

## Next Generation Network Access Technology

## Versatile VPN Client for Mac OS X – Simple and highly secure Remote Access via Internet.

- ▶ **Compatible with VPN gateways (IPsec standard)**
- ▶ **Import of third party configuration files**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Fallback IPsec → HTTPS (VPN Path Finder Technology)**
- ▶ **Strong authentication**
- ▶ **Integration of all security and communication technologies for universal remote access**
- ▶ **FIPS inside**
- ▶ **Free of charge 30 day full version**



## Universality and Communication

The NCP Secure Entry Client for Mac OS X is a communications software product for universal deployment in any remote access VPN environment. Teleworkers work transparently and securely at their mobile or stationary Apple computers, exactly as if working in an office in their corporate environment. Using a VPN gateway from any of the well-known suppliers, highly secure data connections to the gateway can be established using the IPsec protocols, and a connection can be established via any type of network (including iPhone Tethering via USB or Bluetooth). Even when located behind firewalls, whose settings inevitably prevent IPsec data connections, NCP's VPN Path Finder technology ensures that a connection to the remote gateway can always be established.

## Security

The NCP Mac Client provides extensive security mechanisms designed to prevent attacks in any remote access environment. It offers comprehensive security of both the end device and the corporate network.

As well as data encryption, the most important security components are support of One-Time Password (OTP) tokens and certificates in a Public Key Infrastructure (PKI), and a personal firewall that filters according to inbound or outbound rules for ports, IP addresses and segments. These firewall rules can be supplemented with "Friendly Network Detection", enabling the firewall to filter selectively, based on whether or not a friendly network has been detected.

The standard Mac OS X firewall with its graphical user interface is easy to use, but it can only filter inbound connections. Contrast this with the additional security from the bi-directional rules of the NCP Mac Client

firewall; these enable an administrator to restrict the user's Internet access. Or use both firewalls, where special circumstances demand. All Client configurations can be locked by the administrator; then the user can not alter the locked configurations.

Together, all these features ensure the Client machine always has the right level of protection against unauthorized third parties

## Usability and Cost Effectiveness

"Easy to use" for both user and administrator - the NCP Secure Entry Mac Client is simple to install and simple to operate. A graphical, intuitive user interface provides information on all connection and security states. Detailed log information ensures effective assistance from the help desk. A configuration wizard enables easy set up of connection profiles and VPN tunnels can be configured to be established automatically.

"Easy to use" also means reduced costs through less time spent training, less documentation and fewer support calls.

## FIPS Inside

The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051).



