

NCP Secure Client – Juniper Edition

Service Release: 9.30 Build 102
Date: February 2012

1. New Features and Enhancements

The following describe the new features introduced in this release:

Visual Feedback about Status of Tunnel

When the physical communication medium connection, used to establish a VPN tunnel, breaks, the existing VPN tunnel remains established, i.e. the tunnel remains logically active, for an unspecified length of time. Use of the logical tunnel by pre-existing connections can resume when the physical connection has been re-established.

During the period the physical connection is broken, the normally solid green line displayed in the client monitor changes to a dashed green line and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

If the client loses the Internet connection and the tunnel remains logically connected, this status is displayed in a balloon over the tray icon. In this way the user has feedback about the status, even when the monitor is minimized.

Enhancements to Online Help and Tips

The help text has been adapted to the current version of the client. The dialog for profile groups has been enhanced with a help button. All help text is available, as usual, via a help button or, context sensitive, with the F1 key.

2. Problems Resolved

The following problems have been resolved in this release:

Blocked monitor

When displaying a PKI error message via the callback function, if the monitor was minimized during startup before the monitor image was fully displayed, the error message could not be displayed and the monitor was blocked.

Routing tables updated incorrectly

The client monitors DHCP requests on every network adapter, in order to keep IP related information for each adapter. Some situations require that the client triggers a DHCP exchange with a RENEW command. If a RENEW command was issued for an adapter without an IP address or with link status "down", the subsequent route table alterations could not be performed for some minutes.

Error when setting routes in split-tunneling

In some cases routes were incorrectly set when using split-tunneling.

Error in export file on network drive

Until now, a client's profile settings were not directly exported to a file on a network drive as password and pre-shared key were not transferred in such a case.

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)

© NCP engineering E-Mail: info@ncp-e.com ▪ www.ncp-e.com
NCP_RN_Win_Secure_Entry_Client_Juniper_Edition_9_30_102_en.docx

Technical specifications subject to change without notice

- 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, 15-18 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)
- Trace tool for error diagnosis
- Internet Availability Tests

