

## NCP Secure Enterprise SSL- VPN

### Die Lösung

Unter dem Anspruch „Secure Communications“ bietet NCP mit der Secure Enterprise Solution eine ganzheitliche VPN-Softwarelösung mit zentralem Management. Teleworker werden in die Lage versetzt, von beliebigen Standorten auf einfache Weise auf das Firmennetz zuzugreifen. Das zentrale Management bietet als „Single Point of Administration“ die erforderliche Transparenz für Netzwerkadministratoren und Endpoint Policy Enforcement.

Die Sicherheit der zu übertragenden Daten und des Firmennetzes garantieren integrierte, ausschließlich auf Standards basierende Sicherheitsmechanismen, für Firewalling, Datenverschlüsselung und starke User-Authentisierung. Als VPN-Technologien werden sowohl IPSec (Internet Protocol Security) als auch SSL (Secure Socket Layer) unterstützt. Die folgenden Ausführungen beschäftigen sich mit der SSL-VPN-Lösung, wobei auch Einsatzempfehlungen gegenüber einem IPSec-VPN gegeben werden.

### Die Kommunikation

Die SSL-VPN-Lösung von NCP ist modular strukturiert. In Abhängigkeit von den Zugriffsoptionen bietet der SSL-VPN-Server verschiedene Funktionsmodule:

#### Web Proxy und Remote File Access

Diese Funktionalitäten sind standardmäßig im NCP Secure Enterprise SSL-VPN-Server enthalten. Sie ermöglichen den Zugriff auf interne Web-Anwendungen und Microsoft Netzwerklaufwerke über ein Web-Interface. Das Endgerät muss hierzu lediglich über einen SSL-fähigen Web-Browser und Java Script-Fähigkeit verfügen.

Die Web Proxy-Funktionalität ermöglicht autorisierten remote Usern, über einen SSL-Tunnel gesichert auf Intranetressourcen zuzugreifen.

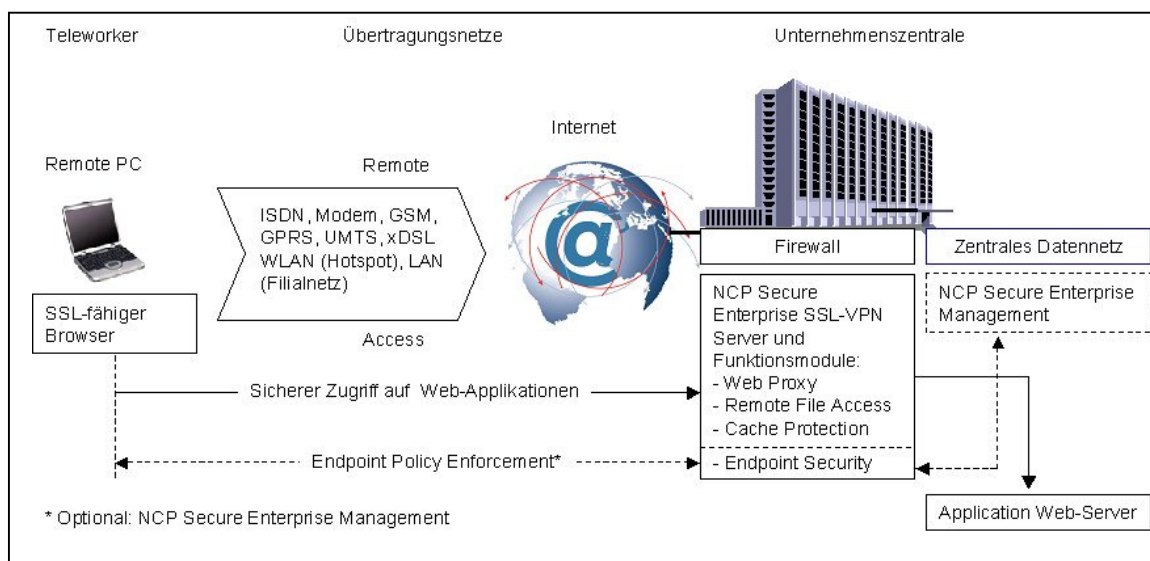


Abbildung 1 Client-loser Zugriff auf Web-Applikationen

Mit Remote File Access hat der Anwender ähnliche Möglichkeiten wie mit dem Datei-Explorer unter Windows. Es können Dateien up- und downgeload oder umbenannt werden. Auch das Erstellen oder Löschen von Verzeichnissen ist möglich.

