

NCP Secure Enterprise Server

Maintenance Release

Windows: 8.05 Build 69

Linux: 8.05 build 28

Date: May 2011

1. New Features and Enhancements

Supported Linux 32 and 64 bit Operating System Distributions

The server software has been tested under the following Linux 32/64 distributions:

- Debian GNU/Linux 5.0.8 Lenny
- Debian GNU/Linux 6.0.0 Squeeze
- SLES SuSE Linux Enterprise Server 11
- Ubuntu LTS 10.04
- Red Hat 5.3
- Fedora 14
- Open SuSE 11.4

Supported Microsoft Windows 32 and 64 bit Operating Systems

The server software has been tested under the following Microsoft Windows 32 and 64 bit operating systems:

- Windows Server 2003 32 bit
- Windows 2003 R2 32 bit
- Windows 2008 SP2 32/64 bit
- Windows 2008 R2 SP1 64 bit

Creation and Distribution of Server Certificates with the PKI Enrollment Plug-in

The Secure Server automatically accepts Server Certificates that have been generated and distributed by the SEM (Secure Enterprise Management).

Issuing a Certificate

Issuing a new Server Certificate is initiated at the management system in the "Server Certificate Configuration", from where it is also sent to the corresponding VPN gateway after the Server Configuration has been created. In the course of this distribution the filename and PIN are removed from the Server Certificate configuration. The procedure, step by step:

- open the Server Configuration plug-in
- select the Secure Server
- select a "Server Certificate Configuration" under "Configuration" [the Server Certificate will be generated for this server configuration]
- press the "New Certificate" tool button
- the dialog for creating a certificate is opened [after inputting the certificate details the certificate is stored in the SEM].
- Before distribution, the Server Configuration must be created with „Create Server Configuration“.

© NCP engineering GmbH , e-mail: info@ncp-e.com , www.ncp-e.com

NCP_Sec_Ep_Server_RN_805_en_v1.1.docx

Technical specification subject to change

page 1 of 12

Renewing a Certificate

As with all other certificates, a Server Certificate can be renewed. This can be done in one of two ways:

- via the Server Configuration plug-in: -Server Configuration / Secure Server / Issued Certificates, or
- via the PKI Enrollment plug-in: PKI Enrollment / Issued Certificates

Alternatively, certificates can be renewed by a script.

When renewing a certificate it is not necessary to create a Server Configuration, distribution takes place immediately if the corresponding gateway is online. The certificate is always stored with the filenames and PIN last entered.

Displaying the Certificate

The certificate currently in use by the gateway is always displayed under the "Server Certificates" node. For this gateway, the certificate issued with the PKI plug-in is displayed under the node "Issued Certificates".

The name of the linked Server Certificate Configuration is displayed under "Info / Certificate Usage".

Prerequisite

- Management Server 2.05 Build 7
- Management Console 2.05 Build 3
- Server Configuration Plug-in 8.05 Build 14
- PKI Enrollment Plug-in 2.05 Build 2
- NCP Secure Server 8.05 Build 20

Querying Server Certificates via SNMP

The following values can be queried via SNMP:

- Subject
- Issuer
- Valid from
- Valid to
- Serial Number
- Fingerprint MD5 + SHA1

Checking the contents of CRL files after download

After downloading, the CRL is checked to see whether it has been completely downloaded (ASN1 syntax check). If the check finds an error, the download is re-initiated after 20 seconds, and, if necessary, afterwards at 5 minute intervals.

An incompletely downloaded CRL could have led to system errors in previous versions.

Transmission of SubCA Certificate

During a check of the Server Certificate by a Client, all certificates in the chain from Root Certificate through to Server Certificate are checked. To enable this to be done it is sufficient for the Root Certificate to be stored locally at the Client, the SubCA Certificate of the certificate chain is transferred from Server to Client during the SSL negotiations and deleted after the check. Prerequisite is a VPN connection using L2Sec.

Automatic Return Route Establishment (ARRE)

In environments with central Secure Enterprise VPN Server Systems configured as Load Balancing HA clusters, this new function ensures that the intermediate gateways responsible for forwarding packets are made aware of which Clients are connected to which central gateways. This is designed to ensure, in such configurations, a correct assignment and forwarding of all response packets back to the correct VPN Client.

