Data Sheet

NCP Secure Enterprise VPN Server

Hybrid IPsec / SSL VPN gateway software
Universal platform for remote access to the company network

- Integrated IP routing and firewall features
- Integration of iPhone, iPad, iOS, Andoid, Windows Phone/Mobile and Blackberry
- Fallback IPsec / HTTPS (NCP VPN Path Finder Technology)
- Bandwidth management
- Network Access Control*
- FIPS inside
- Multi-tenancy
- Endpoint Security (SSL VPN)
- Easy Virtualization, perfect for Cloud VPN
- Elliptic Curve Cryptography (ECC)
- Multi Processor Support

Universality

NCP's Secure Enterprise VPN Server is a component of NCP's comprehensive VPN solution based on NCP's Next Generation Network Access Technology.

The VPN gateway integrates mobile and stationary teleworker into one cross-company data network. The software can be installed on a standard PC running on Windows or Linux and can be used as central switching and monitoring tool behind a firewall in the DMZ (Demilitarized zone) or directly on the public network (Wide Area Network) or as VM Ware.

In IPsec environments, NCP's Secure Enterprise VPN Server is compatible to VPN gateways of established third-party suppliers. It is a universal remote access platform that offers connectivity for all NCP clients and, what is more, for all third party VPN clients based on the IPsec standard.

The solution is further based on international standards and can be smoothly integrated into already existing IT infrastructure.

The modular software architecture of NCP's Secure Enterprise VPN Server offers companies a high degree of planning and investment security. It is possible to scale the number of remote users and VPN tunnels according to need.

Management/Multi-tenancy

Multi-tenancy or "multi company support", enables the concurrent use of a VPN gateway by several companies (resource sharing). Administrators of the connected companies are able to use a comfortable access management system to manage their respective NCP VPN clients*.

The NCP Secure Enterprise Server also now contains a virtual network interface adapter, which is particularly important for cloud and Software as a Service (SaaS) provider environments. It can completely seal off data communication from the gateway operator and surrounding operating systems, and better protect it by decrypting the data, automatically forwarding it into a different VPN tunnel and re-encrypting it.

In large remote access VPN networks with several VPN gateways, NCP's High Availability Services ensure high availability and consistent workload for all installed VPN gateways.

Flexible user management can be executed directly via the VPN gateway or back-end systems, such as RADIUS LDAP or MS Active Directory. Integrated IP routing and firewall functionalities ensure connectivity and security for networking a branch office for example.
Administrators configure and manage the NCP Secure Enterprise VPN Server via the NCP Secure Enterprise Management through plug-in or a web interface. The management feature serves for central control and monitoring of all VPN components. Integrated automatisms optimize performance, ensure transparency, security and economical efficiency of the VPN solution.

NCP VPN Path Finder

With its unique "NCP VPN Path Finder" NCP provides a technology that enables users to use secure remote access even behind firewalls, whose port settings generally deny IPsec communication (e.g. in hotels).

Security/Strong Authentication

The NCP Secure Enterprise VPN Server supports all standards for highly secure data transfer in all remote access environments.
The NCP server supports strong authentication features such as one-time-password-tokens (OTP), text messages (SMS) or hard and software certificates and certificates with elliptic curve cryptography. Based on revocation lists, the server verifies the validity of certificates relative to the Certification Authority offline or online at each dial-in.
The NCP Advanced Authentication integrates a Two-Factor Authentication with a One-Time Password (OTP) in the Secure Enterprise Management via SMS. Each password is created by a random number generator within the NCP Advanced Authentication Connector.

Endpoint Security and Sandbox (Network Access Control = NAC**)

The security status of mobile and stationary end-devices is verified prior to the device gaining access to the corporate network. All parameters are defined centrally and the teleworkers' access rights depend on their compliance to them.
For IPsec VPN access, the options are "disconnect" or "continue in the quarantine zone". For an SSL VPN access, authorization to certain applications will be granted on the basis of pre-defined security levels. During the SSL VPN session all data is stored in NCP's Virtual Private Desktop (Sandbox), which is a work space that is separated from the operating system. After the SSL VPN session has been terminated, the sandbox automatically deletes all data from this container.
This means, meeting the security policies is mandatory for each end-device and the user can neither avoid nor manipulate them.

IPsec and SSL

Using the NCP Secure Enterprise VPN Server, companies are able to set up data connections to their company network on the basis of a IPsec and/or SSL VPN.

With NCP's Secure Client Suite teleworkers have transparent access to all network applications and features - just like in the office. This also includes Voice over IP.

