

NCP Secure Client – Juniper Edition

Release 9.23 build 073

August 2011

1. New Features and Enhancements

The following describes the new enhancement in this release of the NCP Secure Client - Juniper Edition Version 9.23 Build 073:

Importing .spd files - handling encrypted/obfuscated pre-shared keys

In order to preserve the confidentiality of pre-shared keys during the export/import process, the pre-shared key parameter in the .spd file can be encrypted. However, during import by the Secure Client – Juniper Edition, a check is made as to whether the pre-shared key parameter ("PRESHR") is in clear text or encrypted / otherwise obfuscated:

- only clear text "PRESHR" parameters are imported
- any "PRESHR" parameters that are encrypted or obfuscated are ignored and the pre-shared key entry in the resulting profile is left empty.

NCP recommends two different methods for handling encrypted or obfuscated "PRESHR" parameters in .spd files:

1. Import the unaltered .spd file in the normal way and, after the profile has been created from the parameters, modify the pre-shared key in that profile using the monitor menu: Configuration / Profiles - Edit Profile / Security / Pre-shared Key.
Whilst the easier of the two methods, it is not well suited for situations where the .spd file is being imported into more than one or two machines.

Or

2. Modify the "PRESHR" parameter in the .spd file before importing that file. Replace the hexadecimal, pre-shared key string with the clear text pre-shared key to be used in the profile. This option is particularly useful where the same .spd file is to be imported on a number of different Secure Client – Juniper Edition machines.

To modify the "PRESHR" parameter, use the following procedure:

- Make a backup copy of the original .spd file, for use in the event that the file becomes corrupted while being edited.
- Open the .spd file using a text editor.
- Find lines of the form
"PRESHR"=hex:b3,02,03,af,66,cc,97,6a,b3,b7,23,0c,f0,27,92,e4,40,e3
(note: this is just an example and the actual details will vary in the file being edited. See the before and after examples below)
- Replace the string
hex:b3,02,03,af,66,cc,97,6a,b3,b7,23,0c,f0,27,92,e4,40,e3
by the pre-shared key to be used, e.g.
"123ABC456DEF"

Important

- The "PRESHR" string represented in hex could be any length up to the maximum 255 characters. Ensure that all characters in the "PRESHR" parameter are deleted and replaced by the clear text string.
- The clear text pre-shared key string must be enclosed in quotation marks - see example below.
- If the .spd file contains parameters for a number of different profiles, ensure that each set of profile parameters is given the correct "PRESHR" parameter.
- While editing the file, take care not to alter any of the other parameters.

Examples of encrypted (before editing) and clear text (after editing) pre-shared key .spd files:

ENCRYPTED Pre-shared Key (e.g. before editing)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IRE\SafeNet\Soft-PK\ACL\33\MYID]
"CERTIFICATELABEL"=""
"CERTIFICATEISSUER"=hex:
"PORT"=dword:00000000
"PORTNAME"="All"
"NET_INTFC"=""
"InternalIP"=dword:00000000
"AUTOCERT"=dword:00000000
"TYPE"=dword:00000003
"FQDN"=""
"UFQDN"="statewic2@doh.wa.lcl"
"PRESHR"=hex:b3,02,03,af,66,cc,97,6a,b3,b7,23,0c,f0,27,92,e4,40,e3
"DN"=hex:
```

CLEAR Text Pre-shared Key (e.g. after editing)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IRE\SafeNet\Soft-PK\ACL\33\MYID]
"CERTIFICATELABEL"=""
"CERTIFICATEISSUER"=hex:
"PORT"=dword:00000000
"PORTNAME"="All"
"NET_INTFC"=""
"InternalIP"=dword:00000000
"AUTOCERT"=dword:00000000
"TYPE"=dword:00000003
"FQDN"=""
"UFQDN"="statewic2@doh.wa.lcl"
"PRESHR"="123ABC456DEF"
"DN"=hex:
```

.spd files now correctly associated with NCP Secure Client Profile Import

A .spd file is now associated with the profile import function of the NCP Secure Client – a .spd file can be imported by double clicking on the file in a windows browser.

RWSCMD – command "/writeClientInfoCenterData" introduced

Using the new command "RWSCMD /writeClientInfoCenterData" data from the Client Info Center is created and written to a file (this is equivalent to the "Save to file " function in the Client Info Center)

If no filename argument is given then the data is written to "My Documents\ClientInfoCenter.txt".
If a path is given as the argument, the file "ClientInfoCenter.txt" is written into that directory.
If both path and filename are given as an argument then the data is written to that file in that directory.
If the path does not exist, the data is written to "My Documents\ClientInfoCenter.txt".

2. Problems Resolved

The following problems have been resolved:

Resolution of Pre-configured Variables

If a Client configuration made use of placeholders (e.g. %INSTALLDIR%), only the NCP placeholders were resolved, the Windows placeholders were not correctly resolved.
This problem has been resolved.

Other Corrections

- modifications concerned with expiration of the test period.
- the cause of a sporadic crash of the Client monitor after switching users has been identified and resolved.

.spd files with multiple profile data now imported correctly

In previous versions, if a .spd file contained data intended for multiple profiles, these profiles were not created correctly. This problem has now been resolved and all required profiles are created according, exactly, to the layout of the .spd file.

Import of Configuration Files

Configuration files will be interpreted correctly when imported from a network location.

Readability of the Stored Log File

Space characters have been introduced in the Client's stored log file in order to improve readability. For example the following output

20.08.2010 15:19:55IPSec:Start building connection

will now appear as:

20.08.2010 15:19:55 IPSec: Start building connection

In addition the numeric format has been corrected to be dependent on the language chosen:

In English"235,000.15 kByte" compared to the equivalent German "235.000,15 kByte".

Weakness in NCP Secure Client

The NCP Secure Client was shown to be susceptible to a DLL hijacking attack. Such an attack made use of a weakness in the Windows DLL load process.

This weakness has been resolved with patches. Further information about the attack is available for download under:
http://www.ncp-e.com/fileadmin/pdf/service_support/NCP_Client_Vulnerability_Statement_EN.pdf

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. Features List

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

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

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