General description

NCP Secure Enterprise Management is the central component for holistic remote access VPN solutions with integrated RADIUS server and certificate management. As single point of administration it creates the requisite transparency for network administrators to centrally manage mobile and stationary teleworkstations, as well as remote VPN gateways (such as those in branch office networks). The NCP software tool offers all functionalities and automation mechanisms that are required for commissioning and operation of a remote access project.

Fig 1: NCP Secure Enterprise Management – central component of holistic remote access VPN solution

Highlights

- Endpoint Security – comprehensive end device protection and central check
- Minimization of effort for mass rollouts and operation of remote systems
- Central issuing and management of certificates
- Minimization of operating costs (TCO - Total Cost of Ownership)
- Consistent transparency for the administrator thanks to extensive system monitoring
- Risk of incorrect configurations and incorrect operation is minimized
- High-availability (backup) and avoidance of redundant data storage
- High scalability (planning security)
- Integration in existing VPN infrastructures (investment protection)
- Integrated RADIUS Server
Features

NCP Secure Enterprise Management consists of the Management Server and the Management Console. The Management Server is a database-based system and it corresponds with virtually any database via ODBC (e.g. Oracle, MySQL, MS SQL, MS Access, MaxDB). The Management Console is used as front end to call user data or configurations, and to save certificates. All relevant information is stored in the database and is usually integrated in VPN operator’s backup process. Multi-company support makes Secure Enterprise Management a natural choice for implementation at Managed Security Service Providers (MSSP), in so-called “managed VPNs”, or in remote access structures, where multiple companies jointly use one VPN platform (VPN sharing).

Fig. 2: Overview – central management functionalities

In all of these cases administrators of legally autonomous companies must have the capability to manage their “shared” VPN. This is done by forming groups and using a convenient method of assigning rights. Administrators are created in such a manner that each has exclusive access to his area, in other words to the units that he is responsible for managing. The possibility of encroaching on data of other clients in their protected areas is excluded.

The automatic update process enables the administrator to provision software updates centrally for all remote systems, which will be installed automatically the next time the connected to the VPN. If malfunctions occur during the transmission, then the previously existing software version, as well as the configuration, remain unaffected. The software is only updated after complete error-free transmission of all predefined files. All data are transmitted in a highly secure manner, (encrypted in the VPN tunnel).

An integrated RADIUS server is used to store and manage all client link profiles.

The Software Update Service also organizes central distribution of all parameters that are relevant for remote access, such as:
- Configurations (telephone books)
- Software (updates, upgrades)
- Soft certificates (PKCS#12 files) as user or machine certificate
Optionaly the Backup Management Server ensures high-availability of the Management Server, which always has the current data repository available through an integrated replication service.

Fig. 3 Components and functionalities of a managed VPN

All relevant data can be input or transferred interactively via the NCP Management Console, or it can be input or transferred in script-driven processes; i.e. user data, license keys, provider passwords, can be transferred to the Management Server per remote system (= managed unit), e.g. for a rollout. The NCP Secure Enterprise Server, or a server supplied by any manufacturer (see the compatibility list at www.ncp.de) can be implemented as VPN gateway. Secure Enterprise Management can thus be integrated within any existing IT infrastructure and it enables operation even in complex VPN environments.

Another essential feature of the Management Server is license administration of the managed units. All licenses are transferred into a pool and are automatically managed in accordance with specified guidelines. Functional examples:

- Transfer in a configuration per remote client or gateway
- Take-back when an employee leaves a company
- Message in the event that no more licenses are available.

**Management Console**

The Management Console provides powerful plug-ins for configuration and management of the managed units:

- Client Configuration
- System Monitor
- Client Firewall Configuration
- Remote Server Configuration
- Endpoint Policy Enforcement
- PKI enrollment
- RADIUS
**Client Configuration Plug-In**

This plug-in enables configuration and administration of NCP Secure Enterprise Clients. All relevant parameters are predefined and stored in templates. An overview of the specific features:

- Assignment of licenses (serial numbers / activation key)
- Assignment of authentication codes for first connections during the rollout
- Creation and administration of user profiles (telephone book entries)
- Individual menu items and configuration values can be set as “not visible” or “not changeable” for the user.
- Automated configuration of the user profiles for central components (RADIUS, LDAP, SNMP)
- Pre-setting the Personal Firewall; it cannot be manipulated by the remote user
- Extensive logging (versions, time stamps for configuration changes, automatic upload of client log files...)
- VPN profile presets

**System Monitor Plug-In**

This plug-in provides fast information about all important events within a VPN installation, in the form of bargraphs or line diagrams. The administrator can use the system monitor as needed to call up current status information in real time, or to access previously saved data repositories of the remote access environment.

![System Monitor Graphical Interface](image)

**Displays:**

1. **Status information**
   
   The following events can be displayed on a group basis:
   - System restarts
   - Administrator logons (e.g. successful, rejected)
   - Client update logons (e.g. successful, rejected)
   - Software downloads per package
   - RADIUS logons (e.g. successful, rejected)
   
   Ratio displays of two events is possible.
2. History

Display of all events within a certain period:
- Hour, last hour, or the last 2, 3, 4, 6, 12, or 24 hours
- Day; the last 2 or 4 days
- Week; the last week
- Month; last month or month before last
- Current day, current week, current month

Page forward, page back in the respective period in the displayed diagram Colors and views of the diagrams can be freely selected.

**Client Firewall Configuration Plug-In**

The NCP Secure Client software has an integrated Personal Firewall, which can be managed centrally for the enterprise versions. The Client Firewall Configuration plug-in enables granular adjustment of firewall rules per teleworkstation.

