Communication Industries

HPCI

invent

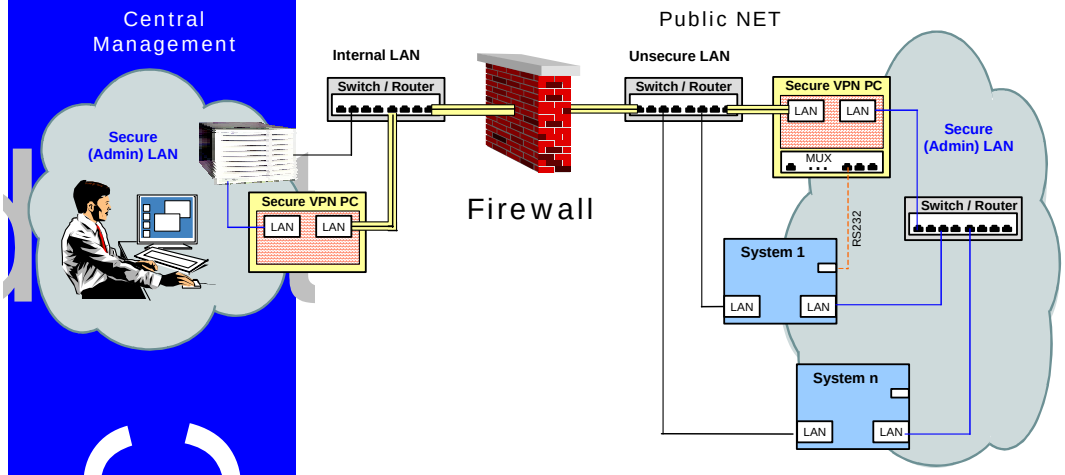
Secure Virtual Private Network

Secure Communication Infrastructure

Management of systems within external networks requires a concept with high security demand, that means encoded data transfer between management server and external systems as well as a minimal opening of the firewall-interface. The implementation of Secure Virtual Private Networks (S-VPN) considers the security aspects mentioned above and offers a tansparent, secure communication infrastructure for any management service.

Transparent Management with HP OpenView

(IT/O-) Communication between external agents and the management server will only take place via the Secure Virtual Private Network (S-VPN), this will be build and monitored by the S-VPN PC that is within the internal network. All data transfer between the S-VPN PC's (yellow in the picture) will be carried out encoded through only one port of the firewall. The implementation of the S-VPN is transparent for the user / the management-application; future (agent-) systems may be integrated easily to the S-VPN by corresponding routing-entries. For a secure access to systems at other locations, the communication infrastructure is modularly extendable by using further S-VPN PCs.



In case, that no separate admin-LAN is available within the public-NET for a secure transfer of the management-information, they may be routed from the external S-VPN PC (not-encoded) via the public-NET to the agents. In this case, an encoding of the (IT/O) communication within the public-NET is possible with the help of an additional product called "HP OpenView Advanced Network Security for IT/O".

S-VPN characteristics

- Transparent access to any system beyond a firewall through an encoded connection using only one port in the firewall
- Use of a SSH-protocol secured PPP-connection as communication infrastructure between internal (secure) and external (insecure) networks
- High security by using 1024 bit keys for authentification and 168 bit (configurable) for encoding the data to be transferred
- Independent monitoring of the communication connections (if necessary with new set-up) through the internal S-VPN; implementation of firewall-rules to protect the S-VPN PCs
- Robust solution architecture by using pre-configured PC's with Linux-operating system, RAM-disc and autoboot-functionality (operating system and software) via CD-ROM; configuration data is saved non-volatile on disc
- Supports (optional) secure communication links via the public ISDN
- Supports (optional) direct access of RS232-console-ports via encoded (LAN-/WAN-) connection
- Simple, transparent integration into (existing) management-environments with HP OpenView IT/Operations

Secure Virtual Private Network

Implementation as a project

Implementation of security-relevant hard- and software within an enterprise-infrastructure always requires an individual, customer-specific configuration of the components in question.

A detailled system documentation and the introduction of the people responsible for the systems into the functionality and configuration of the implemented solution are the basis for a stable production.

The implementation of the S-VPN functionality – optional with the Secure Remote Console function –will take place considering the above mentioned success factors as a ready-to-use (fixed price) project.

Contact

Hewlett-Packard GmbH
HP-Consulting
Frank Freihoff
Phone: +49 6172 / 16-1704
e-Mail: frank_freihoff@hp.com

Hewlett-Packard GmbH 08/2000
HP Consulting

Service Volume of S-VPN:

- Delivery and installation of the required hardware-components (S-VPN PCs)
- Delivery and installation of the bootable operating system-/software CD (and configuration disc) for the RAM-based Linux S-VPN operating system
- Configuration of the network-parameters, creation and distribution of the security-keys for authentification and configuration of the firewall-rules onto the S-VPN PCs
- Actualization of the configuration disc and creation of a back-up disc (disaster recovery)
- Functional test of the customer-specific implementation
- Creation of project documentation and introduction into the functionality and configuration of the S-VPN solution

Optional: (Secure Remote Console Function)

- Delivery / installation of multiplexer and (adapter-) cables for the RS232-connection
- Installation of security software and configuration data at the client systems
- Configuration of the user-specific system-allocation, parametrication of the scripts for building the terminal-windows as well as creation and distribution of the security-key onto the client-systems
- Creation and distribution of the security-keys and configuration of the user-authorization on the S-VPN PC
- Functional test of the customer-specific implementation (client-access, serial-access)
- Extension of the project documentation and introduction to the operation and configuration of Secure Remote Console Function