

NCP Secure Enterprise Management

NCP Secure Enterprise Management (SEM) is the central component for universal 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 VPN project.

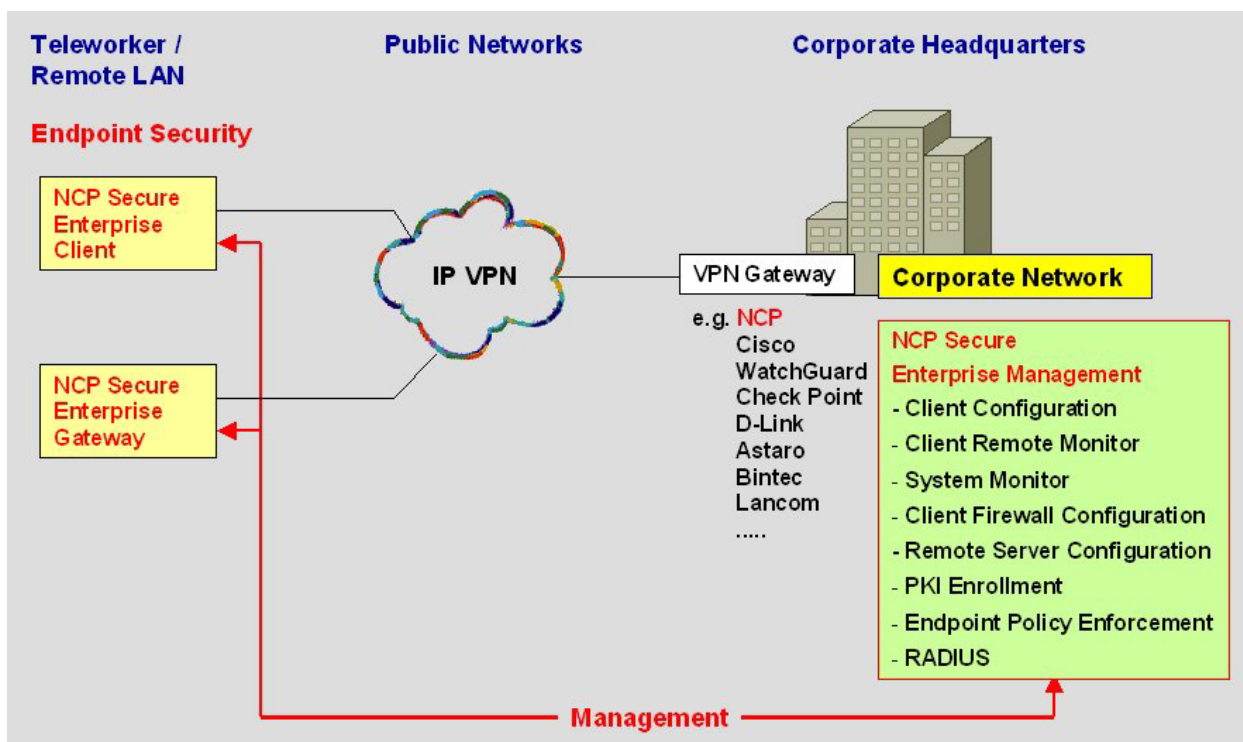
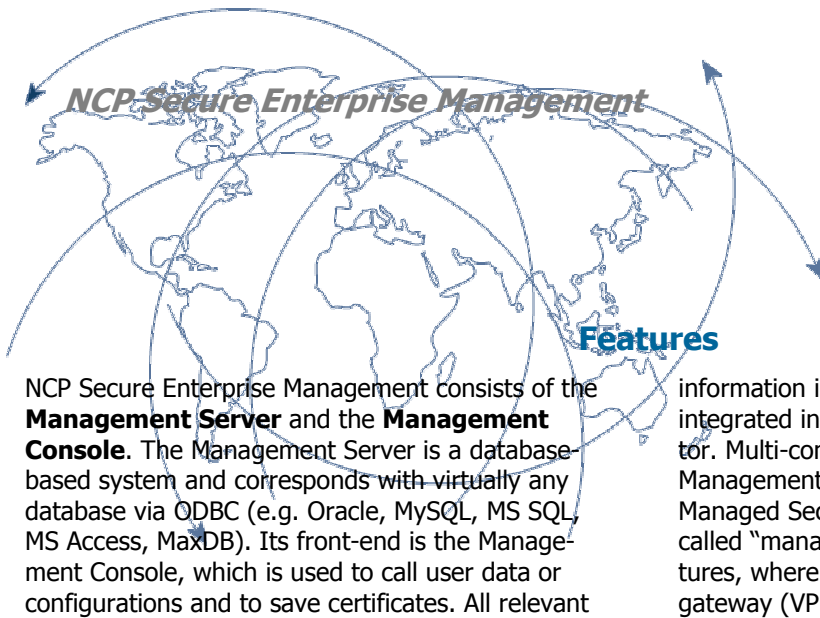


