

NCP SSL VPN – NCP Next Generation Network Access Technology

General

These days, it is a necessity for any company or organisation to have secure access to company data and resources. Employees, business partners and customers require the ability to access the central data network from any location in order to increase productivity and flexibility.

VPN technology is the established standard for transporting and securing sensitive data in public transmission media. It depends on the relevant remote access requirements whether IPsec (Internet Protocol Security) or SSL (Secure Socket Layer) is used as tunnelling protocol.

NCP supports both processes, true to their motto "Next Generation Network Access Technology" and offers a universally applicable VPN platform for corporate networks with its Secure Enterprise Solution. Our customers especially value the ease of use and the fast return on investment (ROI).

The most important components are hybrid VPN Gateways, universal VPN Clients, High Availability Services and central management. It ensures a high transparency for communication and security with its "single point of administration and configuration" feature.

The solution

NCP's SSL VPN solution offers a vast range of coordinated function modules corresponding to the different remote access requirements.

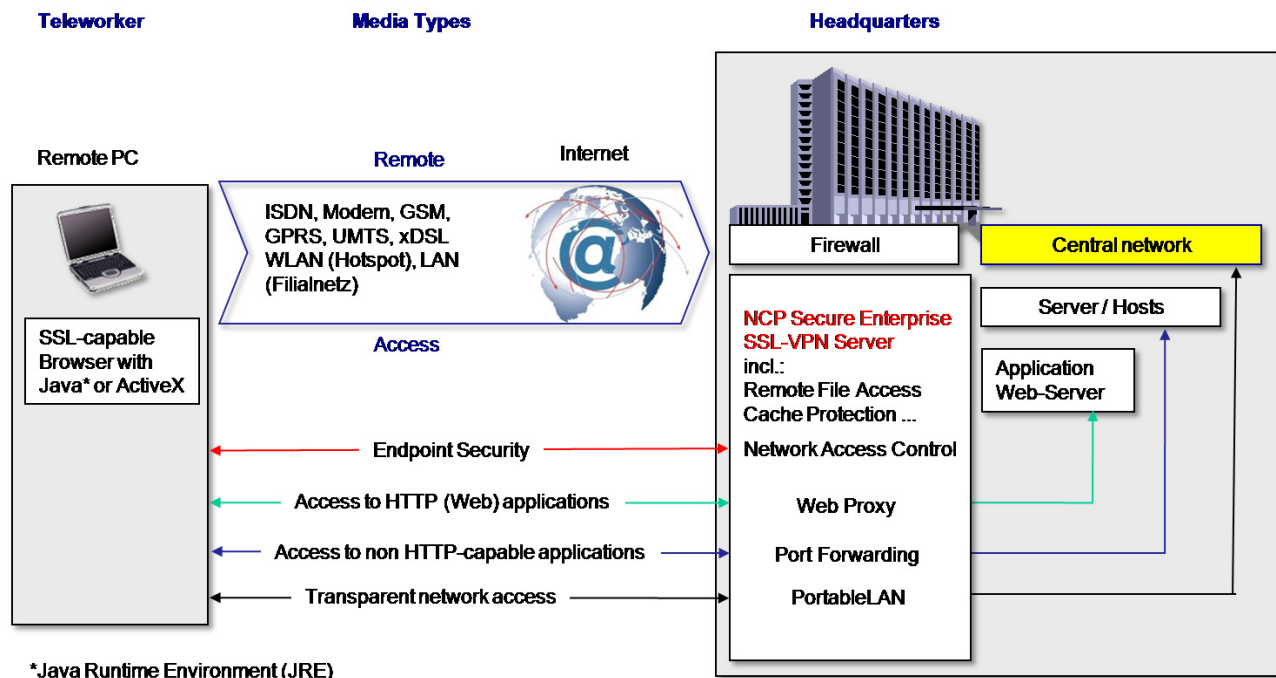


Figure: Overview of functionalities of the NCP Secure Enterprise SSL VPN Server

Overview of function modules:

Web Proxy and File Access

This module enables access to the internal web applications via http and Microsoft network directories via a web interface. The terminal only requires a standard web-browser.

The web proxy functionality allows authorised remote users to access the intranet resources via a secure SSL-tunnel.

When using remote file access, the user has similar options as with the data explorer in Windows. Files can be uploaded or downloaded and renamed. Directories can even be created or deleted.

Port Forwarding and PortableLAN

Many companies require the teleworking station to have access on a range of applications or the transparent network access onto the central LAN. An additional piece of software for the terminal is required for the necessary support of further TCP-based protocols for either remote access type. Java or ActiveX-applet are the available choices and are downloaded to the terminal automatically from the SSL VPN-Server once the connection with the company headquarters has been established.

During a session the user can simultaneously access different applications and servers such as Client/Server and Legacy-application on the central Windows, UNIX/Linux-, Mainframe or AS/400 in the scenario of port forwarding.

NCP PortableLAN is used if a teleworking station shall have transparent access to all applications and resources in the company network similar to an IPsec VPN.

All SSL function modules are included in the standard package of the NCP Secure Enterprise SSL VPN Server. The customer only has to give a number of users who may simultaneously access the VPN Gateway or company network (concurrent user).

Option: Upgrade to IPsec VPN.