Port Forwarding

Dieses Funktionsmodul wird dann benötigt, wenn Client-/Server-Anwendungen auf Basis des TCP/IP-Protokolls genutzt werden sollen. Hierfür ist am Telearbeitsplatz ein Hilfsprogramme erforderlich. Dieses wird mit Hilfe der Java Runtime Environment (JRE), nach dem Verbindungsaufbau zur Firmenzentrale automatisch vom SSL-VPN-Server auf das Endgerät heruntergeladen. Dieser SSL-Thin-Client ermöglicht, dass während einer Session auf verschiedene Applikationen und Server gleichzeitig zugegriffen werden kann. Hier einige Beispiele: E-Mail Clients wie Outlook (Express) oder Thunderbird, Legacy-Anwendungen auf zentralen Windows-, UNIX/Linux-, Mainframe oder AS/400-Hosts.

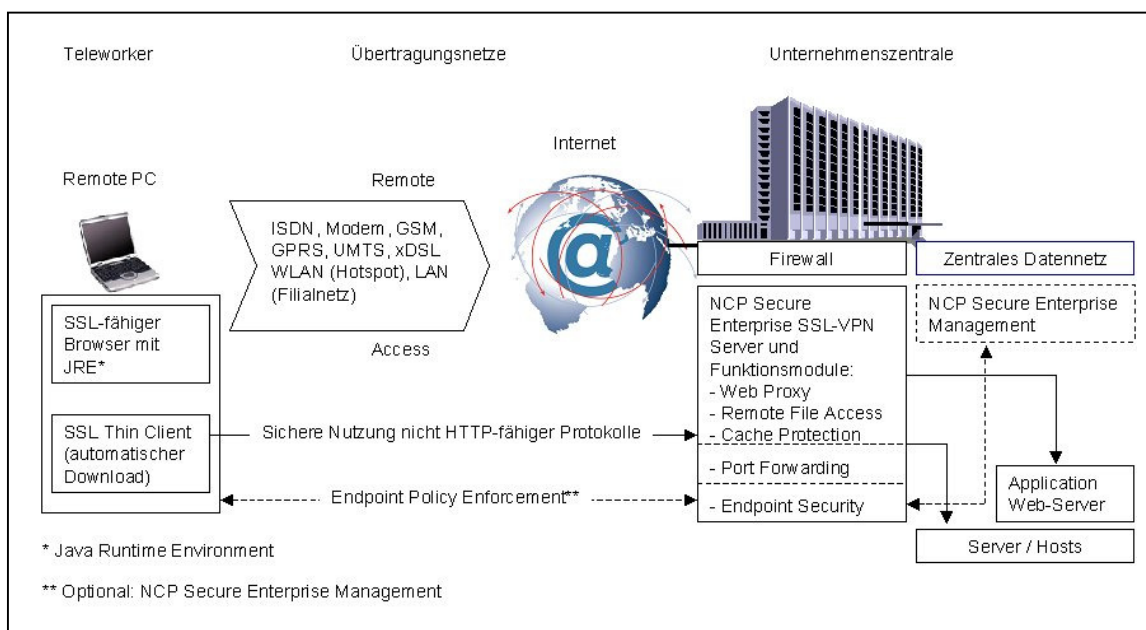


Abbildung 2 Zugriff auf Anwendungen, die auf dem TCP/IP Protokoll basieren (mittels NCP SSL-Thin-Client)

**Die Sicherheit**

Im SSL-VPN werden grundsätzlich alle Anwendungsdaten durch die verschlüsselte Datenverbindungstrecke getunnelt. Wie ist es aber um die Sicherheit des jeweiligen Arbeitsplatzes gegen Ausspähen und sonstigen Attacken bestellt? Wie kann garantiert werden, dass auch in diesem höchst unsicheren Remote Access-Umfeld die Security Policy eines Unternehmens eingehalten wird?