ARRE is implemented in the associated forwarding gateways.

Dynamic Switching of Filter Rules dependent on Endpoint Security Requirements

Dependent on the rules defined, only those Clients that conform to the security policies will be allowed access to the company network. Conformance to the policies is first checked during establishment of the connection. If the connecting Client does not conform to the policies (as defined in the corresponding rules) then that Client's access is restricted to within a quarantine zone. This quarantine zone, a network subnet defined (using filter rules) at the Server, can then be used for making updates available to the Client. If, after the update, the Client conforms to the Endpoint Security policies, that Client is allowed access to the company network, as the Secure Server can enable the Client's access to network subnets or that part of the company network outside the quarantine zone by dynamically switching the filter rules.

During the lifetime of a connection, Endpoint Security checks are carried out at regular, pre-defined intervals. Should one of these checks confirm that the policies are no longer being conformed to, for example, because a virus scanner has been deactivated in the Client, then the Client's access rights are changed in accordance with the pre-defined rules.

Prerequisite for this dynamic switchover during the lifetime of a VPN connection is an NCP Secure Enterprise Server with version 8.05 or higher and an NCP Secure Client with version 9.23 or higher.

External Authentication with LDAP Bind

Should a user wish to use the same password for both connection to the VPN gateway and also for the connection into a domain, this can be managed by external authentication using LDAP Bind. This is done by forwarding the VPN password from the gateway (Secure Server) to the Active Directory Server (LDAP Server). The LDAP server compares the password with the appropriate entry and, if equal, the user is allowed to establish the VPN connection.

Prerequisite for this type of authentication is that the password has already been stored in Active Directory. Passwords in Active Directory cannot be managed (changed or renewed) via the VPN.

The switch for configuring the use of LDAP Bind for Authentication is in the Configuration under "Domain Group / LDAP". If this is set to "On", the password of the user who wishes to connect to the VPN gateway is checked against the corresponding LDAP entry.

Externally authenticated passwords can only be managed via the VPN if Secure Enterprise Management (SEM) is being used with Microsoft Internet Authentication (RADIUS) Server.

LDAP over SSL

LDAP over SSL can now be used with the default port 636. A prerequisite is that the LDAP server supports LDAP over SSL.

RADIUS, LDAP and SEM Forwarding

If a Domain Group in your subnet uses its own RADIUS, LDAP or SEM server instead of a central machine of this type, RADIUS, LDAP or SEM forwarding to that server must be enabled. (this is handled in the Configuration under "Domain Group / General").

The address or name from the configuration field for this Domain Group under "General" (Management Server), "RADIUS" and "LDAP is used for the IP address of the server.

Ensure that only one of the three possible forwarding types is active:

- forwarding via the GRE - activated by setting the GRE Endpoint as the destination gateway
- forwarding via the VPN tunnel - activated by selecting a Link Profile configured for the outgoing (IPsec) connection to the destination gateway, or
- forwarding via VLAN - activated by entering a VLAN ID.

Users of this Domain Group are forwarded to their network area according to those settings. Data packets intended for a RADIUS, LDAP or Management Server are not forwarded as, in most network infrastructures, such machines are used centrally for all domain groups.

Start Web Application with Port Forwarding

If web proxies cannot be used for calling web applications from the SSL VPN start page, then, under Windows, the web applications can also be started via port forwardings. There are two methods available.

1. Calling a web site via a script

In the Port Forwarding Configuration select "Start Application" from the "Start Mode" drop-down, under "Start Command" select the script that the "Default Web Browser" will start; enter the URL of the required web site under "Start Parameter".

2. Calling a web site from the same browser as where the SSL Start Window has been called

In the Port Forwarding Configuration select "Start Browser" from the "Start Mode" drop-down, under "Start Command" enter the URL of the required web site (e.g. <http://www.ncp-e.com>) as in a browser and as remote host enter the same host name or same IP address as under the "Start Command" (e.g. www.ncp-e.com). Port 80 (http) is required as the remote port. (Prerequisite: Internet Explorer >= V. 8.0.)

