NCP
SECURE COMMUNICATIONS

Product Information

Powerful Enterprise VPN Solution and single-user Entry Clients

"BSI recommends setting up a Virtual Private Network (VPN) as the first of five simple IT security measures in the home office."
IT security in the home office in 2020, Federal Office for Information Security (BSI)

Centrally Managed Enterprise VPN

Powerful and flexible remote access infrastructure has become an important factor in ensuring business continuity, not just during the pandemic. Companies that are able to adapt to unexpected situations, via scalable infrastructure and ensuring continual secure communications, can stay on track when it counts.

From single-user licenses to connecting thousands of mobile users, NCP products offer the highest standards of IT security, proudly developed in Nuremberg, Germany. Read on to discover the potential that a centrally managed enterprise VPN can unlock in your organization.

☑ **NCP Secure Entry Clients** are designed for standalone use or smaller installations.

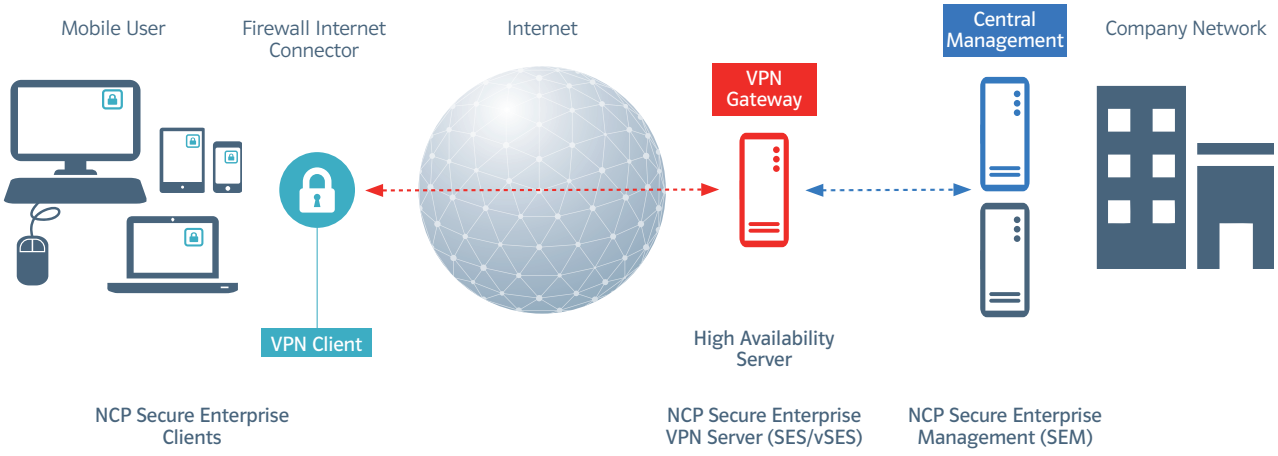
☑ **NCP Secure Enterprise VPN** is suited for larger installations and site-to-site networking (central management, VPN gateway, and enterprise VPN clients)

NCP products also provide secure communication for processing sensitive data in classified scenarios, such as VS-NfD/RESTREINT UE/EU RESTRICTED and NATO RESTRICTED, as well as secure communication for IIoT applications like remote maintenance.

NCP VPN solutions are designed to integrate seamlessly with your Zero Trust strategy and IT security systems.

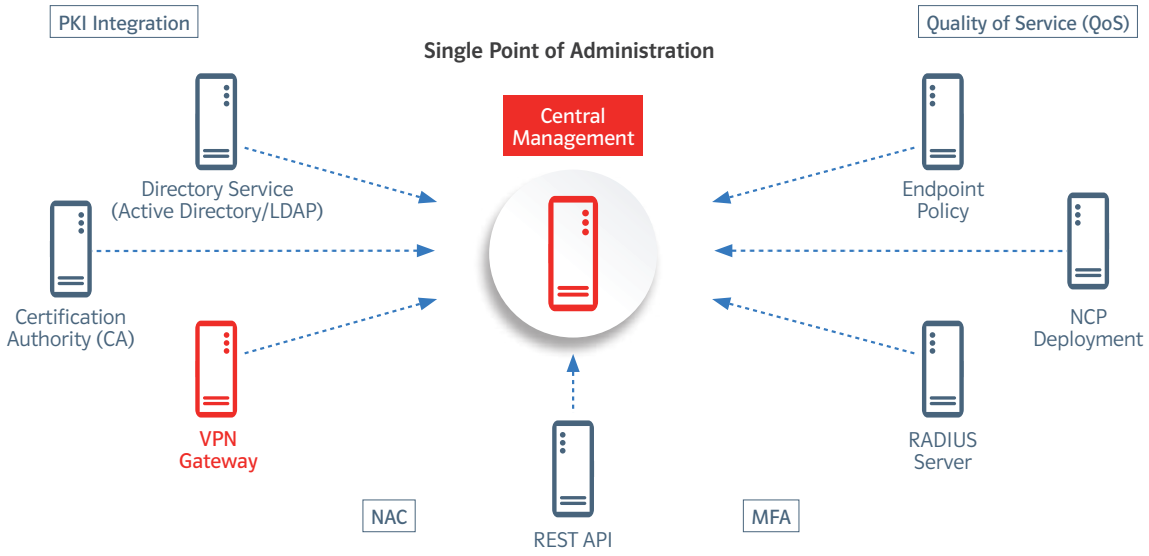
The NCP VPN solution is modular and consists of three components:

