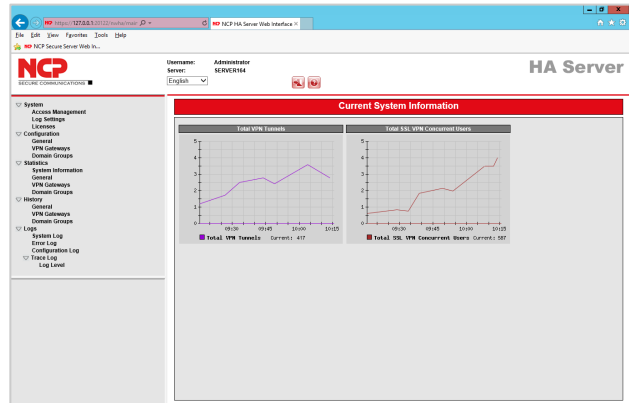# Data Sheet

NCP Secure Enterprise
High Availability Services

Failsafe and load balancing server - High availability and uniform utilization of NCP Secure Enterprise VPN Servers (VPN Gateways)

- Maximum availability of
  NCP Secure Enterprise VPN Server(s)
- Automatic changeover
- All VPN tunnels are available at anytime
- Redundant design (primary failsafe server
  and backup failsafe server)
- Local and remote management

General

NCP Secure Enterprise High Availability Services are components of the holistic NCP Enterprise Solution. They ensure high availability of one or multiple Secure Enterprise VPN Servers and thus high availability of the enterprise's Virtual Private Network. All VPN tunnels are available at all times for data communication with the central data network. Changeover between VPN servers in the event of service or malfunction is automatic. Deployment is as follows depending on the installed number:

- Failsafe Server if number =1
- Load Balancing Server if number >1

Secure Enterprise Failsafe Server

The Failsafe Server is used to ensure sustainable availability of a single Enterprise VPN Server. This is ensured through installation of a backup system in the same configuration as the primary system. The license is included in the standard scope of delivery.

Secure Enterprise Load Balancing Server

For tunnel management extending over multiple Enterprise VPN Servers (server farm) the Load Balancing Server is necessary. It ensures uniform capacity utilization of all available Enterprise Servers, and in the event of service or malfunction it also ensures automatic exclusion of a VPN system from the assignment routine of VPN tunnels for connection requests to the corporate network.

Functionalities

Failsafe Servers as well as Load Balancing Servers react to defective systems. Defective in this regard means that an Enterprise VPN Server no longer responds. The cause could be due to defective hardware (power supply, LAN adapter, motherboard, etc.) operating system error messages, program crashes, or interruptions in the connection to the Failsafe Server or Load Balancing Server. For example, a cause could be shutting down an Enterprise VPN Server for service reasons. In all cases the load is either routed to the backup system or uniformly distributed to the remaining systems. For security reasons both Failsafe as well as Load Balancing Servers are configured redundantly and require a separate IP address. There are several points to bear in mind when assigning permanent, private IP addresses per client*. The system is configured via the Enterprise High Availability Manager (included in the standard scope of delivery).

The Enterprise High Availability Manager can be set up on any console computer in the LAN.

Management

Configure and manage NCP's Secure Enterprise High Availability Services via NCP's Secure Enterprise Management or a web interface.

*) See page 2 "Technical data" instructions

Operating systems

Failsafe and Load Balancing Server	64-Bit: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 Linux Kernel as of version 2.6.16 (distributions on request) Debian GNU/Linux 10.7, Red Hat Enterprise Linux Release 8.2, SUSE Linux Enterprise Server 15.2

Performance range and functionalities

Fault Tolerance	Fault tolerant, redundant system
Load balancing	Dynamic load distribution through analysis of the following function parameters: Number of existing connections, availability of the system, current data throughput and CPU load Number of manageable Enterprise VPN Servers: any number
Redundancy	Failsafe and Load Balancing Servers are designed as primary and backup servers
DEVP	Dynamic VPN Endpoint Protocol for management of the Secure Enterprise VPN Servers
Operating modes	Integrated in the NCP Secure Enterprise VPN Server or dedicated in separate PC hardware
Management	Local and remote via web interface or SEM*
Load Balancing scenario	The Secure Enterprise VPN Servers to be managed can be installed locally and/or at different geographical locations, such as branch offices

Scope of delivery

Failsafe Server	License for primary and backup Failsafe Servers, High Availability Manager, License for VPN Server Backup
Load Balancing Server	License for primary and backup Load Balancing Server
Options	Upgrade for additional tunnels

Instructions

Extending the number of tunnels	The number of tunnels of the Failsafe or Load Balancing Server must correspond to the number of all installed Secure Enterprise VPN Servers (VPN Gateways)
IP addresses	You will find additional information in the manual about "Permanent and dynamic IP addresses in Remote Access VPNs"

*) Secure Enterprise Management (optional)