

NCP SSL VPN – NCP Next Generation Network Access Technology

Allgemeines

Der sichere Zugriff auf Unternehmensdaten und –ressourcen ist heute eine Notwendigkeit für Unternehmen und Organisationen. Um die Produktivität und Flexibilität zu steigern, müssen Mitarbeiter, Geschäftspartner und Kunden die Möglichkeit haben, jederzeit von beliebigen Standorten auf das zentrale Datennetz zuzugreifen.

Etablierter Standard für den Transport und Schutz sensibler Daten in öffentlichen Übertragungsmedien ist die VPN-Technologie. Welches Tunneling-Protokoll zum Einsatz kommt - IPsec (Internet Protocol Security) oder SSL (Secure Socket Layer) - hängt von den jeweiligen Remote Access-Anforderungen ab.

Unter dem Anspruch „Next Generation Network Access Technology“ unterstützt NCP beide Verfahren und bietet mit der Secure Enterprise Solution eine universell einsetzbare VPN-Plattform für Corporate Networks. Unsere Kunden schätzen besonders die einfache Nutzung und den schnellen Return on Investment (ROI).

Die wichtigsten Bausteine sind neben dem hybriden VPN Gateway, universelle VPN Clients, High Availability Services und ein zentrales Management. Als „Single Point of Administration and Configuration“ sorgt es für eine hohe kommunikations- und sicherheitstechnische Transparenz.

Die Lösung

Den unterschiedlichen Remote Access-Anforderungen entsprechend bietet die NCP SSL VPN-Lösung ein breites Spektrum aufeinander abgestimmter Funktionsmodule.

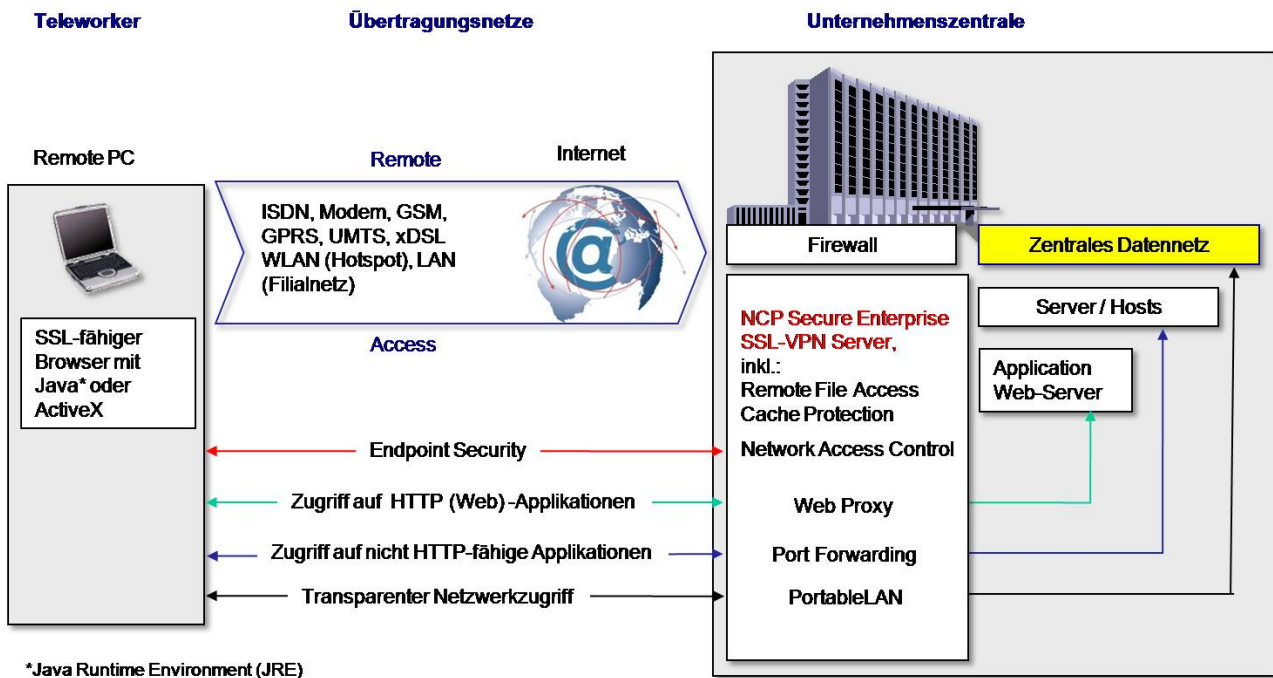


Abb. Übersicht der Funktionalitäten des NCP Secure Enterprise SSL VPN Server

Die Funktionsmodule im Überblick:

Web Proxy und File Access

Dieses Modul ermöglicht den Zugriff auf interne Web-Anwendungen via https und Microsoft Netzwerklaufrer über ein Web-Interface. Das Endgerät muss hierfür lediglich über einen Standard Webbrowser verfügen.

