Release Notes

NCP Secure Enterprise Linux Client

Service Release 3.23 Build 038
Date: February 2012

1. New Features and Enhancements

The following lists the most important features added, in comparison to version 2.10 build 028 of the NCP Secure Enterprise Linux Client and version 2.31 build 013 of the Secure GovNet Client Linux:

Supported by Linux 32 and 64 bit operating systems

The Enterprise Linux Client has been tested on the following distributions :
Ubuntu Desktop 10.04.3 LTS, open SUSE 11.3, 11.4, 12.1, Fedora 16, Debian 5.0.8.

Monitor Graphical User Interface (GUI)

The Enterprise Client Monitor GUI is implemented consistently across all platforms, enabling easy use and configuration by either local users or the Secure Enterprise Management (SEM) administrator. This includes implementations under the Linux, Mac OS X and Microsoft Windows operating systems (see Features).

Multi-Certificate Support and Configuration

A number of individual certificate settings can be stored as a multi-certificate configuration in the Client configuration, and then any one certificate selected, per profile, from the different certificate configurations. This enables authentication using a different certificate against each different VPN server, e.g. a soft certificate against VPN gateway 1 and a certificate stored on a smartcard against VPN gateway 2.

The certificate to be used, for example, for encryption and authentication in L2Sec security mode or for extended authentication in IPsec security mode, can be selected in the "Security" configuration field.

The Client certificate configuration is pre-configurable via:

• Management Server:	Version 2.05
• Management Console:	Version 2.05
• Client Plug-in:	Version from 9.30 Build 48 onwards

VPN Path Finder with Proxy Support

VPN Path Finder switches automatically to the alternative connection protocol TCP Encapsulation with SSL Header (Port 443) as soon as the standard IPsec connection via port 500 or via UDP encapsulation over a freely configurable port is no longer available. This feature is important if the client can only use the HTTPS port 443 and an IPSec only connection is not possible, as can be the case in hotels or hotspots for example.

The feature is configured in the "Advanced IPsec Options" folder in the Profile Settings and in the monitor's Configuration menu.

An NCP gateway (Version 8 and later) is a prerequisite for VPN Path Finder; there an "alternative" port must be configured in the "VPN / IPsec settings" of the "Local System".

If VPN Path Finder is to be used and a proxy server must be used in order to access the Internet, the proxy server of the standard browser can be selected or the address of the company's own proxy entered.

If a connection with VPN Path Finder is established via port 443, this is indicated by an icon in the monitor's status display (right, under the HQ/Gateway). The icon is displayed in the monitor GUI when the VPN connection as connection establishment starts.

Hotspot Login using Browser

The first time the Hotspot Configuration is opened, the default browser is defined for use for hotspot logon (i.e. the default is for hotspot logon to be carried out using the Windows default browser).

Hotspot automation in the Client's Personal Firewall ensures that only requests for resolving IP addresses via DHCP are allowed and all other access attempts between computer and the Wireless LAN (WLAN) are inhibited. The Firewall enables ports 80 and 443 dynamically for logging on to and off from the hotspot when the "Hotspot Logon" menu item is selected, and inhibits the user from accessing the Internet.

Friendly Net Detection

Different firewall rules concerning known (friendly) and unknown networks can be defined by using Friendly Net Detection. E.g.: In a known corporate network special rules can grant access for administration purposes on a PC. However in an unknown network the PC is completely isolated.

The actual specification of a Friendly Network is defined centrally by the administrator. This specification can then be implemented in the Client either using manually pre-defined parameters or by making use of automation provided by Friendly Network Detection (FND). Prerequisite for the automated solution is the installation of a Friendly Net Detection server on that part of the company network referred to as the friendly network.

Manual definition of the friendly network by an administrator and the automatic detection by means of an FND server are not mutually exclusive and can be configured simultaneously using the "Manual" and "Automatic" menu tabs.

The Firewall symbol in the monitor will be green when the computer is connected to a friendly network; it turns red on connecting to an unknown network.

The FND server address can be assigned via DHCP where appropriate. The destination address of an FND server can be distributed from a DHCP server using a DHCP option (15), enabling the Client to detect when it is located in the friendly network. (Addresses of FND servers pre-configured in the Client's Firewall configuration are disabled while the Client continues to obtain the FND address via DHCP). The corresponding parameters are located in the Configuration menu under "Firewall / Friendly Networks / Automatic".

FIPS Inside

The Secure 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 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

Enhanced 3G / UMTS Configuration

A separate parameter folder for Communications Media "GPRS / 3G" ("GPRS / UMTS" in German) has been introduced into the profile settings.

There are three variants for UMTS configuration:

Provider List (default setting): this provides a series of suggested values from which the APN of the provider can be selected.