Fig 1: NCP Secure Enterprise Management – central component of the holistic Secure Communications solution

Highlights:

- Endpoint security – comprehensive protection of the end device and central check
- Minimization of effort for software deployment and commissioning of remote systems
- Reduction of total cost of ownership (TCO), i.e. shortest possible term for return on investment (RoI)
- Constant transparency for the administrator through extensive system monitoring
- Risk of incorrect configurations and incorrect operation is minimized
- High availability and avoidance of redundant data storage
- Scalability for planning security
- Integration in existing VPN infrastructures for investment protection



NCP Secure Enterprise Management consists of the **Management Server** and the **Management Console**. The Management Server is a database-based system and corresponds with virtually any database via ODBC (e.g. Oracle, MySQL, MS SQL, MS Access, MaxDB). Its front-end is the Management Console, which is used to call user data or configurations and to save certificates. All relevant

information is stored in the database and is usually integrated in the backup process of the VPN operator. 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 gateway (VPN sharing).

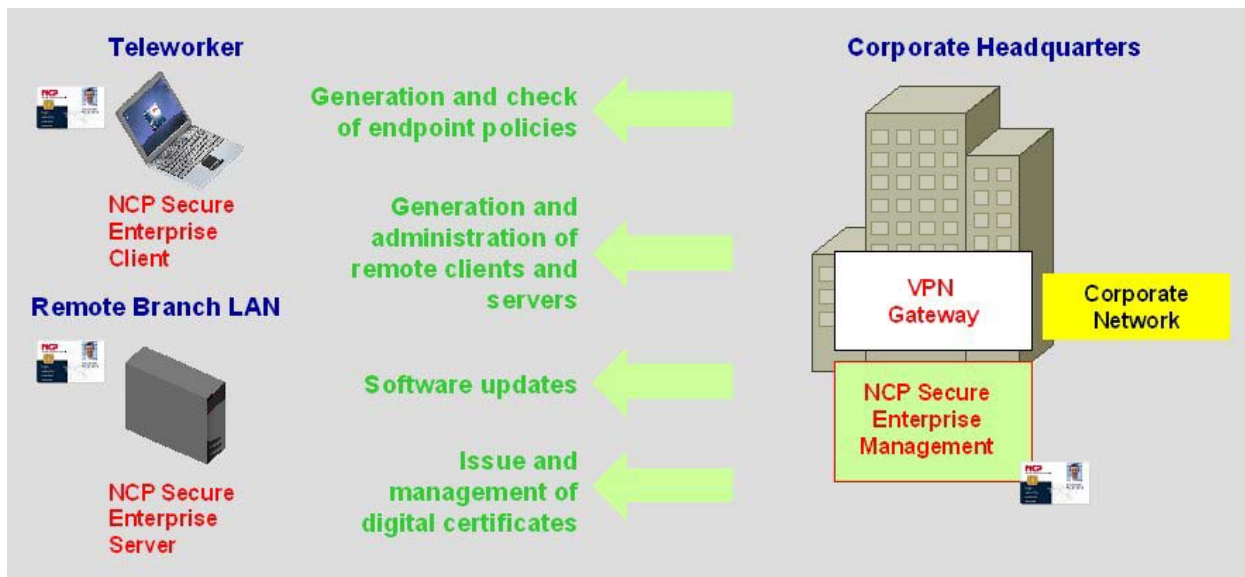


Fig. 2: Overview, central management of remote components

In these cases administrators of legally autonomous companies must have the capability to manage their "shared" VPN. This is done by a convenient method of assigning rights and groups. Each administrator only has access to his area, or in other words to his managed units. It is not possible to access other companies' data.

