Produktinformationen zu
NCP Secure Enterprise-VPN-Server

IT-Services & Solutions
- IT-Dienstleistungen
- IT-Lösungen

... seit 1994

WIUME Ingenieur-Büro

72766 Reutlingen • Birnenweg 15
Tel.: 07121/14474-0 • Fax: 07121/14474-29
www.itdienste.net • info@itdienste.net

NCP SECURE COMMUNICATIONS

Datenblatt

NCP Secure Enterprise VPN Server

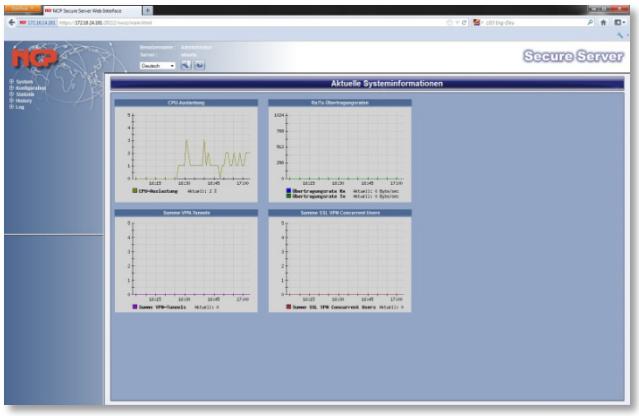
SECURE COMMUNICATIONS

Next Generation Network Access Technology

Hybride IPsec / SSL VPN Gateway Software
Universelle Plattform für den Fernzugriff auf das Firmennetz

- **Integrierte IP-Routing- und Firewall-Funktionalitäten**
- **Fallback IPsec / HTTPS (NCP VPN Path Finder Technology)**
- **Bandbreitenmanagement**
- **Network Access Control***
- **FIPS inside**
- **Mandantenfähigkeit**
- **Endpoint Security (SSL VPN)**
- **NCP Path Finder ®**

FIPS 140-2 Inside



Universalität

Der NCP Secure Enterprise VPN Server ist ein Baustein der ganzheitlichen VPN-Lösung auf Basis von

NCPs Next Generation Network Access Technology.

Über das VPN Gateway werden mobile und stationäre Teleworker in einem unternehmensübergreifenden Datennetz integriert. Die Software kann auf einem Standard-PC unter Windows oder Linux installiert und als zentrale "Schalt- und Kontrollstelle" hinter einer Firewall in der DMZ (Demilitarisierte Zone), direkt am öffentlichen Netz (Wide Area Network) oder als VM-Ware genutzt werden.

In IPsec-Umgebungen ist der NCP Secure Enterprise VPN Server kompatibel zu VPN-Gateways anderer Hersteller. Als universelle Remote Access-Plattform bietet er Connectivity nicht nur für NCP Secure Clients sondern auch für alle Third Party VPN Clients auf Basis des IPsec-Standards.

Die auf internationalen Standard basierende Lösung ist zudem problemlos in bereits vorhandene IT-Infrastrukturen integrierbar.

Der modulare Aufbau des NCP Secure Enterprise VPN Servers bietet Unternehmen ein hohes Maß an Planungs- und Investitionssicherheit. Die Anzahl an Remote Usern und VPN-Tunnel ist nach Bedarf skalierbar.

Mandantenfähigkeit

Die Mandantenfähigkeit auch "Multi Company Support" genannt, ermöglicht die gleichzeitige Nutzung eines VPN Gateways durch mehrere Unternehmen (Ressource Sharing). Über eine komfortable Zugriffsverwaltung lassen sich die NCP VPN Clients durch Administratoren der angebundenen Unternehmen managen*. Das prätestiniert die NCP-Lösung u.a. auch für den Einsatz bei Managed Security Service Providern bzw. in Cloud-Umgebungen.
In großen Remote Access VPN-Netzen mit mehreren VPN Gateways sorgen die NCP High Availability Services für hohe Verfügbarkeit und gleichmäßige Auslastung aller installierten VPN Gateways.
Die Benutzerverwaltung erfolgt flexibel über Backend-Systeme wie z.B. RADIUS, LDAP oder MS Active Directory.oder auch direkt am VPN-Gateway Integrierte IP-Routing und Firewall-Funktionalitäten sorgen für die erforderliche Connectivity und Sicherheit z.B. bei Filialanbindungen.