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

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

Port Forwarding und PortableLAN

Viele Unternehmen benötigen am Telearbeitsplatz den Zugriff auf eine Vielzahl von Anwendungen bzw. den transparenten Netzwerkzugriff auf das zentrale LAN. Für die erforderliche Unterstützung weiterer TCP-basierte Protokolle wird in beiden Remote Access Varianten eine zusätzliche Software am Endgerät benötigt. Diese steht wahlweise als Java oder ActiveX-Applet zur Verfügung und wird nach dem Verbindungsaufbau zur Firmenzentrale automatisch vom SSL VPN-Server auf das Endgerät heruntergeladen.

Im Falle des Port Forwarding kann der User während einer Session gleichzeitig auf verschiedene Applikationen und Server wie beispielsweise Client/Server- und Legacy-Applikationen auf zentralen Windows-, UNIX/Linux-, Mainframe oder AS/400-Hosts zugreifen.

Soll von einem Telearbeitsplatz aus ähnlich einem IPsec VPN, transparent auf alle Applikationen und Ressourcen im Firmennetz zugegriffen werden, kommt NCP PortableLAN zum Einsatz.

Alle SSL-Funktionsmodule sind im Standardlieferungsumfang des NCP Secure Enterprise SSL VPN Servers enthalten. Der Kunde muss lediglich die Anzahl der User festlegen, die gleichzeitig auf das VPN Gateway bzw. Firmennetz zugreifen können (Concurrent User).

Option: Upgrade auf IPsec VPN.

Die Sicherheit

Sicherheit und Zugriffskontrolle sind bei Remote Access von zentraler Bedeutung. Es muss nachhaltig verhindert werden, dass Daten während der Übertragung abgehört, gelöscht oder manipuliert werden und unberechtigte Dritte auf das Firmennetz zugreifen. Neben einer leistungsfähigen Datenverschlüsselung geht es um die Abschottung des Endgerätes. Das bewirkt eine starke User-Authentisierung in Verbindung mit einer umfassenden Netzwerkzugriffskontrolle. Das NCP Security Management bietet alle Sicherheitsvorkehrungen, die entsprechend der Unternehmens-Policy sowohl stationäre als auch mobile Telearbeitsplätze zuverlässig schützt.

Starke Authentisierung

Beim externen Zugriff auf das Firmennetz müssen alle User zuverlässig authentisiert werden. User-ID und Passwort sind nicht ausreichend. Zu groß ist die Gefahr, dass ein Nutzer diese innerhalb einer Web-Konfiguration am temporären Arbeitsplatz abspeichert oder er ausgespäht wird und damit unberechtigte Zugriffe durch Dritte ermöglicht werden. Die NCP Secure Communications-Lösung unterstützt deshalb eine starke Authentisierung mittels Einmalpasswort-Tokens (OTP) oder Zertifikaten.

Network Access Control (NAC)

Alle Endgeräte werden vor dem Zugriff auf das Firmennetz auf den aktuellen Sicherheitszustand hin überprüft. Entsprechend zentral definierter Sicherheitslevels erfolgt bei jedem Verbindungsaufbau zum Firmennetz eine Sicherheitseinstufung. Abhängig davon wird die Zugriffsberechtigung des Teleworkers festgelegt.

Das NAC-Funktionsmodul ist fester Bestandteil des NCP Secure Enterprise Server und kann Verbindung mit den Funktionsmodulen Port Forwarding und PortableLAN genutzt werden.

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

Folgende Parameter können überprüft werden:

- Betriebssystem-Informationen (Art und Version, Service Pack, Hotfixes)
- Dienste-Informationen (installiert, gestartet, gestoppt)
- Datei-Informationen (Datum, Dateiversion, MD5-Hash)
- Status eines Virenschanners (Hersteller, Version, up-to-date)
- Inhalte bestimmter Registry-Werte

Cache Protection

Dieses Funktionsmodul schützt die übertragenen Daten auf dem entfernten Endgerät vor Diebstahl. Alle betrachteten Web-Seiten aus dem Unternehmensnetz werden nach dem Verbindungsabbau automatisch aus dem Cache gelöscht.

