

NCP Secure Client – Juniper Edition

Release 9.23 build 17
July 2010

1. New Features and Enhancements

The following describes new features and enhancements available in the NCP Secure Client - Juniper Edition release 9.23 build 017:

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

Support for Juniper gateways with Junos and ScreenOS operating systems

2. Problems Resolved in this Version

On Windows 7, data could not be transferred over a VPN tunnel when the supporting Internet connection was via a UMTS / Mobile Broadband link not established by the NCP Secure Client – Juniper Edition. This problem has been resolved.

3. Known Issues

- None -

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

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. Revision History

Features of the previous release 9.22 build 005:

Operating Systems

Windows (32 Bit): Windows7, Windows Vista, Windows XP
Windows (64 Bit): Windows7, Windows Vista, Windows XP

Requirement

Juniper IPsec Gateway (support for ScreenOS)

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

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; Entrust Ready
- 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#, 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
- Client Monitor can be tailored to include company name or support information