- **Centrally managed infrastructure for managing and monitoring**
- **Secure gateway (virtual appliance optional)**
- **Clients for Windows, macOS, Linux, Android and iOS**



NCP Secure Enterprise Management

With **NCP Secure Enterprise Management (SEM)**, you can manage your remote access network from a central location. This means that administrators no longer have to balance a large number of standalone solutions and consoles. SEM serves as a single point of administration, where IT administrators can make policy changes without interrupting business continuity.



Benefits of NCP Secure Enterprise Management for VPN

- Automated mass rollout
- Central client/server configuration, certificate and license management
- Automated software updates
- Integration into existing identity management systems (LDAP, Active Directory, etc.)
- Supports multitenancy and service provider infrastructure
- Comprehensive monitoring and reporting
- Integrated RADIUS server
- Advanced authentication

The Secure Enterprise Management system includes powerful features for configuring and managing VPN clients and servers from a single point of administration.

IPsec VPN Gateway Software

The **NCP Secure Enterprise VPN Server (SES)** has a modular software architecture and maximum scalability for organizations looking to adapt their remote access network and site-to-site networking based on demand.

With SES, organizations can build a powerful VPN infrastructure that grows with business demands and can flexibly adapt to changing requirements when it counts. For example, this means even from starting out with some 500 users to supporting many thousands of users later on.

Benefits of the NCP Secure Enterprise VPN Server

- Software-based with multitenancy support
- Manage more than 10,000 concurrent sessions per system
- Integrated IP routing and firewall features
- Universal software components for remote access, site-to-site networking and IIoT
- Integrated two-factor authentication + TOTP
- High availability through fail-safe mode and load balancing
- Policy changes "on the fly"
- NCP VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Network Access Control
- Endpoint security (with SEM)
- Certificate-based authentication (also for iOS devices)

The modular software architecture and maximum scalability of SES/vSES allow organizations to expand remote access and site-to-site networking on demand.

The system performance can be expanded to support more than 10,000 users and high availability systems can support a potentially unlimited number of users.

Virtual VPN Appliance

The **NCP Virtual Secure Enterprise VPN Server (vSES)** comprises the VPN server, high-availability services and a hardened operating system. Installing the appliance only requires a virtual environment.
The hardened operating system is optimized for maximum security.

Maximum scalability and a comprehensive update concept are valuable features for effective VPN management. Provided in a complete package, a VPN appliance is not only easier to manage but also cost-efficient by saving the need for developing in-house expertise.

Benefits of the vSES Appliance

- Hardened and comprehensive Linux/Debian based solution
- Compatible with common virtual environments
- Maximum scalability thanks to multiprocessor/ multi-core support
- VPN Path Finder Technology (Fallback IPsec/HTTPS)