It is possible to assign an NCP Secure Client the same IP address at each connection setup. This IP address is a private IP address from the address range of the company. This enables identification of each teleworker through his IP address and simplifies remote administration and support for the user.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · 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

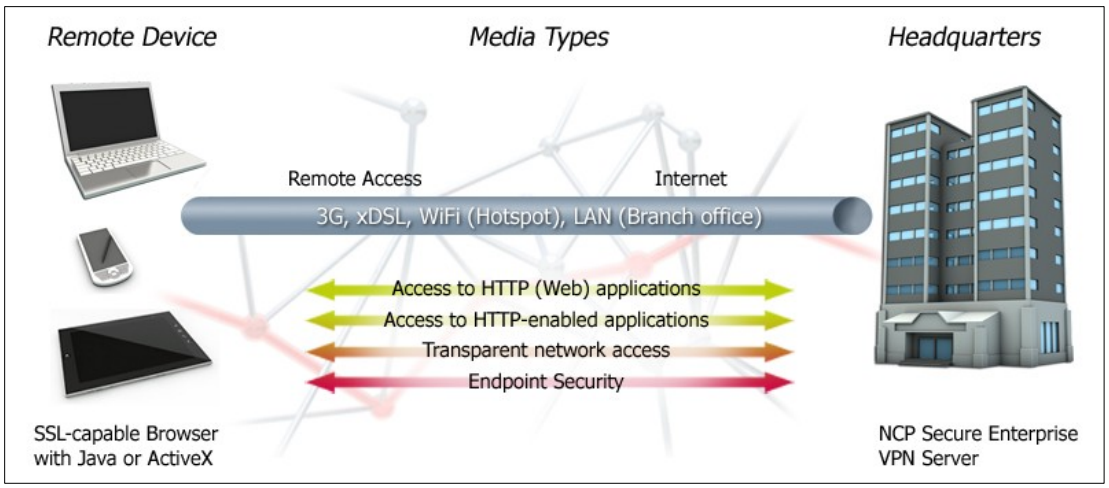
With dynamic assignment of an IP address from a pool, the system reserves the address for a certain user within a defined period (lease time). In case changing IP addresses are used, the NCP Secure Enterprise VPN Server also supports Dynamic DNS (DynDNS) for reachability of the VPN gateway.
NCP's SSL VPN solution offers the following options for access to the company network:

- **Web Proxy –** This module provides authorized users with secure access to internal web applications.
- **Port Forwarding** – The Thin Client provides access to Client-/Server Applications (TCP/IP). Connection to local client applications (http enabled) via port forwarding. The system automatically downloads the Thin Client to the end-device and is required for additional security options like cache protection, endpoint security and NCP's Virtual Private Desktop.
- **PortableLAN –** The Fat Client offers transparent network access and has to be installed on each end device.

For detailed information, please refer to the separate data sheet of the NCP SSL VPN Server.

*) Only in connection with NCP's Secure Enterprise Management

**) Network Access Control is a fixed part of NCP's SSL VPN Gateways. An IPsec VPN, however, requires the use of NCP's Secure Enterprise Management



IPsec VPN and SSL VPN – general

Operating Systems	64 bit: Windows Server 2008, Windows Server 2008 R2, Windows 2012 / 2012 R2 Linux Kernel 2.6 as of 2.6.16 (distributions on request)
Management	Administrators configure and manage NCP's Secure Enterprise VPN Server via the NCP Secure Enterprise Management through VPN Server plug-in or a web interface
Network Access Control (Endpoint Security)	Endpoint Policy Enforcement for incoming data connections. Verification of predefined, security-relevant client parameters. Measures in the event of target/actual deviations in IPsec VPN: ▪ Disconnect or continue in the quarantine zone with instructions for action (Message box) or start of external applications (e.g. virus scanner update), logging in Log files. (Please refer to the Secure Enterprise Management data sheet for more information) Measures in the event of target/ actual deviations in SSL VPN: ▪ Individual grading of access authorization to certain applications in accordance with defined security levels
Dynamic DNS (DynDNS)	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 has to support DNS resolution - as do NCP Secure Clients)
DDNS	Registration of the connected VPN clients at the Domain Name Server via DDNS, reachability of the VPN client under a (permanent) name in spite of changing IP address
Network Protocols	IP, VLAN support
Multi-Tenancy	Group capability; support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth limitation, etc.)
User Administration	Local user administration (up to 750 users); OPT server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
FIPS Inside	The IPsec client integrates cryptographic algorithms according to the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms, is certified according to FIPS 140-2 (Certificate #1051).