NCP VPN Path Finder

Mit dem "NCP VPN Path Finder" stellt NCP eine einzigartige Technologie bereit, die Remote Access auch hinter Firewalls ermöglicht, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert (z.B. in Hotels).

Management

Konfiguration und Verwaltung des NCP Secure Enterprise VPN Servers erfolgen über das NCP Secure Enterprise Management* mittels Plug-in oder über ein Webinterface. Die Managementfunktionen dienen der Steuerung und Überwachung aller VPN-Komponenten. Integrierte Automatismen sorgen für Transparenz, Optimierung der Performance, Sicherheit und Wirtschaftlichkeit der VPN-Lösung. Schnittstellen zu Datenbanken und Verzeichnisdiensten bieten ein Höchstmaß an Integration in bereits vorhandene IT-Umgebungen.

Sicherheit

Der NCP Secure Enterprise VPN Server bietet alle Standards für eine hochsichere Datenübertragung in jeder Remote Access Umgebung

Starke Authentisierung

Unterstützt werden starke Authentisierung durch Einmalpasswort mittels Token (OTP) oder SMS sowie Hard- und SoftwareZertifikate. Die Gültigkeit von Zertifikaten wird bei jedem Verbindungsaufbau anhand von Sperrlisten offline oder online gegenüber der Certification Authority (CA) überprüft.

Endpoint-Security und Sandbox (Network Access Control = NAC**)

Mobile wie auch stationäre Endgeräte können vor dem Zugriff auf das Firmennetz auf deren aktuellen Sicherheitszustand hin überprüft werden. Alle Parameter werden dabei zentral vorgegeben. In Abhängigkeit davon erfolgt die Zugriffsberechtigung des Teleworkers.

In einem IPsec-VPN bestehen die Optionen "Disconnect" oder "Verbleib in der Quarantänezone". In einem SSL-VPN werden Zugriffsberechtigungen auf bestimmte Applikationen nach vorher festgelegten Sicherheitsstufen erteilt. Während einer SSL VPN-Session werden alle gespeicherten Daten in einem vom Betriebssystem abgekoppelten Arbeitsbereich – dem NCP Virtual Private Desktop (Sandbox) - verschlüsselt abgelegt. Nach Beendigung der SSL VPN-Session werden alle in diesem "Container" abgelegten Informationen gelöscht.

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

IPSec und SSL

Über den NCP Secure Enterprise VPN Server können Unternehmen beliebig Datenverbindungen auf Basis eines IPsec- und/oder SSL-VPN zum Firmennetz aufbauen.

Dem Anwender werden über die NCP Secure Client Suite alle Netzwerkapplikationen und -funktionalitäten transparent wie im Büro, an dessen Telearbeitsplatz zur Verfügung gestellt. Das betrifft u.a. auch Voice over IP.

Dem NCP Secure Client kann bei jeder Verbindung die gleiche IP-Adresse zugewiesen werden. Hierbei handelt es sich um eine private IP-Adresse aus dem Adressbereich des Unternehmens. Jeder Telearbeiter ist somit eindeutig anhand seiner IP-Adresse identifizierbar. Dies vereinfacht die remote Administration und Unterstützung der User durch den zentralen Support.

Bei dynamischer Zuweisung einer IP-Adresse aus einem Pool wird diese innerhalb einer definierten Haltedauer (Lease Time) für einen bestimmten User reserviert. Für die Erreichbarkeit des VPN-Gateways auch bei wechselnden IP-Adressen unterstützt der NCP Secure Enterprise VPN Server Dynamic DNS (DynDNS).