APN from SIM card: the APN is read from the SIM card. (This only works when an APN is configured in the SIM card).

User defined: the user must enter the required parameters manually.

The provider list can be extended by adding entries to the "APN.ini" file (located in the installation directory), as appropriate.

2. Problems Resolved

None

3. Known Issues

None

4. Getting Help for the NCP Secure Enterprise Linux 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/products/central-managed-vpn-solution/vpn-client.html

For further assistance with the NCP Secure Enterprise Linux Client, visit:
http://www.ncp-e.com/en/about-us/contact.html

Mail: mailto:helpdesk@ncp-e.com?subject=A: NCP Secure Enterprise Client - Helpdesk message

5. Features

Central Management

As the ***Single Point of Management***, NCP's Secure Enterprise Management (SEM) provides functionality and automation for the rollout, commissioning and efficient use of Secure Enterprise Clients. The Secure Enterprise Management (SEM) makes use of a VPN connection or the LAN (when on the company network), to automatically provide NCP Secure Enterprise Clients with:

- configuration updates,
- certificate updates, and
- updates to the Update Client

Network Access Control / Endpoint Security

The policies for Endpoint Security (Endpoint Policy Enforcement)) are created centrally at the Secure Enterprise Management (SEM) and each NCP Secure Enterprise Client is only permitted access to the company network in accordance with the corresponding rules.

High Availability Services

The NCP Secure Enterprise Client supports the NCP HA Services. These services are client server based and can be used in two different operating modes: load balancing or failsafe mode. Regardless of the load on the server or whether a server has failed, the VPN connection to the corporate network is established and maintained reliably, in the background and without any delay for the user of the NCP Secure Enterprise Client.

Operating Systems

Linux 32 & 64 bit

Distributions: Ubuntu Desktop: 10.04.3 LTS; openSUSE: 11.3, 11.4, 12.1; Fedora 16; Debian 5.0.8

Security Features

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

Virtual Private Networking

- RFC conformant IPsec (Layer 3 Tunneling)
  - IPsec Tunnel Mode
  - 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
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)

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)
- User authentication:
  - XAUTH for extended user authentication
    - One-time passwords and challenge response systems
    - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
  - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying
- PAP, CHAP
- Pre-Authentication (Authentication before VPN establishment)
- Secure hotspot logon using HTTP
- 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

Hash / Message Authentication Algorithms

- SHA1, 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
- Support for certificates in a PKI
  - Smart cards and USB tokens
    - PKCS#11 interface for encryption tokens (smart cards and USB)
    - Smart card operating systems
  - TCOS 1.2, 2.0 and 3.0
  - Smart card reader systems
    - PC/SC
  - Soft certificates
    - PKCS#12 interface for private keys in soft certificates
- PIN policy: administrative specification of 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)
  - Certificate Management Protocol (CMP)[i]

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, the DHCP server's MAC address or an NCP FND server[i]

- Supports secure hotspot logon feature
- Differentiated filter rules relative to:
    - Protocols, ports or IP addresses
    - LAN adapter protection,
- Central administration (optional)[ii]
- IPv4 support

Endpoint Security

- Endpoint Policy Enforcement [ii]

Networking Features

Secure Network Interface

- LAN Emulation
    - NCP Virtual Ethernet adapter with NDIS interface
    - Wireless Local Area Network (WLAN) support
    - Wireless Wide Area Network (WWAN) support

Network Protocol

- IP

Communications Media

- LAN
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN
- ISDN
- Automatic Media Detection (AMD)

Dialers

- NCP Secure Dialer

Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value

IP Address Allocation

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

VPN Path Finder

- NCP Path Finder Technology
  - Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available [iii]

Data Compression

- IPsec Compression: lzs, deflate

Link Firewall

- Stateful Packet Inspection

Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming [iii]

Point-to-Point Protocols

- PPP over Ethernet
- PPP over GSM,
- PPP over ISDN,
- PPP over PSTN,
  - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Standards Conformance

Internet Society RFCs and Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol (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)

FIPS Inside

The Secure 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 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

Client Monitor

Intuitive Graphical User Interface

- Language support (English, German)

- Monitor & Setup: en, de
- Online Help and License en, de
- 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)
- Integrated support of Mobile Connect Cards (PCMCIA, embedded)
- Password protected configuration and profile management
- Trace tool for error diagnosis

Notes

[i] 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

[ii] Prerequisite: NCP Secure Enterprise Management

[iii] Prerequisite: NCP Secure Enterprise Server V 8.0 and later

More information on the NCP Secure Enterprise Linux Client is available on the Internet at:
http://www.ncp-e.com/en/products/central-managed-vpn-solution.html