Remote units are automatically updated in time intervals, which can be set individually. All update files are encrypted and transmitted securely in the VPN tunnel. 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 pre-defined files.

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:

- configurations (profiles),
- software (updates, upgrades),

- soft certificates (PKCS#12 files) as user or machine certificate,
- issuer certificates (root certificates),
- international telephone books (e.g. iPass, MCI, GoRemote, Infonet, Uunet)

Optionally the Backup Management Server ensures high availability of the system, which always has the current data repository through an integrated replication service.

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 deployment. The NCP Secure Enterprise Gateway, or any standard conform IPSec gateway supplied by any manufacturer, can be implemented as VPN gateway (see the compatibility list at www.ncp.de). Secure Enterprise Management can thus be integrated within any existing IT infrastructure and it enables operation even in complex VPN environments.

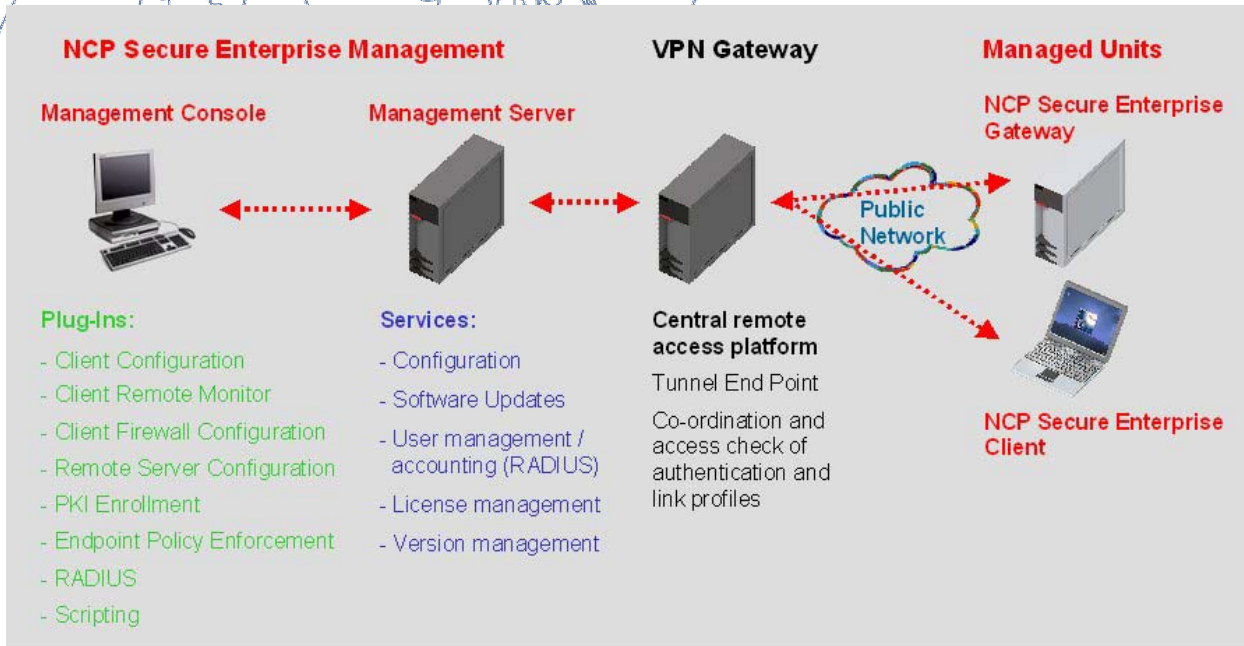


Fig. 3: Components and functionalities of Secure Enterprise Management

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

- transfer in a profile per remote client or gateway,
- take-back when an employee leaves a company,
- message to the admin, if no more licenses are available.