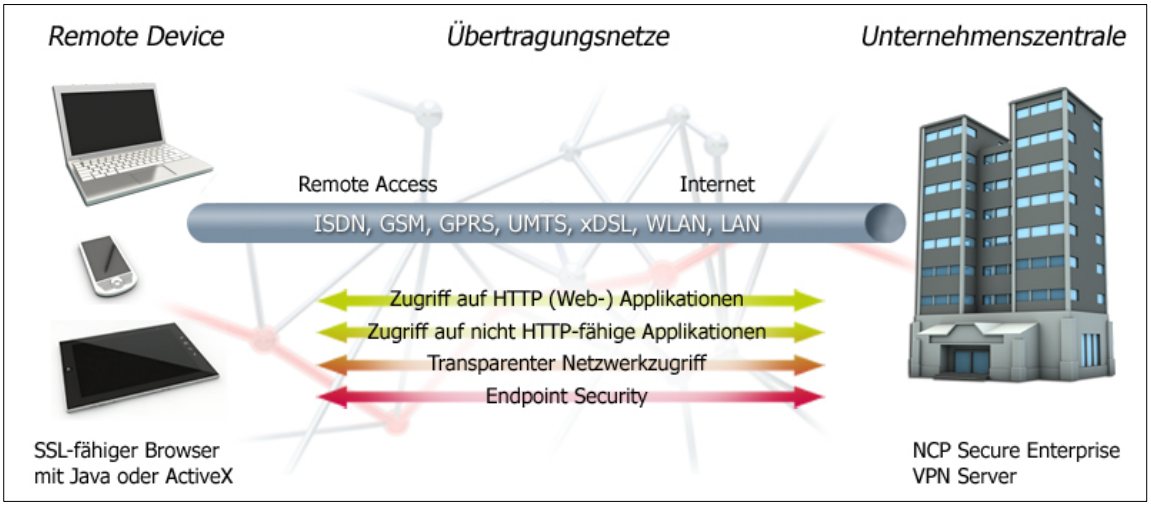
Bei der NCP SSL VPN-Lösung haben Unternehmen folgende Optionen:

- **Web Proxy** - Dieses Modul ermöglicht autorisierten Benutzern den sicheren Zugriff auf interne Web-Applikationen.
- **Port Forwarding** – Der Thin Client dient für den Zugriff auf Client-/Server-Anwendungen (TCP/IP). Anbindung lokaler Client-Applikationen (http-fähig) via Port Forwarding. Dieser Thin Client wird bei jedem Zugriff automatisch auf das Endgerät heruntergeladen und ist Voraussetzung für die Nutzung zusätzlicher Sicherheitsoptionen wie Cache Protection, Endpoint Security und NCP Virtual Private Desktop.
- **PortableLAN** – Dieser Fat Client bietet transparenten Netzwerkzugriff und ist auf jedem Endgerät zu installieren.

Ausführliche Informationen entnehmen Sie bitte dem separaten Datenblatt zum NCP SSL VPN Server)

*) Nur in Verbindung mit dem NCP Secure Enterprise Management

**) Network Access Control ist fester Bestandteil des NCP SSL VPN Gateways. In einem IPsec VPN ist hierzu das NCP Secure Enterprise Management erforderlich



