

NCP Secure Entry Mac Client

Service Release 2.02 Build 14
October 2011

1. Changes in Version 2.02 Build 14

DNS Domains to be resolved in the Tunnel

Regardless of whether or not Split Tunneling is in use, which DNS queries must be routed through the tunnel can be defined in the configuration field "IPsec Address Allocation"; enter the DNS name required under "DNS Domains to be resolved in the Tunnel".

In a newly created VPN profile the default entry in "DNS Domains to be resolved in the Tunnel" is blank, i.e. the default is that all DNS queries are routed outside the tunnel to the DNS server that has been allocated in the Internet (by the provider).

2. Problems Resolved

Selection of a defined VPN Connection

Under certain circumstances a VPN Profile could not be selected from the profile selection in the Client Monitor. This problem has been resolved.

Communication between Central Site and Client when using XAUTH

When Extended Authentication (XAUTH) was being used, the communication between the central site and the Client would fail meaning that the dialogue with the central site for requesting a new password was not correctly displayed (e.g. when using external authentication). This problem has been resolved.

3. Known Issues

None

4. Getting Help for the NCP Secure Entry Mac Client

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

<http://www.ncp-e.com/en/downloads.html>

For further assistance with the NCP Secure Entry Mac Client, visit:

<http://www.ncp-e.com/en/about-us/contact.html>

Mail: helpdesk@ncp-e.com



5. Features

Operating Systems

Mac OS X 10.5 Leopard (Intel) & Mac OS X 10.6 Snow Leopard, Mac OS X 10.7 Lion

Security Features

The NCP Secure Entry Mac Client supports the Internet Society's Security Architecture for the Internet Protocol (IPsec) and all the associated RFCs.

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address or an NCP FND server¹)
- Differentiated filter rules relative to: protocols, ports and addresses, LAN adapter protection
- In contrast to the application based configuration of the built-in Mac OS X firewall, the configuration of this firewall is port based.

Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2)
- Communication only in the tunnel
- Message Transfer Unit (MTU) size fragmentation and reassembly
- Dead Peer Detection (DPD)
- Event log
- Network Address Translation-Traversal (NAT-T)
- IPsec Tunnel Mode

Authentication

- Internet Key Exchange (IKE):
 - Aggressive mode and Main mode,
 - Quick mode
 - Perfect Forward Secrecy (PFS)
 - IKE Config. mode for dynamic allocation of private IP (virtual) address from address pool
 - Pre-shared secrets or RSA Signatures (and associated Public Key Infrastructure)
- XAUTH for extended user authentication
 - one-time passwords and challenge response systems
 - Access details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
 - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying (PFS)
- IEEE 802.1x:
 - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
 - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): - relative to switches and access points on the basis of certificates (layer 2)
- RSA SecurID ready

Encryption and Encryption Algorithms

- 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

FIPS Inside

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051). FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 bits)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit, or Triple DES

Hash / Message Authentication Algorithms

- SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- PKCS#11 interface for encryption tokens (USB and smartcards)
- PKCS#12 interface for private keys in soft certificates
- Administrative specification for PIN entry to any level of complexity
- Revocation:
 - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
 - Certification Authority Revocation List, (CARL formerly ARL)
 - Online Certificate Status Protocol OCSP

Networking Features

Secure Network Interface

- Interface Filter
 - NCP Interface Filter interfaces to all standard Network Interfaces from the PPP and Ethernet families.
 - Wireless Local Area Network (WLAN) support
 - Wireless Wide Area Network (WWAN) support

Network Protocol

- IP

Communications Media

- LAN
- Communications media supported using Apple or 3rd party media interfaces and management tools:
 - LAN / Ethernet
 - Wi-Fi
 - GPRS / 3G and GSM

- ISDN
- Modem
- iPhone tethering via USB or Bluetooth

Split Tunneling

When using Split-Tunneling, those domains whose DNS packets are to be routed via the VPN Tunnel can be specified exactly

VPN Path Finder

- NCP VPN Path Finder Technology
 - 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)

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS): gateway selection using a public IP address allocated by querying a DNS server

Line Management

- Dead Peer Detection with configurable time interval

Data Compression

- IPCOMP (LZS), deflate

Additional Features

- 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 (RFC2401 - 2409),
 - 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 (intuitive graphical user interface)

- Bilingual (English, German)
- Traffic light icon indicates connection status
- Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Configuration locks
- Monitor can be tailored to include company name or support information
- A "Tip of the Day" field for configuration tips and application examples is incorporated in the Client Monitor
- The client monitor can be started with both its maximized window and minimized as an icon in the menu bar

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

More information on NCP Secure Entry Mac is available on the internet at:
<http://www.ncp-e.com/en/products/ipsec-client.html>
You can test a free, 30-day full version of the Secure Entry Mac Client her:
<http://www.ncp-e.com/en/downloads/software.html>