Placeholders for Simplifying the Configuration

In order to simplify the complex configuration process, "Placeholders for SSL VPN Parameters" are available in the SSL VPN configuration of the Link Profile. (see below)

In the "Link-Profile / SSL VPN" configuration fields, resolvable values for "Remote Host" and "Start Parameter" can be held in these placeholders (%SSLVPNPARAM1% to %SSLVPNPARAM5%) which are then resolved, on a user specific basis, via the assignment in the Link Profile.

Placeholders can also be used in SSL VPN applications, for sharing of corresponding directories on the network. Providing that the name of the user's personal directory is identical with his/her username that must be entered at the login page, the directory can be referenced as follows:

`\ncp\%SSLVPNUSERNAME%`

If the username given at the login page includes a suffix (e.g. ABC@DomainGroup1), the suffix can be omitted by using the placeholder %USERNAME%, enabling just the username before the @ character (e.g. ABC) to be entered.

The placeholder is replaced with its specific value. If, for example, for %SSLVPNPARAM1% the value "116.2.1" is entered, the result is that the value for "Remote Host" is generated as follows:

Remote Host = 198.%SSLVPNPARAM1% ⇒ 198.116.2.1

The placeholder can be used in the configuration of the SSL VPN application Port Forwarding for "Remote Host" and "Start Parameter" and for the configuration of SSL VPN application Network Share for "Directory". In addition, a parameter can be made up of multiple placeholders. The same placeholders can also be used in RADIUS and LDAP configurations.

Design of the SSL VPN Start Page

Information text (e.g. support messages with e-mail and phone number etc.), in both English and German, can be included in the start page for the SSL VPN user. If nothing is entered then the default text is displayed and if "none" is entered, nothing is displayed. (details to be displayed are configured under the "SSL VPN Listener").

The NCP company logo and the "SSL VPN" product description can be replaced by other images.

- The "LH graphic" should be 740 x 180 pixels at 72 dpi.
- The "RH graphic" should be 205 x 80 pixels at 72 dpi.
The graphics will be displayed in this size on the left or right hand side respectively.
- The graphics format (GIF; JPEG, PNG, etc) must be supported by the browser(s) to be used.

The graphics files are stored in the following directory:

MS Windows [PROGRAMFILES]\ncp\secureserver\sslvpn\customimages

Linux \usr\local\ncp\ses\sslvpn\customimages

In the configuration the filenames are entered without the path.

Enhancement to the DDNS Configuration

In the Domain Group under the DDNS folder, an interval can be specified which defines how often the assignment of username and IP address of the currently connected Client should be updated and resent to the DNS server. Through the update of the name or address resolution, deletion of the name or

address resolution by the DNS server can be compensated for by the choice of a suitable interval. The interval is entered in seconds. If an interval of 0 seconds is entered, updates are not performed.

The "Lease Time" defines how long the name resolution for this Domain Group in the VPN, is valid, i.e. the maximum length of time username should be held in the DNS server. The default setting is one day.

Password for a New Administrator

If a new, additional administrator is added to the system via the web interface, a password, the "initial password", must be setup at the same time. After the first login using this "initial password", the new administrator can change the password. The button for resetting the password is therefore not available.

The password for the first administrator - "Administrator" - must still be entered at the first login - this has not changed.

Support for SSL VPN Port Forwarding under MAC OS X

The following start script has been implemented to support Port Forwarding under MAC OS X:

- SSH Client Session (for Windows, Linux and Mac)
- Remote Desktop Client (for Windows and Mac)

Extended SSL VPN Support for Mobile Enduser Devices

In future, the following platforms will support access to company internal web applications, e.g. the Intranet, via SSL VPN using the default web browser of the platform:

- Apple iOS (iPhone, iPad)
- Google Android
- Microsoft Windows Phone or Mobile 7
- RIM Blackberry (from Blackberry 6)

VPN via L2TP over IPsec for Android and IPsec for Apple iOS

The VPN gateway allows connections to be established, via L2TP over IPsec, from enduser devices based on Android. I.e. every Android based device can establish a connection with the VPN gateway using the default, pre-installed VPN Client. This also applies to iOS devices from Apple, using the pre-installed VPN IPsec Client.

Improved Web Proxy Functionality

The Web Proxy functionality has been completely rewritten and now supports more functions and web sites and considerably increases the compatibility of web application access via SSL VPN.

