



**NCP**

SECURE COMMUNICATIONS ■

## Data Sheet

# NCP Virtual Secure Enterprise VPN Server



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

- Hardened solution for maximum security
- Compatible with major virtualization platforms
- Integrated High Availability Server for operating multiple NCP Virtual Secure Enterprise VPN Servers in a load balancing or failsafe 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 Virtual Secure Enterprise VPN Server is a NCP Secure Enterprise Server solution that can be installed in a virtual environment. It is based on a hardened Linux operating system which is optimized for maximum security. As the virtual appliance is already configured, administrators only need expert VPN knowledge.

Remote users, offices and IIoT devices can all be connected via a cross-company network managed by the NCP virtual appliance. The NCP Virtual Secure Enterprise VPN Server can be easily integrated into existing IT infrastructure in any remote access scenario through standard interfaces.

### Comprehensive updates

The update feature covers NCP Secure Enterprise VPN Server, HA Server\*\*, and the operating system. NCP releases updates including security patches and feature enhancements in a product-specific repository.



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 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. \*

In large remote access VPN networks with several VPN gateways, the NCP High Availability Server ensures high availability and load balancing across all 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). If the VPN gateway is not available, NCP VPN Path Finder switches automatically to a modified IPsec mode which establishes the VPN tunnel via the HTTPS port.

### Security/Strong Authentication

The NCP Virtual 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\*\*)

Endpoint Security or Network Access Control (NAC) checks that end devices comply with security policies before granting access to the company network. The security policy parameters are managed centrally and control the level of access granted to the user. For IPsec VPNs, the access control 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  
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.

## General

Virtual Appliance	<p>Virtual appliance with hardened operating system; available as an ISO image for installation within a virtual environment.</p> <ul style="list-style-type: none"> <li>• VMware vSphere Hypervisor (ESXi) 6.7.0</li> <li>• VMware Workstation Version 15.5</li> <li>• Microsoft Hyper-V for Windows Server 2019</li> <li>• Debian KVM version 10.6</li> </ul>
Management	The NCP Secure Enterprise Management VPN Server Plug-in or the web interface are used to configure and manage the server.
HA Server	Operation of several NCP Virtual Secure Enterprise VPN Servers in a load balancing or failsafe network
Endpoint Security* (Network Access Control)	<p>Endpoint policy enforcement for incoming connections</p> <p>Verification of predefined, security-relevant client parameters.</p> <p>Measures in the event of target/actual deviations in IPsec VPN:</p> <ul style="list-style-type: none"> <li>• 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.)</li> </ul>
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*	<p>Group capability; support of max. 1024 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth management)</p> <p>Multiple Server Certificates</p> <ul style="list-style-type: none"> <li>• Alternative default certificates can be configured for other domain groups.</li> <li>• 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)</li> </ul>
User Administration	Local user administration; 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).

	<p>FIPS conformance will always be maintained when the following algorithms are used for set up and encryption of a VPN connection:</p> <ul style="list-style-type: none"> <li>• Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 bits)</li> <li>• Hash algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits</li> <li>• Encryption algorithms: AES 128, 192 and 256 bits or Triple DES</li> </ul>
Client/User Authentication Processes	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), username and password (XAUTH)
<b>Certificates (X.509 v.3)</b>	
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 download of revocation lists from the CA at predefined intervals; Online validation of certificates via OCSP or OCSP over http
<b>Connection Management</b>	
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)
<b>IPsec VPN</b>	
Virtual Private Networking	<p>IPsec (Layer 3 tunneling), RFC-conformant;</p> <p>Automatic adjustment of MTU size, fragmentation and reassembly;</p> <p>DPD;</p> <p>NAT Traversal (NAT-T);</p> <p>IPsec modes: Tunnel Mode, Transport Mode</p> <p>Seamless Rekeying; PFS</p>
Internet Society RFCs and Drafts	<p>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)</p>
Encryption	<p>Symmetric processes: AES (CBC/CTR/GCM) 128, 192, 256 bits;</p> <p>Blowfish 128, 448 bits; Triple-DES 112, 168 bits;</p> <p>Dynamic processes for key exchange: RSA to 4096 bits;</p> <p>Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30;</p> <p>Hash algorithms: SHA-1, SHA 256, SHA 384 or SHA 512</p>
Firewall	<p>Stateful packet inspection;</p> <p>IP-NAT (Network Address Translation);</p>

	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	<p>IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS</p> <p>Support for certificates in a PKI: Soft certificates, certificates with ECC technology; Pre-shared keys;</p> <p>One-time passwords and challenge response systems; RSA SecurID ready</p>
IP Address Allocation	<p>DHCP (Dynamic Host Control Protocol) over IPsec;</p> <p>DNS: Selection of the central gateway with dynamic public IP address by querying the IP address via a DNS server;</p> <p>IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP)</p> <p>Different pool can be assigned depending on the connection medium. (Client VPN IP)</p>
Data Compression	IPCOMP (Lzs), Deflate
Installation requirements	<p>Minimum requirements for installation within a virtual environment:</p> <p>Virtual machine: Currently only available for <b>VMware vSphere Hypervisor (ESXi)</b>; Hyper V and KVM are available with the release of VSES 12.1)</p> <ul style="list-style-type: none"> <li>• BIOS (not UEFI)</li> <li>• Approximately 5 GB storage</li> <li>• Minimum 2GB RAM</li> <li>• Multiple processors for production systems</li> </ul> <p>Select "Debian 9" when creating the VM</p>
Recommended VPN Clients / NCP Secure Entry Clients NCP Secure Enterprise Clients	<p>Windows 32/64, macOS, Android</p> <p>Windows 32/64, macOS, iOS, Android, Linux</p>


**NCP PATH FINDER®**





**NCP**

SECURE COMMUNICATIONS ■

NCP engineering GmbH  
Dombuehler Str. 2  
90449 Nuremberg  
Germany

+49 911 9968 0  
[info@ncp-e.com](mailto:info@ncp-e.com)  
[www.ncp-e.com](http://www.ncp-e.com)

NCP engineering, Inc.  
19321 US Highway 19 N, Suite 401  
Clearwater, FL 33764  
USA

+1 650 316 6273  
[info@ncp-e.com](mailto:info@ncp-e.com)  
[www.ncp-e.com](http://www.ncp-e.com)