Data Sheet

NCP Virtual Secure Enterprise VPN Server

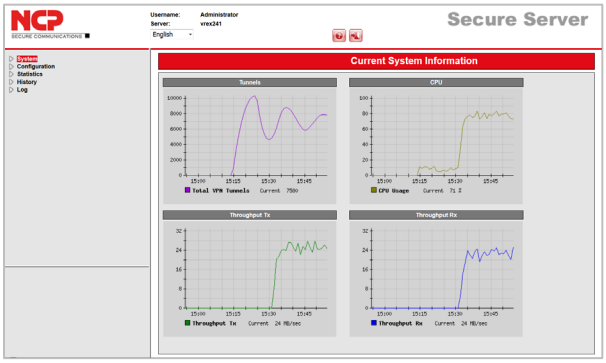
Powerful virtual IPsec VPN appliance
Universal platform for remote access to the company network

- Hardened all-in-one solution for highly secure operation
- Compatible with popular virtualization solutions
- High scalability through multi-processor/core support
- Integrated High Availability Server for operating multiple NCP Virtual Secure Enterprise VPN Servers in a load balancing or failsafe network
- Compatible with NCP Secure VPN Clients for Windows, macOS, Linux, iOS, Android and numerous other IPsec VPN clients
- VPN Path Finder technology (Fallback IPsec / HTTPS)
- Integrated IP routing and firewall features
- Bandwidth management
- FIPS Inside
- Multi-Tenancy
- Endpoint Policy Enforcement*
- Elliptic Curve Cryptography (ECC)

Universality

The NCP Virtual Secure Enterprise VPN Server is a further development of the proven NCP Secure Enterprise VPN Server which is suitable for installation in a virtual environment. The underlying Linux operating system is optimized for the application and offers maximum security thanks to various hardening measures. Administrators do not require any non-VPN expertise, as all functions of the virtual appliance are already configured.

Remote employees, branch offices and devices from IIoT environments can be integrated into a cross-company data network through the virtual appliance.



The NCP Virtual Secure Enterprise VPN Server can be easily integrated into existing IT infrastructure through standard interfaces in any remote access scenario.

Update functionality

The integrated update functionality serves both the core components NCP Secure Enterprise VPN Server and HA Server**, and the underlying operating system. Updates are released by NCP in a product-specific repository and can include security patches and feature enhancements for the overall system.
Subscription-based licensing allows users to receive all application and security updates free of charge.

Management/Multi-tenancy

Multi-tenancy or multi-company support benefits service providers by enabling the simultaneous use of a VPN gateway by several companies (resource sharing). Administrators can be assigned for each company thanks to the multi-tenancy capability of NCP Secure Enterprise Management.

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

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

User administration is managed flexibly via back-end systems such as RADIUS, LDAP, MS Active Directory or directly via the VPN gateway. Integrated IP routing and firewall features provide the necessary connectivity and security for networking a branch office for example.

Administrators configure and manage the NCP Secure Enterprise Server via the NCP Secure Enterprise Management through a plug-in or web interface. All VPN components can be monitored and managed centrally through the management feature. 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 feature, NCP enables secure remote access even behind firewalls that are configured to block IPsec traffic (such as in hotels). This switches automatically to a modified IPsec mode that uses the available HTTPS port for the VPN connection.

Security/Strong Authentication

NCP Secure Enterprise Server supports strong authentication features such as one-time-password-tokens (OTP), public key infrastructure (PKI) and certificates with elliptic curve cryptography. Certificates are validated against the Certification Authority (CA) based on revocation lists (online or offline) each time a connection is established.
NCP Advanced Authentication integrates two-factor authentication via SMS. Users can receive a one-time password via the NCP Advanced Authentication Connector or via SMS.

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 remote workers are granted access rights based on their compliance to them. For IPsec VPN access, the options are "disconnect" or "continue in the quarantine zone".

IPsec VPN

NCP Secure Enterprise Server can establish as many connections to the company network as needed via the IPsec protocol. NCP Secure Client can be assigned the same private IP address on each connection. from the address range of the company. This means that each teleworker can be identified by IP address which simplifies remote administration and support.
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) If the device is assigned a dynamic IP address, the VPN Gateway also supports Dynamic DNS (DynDNS).

*) Only in connection with NCP Secure Enterprise Management.
Connecting NCP Virtual Secure Enterprise VPN Server to NCP Secure Enterprise Management will be available from version 12.1.

**) The HA Server included in the Virtual NCP Secure Enterprise VPN Server requires a separate subscription license to operate.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

General

Virtual Appliance	Virtual appliance with hardened operating system: available as an ISO image for installation within a virtual environment e.g. VMware ESX Server, VMware Workstation (Microsoft Hyper-V for Windows Server 2017/2019 and KVM under development)
Management	Administrators configure and manage NCP Secure Enterprise VPN Server via the NCP Secure Enterprise Management through the VPN Server plug-in or a web interface
HA Server	Integration of several NCP Virtual Secure Enterprise VPN Servers in a load balancing or failsafe network
Endpoint Security* (Network Access Control)	Endpoint policy enforcement for incoming 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), 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 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 dynamic 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.) Multiple Server Certificates • Alternative certificates can be configured for other domain groups. • The Virtual Secure Enterprise VPN Server can select the most suitable certificate based on the client's request (for example the certificate with the longest validity period).
User Administration	Local user administration; OPT server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • 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

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 #1747). 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
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	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
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

Connection Management

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

IPsec VPN

Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-compliant; Automatic adjustment of MTU size, fragmentation and reassembly; DPD; NAT Traversal (NAT-T); IPsec modes: Tunnel Mode, Transport Mode Seamless Rekeying; PFS

Data Sheet

NCP Virtual Secure Enterprise VPN Server

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 according 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 IPsec/HTTPS (port 443) if port 500 is blocked or UDP encapsulation is not possible
Seamless Roaming	With Seamless Roaming, the system automatically connects the VPN tunnel to a different Internet communication medium (LAN / Wi-Fi / 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; IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS Support of 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 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) Different pool can be assigned depending on the connection medium. (Client VPN IP)
Data Compression	IPCOMP (lzs), Deflate
Recommended System Requirements / Compatibility	
NCP Secure Entry Clients	Windows 32/64, MacOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux iOS

FIPS VALIDATED 140-2

NCP PATH FINDER

Next Generation Network Access Technology