

NCP Secure Client – Juniper Edition

Service Release: 9.30 Build 75
Date: November 2011

1. New Features and Enhancements

The following describe the new features introduced in this release:

Project Logo has been renamed Custom Branding Option

"Project Logo" option has been renamed in this and future versions to "Custom Branding Option", in all languages.

Testing for Internet Availability

Network Tests are an option in the Client Monitor's Help Menu and these can be used to test Internet availability. They support both PING to an IP Address in the Internet as well as resolution of an Internet Domain Name to an IP address. Domain names should be of the form "ncp-e.com".

Enter the address and press the corresponding Test button.

The test results are displayed via a symbol (success: green tick, failure: red cross). More details are displayed in a clear text log.

Animation of Connection Establishment

The user gets an optical feedback immediately after the Connect button has been pressed, in the form of a rotating symbol. This symbol, signaling the process of connection establishment, is displayed for the duration of this process. If the connection cannot be established, the rotating symbol disappears and an error message is displayed in the Client Monitor's graphics field instead of the normal green connection bar.

Automated Search for New Software Update

If the menu item "Search for Updates" is called, a new dialog is displayed via which the search cycle (never, daily, weekly, monthly) can be configured. In addition there is a new button "Search now".

Command Line Tool "NcpClientCmd"

Alternative command line program to "rws cmd", which does not make use of graphical output.

2. Problems Resolved

None

3. Known Issues

None

4. Getting Help for the NCP Secure Client – Juniper Edition

For further assistance with the NCP Secure Client – Juniper Edition, visit:

<http://www.ncp-e.com/en/about-us/oem-partners/ncp-juniper-cooperation.html>

Mail: juniperhelpdesk@ncp-e.com

5. Features

Operating Systems

Windows (32 Bit): Windows7, Windows Vista, Windows XP

Windows (64 Bit): Windows7, Windows Vista, Windows XP

Support for Juniper gateways with Junos and ScreenOS operating systems

Prerequisite

Juniper IPsec Gateway (support for ScreenOS)

Licensing

The NCP Secure Client – Juniper Edition supports three types of licensing/activation:

Offline Activation

- In offline activation, a file must first be generated by entering a license key and serial number. This must then be sent to the NCP Activation Server which then returns an activation key. This key must then be used to activate the Client.

Online Activation

- In online activation the licensing data entered via a Wizard is validated, via the Internet, with the NCP Activation Server before being used to activate the Client.

Licensing using an Initialization File

- The Client uses an Initialization File, distributed by an administrator, to authenticate itself with the Licensing Server, via the corporate VPN network. The Client uses the actual license received for activation. (Prerequisite: NCP Local License Server)

Security Features

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

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)
- User authentication:
 - XAUTH for extended user authentication
 - one-time passwords and challenge response systems
- Support for certificates in a PKI:
 - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying (PFS)
- 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-1, 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)
- Smart card operating systems:
 - TCOS 1.2, 2.0 and 3.0
- Smart card reader interfaces:
 - PC/SC, CT-API
- PKCS#12 interface for private keys in soft certificates
- CSP for use of user certificates in Windows certificate store PIN policy
- 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

LAN Emulation

- Virtual Ethernet adapter with NDIS-Interface

Network Protocol

- IP

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

Additional Features

- Import of the file formats: *.ini, *.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
- Client Info Center – overview of
 - General information – version number, 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 and paste function)
- Password protected configuration and profile management
- Trace tool for error diagnosis