Endpoint Security

NCP bietet mit Secure Enterprise Communication eine umfassende Endpoint-Security-Lösung. Alle Endgeräte werden vor deren Zugriff auf das Firmennetz auf ihren aktuellen Sicherheitszustand hin überprüft. Entsprechend der zentral definierten Sicherheitslevel erfolgt bei jedem Verbindungsaufbau zum Firmennetz eine Sicherheitseinstufung. Abhängig davon wird der Teleworker berechtigt, auf bestimmte Applikationen zuzugreifen.

Für die Umsetzung der Endpoint-Security ist zusätzlich das NCP Secure Enterprise Management erforderlich. Mit Hilfe des Plug-In „Endpoint Policy Enforcement“ werden die Policies erstellt und an den NCP SSL-VPN-Server übertragen. Zwischen diesem und dem NCP SSL Thin Client erfolgt letztlich die Aushandlung des Sicherheitslevels.

Die Einhaltung der vorgegebenen Sicherheitsrichtlinien ist zwingend und vom Anwender nicht umgeh- bzw. manipulierbar.

Folgende Client-Parameter können verifiziert werden:

- Betriebssystem-Informationen (Art und Version, Service Pack, Hotfixes)
- Dienste-Informationen (installiert, gestartet, gestoppt)
- Datei-Informationen (Datum, Dateiversion, MD5-Hash)
- Status eines Virens scanners (Hersteller, Version, etc)
- Inhalte bestimmter Registry-Werte
- Informationen der Cisco NAC Schnittstelle
- Informationen des Microsoft Security Centers

### Starke Authentisierung

Beim externen Zugriff auf das Firmennetz müssen die zugreifenden Personen zuverlässig authentisiert werden. User-ID und Passwort sind oft nicht ausreichend. Zu groß ist die Gefahr, dass ein Nutzer diese innerhalb einer Web-Konfiguration am temporären Arbeitsplatz abspeichert oder ausgespäht werden und damit unberechtigte Zugriffe durch Dritte ermöglicht. Das NCP Security Management bietet auch unter SSL eine starke Authentisierung mittels Einmalpasswort-Tokens (OTP) oder Zertifikaten.

### Cache Protection

Dieses Funktionsmodul ist im Standardlieferungsumfang des NCP Secure Enterprise SSL-VPN-Servers enthalten. Bei Verwendung des Internet Explorers schützt es die übertragenen Daten auf dem Endgerät vor Diebstahl. Alle heruntergeladenen Web-Seiten aus dem Unternehmensnetz werden nach dem Verbindungsabbau automatisch gelöscht. Bei Firefox und Netscape ist dieses Feature nicht erforderlich, da HTML-Seiten, die mit SSL/TLS übertragen werden, nicht selbsttätig am Tele-arbeitsplatz abgespeichert werden.

### **Einsatzempfehlungen für SSL- und IPSec-VPN**

**IPSec-VPNs** sind heute eine feste Größe bei der Planung und Umsetzung einer sicheren Unternehmenskommunikation in einem Intranet. Sie gestatten aufgrund der Client-/Serverstruktur eine „Erweiterung des LANs über die Firmengrenze hinaus“. Der transparente Netzwerkzugang gestattet die Nutzung aller Applikationen (auch VoIP) ohne spezielle Anpassungen - auf höchstem Sicherheitsniveau. Ein zentrales Management sorgt für den zuverlässigen Betrieb eines VPNs und die erforderliche Netzwerktransparenz.

Ein **SSL-VPN** bietet sich immer dann an, wenn folgende Anforderungsprofile gegeben sind:

- Anbindung externer Partner an das Firmennetz. Hier besteht oft nicht die Möglichkeit, den Einsatz einer IPSec-Lösung durchzusetzen.
- Sporadischer Remote Access über „Fremdrechner“ auf das Firmennetz
- Kein transparenter Zugriff auf das Firmennetz für Mitarbeiter wie am Büroarbeitsplatz, d.h. Nutzung einzelner Applikationen
- Alternativer Zugang, wenn z.B. die Firmen Policy des Kunden IPSec verbietet.

