MB RAM

\*) depends on the type of end-device. Mobile end-devices like Tablet PCs (using IOS or Android), Smartphones, PDAs and others have some restrictions

\*\*\*) The specified values are approximate values that are significantly influenced by user behavior or the applications. If you anticipate many concurrent file transfers (file upload and download) then we recommend increasing the memory value cited above by a factor of 1.5.