The security

Security and access control are of central importance for remote access. It has to be sustainably prevented that data is intercepted, deleted or manipulated during transmission and that unauthorized third parties access the company network. In addition to an efficient data encryption it also concerns safeguarding the terminal. Strong user-authentication in combination with integrated network access control ensure this security. NCP Security Management offers all security precautions which also reliably protect fixed as well as mobile teleworking stations according to the company policy.

Strong authentication

All users have to be authenticated reliably during external access onto the company network. User-ID and password is not sufficient. The danger that a user saves this information in a web configuration on the temporary workstation is too big as well as the danger persists that he is spied on and hence third parties may gain unauthorised access. NCP Secure Communications solution therefore supports a strong authentication via one-time-password tokens (OTP) or certificates.

Network Access Control (NAC)

All terminals are checked on their current security status prior to accessing the company network. As per the centrally defined security level, a security level is assigned during each connection establishment to the company network. As per these results, the teleworker's access rights are assigned.

The NAC function module is a fix component of the NCP Secure Enterprise Server and can be used in connection with the Port Forwarding and PortableLAN function modules.

Adherence to security directives is compulsory and may not be manipulated or avoided by the user.

The following parameters can be checked:

- Operating system information (type and version, service pack, hotfixes)
- Services information (installed, started, stopped)

- File information (date, file version, MD5-Hash)
- Status of the virus scanner (manufacturer, version, up-to-date)
- Contents of certain registry values

Cache Protection

This function module protects the transmitted data on the remote terminal against theft. All web-pages viewed in the company network are automatically deleted from the cache after the connection is stopped.

Recommended use

Whichever VPN technology should be used for the secure external data communication is no longer influenced by the argument of "complexity". Users do not require technical background knowledge and administrators gain the required network transparency via the central management services.

The most important decisive criteria are the user scenarios, i.e. the answer to these questions:

- Shall the access be to the overall network or only onto a certain application?
- Which terminals and transmission media are used?
- What does the remote access environment look like? Are the terminals controllable by the company ("trusted") or not ("untrusted")?

IPsec VPN

IPsec VPNs (Network Layer VPNs) are an established component for external company communication via the internet. They allow the teleworker permanent access ("always-on") onto the company network and increase their productivity drastically due to the underlying Client/Server architecture. The central LAN (ethernet) is "expanded far beyond the company borders" and allows a complete integration of employees into the business processes – at any time and anywhere. Main characteristics are the high performance and the redundant connectivity. This applies both to the transmission paths as well as the central VPN-Gateway.

Cost-intensive adjustments of applications become redundant. A central management ensures the reliable and economic operation of the VPN. Existing Active Directory, RADIUS, LDAP-Server, CAs (Certification Authority) and other databases can be easily integrated into the overall solution.

SSL VPN

The use of SSL VPN technology is the solution for any scenario, where no broad access is required or desired onto the company network, or if the installation of a VPN Client software on the teleworking station is not possible. SSL VPNs offer an alternative to access certain central applications and resources from an untrusted network.

Here are some examples:

- Connection of external partner to the company network. The use of an IPsec solution is in this scenario often not an option.
- Sporadic remote access via "unknown computer" to the company network.
- It is not desired that e.g. business partners or customers have transparent access onto the company network.
- Employees only have to access emails, individual documents on the intranet or only use certain applications.
- Alternative access, if e.g. the customer's company policy does not allow IPsec.

IPsec and SSL do not exclude each other. Most companies use both VPN protocols in parallel. NCP offers a hybrid VPN Client for users in an IPsec VPN, which can also communicate in environments which have no release for a Layer 2 based VPN, but only via the standard internet access (http/https). A special protocol procedure ensures that the software adjusts itself automatically to the current remote access environment and that the establishment of a data connection to the company network is possible.

Technical Reference

Software requirements for the teleworking station when using:

- Web Proxy / Remote File Access
Standard Web-browser with SSL/TLS- and Java Script-compatibility
- Port Forwarding
Web-browser with SSL/TLS- and Java Script-compatibility
Java Runtime Environment (>= V.5.0) or ActiveX
NCP SSL Thin Client (Windows XP and Vista 32/64, Linux)
- Endpoint Security
Web-browser with SSL/TLS- and Java Script-compatibility
Java Runtime Environment (>= V.5.0) or ActiveX Control
NCP SSL Thin Client (Windows XP and Vista 32/64, Linux)
- PortableLAN
Web-browser with SSL/TLS- and Java Script-compatibility
Java Runtime Environment (>= V.5.0) or ActiveX Control
NCP PortableLAN-Client (Windows XP and Vista 32/64)
- Cache Protection for Internet Explorer V.6,7 and 8
Web-browser with SSL/TLS- and Java Script-compatibility
Java Runtime Environment (>= V.5.0)
NCP SSL Thin Client (Windows XP and Vista 32/64)

Recommended system requirements:

Number of users (Concurrent Users)	CPU / Clock Timing	Main Storage
10	Intel Pentium III 700 MHz or comparable x86 Processor	512 MB
50	Intel Pentium IV 1.5 GHz or comparable x86 Processor	512 MB
100	Intel Dual Core 1.83 GHz or comparable x86 Processor	1024 MB
200	Intel Dual Core 2.66 GHz or comparable x86 Processor	1024 MB

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 storage values by a factor of 1.5.