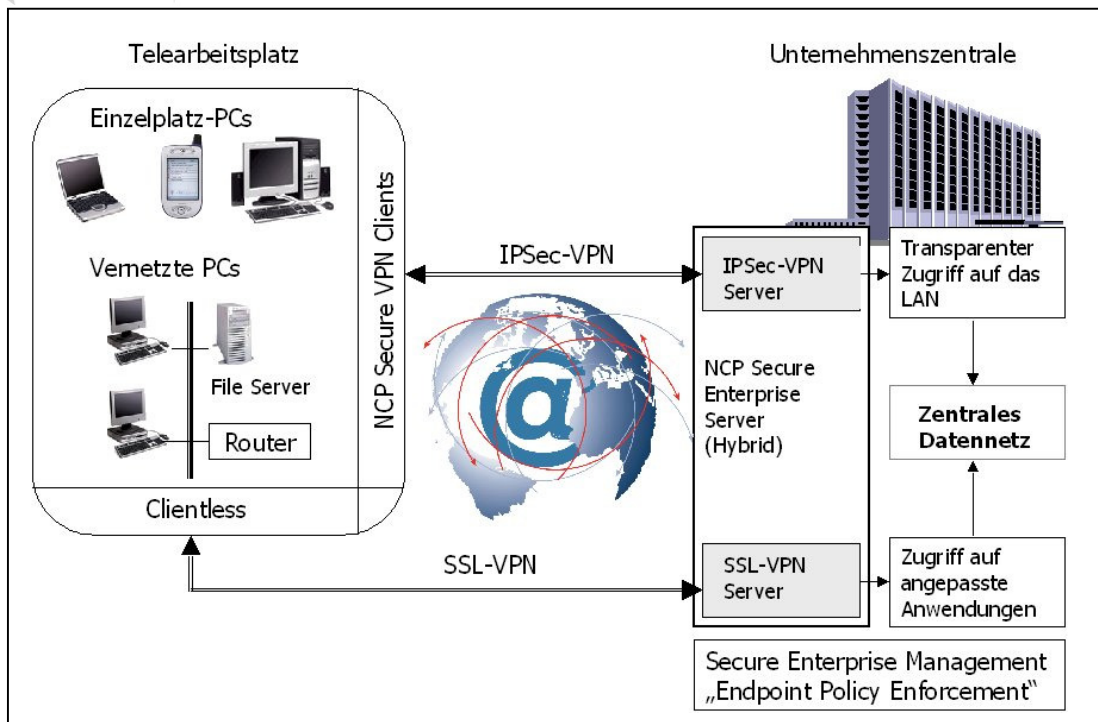


Abbildung 3 NCP Secure Communications – Hybrider Secure Enterprise Server

## Technische Hinweise

### Software-Anforderungen an den Telearbeitsplatz bei Nutzung von:

- Web Proxy / Remote File Access  
Web-Browser mit SSL/TLS- und Java Script-Fähigkeit
- Port Forwarding  
Web Browser mit SSL/TLS- und Java Script-Fähigkeit  
Java Runtime Environment (>= V.5.0)  
NCP SSL-Thin Client (Win 32 und Linux)
- Endpoint Security  
Web Browser mit SSL/TLS- und Java Script-Fähigkeit  
Java Runtime Environment (>= V.5.0)  
NCP SSL-Thin-Client (Win 32 und Linux)
- Cache Protection für Internet Explorer V.5, 6 und 7  
Web Browser mit SSL/TLS- und Java Script-Fähigkeit  
Java Runtime Environment (>= V.5.0)  
NCP SSL-Thin-Client (Win 32 )

Getestete Web Browser: Internet Explorer V.5, 6 und 7; Firefox; Netscape.

Empfohlene Systemvoraussetzungen:

Anzahl der Benutzer (Concurrent User)	CPU / Taktung	Arbeitsspeicher
10	Intel Pentium III 700 MHz oder vergleichbarer x86 Prozessor	512 MB
50	Intel Pentium IV 1,5 GHz oder vergleichbarer x86 Prozessor	512 MB
100	Intel Dual Core 1,83 GHz oder vergleichbarer x86 Prozessor	1024 MB
200*	Intel Dual Core 2,66 GHz oder vergleichbarer x86 Prozessor	1024 MB

\*) Empfehlung: max. 200 CUs pro Server

Die angegebenen Werte sind Richtgrößen, die stark vom Benutzerverhalten bzw. den Anwendungen beeinflusst werden.

Wenn mit vielen gleichzeitigen Dateitransfers (Datei Up- und Download) zu rechnen ist, empfehlen wir den oben angegebenen Speicherwert um den Faktor 1,5 zu erhöhen.