Einsatzempfehlungen

Welche VPN-Technologie für die sichere, externe Datenkommunikation genutzt werden soll, wird bei der NCP-Lösung nicht mehr von dem Argument „Komplexität“ beeinflusst. Anwender müssen über kein technisches Hintergrundwissen verfügen und Administratoren erhalten über zentrale Managementservices die erforderliche Netzwerktransparenz.

Wichtigste Entscheidungskriterien sind die Nutzungsszenarien, also die Beantwortung der Fragen:

- Soll der Zugriff auf das gesamte Netzwerk oder nur auf bestimmte Applikationen erfolgen?
- Welche Endgeräte und Übertragungsmedien werden genutzt?
- Wie sieht die Remote Access-Umgebung aus? Sind die Endpunkte vom Unternehmen kontrollierbar („trusted“) oder nicht („untrusted“)?

IPsec VPN

IPsec VPNs (Network Layer VPNs) sind in der externen Unternehmenskommunikation via Internet eine feste Größe. Sie ermöglichen den Teleworkern aufgrund der Client-/Serverarchitektur den permanenten Zugriff („Always-On“) auf das Firmennetz und erhöht deren Produktivität erheblich. Das zentrale LAN (Ethernet) wird „über die Firmengrenze hinaus erweitert“ und bedingt eine vollständige Integration von Mitarbeitern in die Geschäftsprozesse – zu jeder Zeit und überall. Wesentliche Eigenschaften sind die hohe Performance und redundante Konnektivität. Das betrifft sowohl die Übertragungswege als auch zentralen VPN-Gateways.

Kostenintensive Anpassungen von Applikationen entfallen. Ein zentrales Management sorgt für den zuverlässigen und wirtschaftlichen Betrieb des VPN. Bestehende Active Directory-, RADIUS-, LDAP-Server, CAs (Certification Authority) und sonstige Datenbanken können auf einfache Weise in die ganzheitliche Lösung integriert werden.

SSL VPN

In allen Fällen, wo kein umfassender Zugriff auf das Firmennetz erforderlich bzw. gewünscht ist, oder die Installation einer VPN Client-Software auf dem Telearbeitsplatz nicht möglich ist, bietet sich die Nutzung von SSL VPN-Technologie an. SSL VPNs bieten eine alternative Methode, um von einem untrusted Netzwerk aus auf bestimmte zentrale Applikationen und Ressourcen zuzugreifen.

Hier einige Beispiele:

- 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
- Es ist kein transparenter Zugriff auf das Firmennetz z.B. von Geschäftspartnern und Kunden gewünscht
- Mitarbeiter sollen nur E-Mails abrufen, auf einzelne Dokumente vom Intranet zugreifen oder nur bestimmte Applikationen nutzen.
- Alternativer Zugang, wenn z.B. die Company Policy des Kunden IPsec verbietet.

IPsec und SSL schließen sich nicht aus. In den meisten Unternehmen werden beide VPN-Protokolle parallel genutzt. Für Anwender in einem IPsec VPN, die auch in Umgebungen kommunizieren sollen, in denen kein Layer2 basiertes VPN freigegeben ist, sondern nur der übliche Internetzugriff (http/https), bietet NCP einen hybriden VPN Client. Ein spezielles Protokollverfahren bewirkt, dass sich die Software automatisch an die aktuelle Remote Access-Umgebung anpasst und den Aufbau einer Datenverbindung zum Firmennetz ermöglicht.

Technische Hinweise

Software-Anforderungen an den Telearbeitsplatz bei Nutzung von:

- Web Proxy / Remote File Access
Standard Webbrowser mit SSL/TLS- und Java Script-Fähigkeit
- Port Forwarding
Web Browser mit SSL/TLS- und Java Script-Fähigkeit
Java Runtime Environment (>= V.5.0) oder ActiveX
NCP SSL Thin Client (Windows XP und Vista 32/64, Linux)
- Endpoint Security
Web Browser mit SSL/TLS- und Java Script-Fähigkeit
Java Runtime Environment (>= V.5.0) oder ActiveX Control
NCP SSL Thin Client (Windows XP und Vista 32/64, Linux)
- PortableLAN
Web Browser mit SSL/TLS- und Java Script-Fähigkeit
Java Runtime Environment (>= V.5.0) oder ActiveX Control
NCP PortableLAN-Client (Windows XP und Vista 32/64)
- Cache Protection für Internet Explorer V.6,7 und 8
Web Browser mit SSL/TLS- und Java Script-Fähigkeit
Java Runtime Environment (>= V.5.0)
NCP SSL Thin Client (Windows XP und Vista 32/64)

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

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.