FIPS 140-2 Inside

Technical data

<b>Operating Systems</b>	Mac OS X 10.5 Leopard (Intel) and Mac OS X 10.6 Snow Leopard
<b>Security Features</b>	The NCP Secure Entry Mac Client supports the Internet Society's RFC 4301 – Security Architecture for the Internet Protocol (IPsec) and all the associated RFCs.
<b>Personal Firewall</b>	<ul style="list-style-type: none"> <li>• Stateful Packet Inspection</li> <li>• IP-NAT (Network Address Translation)</li> <li>• Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address or an NCP FND server )</li> <li>• Differentiated filter rules relative to: protocols, ports and addresses, LAN adapter protection</li> <li>• In contrast to the application based configuration of the built-in Mac OS X firewall, the configuration of this firewall is port based.</li> </ul>
<b>Virtual Private Networking</b>	<ul style="list-style-type: none"> <li>• IPsec (Layer 3 Tunneling)</li> <li>• IPsec proposals negotiated via IPsec gateway (IKE Phase 1, IPsec Phase 2)</li> <li>• Communication only in tunnel</li> <li>• Message Transfer Unit (MTU) size fragmentation and reassembly</li> <li>• Dead Peer Detection (DPD)</li> <li>• Event log</li> <li>• Network Address Translation-Traversal (NAT-T)</li> <li>• IPsec Tunnel Mode</li> </ul>
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• Internet Key Exchange (IKE):             <ul style="list-style-type: none"> <li>◦ Aggressive mode and Main mode,</li> <li>◦ Quick mode                 <ul style="list-style-type: none"> <li>▪ Perfect Forward Secrecy (PFS)</li> </ul> </li> <li>◦ IKE Config. mode for dynamic allocation of private IP (virtual) address from address pool</li> <li>◦ Pre-shared secrets or RSA Signatures (and associated Public Key Infrastructure)</li> </ul> </li> <li>• User authentication:             <ul style="list-style-type: none"> <li>◦ XAUTH for extended user authentication                 <ul style="list-style-type: none"> <li>▪ one-time passwords and challenge response systems</li> </ul> </li> </ul> </li> <li>• Support for certificates in a PKI:             <ul style="list-style-type: none"> <li>◦ Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations</li> </ul> </li> <li>• Seamless rekeying (PFS)</li> <li>• RSA SecurID ready</li> </ul>
<b>Encryption and Encryption Algorithms</b>	Symmetrical: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange Perfect Forward Secrecy
<b>FIPS Inside</b>	The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051). FIPS compatibility is always given if the following algorithms are used for set up and encryption of the IPsec connection: <ul style="list-style-type: none"> <li>• DH Group: Group 2 or higher (DH starting from a length of 1024 Bit)</li> <li>• Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit</li> <li>• Encryption Algorithms: AES with 128, 192 and 256 Bit or Triple DES</li> </ul>
<b>Hash / Message Authentication Algorithms</b>	<ul style="list-style-type: none"> <li>• SHA-256, SHA-384, SHA-512, MD5</li> <li>• Diffie Hellman groups 1, 2, 5, 14 used for asymmetric key exchange and PFS</li> </ul>
<b>Public Key Infrastructure (PKI) - Strong Authentication</b>	<ul style="list-style-type: none"> <li>• X.509 v.3 Standard;</li> <li>• PKCS#11 interface for encryption tokens (USB and smartcards);</li> <li>• PKCS#12 interface for private keys in soft certificates;</li> <li>• PIN policy; administrative specification for PIN entry in any level of complexity;</li> <li>• Revocation:             <ul style="list-style-type: none"> <li>◦ End-entity Public-key Certificate Revocation List (EPRL formerly CRL)</li> <li>◦ Certification Authority Revocation List, (CARL formerly ARL)</li> <li>◦ Online Certificate Status Protocol OCSP</li> </ul> </li> </ul>
<b>Networking Features</b>	Any type of network, iPhone tethering via USB or Bluetooth
<b>Network Protocol</b>	IP
<b>NCP VPN Path Finder</b>	Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available (prerequisite: NCP Secure Enterprise Server V 8.0 and later)
<b>IP Address Allocation</b>	<ul style="list-style-type: none"> <li>• Dynamic Host Control Protocol (DHCP)</li> <li>• Domain Name Service (DNS) : gateway selection using a public IP address allocated by querying a DNS server</li> </ul>
<b>Line management</b>	DPD with configurable time interval;
<b>Data Compression</b>	IPCOMP (lzs), deflate
<b>Additional Features</b>	UDP encapsulation, import of the file formats:*.ini, *.pcf, *.wgx, *.wge and *.spd.

## Internet Society RFCs and Drafts

- Security Architecture for the Internet Protocol and assoc. RFCs (RFC4301 – 4304, 4385, 4307 – 4309),
  - Internet Key Exchange Protocol V2 (IKEV2) (includes IKMP/Oakley) (RFC 4306),
  - 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 Intuitive, Graphical User Interface

- Bilingual (English, German)
- Traffic light icon indicates connection status
- Client Info Center – overview of
  - General information - version#, MAC address etc
  - Connection – current status
  - Services/Applications – process(es) – status
- Certificate Configuration – PKI certificates in use etc.
- Configuration, Connection Statistics, Log-book (color coded, easy copy&paste function)
- Password protected configuration and profile management
- Trace tool for error diagnosis

\*) If you wish to download NCP's FND server as an add-on, please click here: <http://www.ncp-e.com/en/downloads/software.html>

Option: central management and endpoint security (upgrade NCP Secure Enterprise Client)

More information on NCP Secure Entry Client is available on the Internet at:  
<http://www.ncp-e.com/en/products/universal-ipsec-client.html>

You can test a free, 30-day full version of Secure Entry Mac Client here: <http://www.ncp-e.com/en/downloads/software.html>