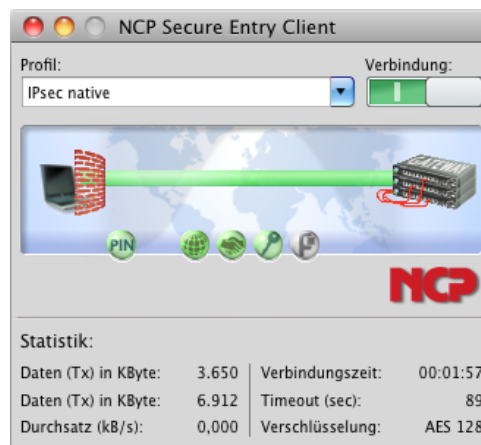


Next Generation Network Access Technology

Universeller VPN Client für Mac OS X

- ▶ **Kompatibilität zu VPN Gateways (IPsec-Standard)**
- ▶ **Importfunktion für unterschiedliche Dateiformate**
- ▶ **Integrierte, dynamische Personal Firewall**
- ▶ **Fallback IPsec / HTTPS (VPN Path Finder Technology)**
- ▶ **Starke Authentisierung**
- ▶ **Integration aller für Remote Access erforderlichen Sicherheits- und Kommunikationstechnologien**
- ▶ **FIPS inside**
- ▶ **Kostenlose 30-Tage Vollversion**



Universalität und Kommunikation

Der NCP Secure Entry Mac Client ist eine Kommunikationssoftware für den universellen Einsatz in beliebigen Remote Access VPN-Umgebungen. Mobile und stationäre Teleworker arbeiten an ihren Apple Computern in der gewohnten Weise wie am Büroarbeitsplatz. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen zu VPN Gateways aller namhaften Anbieter hergestellt werden. Der Verbindungsaufbau erfolgt über beliebige Netze (auch iPhone Tethering via USB oder Bluetooth). Teleworker können von jedem Standort, weltweit auf das zentrale Datennetz zugreifen. Die NCP VPN Path Finder Technology ermöglicht Remote Access auch hinter Firewalls, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert.

Sicherheit

Die Sicherheitsmechanismen des NCP Secure Entry Mac Clients bieten einen umfassenden Schutz des Endgerätes und Firmennetzes vor jedweden Attacken unberechtigter Dritter.

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). Mittels der Personal Firewall können Regelwerke für: Ports, IP-Adressen und Segmente definiert werden. Die „Friendly Net Detection“, d.h. die automatische Erkennung von sicheren und unsicheren Netzen, aktiviert in Abhängigkeit davon die erforderlichen Firewall-Regeln.

Alle Client-Einstellungen können durch den Administrator gegenüber Veränderungen durch den Anwender gesperrt werden.

Der IPsec Client verfügt über einen kryptografischen Algorithmus nach FIPS-Standard. Das eingebettete Kryptografiemodul ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

Usability und Wirtschaftlichkeit

„Easy-to-use“ für Anwender und Administrator – d.h. die einfache Bedienung und Installation des NCP Secure Entry Mac 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. Ein Konfigurations-Assistent ermöglicht das einfache Anlegen von Profilen. Usability bedeutet auch Kosteneinsparungen durch Reduzierung des Schulungsaufwands, weniger Dokumentation und nachhaltige Entlastung des zentralen Helpdesk.



FIPS 140-2 Inside

Technische Daten

Betriebssysteme	Mac OS X 10.5 Leopard (Intel) und Mac OS X 10.6 Snow Leopard
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines NCP FND-Servers*); differenzierte Filterregeln bezüglich: Protokolle, Adressen und Ports, Schutz des LAN-Adapters Im Gegensatz zur applikationsbasierten Konfiguration der Mac OS X-Firewall ist die Konfiguration dieser Firewall portbasierend.
Virtual Private Networking	Unterstützung aller IPsec Standards nach RFC; IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKE, IPsec Phase 2); Event log; Kommunikation nur 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	Integrierter, kryptografischer Algorithmus nach FIPS-Standard (Federal Information Processing Standard). Das eingebettete Kryptografiemodul ist nach FIPS 140-2 zertifiziert (Zertifikat #1051). Die FIPS Kompatibilität ist immer gegeben, wenn die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: - DH-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 und 256 Bit oder Triple DES
Authentisierungsverfahren	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; Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens; Multi-Zertifikatskonfiguration;Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; ORSA SecurID Ready.
Starke Authentisierung - Standards	X.509 v.3 Standard; PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); 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, <i>vorm. CRL</i>), CARL (Certification Authority Revocation List, <i>vorm. ARL</i>).
Networking Features	Beliebige Netze, iPhone Tethering via USB oder Bluetooth
Netzwerkprotokoll	IP
VPN 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 Server 8.0)
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
Line Management	DPD mit konfigurierbarem Zeitintervall
Datenkompression	IPCOMP (Izs), Deflate
Weitere Features	UDP-Encapsulation; Importfunktion der Dateiformate: *.ini, *.pcf, *.wgx, *.wge und *.spd.
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, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch); Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre

*) NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden: <http://www.ncp-e.com/de/downloads/software.html>

Optional: Zentrales Management und Endpoint Security (Upgrade auf NCP Secure Enterprise Mac Client)

Weitere Informationen zum NCP Secure Entry Mac Client finden Sie hier:
<http://www.ncp-e.com/de/loesungen/produkte/universeller-ipsec-client.html>

Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen: <http://www.ncp-e.com/de/downloads/software.html>