Datenblatt

NCP Secure Enterprise Linux Client

Next Generation Network Access Technology

Universelle, zentral managebare VPN Client Suite für Linux

- **Zentrales Management und Network Access Control**
- **Kompatibilität zu VPN Gateways (IPsec Standard)**
- **Integrierte, dynamische Personal Firewall**
- **Fallback IPsec / HTTPS (VPN Path Finder Technology)**
- **Starke Authentisierung**
- **Multi Zertifikatsunterstützung**
- **FIPS Inside**
- **Integrierte Unterstützung von 3G/4G Hardware**
- **Integration aller für Remote Access erforderlichen Sicherheits und Kommunikationstechnologien**
- **Kostenlose 30-Tage-Vollversion**

Universalität und Kommunikation

Der NCP Secure Enterprise Linux Client ist ein Baustein von NCP's „Next Generation Network Access Technology", der ganzheitlichen Remote Access VPN-Lösung. Mobile und stationäre Teleworker arbeiten in der gewohnten Weise wie am Büroarbeitsplatz. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen auch zu VPN Gateways aller namhaften Anbieter hergestellt werden. Mittels beliebiger Endgeräte mit Linux 32 oder 64 Bit-Betriebssystemen, können Teleworker von jedem Standort, weltweit auf das zentrale Datennetz zugreifen. Die NCP VPN Path Finder Technology ermöglicht Remote Access auch hinter Firewalls bzw. Proxies, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert.

Sicherheit

Die Sicherheitsmechanismen des NCP Secure Enterprise Linux Clients bieten einen umfassenden Schutz des Endgerätes und Firmennetzes vor jedweden Attacken unberechtigter Dritter. Das gilt auch an Hotspots, insbesondere während des An- und Abmeldevorganges am WLAN. Wichtigste Security-Bausteine sind neben der Datenverschlüsselung: eine dynamische Personal Firewall, die Unterstützung von OTP-Tokens (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure) sowie Endpoint Security*. Die für Remote Access optimierte Network Access Control-Lösung von NCP verhindert nachhaltig den Zugriff unzureichend geschützter Endgeräte auf das zentrale Datennetz. Mittels der Personal Firewall können Regelwerke für Ports, IP-Adressen, Segmente und Applikationen definiert werden. Die „Friendly Net Detection", d.h. die automatische Erkennung von sicheren und unsicheren Netzen, aktiviert situationsabhängig die jeweils erforderlichen Firewall-Regeln. Die NCP Personal Firewall ist im Gegensatz zu herkömmlichen Firewalls bereits beim Systemstart aktiv und ist zentral administrierbar*. Das Feature Multi-Zertifikatsunterstützung ermöglicht VPN-Verbindungen mit unterschiedlichen Firmen, die jeweils ein eigenes Benutzerzertifikat erfordern. Alle Client-Einstellungen können durch den Administrator vor Veränderungen durch den Anwender gesperrt werden.
Das Kryptografiemodul, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Usability und Wirtschaftlichkeit

„Easy-to-use" für Anwender und Administrator, d.h. einfache Bedienung und Installation des NCP Secure Enterprise Clients ist einzigartig am Markt. Die grafische, intuitive Benutzeroberfläche informiert über alle Verbindungs- und Sicherheitsstati vor und während einer Datenverbindung. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Die Mediatype-Erkennung wählt automatisch das jeweils schnellste, vorhandene Übertragungsnetz aus. Ein Konfigurations-Assistent ermöglicht das einfache Anlegen von Profilen. Die integrierte Unterstützung von Mobile Connect Cards für UMTS / GPRS macht die Installation der Benutzeroberfläche des Kartenlieferanten überflüssig. Ein Textfeld im Monitor kann beliebig gestaltet werden, z.B. mit Firmenlogo oder Supporthinweisen. Usability bedeutet auch Kosteneinsparungen durch Verringerung des Schulungsaufwands, weniger Dokumentation und Entlastung des Helpdesk.

Zentrales Management

Das NCP Secure Enterprise Management bietet unter dem Anspruch „Single Point of Administration" alle Funktionalitäten und Automatismen für den wirtschaftlichen Betrieb eines ganzheitlichen Remote Access VPN. Rollout, Inbetriebnahme und den wirtschaftlichen Betrieb eines ganzheitlichen Remote Access VPN.

*) Installation eines NCP Secure Enterprise Managements erforderlich

Technische Daten

Betriebssysteme	32/64 Bit: Ubuntu Desktop 10.04.3 LTS, open SUSE 11.3, 11.4, 12.1, Fedora 16, Debian 5.0.8
Security Features	Der NCP Secure Client unterstützt alle IPsec Standards nach RFC
Personal Firewall **Firewall Configuration***	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (FND)**, Auswertung von: aktueller Netzwerkadresse und IP-Adresse; automatische FND, Secure Hotspot Logon; differenzierte Filterregeln bezüglich: Protokolle, Ports und Adressen, Schutz des LAN-Adapters, zentrale Administration mit Client Firewall Configuration Plug In*
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec - Gateway (IKE, IPsec Phase 2); Event log; Kommunikation im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption)	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1,2,5,14
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
Authentisierungs-verfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS;PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); 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.
Starke Authentisierung – Standards **PKI Enrollment***	X.509 v.3 Standard; Entrust Ready PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2 and 2.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, *vorm. CRL*), CARL (Certification Authority Revocation List, *vorm. ARL*), OCSP. CMP* (Certificate Management Protocol),
Network Access Control	Endpoint Policy Enforcement*
Networking Features	LAN Emulation: Virtual Ethernet-Adapter
Netzwerkprotokolle	IP
Dialer	NCP Internet Connector
VPN Path Finder NCP PATH FINDER	NCP VPN Path Finder Technology* mit Proxy-Unterstützung, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP Secure Enterprise Server 8.0)
Weitere Features	Automatische Medientyp-Erkennung; UDP-Encapsulation, Multi-Zertifikatsunterstützung
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Festnetze: analoges Fernsprechnetz, ISDN, xDSL, LAN Funknetze: GSM, GPRS, UMTS, LTE (abhängig von eingesetzter Hardware), Internet
Line Management	DPD mit konfigurierbarem Zeitintervall; Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert);
Datenkompression	IPCOMP (lzs), Deflate
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3498, RFC 3947: IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Client Monitor **Intuitive, grafische Benutzeroberfläche**	Mehrsprachig (Deutsch, Englisch); intuitive Bedienung; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files, Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; Integrierte Unterstützung von Mobile Connect Cards (PCMCIA, embedded); Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre

*) Voraussetzungen: NCP Secure Enterprise Management und /oder NCP Secure Enterprise Server
**) Download des NCP FND Servers: http://www.ncp-e.com/de/downloadstatistik/secure-entry-client/friendly-net-detection-server.html
Weitere Informationen zu NCP Secure Enterprise Clients: http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/vpn-client.html