Preventing Cross Site Scripting

A Cross Site Scripting weakness in the web interface and SSL VPN has been corrected. Cross Site Scripting by entering Java Script elements in the configuration field of the web interface and SSL VPN is now inhibited.

Restriction of the Cipher Suite

In order to improve security only the following cipher suites are allowed for SSL encryption for access to the configuration web interface: AES256-SHA / DES-CBC3-SHA / AES128-SHA .

Therefore the access to the web interface using Internet Explorer version < 7 is no longer supported. Other common browsers (e.g. Firefox) are not affected by this change.

2. Problems Resolved

- None

3. Known Issues

- None

4. Getting Help for the NCP Secure Enterprise 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.html>

For further assistance with the NCP Secure Enterprise Server, visit:
<http://www.ncp-e.com/en/about-us/contact.html>

Mail: helpdesk@ncp-e.com

5. Revision History

Features of the previous release 8.03:

Operating Systems and Hardware

32 bit Operating Systems

- Windows 2003 Server, Windows 2003 R2, Windows Server 2008
- Linux Kernel from 2.6.16 (distributions on request).

64 bit Operating Systems

- Windows Server 2008, Windows Server 2008 R2

Recommended System Requirements

Computer CPU:

- Pentium III (or higher) 150 MHz or comparable x86 processor, 512 MB RAM (minimum), per 250 concurrently useable tunnels 64 MB RAM.

Clock speed:

- Data throughput of app. 4,5 mbit/s can be realized for each 150 MHz with a Single Core CPU (including encryption)
- Data throughput of app. 9 mbit/s can be realized for each 150 MHz with a Dual/Quad Core CPU (including encryption).

System Requirements for Concurrent SSL VPN Sessions

10 Concurrent Users (CU)

- CPU: Intel Pentium III 700 MHz or comparable x86 processor, 512 MB RAM

50 Concurrent Users

- CPU: Intel Pentium III 1.5 MHz or comparable x86 processor, 512 MB RAM

100 Concurrent Users

- CPU: Intel Dual Core 1.83 GHz or comparable x86 processor, 1024 MB RAM

200 Concurrent Users

- CPU: Intel Dual Core 2.66 GHz or comparable x86 processor, 1024 MB RAM

Depends on the type of end-device. Mobile end-devices such as Tablet PCs (using iOS or Android), Smartphones, PDAs and others have some restrictions.

The specified values are approximate values that are significantly influenced by user behavior or the applications. If you anticipate many concurrent file transfers (file upload and download) then we recommend increasing the memory value by 50%.

Network Protocols

IP (Internet Protocol), VLAN support

Management

The NCP Secure Enterprise VPN Server is configured and managed either via an NCP Secure Enterprise Management using the Secure Server plug-in or directly via the Web Interface.

Network Access Control (Endpoint Security)

- Endpoint Policy Enforcement for incoming data connections.
- Verification of predefined, security relevant Client parameters.

- Measures in the event of target/actual deviation in IPsec VPN:
 - Disconnect or continue in the quarantine zone with instructions for action
 - Message in Messagebox or start of external applications (e.g. virus scanner update),
- Logging in Logfiles (see the Secure Enterprise Management data sheet for more information).
- Measures in the event of target/actual deviation in SSL VPN:
 - Granular reduction in access authorization to certain applications in accordance with defined security levels.

Dynamic DNS (DynDNS)

- Connection establishment via Internet with dynamic IP addresses.
- Registration of each current IP address with an external Dynamic DNS provider. In this case the VPN tunnel is established via name assignment (prerequisite: The VPN client must support DNS resolution - NCP Secure Clients support this functionality)

DDNS

- Extension of the Domain Name Server (DNS), reachability of the VPN client under a (permanent) name despite a varying IP address

Multi Company Support

- Group capability, support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth limitation, etc.)

User Administration

- Local user administration (up to 750 users),
- External authentication via
 - OPT server,
 - RADIUS,
 - LDAP,
 - Novell NDS,
 - MS Active Directory Services

Statistics and Logging

- Detailed statistics,
- Logging functionality,
- Sending SYSLOG messages

Client/User Authentication Process

- OTP token,
- User and hardware certificates (IPsec) according to X.509 v.3,
- User name and password (XAUTH)

Certificates (X.509 v.3)

Server Certificates

- Certificates can be used that are provided via the following interfaces:
 - PKCS#11 interface for encryption tokens (USB and smart cards);
 - PKCS#12 interface for private keys in soft certificates

Revocation Lists

Revocation:

- EPRL (End-entity Public-key Certificate Revocation List, formerly CRL),
- CARL (Certification Authority Revocation List, formerly ARL)

Online check

Automatic download of revocation lists from the CA at predefined intervals.