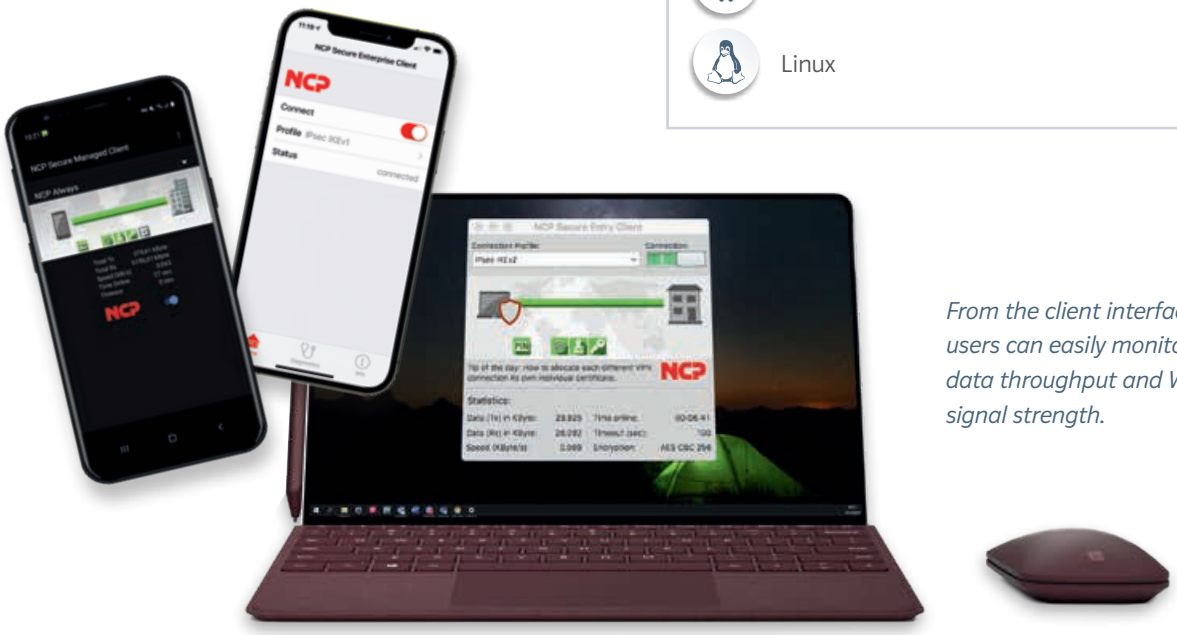
IPsec VPN Client Suite

The **NCP Secure Enterprise Clients** allow users to easily and securely connect to your network or resources, supporting all major operating systems and devices. Thanks to the SEM, IT administrators can configure and manage individual users or groups from a central point of administration, even in systems with several hundred or thousands of users.

IT administration effort is reduced significantly with the ability to manage installations and update remote users (in most cases without physical access to the devices).

NCP Enterprise Clients support the following operating systems:

- Windows 11 and 10
- macOS 12 Monterey and macOS 11 Big Sur
- iOS
- Android
- Linux



From the client interface, users can easily monitor data throughput and Wi-Fi signal strength.

A VPN client with an integrated firewall is a smart solution to many security threats.

When accessing company resources from external locations, there are many different scenarios and authentication layers: home office and other networks at customer/partner sites, public hotspots and network access from abroad, etc. NCP VPN clients master the challenges of remote access in a straightforward and secure way.

Thanks to intuitive features, the VPN client maintains secure communication seamlessly, without the user having to intervene or potentially misconfiguring the software.

- **Friendly Net Detection** – determines whether an end device is connected to a public network or a trusted network. The dynamic personal client firewall rules are adapted to the network's trust level and the VPN tunnel is established or disconnected automatically.
- **Hotspot Logon** – protects users when logging on to a hotspot provider via an unsecured Wi-Fi network.
- **Home Zone function** – the NCP client is automatically configured to allow users to access local network devices, such as a printer, but internet traffic is forwarded securely through the VPN tunnel.

IPsec VPN clients for single-user devices running Windows, macOS, or Android

NCP Secure Entry Clients are designed for standalone use or smaller installations (such as less than 100 remote employees). They enable secure communication with the company network and are available for Windows, macOS and Android.

The intuitive user interface shows the connection and security status before and during the connection. All clients are compatible with common VPN gateways (e.g. Cisco, Juniper Networks, Palo Alto, etc.) and can be easily integrated into existing network structures.

Although the entry level solution is designed for smaller installations, it has an advanced range of features. Compared to classical VPN software, NCP Secure Entry Clients benefit users with additional, practical features:

- Secure Hotspot Logon with Wi-Fi Manager
- Home Zone
- Biometric Authentication support
- Quality of Service
- and many more!

NCP Secure Entry Clients are designed for small deployments with up to 100 workstations.

NCP Secure Entry Client is unparalleled in its ease-of-use. The intuitive user interface shows the user the connection and security status before and during the connection.

Features of NCP VPN Software:

Path Finder Technology
VPN in IPsec hostile environments, e.g. hotspots or countries where internet access is restricted

Always On
Work as though you were in the office – anytime and anywhere

Seamless Roaming and Internet Connector
Automatic media detection/switching between LAN/Wi-Fi/mobile network without user interaction

Endpoint Policy Check
Validates the security status of the end device, e.g. virus scanner, OS version, domain affiliation, etc.

Quality of Service
Prioritization of bandwidth for time-critical applications, e.g. video conferencing or Skype/Microsoft Teams

Dynamic Personal Client Firewall
Integrated dynamic firewall with additional features (Friendly Net Detection, Hotspot Logon, Home Zone)

Friendly Net Detection
Automatic adaption of firewall rules in trusted networks

Hotspot Logon
Secure use of public hotspots (VPN access despite captive portal)

Home Zone
Use local network devices, such as printers, in home office while communicating with the company network exclusively via VPN tunnel.

Multitenancy
Manage multiple customers or business divisions centrally but independently of one another.

Windows Pre-logon
Login to the local Windows system *after* establishing a VPN tunnel and authenticating the user in the Windows domain via the Active Directory

NCP
SECURE COMMUNICATIONS

Do you have any questions or would you like to make an appointment for a product demonstration? Please connect with us.

The Americas

NCP engineering, Inc.

19321 US Highway N, Suite 401
Clearwater, FL 33764
USA

+1 650 316-6273

sales@ncp-e.com
www.ncp-e.com

Europe, Asia and Pacific

NCP engineering GmbH

Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968-333

sales@ncp-e.com
www.ncp-e.com

We look forward to discussing your VPN needs with you.