Technische Daten

IPsec VPN und SSL VPN – Allgemeines

Betriebssysteme	32-Bit: Windows 2003 Server, Windows 2003 R2, Windows Server 2008 Linux Kernel 2.6 ab Version 2.6.16 (Distributionen auf Anfrage) 64-Bit: Windows Server 2008, Windows Server 2008 R2 Linux Kernel 2.6 ab Version 2.6.16 (Distributionen auf Anfrage)
Management	Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management mittels VPN Server Plug-in oder über Webinterface
Network Access Control (Endpoint Security)	Endpoint Policy Enforcement für kommende Datenverbindungen. Überprüfung vordefinierter, sicherheitsrelevanter Client-Parameter Maßnahmen bei Soll-/Ist-Abweichungen im IPsec VPN: ‣ Disconnect oder Verbleib in die Quarantänezone mit Handlungsanweisungen (Messagebox) oder Starten externer Anwendungen (z.B. Virenscanner-Update), Protokollierung in Logfiles. (siehe hierzu Datenblatt „NCP Secure Enterprise Management“). Maßnahmen bei Soll-/Ist-Abweichungen im SSL VPN: ‣ Granulare Abstufung der Zugriffsberechtigungen auf bestimmte Applikationen entsprechend vorgegebener Sicherheitslevels.
Dynamic DNS (DynDNS)	Verbindungsaufbau via Internet mit dynamischen IP-Adressen. Registrierung der jeweils aktuellen IP-Adresse bei einem externen Dynamic DNS-Provider. Die Etablierung des VPN-Tunnels erfolgt dann über Namenszuordnung (Voraussetzung: VPN Client unterstützt DNS-Auflösung – wie NCP Secure Clients)
DDNS	Registrierung der verbundenen VPN Clients am Domain Name Server via DDNS, Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse
Netzwerkprotokolle	IP, VLAN-Support
Mandantenfähigkeit	Gruppenfähigkeit; Unterstützung von max. 256 Domänen-Gruppen (d.h. Konfiguration von: Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.)
Benutzerverwaltung	Lokale Benutzerverwaltung (bis zu 750 Benutzer); OTP-Server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistik und Logging	Detaillierte Statistik, Logging-Funktionalität , Versenden von SYSLOG-Meldungen
FIPS Inside FIPS 140-2 Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: ‣ Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) ‣ Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit ‣ Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES
IF-MAP	Das Gesamtziel des ESUKOM Vorhabens ist die Konzeption und Entwicklung einer Echtzeit-Sicherheitslösung für Unternehmensnetze, die basierend auf der Konsolidierung von Metadaten arbeitet. Dabei soll insbesondere der durch mobile Endgeräte wie Smartphones erzeugten Bedrohungslage Rechnung getragen werden. ESUKOM setzt auf die Integration vorhandener Sicherheitslösungen (kommerziell und Open Source) basierend auf einem einheitlichen Metadatenformat gemäß der IF-MAP-Spezifikation der Trusted Computing Group (TCG). Derzeit kann der IF-MAP Server der Fachhochschule Hannover kostenfrei für Tests genutzt werden. Die URL lautet http://trust.inform.fh-hannover.de
Client/Benutzer Authentifizierungsverfahren	OTP-Token, Zertifikate (X.509 v.3): Benutzer- und Hardwarezertifikate (IPsec), Benutzername und Password (XAUTH)

Zertifikate (X.509 v.3)

Server-Zertifikate	Es können Zertifikate verwendet werden die über folgende Schnittstellen bereitgestellt werden: PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); PKCS#12 Interface für Private Schlüssel in Soft-Zertifikaten
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, *vorm. CRL*), CARL (Certification Authority Revocation List, *vorm. ARL*)
Online Check	automatische Downloads der Sperrlisten einer CA in bestimmten Zeitintervallen; Online-Check: Überprüfung der Zertifikate mittels OCSP oder OCSP over http

IPsec VPN und SSL VPN – Verbindungsmanagement

Übertragungsmedien	LAN; Direktbetrieb am WAN: Unterstützung von max. 120 ISDN B-Kanälen (SO, S2M)
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert)
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool-Adressverwaltung	Reservierung einer IP-Adresse aus einem Pool innerhalb einer definierten Haltedauer (Lease Time)
Lockruf	Direktanwahl des dezentralen VPN Gateways über ISDN, „Anklopfen im D-Kanal"

IPsec-VPN

Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; Automatische Behandlung der MTU Size, Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS.
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (inkl. MOBIKE), XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Verschlüsselung	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 4096 Bits; Diffie-Hellman Groups 1,2,5,14; Hash Algorithmen: (MD5), SHA1, SHA 256, SHA 384, SHA 512
Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN-Adapterschutz
VPN Path Finder NCP PATH FINDER	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP Secure Enterprise VPN Server 8.0)
Seamless Roaming	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird.
Authentisierungsverfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens; Pre-Shared Keys; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.
IP Address Allocation	DHCP (Dynamic Host Control Protocol) over IPsec; DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse an die Clients aus dem internen Adressbereich (private IP).
Datenkompression	IPCOMP (lzs), Deflate