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · 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

	If you use one of the following algorithms for set-up and encryption of an IPsec connection, FIPS compatibility is always given: ▪ Diffie Hellman-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
IF-MAP	The overall aim of the ESUKOM Project is the design and development of a real time security solution for company networks which works on the basis of consolidating meta data. The special focus of the project is the threat resulting from mobile end-devices, e.g. smartphones. ESUKOM focuses on the integration of existing security solutions (commercial and open source) which are based on a consistent meta data format according to IF-MAP specifications of the Trusted Computing Group (TCG). The IF-MAP server of the Hannover University of Applied Science and Arts can currently be used for free-of-charge testing. The URL is: http://trust.f4.hs-hannover.de/
Client/User Authentication Processes	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), user name and password (XAUTH)

Certificates (X.509 v.3)

Server Certificates	It is possible to use certificates which 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
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL)
Online Check	Automatic downloads of revocation lists from the CA at certain intervals; Online check: Checking certificates via OCSP or OCSP over http

IPsec VPN and SSL VPN - dial-in management

Communication Media	LAN; direct operation on the WAN: Support of max. 120 ISDN B-channels (So, S2M)
Line Management	DPD with configurable time interval; Short Hold Mode; channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges)
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Pool Address Management	Reservation of an IP address from a pool within a defined period (lease time)
Trigger Call	Direct dial of the distributed VPN gateway via ISDN, "knocking in the D-channel"

IPsec VPN

Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-conformant; Automatic treatment of MTU size, fragmentation and reassembly; DPD; NAT-Traversal (NAT-T); IPsec modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (incl. MOBIKE), XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP
Encryption	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 1,2,5,14-21, 25, 26; Hash algorithm: MD5, SHA1, SHA 256, SHA 384, SHA 512
Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Port filtering; LAN adapter protection
VPN Path Finder	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500, respectively UDP encapsulation is not possible (Prerequisite: NCP Secure Enterprise VPN Server 8.0)
Seamless Roaming	With Seamless Roaming, the system automatically connects the VPN tunnel to a different Internet communication medium (LAN/ WiFi/ 3G/ 4G) without changing the IP address, so that the communication of the application through this tunnel is not interfered with and the application's session is not disconnected
Authentication Processes	IKE (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; Support of certificates in a PKI: Soft certificates, smart cards, USB tokens, certificates with ECC technology; Pre-shared keys; One-time passwords and challenge response systems; RSA SecurID ready

IP Address Allocation	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)
Data Compression	IPCOMP (lzs), Deflate
Recommended System Requirements Computer	CPU: Pentium III or higher or compatible CPU RAM: 512 MByte minimum plus 0.256 MByte per simultaneously used VPN tunnel; i.e. 64 MByte with 250 concurrently usable VPN tunnels Data Throughput (including symmetric encryption): Single Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*8.5 MBit/s. Dual Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*12.5 MBit/s. Triple Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*15.5 MBit/s. Quad Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*17.5 MBit/s. As can be seen in the approximation formula for data throughput above, a further increase in the number of CPU cores does not provide for an increase in proportion to data throughput
Recommended VPN clients / compatibility	
NCP Secure Entry Clients	Windows 32/64, Mac OS, Windows Mobile, Android
NCP Secure Enterprise Clients	Windows 32/64, Mac OS, Windows Mobile, Android, Windows CE, Linux
Third Party VPN Clients	iOS

SSL-VPN

Protocols	SSLv1, SSLv2, TLSv1 (Application Layer Tunneling)
Web Proxy	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
Secure Remote File Access*	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
Port Forwarding	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) and Linux

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · 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

Data Sheet

NCP Secure Enterprise VPN Server

NCP Virtual Private Desktop	The Virtual Private Desktop is a work space which is disconnected from the basic operating system and only temporarily available during one SSL VPN session. Any application which the user starts in this work space, is disconnected from the operating system and the virtual private desktop stores the application data in an AES-encrypted container, for example attachments to emails. After the SSL VPN session has been terminated, the sandbox automatically deletes all data from this container
Cache Protection for Internet Explorer 7, 8 and 9	All transmitted data will be automatically deleted from the end-device after disconnect. 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)
PortableLAN	Transparent access to the 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)
Single Sign-on	Single sign-on is used in all those cases in which the web server logon requires the same access data as the SSL VPN Client. It is possible to centrally manage user ID and password via Active Directory, RADIUS or LDAP. Depending on the application, you can distinguish between single sign-on with HTTP authentication (Basic (RFC2617), HTTP Digest (RFC2617) and NTLM (Microsoft)) and single sign-on according to the post-form method. Single Sign-on has been tested with Web applications like Outlook Web Access (OWA) 2003, 2007 and 2010, RDP Client and CITRIX Web interface 4.5, 5.1. Single Sign-on with Port Forwarding is only supported by applications that are able to accept parameter (like user ID and password) in their command line
Recommended System Requirements*	**1-100 Concurrent User:** CPU: Intel Dual Core 1,83 GHz or comparable x86 Processor, 1024 MB RAM **200+ Concurrent User:** CPU: Intel Dual Core 1,83 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 given values are recommended values that are strongly influenced by user attitudes / applications. If there are many simultaneous data transfers (data uploads and downloads) to calculate, we recommend raising the above given memory values by a factor of 1.5

FIPS 140-2 Inside

Next Generation Network Access Technology