The following configuration parameters can be set:
- Application-independent and connection-independent filter rules
- Filter rules based on protocol, port and address
- Specifications for detection of “friendly networks” (IP address network, network mask, IP address of the DHCP server, MAC address)
- Logging settings
- Central specification of the user’s possibilities to access the firewall configuration.
- FND configuration (Friendly Net Detection)

**Remote Server Configuration Plug-In**

This plug-in enables configuration and administration of decentralized NCP Secure Enterprise Gateways. Analogous to the Client Configuration plug-in, general templates are created, which are used as the basis for individual VPN gateway configurations. In holistic remote access VPN solutions, the issue is managing individual teleworkstations, as well as geographically distributed VPN gateways. The following parameter groups can be predefined or configured:

- Link profiles
- IKE and IPSec policies
- Routing information
- Creating certificates (machine certificates)
- License and version management

**PKI Enrollment Plug-In**

This function module is the connecting link between a Public Key Infrastructure (PKI) and the remote access VPN environment. The PKI Enrollment plug-in functions as Registration Authority (RA) and manages the creation as well as the administration of electronic certificates (X.509 v3) in conjunction with different Certification Authorities (CA). Supported CAs: T-Telesec NetPass, Microsoft, NCP Demo CA, others (e.g. RSA Keon) are possible via CMP (Certificate Management Protocol) A generated certificate can optionally be stored as soft certificate (PKCS#12) or on hardware, e.g. smart card or USB token (PKCS#12). The NCP Demo CA that ships with the product can be used to simulate a PKI during the test phase, however it is not intended for productive implementation. Conversion to an external CA is problem-free.

The most important functionalities:

- Creation of certificates (also bulk mode)
- Extension of certificates (PKCS#7)
- Blocking certificates
- Distributing certificates via the NCP Secure Management Server
Creating the user configuration via LDAP in the directory service
Creating a PAC (Personal Authentication Code) letter for the initial connection (initialization, licensing)

**Endpoint Policy Enforcement Plug-In (endpoint security)**

Use this plug-in to define all security-relevant parameters that must be checked prior to an access to the corporate network. Compliance with the specified security policies is mandatory and cannot be bypassed or manipulated by the user.

The system can check for the following client parameters:
- Operating system information e.g. version, hot fix status
- Secure Enterprise Client software version
- Services information
- File information
- Status of a virus scanner
- Contents of certain registry values
- Contents of certificates (user and hardware certificate)

Deviations from the target specifications are logged and can trigger different messages or actions, such as:
- Message display on the client
- Outputting a message in the monitor log
- Sending a message to the Management Server
- Sending a message to a Syslog server
- Release of all firewall rules or of a certain firewall rule
- VPN connection disconnect

**RADIUS Plug-In**

The RADIUS interface is optionally available for configuration of managed units (users) in the central VPN gateway.

This plug-in is used to manage the integrated RADIUS server and it is responsible for the following functions:
- Automatic creation of RADIUS accounts via the client and remote server configuration plugins
- Support of PAP/CHAP requests
- Capture of accounting data
- Blocking users if there are repeated incorrect logon attempts
- Management of multiple RADIUS configurations of various gateways
- RSA Authentication Manager proxy functionality

Optionally: Redundancy through backup RADIUS servers

Advantage: Existing RADIUS servers can be combined, i.e. they can be replaced in an economical manner.
Technical data:

**Current version:**
V 1.03

Supported functionalities / available plug-ins:
Automatic Update, License Management, Remote Service Configuration, Client Firewall Configuration, Client Configuration, RADIUS.

Version-version prerequisites for managed units:
- Secure Enterprise Client as of V 7.2
- Secure Enterprise Gateway as of V 6.09

**Scope of delivery:**
Management Server
Management Console (with all available plug-in's)
(Database system is not included in the scope of delivery)

Options:
- Managed Units
- Secure Enterprise Management Server Backup

**System requirements:**
- Operating systems:

Additional information for Management Servers:
- 512 MB RAM
- CPU at least Pentium III-800 MHz (depending on the number of managed units)
  With RADIUS plug-In: Pentium IV-1.5 GHz
- Hard disk: At least 50 MB free disk capacity plus disk capacity for log files and app. 20 MB per software package

**Supported databases:**
Oracle as of version 9.0
MySQL as of version 4.0
Microsoft SQL Server as of SQL Server 2000

**Supported Certification Authorities**
Microsoft Certificate Services:
- As "standalone CA": As of Windows 2000 Server
- As "integrated CA in the domain":
  - As of Windows 2000 (certificate templates cannot be adapted)
  - As of Windows 2003 Enterprise Server
Supported virus scanners:

- Under Windows XP SP2 all virus scanners can be queried that supply their status to the Security Center via WMI (Windows Management Instrumentation) or NAC (Network Admission Control).
- The following are supported under all Windows operating systems:
  - H+B Antivirus: Product version and version of the virus definition file can be determined
  - McAfee: Product version and version of the virus definition file can be determined

Supported RFC's and drafts:

RFC 2138  Remote Authentication Dial In User Service (RADIUS)
RFC 2139  RADIUS Accounting
RFC 2433  Microsoft CHAP
RFC 2759  Microsoft CHAP V2
RFC 2548  Microsoft Vendor-specific RADIUS Attributes
RFC 3579  RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 2716  PPP EAP TLS Authentication Protocol
RFC 2246  The TLS Protocol
RFC 2284  PPP Extensible Authentication Protocol (EAP)
RFC 2716  Certificate Management Protocol
RFC 2511  Certificate Request Message Format
Draft-ietf-pkix-cmp-transport-protocols-04.txt  Transport Protocols for CMP
Draft-ietf-pkix-rfc2511bis-05.txt  Certificate Request Message Format (CRMF)