Empfohlene Systemvoraussetzungen

Rechner	CPU: Pentium III (oder höher) 150 MHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher (Mindestausstattung), pro 250 gleichzeitig nutzbarer Tunnel 64 MB Arbeitsspeicher. Taktung: pro 150 MHz bei einer Single Core CPU ein Datendurchsatz von ca. 4,5 Mbit/Sek. realisiert werden (incl. symmetrischer Verschlüsselung), pro 150 MHz bei einer Dual/Quad Core CPU kann ein Datendurchsatz von ca. 9 Mbit/Sek. realisiert werden (incl. symmetrischer Verschlüsselung)

Empfohlene VPN Clients / Kompatibilitäten

NCP Secure Entry Clients	Windows 32/64, Mac OS, Windows Mobile, Android
NCP Secure Enterprise Clients	Windows 32/64, Mac OS, Windows Mobile, Android, Windows CE, Linux, Symbian
Third Party VPN Clients	iOS

SSL-VPN

Protokolle	SSLv1, SSLv2, TLSv1 (Application-Layer Tunneling)
Web Proxy	Zugriff auf interne Web-Anwendungen und Microsoft Netzlaufwerke über ein Web-Interface. Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität
Secure Remote File Access*	Up- und Download, Erstellen und Löschen von Verzeichnissen, entspricht in etwa den Funktionalitäten des Datei-Explorers unter Windows. Voraussetzungen am Endgerät: siehe Web Proxy
Port Forwarding	Zugriff auf Client-/Server-Anwendungen (TCP/IP), Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V1.5) oder ActiveX, SSL Thin Client für Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit) und Linux
NCP Virtual Private Desktop	Der Virtual Private Desktop ist ein vom Basis-Betriebssystem abgekoppelter Arbeitsbereich, der dem Anwender für eine SSL VPN-Session zur Verfügung gestellt wird. Anwendungen, die in diesem Bereich gestartet werden, werden vom Basis-Betriebssystem entkoppelt. Innerhalb des Virtual Private Desktop gespeicherte Daten, beispielsweise Dateianhänge empfangender E-Mails, werden in einem Container AES-verschlüsselt gespeichert. Bei Beendigung der SSL VPN-Session werden alle im Container abgelegten Dateien gelöscht.
Cache Protection für Internet Explorer 7, 8 und 9	Alle übertragenen Daten werden nach dem Verbindungsabbau automatisch am Endgerät gelöscht. Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V5.0), SSL Thin Client für Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)
PortableLAN	Transparenter Zugriff auf das Firmennetz Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V5.0) oder ActiveX Control, PortableLAN Client für Windows 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)
Single Sign-on	Single Sign-on kann immer dann eingesetzt werden, wenn die Web Server-Anwendung die gleichen Zugangsdaten benötigt wie der SSL VPN Client. Die zentrale Verwaltung von Benutzername und Passwort kann dazu unter anderem über Active Directory, RADIUS oder LDAP erfolgen. Je nach Anwendung kann zwischen Single Sign-on mit HTTP-Authentisierung (Basic (RFC2617), HTTP Digest (RFC2617) und NTLM (Microsoft)) oder Single Sign-on nach der Post Form-Methode unterschieden werden. Single Sign-on mit Web-Applikationen wurde mit Outlook Web Access (OWA) 2003, 2007 und 2010, RDP Client und CITRIX Webinterface 4.5, 5.1 getestet. Single Sign-on mit Port Forwarding wird nur von Anwendungen unterstützt, die Parameter (wie Benutzername und Passwort) in ihrer Kommandozeile entgegennehmen können

Empfohlene Systemvoraussetzungen*

Anzahl Concurrent User	Rechner
1-100 Concurrent User	CPU: Intel Dual Core 1,83 GHz oder vergleichbarer x86 Prozessor, 1024 MB Arbeitsspeicher
200+ Concurrent User	CPU: Intel Dual Core 2,66 GHz oder vergleichbarer x86 Prozessor, 1024 MB Arbeitsspeicher

*) Abhängig vom Endgerätetyp. Es gibt Einschränkungen bei mobilen Endgeräten wie Tablet PCs (z.B. unter iOS, Android), Smartphones, PDAs etc.

**) 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.