Management Console

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

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

- 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, etc.).

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.

Specific features:

- assignment of licenses (serial number / activation key);
- assignment of authentication codes for first connections during the rollout;
- creation and administration of user profiles;

Client Remote Monitor plug-in

This plug-in monitors the NCP Secure Enterprise Clients (under Windows only). Access on the remote PC can alternatively be executed via TCP/IP, an ISDN, or modem connection via the analog telephone network. Thus, central support is independent of an active VPN connection of the client. Access to the teleworkstation can only occur with the consent of the teleworker, and it is limited to the Client Monitor.

Overview of available information and functionalities:

- versions (e.g. operating systems, client software, ISDN CAPI);
- network adapter properties;
- insight into traces and log files for error analysis;
- displaying the connection states;
- specification of budgets for connection management.

System Monitor plug-in

This plug-in provides quick information about all important events within the monitored virtual private network as bar or line graphs. The administrator can use the System Monitor for calling current status information in real time, as required. He can also access stored data of the remote access environment.

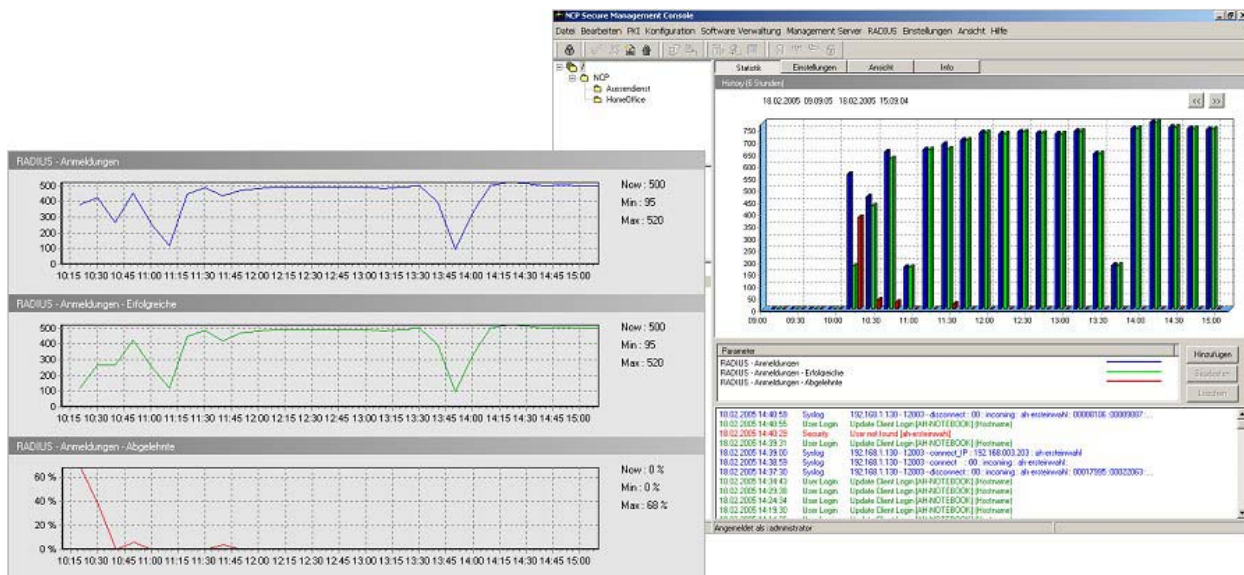


Fig. 4: System Monitor graphical interface

The following status events can be displayed:

- system reboots,
- administrator logons (successful / denied),
- client update logons (successful / denied),
- software downloads per package,
- RADIUS logons (successful / denied).

It is also possible to view the ratio of two events.

The events history can be displayed for a specified period:

- hours: last 1, 2, 3, 4, 6, 12, 24,
- days: last 2 or 4,
- weeks: last 1,
- months: last or penultimate,
- current day, current week, current month

The displayed graph allows to leaf up and down in the specified period. Colors and views can be selected.

Client Firewall Configuration plug-in

The NCP Secure Client software has an integrated Personal Firewall, which can be managed centrally. 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.

