

## Technische Daten

### IPsec VPN und SSL VPN - Allgemeines

<b>Betriebssysteme</b>	32-Bit: Windows 2000, Windows XP Prof., Windows 2003 Server, Windows Server 2008 (Beta), Linux Kernel 2.4 ab Version 2.4.10; Kernel 2.6 ab Version 2.6.12 (Distributionen auf Anfrage). 64-Bit: Windows Server 2008
<b>Management</b>	Server Manager, lokale und remote Administration über SNMP over SSL bzw. SNMP; Zugriffsverwaltung (mehrere Administratoren); Verbindungstests; Traces; Konfiguration, Web-Interface
<b>Network Access Control (Endpoint Security)</b>	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. Virenschanner-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.
<b>Dynamic DNS (DynDNS)</b>	Verbindungsaufbau via Internet mit dynamischen IP-Adressen. Registrierung der jeweils aktuellen IP-Adresse beim einem externen Dynamic DNS-Provider. Die Etablierung des VPN-Tunnels erfolgt dann über Namenszuordnung (Voraussetzung: VPN Client unterstützt DNS-Auflösung – wie NCP Secure Clients)
<b>DDNS</b>	Erweiterung des Domain Name Servers (DNS), Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse
<b>Netzwerkprotokolle</b>	IP
<b>Multi Company Support</b>	Gruppenfähigkeit; Unterstützung von max. 256 Domänen-Gruppe (d.h. Konfiguration von: Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.)
<b>Benutzerverwaltung</b>	Lokale Benutzerverwaltung (bis zu 750 Benutzer); OTP-Server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
<b>Statistik und Logging</b>	Detaillierte Statistik, Logging-Funktionalität, Versenden von SYSLOG-Meldungen
<b>Client/Benutzer Authentifizierungsverfahren</b>	OTP-Token, Zertifikate (X.509 v.3): Benutzer- und Hardwarezertifikate (IPsec), Benutzername und Passwort
<b>Zertifikate (X.509 v.3)</b>	
Server-Zertifikate	Es können Zertifikate verwendet werden die über folgende Schnittstellen bereitgestellt werden: PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); integrierte Unterstützung von Smart Cards über PC/SC, CT-API (Karten auf Anfrage); PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten;
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, <i>vorm. CRL</i> ), CARL (Certification Authority Revocation List, <i>vorm. ARL</i> )
Online Check	automatische Downloads der Sperrlisten von der CA in bestimmten Zeitintervallen; Online-Check: Überprüfung der Zertifikate mittels OSCP oder OSCP over http gegenüber der CA

### IPsec VPN und SSL VPN - Einwahl

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

## IPsec-VPN

<b>Virtual Private Networking</b>	IPsec (Layer 3 Tunneling), RFC-konform; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS.
<b>Internet Society RFCs und Drafts</b>	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP
<b>Verschlüsselung</b>	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 Hash Algorithmen: (MD5), SHA1, SHA 256, SHA 384, SHA 512
<b>Firewall</b>	Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN-Adapterschutz
<b>Authentisierungsverfahren</b>	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 Secrets; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready.
<b>IP Address Allocation</b>	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).
<b>Datenkompression</b>	IPCOMP (Izs), Deflate
<b>Empfohlene Systemvoraussetzungen</b>	
<b>Rechner</b>	CPU: Pentium III (oder höher) 150 MHz oder vergleichbarer x86 Prozessor, 256 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)

## SSL-VPN

<b>Protokolle</b>	SSLv1, SSLv2, TLSv1 (Application-Layer Tunneling)
<b>Web Proxy</b>	Zugriff auf interne Web-Anwendungen und Microsoft Netzlaufwerke über ein Web-Interface. Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität
<b>Secure Remote File Access</b>	Up- und Download, Erstellen und Löschen von Verzeichnissen, entspricht in etwa den Funktionalitäten des Datei-Explorers unter Windows.  Voraussetzungen am Endgerät: siehe Web Proxy
<b>Port Forwarding</b>	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 Vista (32/64-Bit), Windows XP (32/64-Bit) und Linux,
<b>Cache Protection für Internet Explorer V.6, 7 und 8</b>	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 Windows Vista (32/64-Bit), Windows XP (32/64-Bit)
<b>PortableLAN</b>	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 Vista (32/64-Bit), Windows XP (32/64-Bit)
<b>Empfohlene Systemvoraussetzungen*</b>	
<b>Anzahl Concurrent User</b>	<b>Rechner</b>
<b>10 Concurrent User (CU)</b>	CPU: Intel Pentium III 700 MHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher
<b>50 Concurrent User</b>	CPU: Intel Pentium VI 1,5 GHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher
<b>100 Concurrent User</b>	CPU: Intel Dual Core 1,83 GHz oder vergleichbarer x86 Prozessor, 1024 MB Arbeitsspeicher
<b>200 Concurrent User</b>	CPU: Intel Dual Core 2,66 GHz oder vergleichbarer x86 Prozessor, 1024 MB Arbeitsspeicher

\*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.