Online check: Checking certificates via OCSP or OCSP relative to the CA over http

IPsec VPN and SSL VPN – Connections

Transmission media

- LAN
- Direct operation on the WAN: Support of max. 120 ISDN B-channels (So, S)

Line management

- DPD with configurable time interval
- Short Hold Mode
- Channel bundling (dynamic in ISDN) with freely configurable threshold value
- Timeout (controlled by time and charges)

Point-to-Point protocols

- PPP over ISDN,
- PPP over GSM,
- PPP over PSTN,
- PPP over Ethernet,
- LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Pool address management

Reservation of an IP address from a pool within a defined period (lease time)

Trigger call

Direct dial of the distributed VPN gateway via ISDN, "knocking in the D-channel"

Virtual Private Networking with IPsec

Virtual Private Networking

- IPsec (Layer 3 tunneling), RFC-conformant
- MTU size fragmentation and reassembly
- DPD (Dead Peer Detection)
- NAT-Traversal (NAT-T)
- IPsec modes: Tunnel Mode, Transport Mode
- Seamless Rekeying; PFS.

Internet Society RFCs and Drafts

- RFC 2401 –2409 (IPsec)
- RFC 3947 (NAT-T negotiations)
- RFC 3948 (UDP encapsulation)
- IP Security Architecture
- ESP
- ISAKMP/Oakley
- IKE
- XAUTH
- IKECFG

- DPD
- NAT Traversal (NAT-T)
- UDP encapsulation
- IPCOMP

Encryption

Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits;
Dynamic processes for key exchange: RSA to 4096 bits; Diffie-Hellman Groups 1,2,5,14;
Hash algorithm: MD5, SHA1, SHA 256, SHA 384, SHA 512

Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Port filtering
- LAN adapter protection

VPN Path Finder

NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible.

Authentication Processes

- IKE (Aggressive and Main Mode), Quick Mode
- XAUTH for extended user authentication
- Support for certificates in a PKI: Soft certificates, smart cards, and USB tokens: Pre-shared keys
- One-time passwords, and challenge response systems
- RSA SecurID ready.

IP Address Allocation

- DHCP (Dynamic Host Control Protocol) over IPsec;
- DNS: Selection of the central gateway with changing public IP address by querying the IP address via a DNS server;
- IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP).

Data Compression

- IPCOMP (lzs), Deflate

SSL VPN

Protocols

- SSLv1,
- SSLv2,
- TLSv1 (Application Layer Tunneling)

Web Proxy

Access to internal web applications and Microsoft network drives via a web interface. Prerequisites for the end device: SSL-capable web browser with Java Script functionality

Secure Remote File Access*

Upload and download, creating and deleting directories, approximately corresponds to the functionalities of the File Explorer under Windows. Prerequisites for the end device: See Web Proxy

Port Forwarding

Access to client/server applications (TCP/IP)

Prerequisites for the end device:

- SSL-capable web-browser with Java Script functionality,
- Java Runtime Environment (\geq V5.0) or ActiveX,
- SSL Thin Client for Windows 7 (32/64 bit), Windows Vista (32/64 bit), Windows XP (32/64 bit) and Linux

PortableLAN

Transparent access to corporate network

Prerequisites for the end device:

- SSL-capable web-browser with Java Script functionality,
- Java Runtime Environment (\geq V5.0) or ActiveX control,
- PortableLAN Client for Windows 7 (32/64 bit), Windows Vista (32/64 bit), Windows XP (32/64 bit)

Cache Protection

Required when using Internet Explorers. All transmitted data on the end device will be deleted automatically after the connection is disconnected.

Prerequisites for the end device:

- Java Runtime Environment (\geq V5.0),
- SSL Thin Client for Windows 7 (32/64 bit), Windows Vista (32/64 bit), Windows XP (32/64 bit)