Remote Server Configuration plug-in

This plug-in enables configuration and administration of remote NCP Secure Enterprise Gateways. Analogously 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 issue as well as the administration of digital certificates (X.509 v3) in conjunction with different Certification Authorities (CA). Currently the Microsoft CA and T-Telesec NetPass are supported. Other CAs, 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 which comes 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:

- issue of certificates (also bulk mode),
- renewal of certificates (PKCS#7),
- denying 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

All security-relevant parameters are defined in this plug-in. Compliance with the specified security policies is mandatory and checked prior to an access to

the corporate network. It cannot be bypassed or manipulated by the user.

The system can check for the following client parameters:

- operating system information
- 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

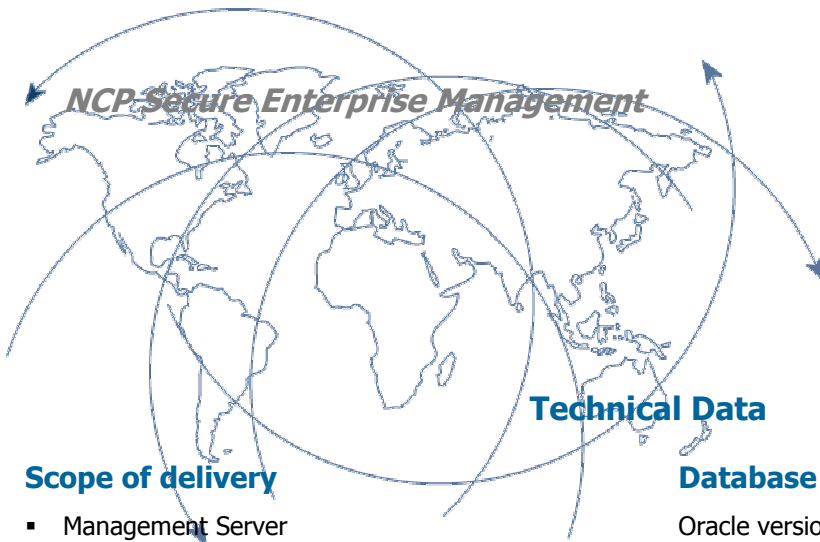
Optionally the RADIUS interface is available for configuration of the managed units in the central VPN gateway.

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 plug-ins,
- 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,

Optional: Redundancy through backup RADIUS server.

Advantage: Previously existing RADIUS servers can be grouped, i.e. they can be replaced in an economical manner.



Scope of delivery

- Management Server
- Management Console (with all plug-ins)

Database system is not included in the scope of delivery.

Options:

- Managed Units
- Management Server Backup
- Secure Enterprise Managed Bundles (consisting of Secure Client, Managed Unit and Managed Backup Unit)

System requirements for Management Server

Operating system:
Windows 2000, XP, 2003 Server, Linux

RAM: 512 MB

CPU: min. 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

System requirements for Management Console

Operating system:
Windows 98SE, 2000, XP, ME, 2003

Version requirements for Managed Units

Secure Enterprise Management supports the following Managed Units:

- NCP Secure Enterprise Client version 7.2 or higher
- Secure Enterprise Gateway version 6.09 or higher

Database specifications

Oracle version 9.0 or higher

MySQL version 4.0 or higher

Microsoft SQL Server version SQL Server 2000 or higher

Microsoft CA specifications

Microsoft Certificate Services are supported

- as "stand alone CA": Windows 2000 Server or higher
- as integrated CA in a domain:
Win 2000 Server (no certificate templates)
Windows 2003 Enterprise Server

Virus scanners

Windows XP SP2:

All virus scanners can be called that send their status to the Microsoft Security Center via Windows Management Instrumentation (WMI).

The following virus scanners are supported under all Windows OS:

- H+B Antivirus
Version number of product and virus definition are checked.
- McAfee
Version number of product and virus definition are checked.

Supported Internet Society RFCs & 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)

Important note on the current version of the Secure Enterprise Management

The current version 1.01 does not yet support all functionalities and plug-ins. The following plug-ins are available:

- Automatic Update
- Client Configuration
- RADIUS

