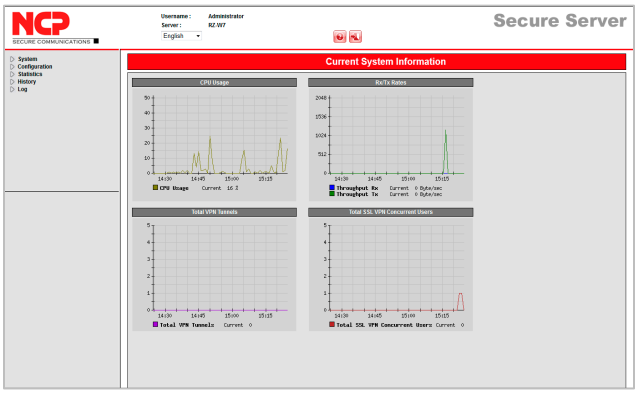
Data Sheet

NCP Secure Enterprise VPN Server

Powerful IPsec VPN gateway
Universal platform for remote access to the company network

- Highly scalable through multi-processor support
- Integrated IP routing and firewall features
- Compatible with NCP Secure VPN Clients for Windows, macOS, Linux, iOS, Android and other IPsec VPN clients
- Fallback IPsec / HTTPS (NCP VPN Path Finder Technology)
- Automatic tunnel forwarding
- FIPS inside
- Multi-tenancy
- Endpoint Policy Enforcement / Network Access Control*
- Elliptic Curve Cryptography (ECC)



Universality

NCP Secure Enterprise VPN Server integrates mobile and stationary users into one cross-company network. It can be installed on a Windows or Linux server and provides a complete remote access and management system either behind a firewall in the DMZ (Demilitarized zone), directly connected to the internet or as a virtual appliance.
In IPsec environments, NCP Secure Enterprise VPN Server is compatible with common third-party VPN gateways and can be integrated seamlessly into existing IT infrastructure. As a universal remote access platform, it offers connectivity for all NCP clients and third party VPN clients based on the IPsec standard.

The modular software architecture of NCP Secure Enterprise VPN Server offers companies a high degree of planning and investment certainty. 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 benefits service providers by allowing several companies to use a VPN gateway at the same time (resource sharing). Administrators can be assigned for each company through NCP Secure Enterprise Management Server. *

The NCP Secure Enterprise Server includes 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, the NCP High Availability Server ensures high availability and load balancing across all VPN gateways. Users can be managed flexibly via the VPN gateway or back-end systems, such as RADIUS, LDAP or MS Active Directory. Integrated IP routing and firewall features ensure connectivity and security for networking company offices.

Administrators can configure and manage NCP Virtual Secure Enterprise Server via the NCP Secure Enterprise Management Plug-in or the web interface. All VPN components can be monitored and managed centrally through the management features. Automated processes help to ensure transparency, optimize performance and security, and increase the cost-effectiveness of the VPN solution.

NCP VPN Path Finder

With its unique VPN Path Finder technology, NCP enables secure remote access even behind firewalls that are configured to block IPsec traffic (such as in hotels).

Security/Strong Authentication

The NCP Secure Enterprise VPN Server supports strong security features such as one-time-password-tokens (OTP), public key infrastructure (PKI) and certificates with elliptic curve cryptography. Each time a connection is established, certificates are validated against Certification Authority (CA) revocation lists (online or offline).

Two-factor authentication via SMS is provided via the Advanced Authentication feature. One-time passwords can be sent to users via the NCP Advanced Authentication Connector or through an SMS service provider.

Endpoint Security (Network Access Control = NAC*)

The security status of mobile and stationary end devices is verified before access is granted to the company network. The security policy parameters are managed centrally and control the level of access granted to the user. For IPsec VPN access, the options are "disconnect" or "continue in the quarantine zone".

IPsec VPN

NCP Virtual Secure Enterprise Server can handle a highly scalable number of connections to the company network via an IPsec VPN. NCP Secure Client users can be assigned the same private IP address from a pool assigned by the company each time they connect to the network. This makes remote administration much easier as each user can be identified by their IP address. If the IP address is assigned dynamically from a pool, it will be reserved for the user for a defined period (lease time). Dynamic DNS (DynDNS) ensures that the VPN Gateway is still reachable if the device is assigned a dynamic IP address.

*) Only with NCP Secure Enterprise Management

Data Sheet

NCP Secure Enterprise VPN Server

IPsec VPN – general

Operating Systems	Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 Debian, Red Hat or other Linux distributions with kernel version from 3.10, glibc from 2.17
Management	Administrators can configure and manage NCP Virtual Secure Enterprise Server via the NCP Secure Enterprise Management Plug-in or the 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 • Disconnect or continue in the quarantine zone with instructions for action (message box) or start of external applications (e.g. virus scanner update), recording events in log files. (Please refer to the Secure Enterprise Management data sheet for more information)
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. (The VPN client must support DNS resolution, this is supported by NCP Secure Clients.)
DDNS	Connected VPN clients are registered with the domain name server via Dynamic DNS (DDNS), meaning that VPN clients with dynamic IPs can be reached via a (permanent) name
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) • Alternative default certificates can be configured for other domain groups. • The Virtual Secure Enterprise VPN Server can select the most suitable certificate based on the client request (for example the certificate with the longest validity period).
User Administration	Local user administration (up to 750 users); OTP 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 based on the FIPS standard. The embedded cryptographic module containing the corresponding algorithms has been validated as conformant to FIPS 140-2 (Certificate #1747) FIPS conformance will always be maintained when the following algorithms are used for set up and encryption of a VPN connection: • Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 bits) • Hash Algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits • Encryption algorithms: AES with 128, 192 and 256 bits 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 metadata. The project focuses on threats arising from mobile end devices, such as 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 predefined intervals; Online validation of certificates via OCSP or OCSP over http

Connection Management

Line Management	Dead Peer Detection (DPD) with configurable time interval; Timeout (controlled by duration and charges)
Point-to-Point Protocols	LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool Address Management	Reservation of an IP address from a pool for a defined period of time (lease time)

IPsec VPN

Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-conformant; Automatic adjustment 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), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2 authentication conformant to RFC 7427 (padding process)
Encryption	Symmetric processes: AES (CBC/CTR/GCM) 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, 25-30; Hash algorithms: SHA-1, SHA 256, SHA 384 or SHA 512
Firewall	Stateful packet inspection; IP-NAT (Network Address Translation); Port filtering; LAN adapter protection
VPN Path Finder	NCP Path Finder Technology: Fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
Seamless Roaming	With Seamless Roaming in the NCP Secure Client, the system can automatically transfer the VPN tunnel to a different communication medium (LAN / Wi-Fi / 3G / 4G) without changing the IP address to avoid interrupting communication via the VPN tunnel or disconnecting application sessions.
Authentication Processes	IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS Support for certificates in a PKI: Soft certificates, 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 dynamic 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) Different pool can be assigned depending on the connection medium. (Client VPN IP)
Data Compression	IPCOMP (lzs), Deflate
Recommended VPN Clients / Compatibility	
NCP Secure Entry Clients	Windows 32/64, macOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux