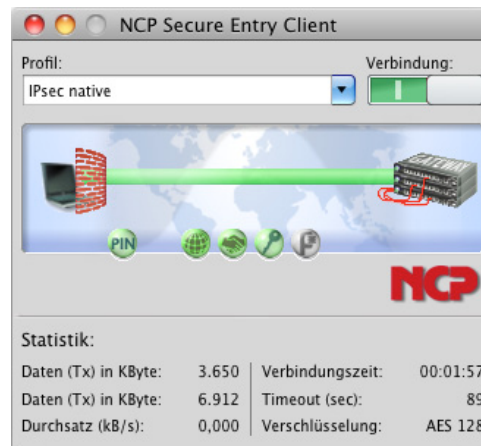


Next Generation Network Access Technology

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. Gegenüber der grafisch konfigurierbaren Firewall im Mac OS X sind auch Firewall-Regeln für ausgehende Verbindungen konfigurierbar. Der Administrator hat somit die Möglichkeit, dem Anwender nur restriktiven Zugriff auf das Internet zu gewähren. 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 integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, 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. Wahlweise lässt sich die Benutzeroberfläche des Clients auch platzsparend in der Menüleiste von Mac OS X minimiert darstellen. 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), Mac OS X 10.6 Snow Leopard und OS X 10.7 Lion
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 und ausgehende Regeln sind ebenso möglich.
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)	<ul style="list-style-type: none"> ▸ 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	<p>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 die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:</p> <ul style="list-style-type: none"> ▸ 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	<ul style="list-style-type: none"> ▸ Internet Key Exchange (IKE): <ul style="list-style-type: none"> ▸ Aggressive Mode und Main Mode ▸ Quick Mode ▸ Perfect Forward Secrecy (PFS) ▸ IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP) ▸ Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure) ▸ Benutzer-Authentisierung: <ul style="list-style-type: none"> ▸ XAUTH für erweiterte Benutzer-Authentisierung ▸ One-Time-Passwörter und Challenge Response Systeme ▸ Zugangsdaten aus Zertifikaten (PKI) ▸ Unterstützung von Zertifikaten in einer PKI: <ul style="list-style-type: none"> ▸ Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und PKCS#12 ▸ Seamless Rekeying (PFS) ▸ IEEE 802.1x: <ul style="list-style-type: none"> ▸ Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2) ▸ Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): - gegenüber Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2) ▸ RSA SecurID Ready
Starke Authentisierung - Standards	<ul style="list-style-type: none"> ▸ X.509 v.3 Standard; ▸ PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); ▸ PKCS#12 Interface für Soft Zertifikate; ▸ 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).
Networking Features	
Sichere Netzwerk-Schnittstelle	<ul style="list-style-type: none"> ▸ Interface Filter <ul style="list-style-type: none"> ▸ NCP Interface-Filter stellen die Schnittstelle zu allen Netzwerk-Interfaces der PPP- und Ethernet-Familie her. ▸ Volle Unterstützung von Wireless Local Area Network (WLAN) ▸ Volle Unterstützung von Wireless Wide Area Network (WWAN)
Netzwerkprotokoll	IP
Verbindungs-Medien	<ul style="list-style-type: none"> ▸ LAN ▸ Unterstützte Verbindungsmedien für Apple oder Medienschnittstellen und Management Tools von Drittherstellern:

	<ul style="list-style-type: none"> ▶ LAN / Ethernet ▶ WLAN ▶ GPRS / UMTS und GSM ▶ ISDN ▶ Modem ▶ iPhone tethering via USB oder Bluetooth
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 (LZS), Deflate
Weitere Features	UDP-Encapsulation; Importfunktion der Dateiformate: *.ini, *.pcf, *.wgx, *.wge und *.spd.
Internet Society RFCs und Drafts	<p>Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),</p> <ul style="list-style-type: none"> ▶ Internet Key Exchange Protocol (IKE) (includes IKMP/Oakley) (RFC 2406), ▶ Negotiation of NAT-Traversal in the IKE (RFC 3947), ▶ UDP encapsulation of IPsec Packets (RFC 3948), ▶ IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
Client Monitor	<ul style="list-style-type: none"> ▶ Mehrsprachigkeit (Englisch, Deutsch) <ul style="list-style-type: none"> ▶ Monitor & Setup: de, en ▶ Online Hilfe und Lizenz: de, en
Intuitive, grafische Benutzeroberfläche	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; Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden. Start des Monitors optional automatisch nach Systemstart als Vollbild oder als Icon in der Menüleiste
Tipps des Tages	In die Oberfläche des Client-Monitors ist ein Feld für Konfigurationstipps und Anwendungsbeispiele integriert. Mit einem Mausklick auf dieses Feld wird eine HTML-Seite mit Beschreibung zum jeweils wechselnden Tages-tipp geöffnet, die über Handhabung und Leistungsmerkmale des Clients informiert.
Projekt-Logo	Über ein zusätzliches Informationsfeld in der Monitor-Oberfläche, dem Banner, wird per Mausklick eine lokale HTML-Seite geöffnet. Das Banner kann durch Ihr Firmenlogo ersetzt werden, die lokale HTML-Seite durch eine andere Ihrer Wahl. Beide Dateien befinden sich im Installationsverzeichnis des Entry Clients unter /ProjectLogo als logo_de.png und secure_entry_banner_de.html. Zusätzlich kann eine Quick-Info angezeigt werden wenn der Mauszeiger das Banner-Feld bzw. das Logo berührt.

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

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