NCP Secure Friendly Net Detection Server (Linux)

Major Release: **2.10 rev. 25694**
Date: **September 2015**

Prerequisites

Operating System Support

The following Operating Systems are supported with this release:

- Cent OS 7.1 (64 bit)
- Debian GNU/Linux 8.1.0 (64 bit)
- SUSE Linux Enterprise Server 12 (64 bit)
- Ubuntu Server 14.04.4 (64 bit)

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Modifications according to the new version

3. Known Issues

None

Service Release: **2.00 rev. 17595**
Date: **July 2014**

Prerequisites

Operating System Support

The following Operating Systems have been tested:

- Cent OS 6.4 (32 bit)
- Debian 7.3.0 (64 bit)
- Sles 11 SP3 (64 bit)
- Ubuntu Server 14.04.4 (64 bit)

4. New Features and Enhancements

None

5. Improvements / Problems Resolved

Open SSL 1.0.1 H after expert assessment of 5. June 2014

The 5. June 2014 expert assessment of the security breach resulted in the release of Open SSL 1.0.1 and this version has been implemented in the latest version of the NCP Secure Friendly Net Detection Server.
(See https://www.openssl.org/news/secadv_20140605.txt)

6. Known Issues

None

Service Release: **2.00 rev. 16756**
Date: **April 2014**

Prerequisites

Operating System Support

The following Operating Systems have been tested:

- Cent OS 6.4 (32 bit)
- Debian 7.3.0 (64 bit)
- Sles SP3 (64 bit)
- Ubuntu Server 12.04.4 (64 bit)

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

OpenSSL Heartbleed-Bugs (CVE-2014-0160)

OpenSSL Heartbleed Bug - cryptographic library - problem resolved

3. Known Issues

None

Service Release: **2.00 build 16224 (Linux)**
Date: **March 2014**

Prerequisites

Operating System Support

The following Operating Systems have been tested:

- Cent OS 6.4 (32 bit)
- Debian 7.3.0 (64 bit)
- Sles SP3 (64 bit)
- Ubuntu Server 12.04.4 (64 bit)

1. New Features and Enhancements

First release of this product

See the "Features" section 5 for a brief description of the product features.
See the accompanying readme for installation notes and instructions.

2. Improvements / Problems Resolved

None

3. Known Issues

None

4. Getting Help for the NCP Secure Friendly Net Detection Server

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/downloads/software/version-information.html

For further information about the Enterprise Client, visit:

http://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-vpn-client-suite.html

For further assistance with the NCP Secure Friendly Net Detection Server (Win32/64), visit:

http://www.ncp-e.com/en/company/contact.html

5. Features

Friendly Net Detection – a vital part of NCP's security management

Friendly Net Detection (FND) is a technology that enables a Secure Client computer to automatically recognize a "friendly network".

FND is a classic client / server application that can be centrally administered:

- The FND server (FNDS) is a separate service, installed, independent of the VPN Gateway, on any computer within the "known company network". Prerequisite for the use of FND is installation of an FNDS in a network that has been declared as the "friendly network". This service has to be available from all parts of that network; i.e. in some cases, router settings may have to be changed.
- The FND client (FNDC) is part of NCP's Secure Client Suite and is configured via the Client's firewall settings. If an employee connects his end-device to the company network, the FNDC tries to contact the configured FNDS. If the FNDS is able to authenticate with the Client, it is confirmed that the device is within an Friendly Net and the NCP Secure Client's firewall rules are automatically changed accordingly.
- The administrator centrally sets all "Friendly Net" rules of the NCP Secure Client's Personal Firewall, a standard component the NCP Secure Entry and Enterprise Clients. Standard "administrator locks" can be used, where required to prevent the user from manipulating or deactivating those rules. In large Remote Access VPN's, all templates and changes of all configuration parameter of the NCP Secure Client are ideally carried out with NCP's Secure Enterprise Management (SEM) System as "Single Point of Administration".

The FND technology is based on established standards, a fact which ensures consistent system security while protecting system from errors which are frequent in proprietary solutions.

Operating Systems

See Prerequisites on page 1.

Security Features

Authentication

- EAP, TLS or Certificate-based authentication of contact between NCP FND Server and NCP Secure Client
- Support for certificates in a PKI:
  - Soft certificates