Communication Industries

HP OpenView

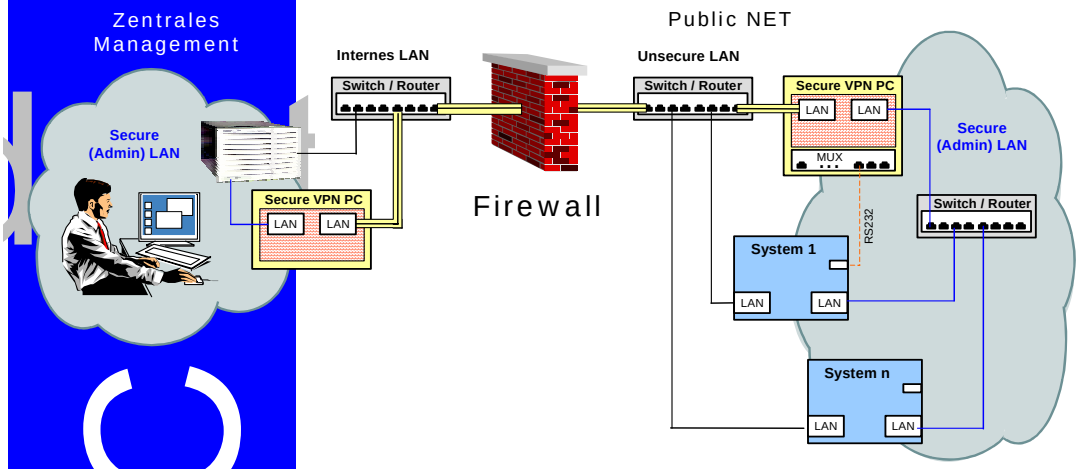
Secure Virtual Private Network

Sicherere Kommunikationsinfrastruktur

Das Management von Systemen in externen Netzbereichen setzt ein Konzept mit hohen Sicherheitsanforderungen, d.h. verschlüsselter Datenübertragung zwischen dem Managementserver und den externen Systemen sowie einer minimalen Öffnung der zwischengeschalteten Firewall voraus. Die Implementierung eines Secure Virtual Private Networks (S-VPN) berücksichtigt die vorgenannten Sicherheitsaspekte und bietet eine transparente, sichere Kommunikationsinfrastruktur für beliebige Managementdienste.

Transparentes Management mit HP OpenView

Die (IT/O-) Kommunikation zwischen den externen Agenten und dem Managementserver erfolgt ausschließlich über das Secure Virtual Private Network (S-VPN), welches von dem im Internen Netz befindlichen S-VPN PC aufgebaut und überwacht wird. Der komplette Datentransfer zwischen den S-VPN PCs (im Bild gelb dargestellt) erfolgt verschlüsselt über nur einen Port der Firewall. Die Implementierung des S-VPN ist für den Benutzer / die Management-Applikation transparent, zukünftige (Agenten-) Systeme können durch entsprechende Routing-Einträge einfach in das S-VPN integriert werden. Die Kommunikationsinfrastruktur ist, durch Einsatz weiterer S-VPN PCs -für den sicheren Zugriff auf Systeme an anderen Standorten-, modular erweiterbar.



Für den Fall, daß im Public-NET kein separates Admin-LAN zur sicheren Übertragung der Management-Informationen zur Verfügung steht können diese vom externen S-VPN PC (unverschlüsselt) über das Public-NET zu den Agenten geroutet werden. Eine Verschlüsselung der (IT/O-) Kommunikation im Public-NET kann in diesem Fall mit Hilfe des zusätzlichen Produkts "HP-OpenView-Advanced Network Security for IT/O“ erfolgen.

S-VPN Eigenschaften

- Transparenter Zugriff auf beliebige Systeme jenseits einer Firewall über eine verschlüsselte Verbindung bei Verwendung nur eines Ports in der Firewall
- Nutzung einer über das SSH-Protokoll gesicherten PPP-Verbindung als Kommunikationsinfrastruktur zwischen den internen (sicheren) und externen (unsicheren) Netzbereichen
- Hohe Sicherheit durch Verwendung von 1024 Bit Schlüssel zur Authentifizierung und 168 Bit (konfigurierbar) zur Verschlüsselung des Datentransfers
- Selbstständige Überwachung der Kommunikationsverbindungen (ggf. mit Neuaufbau) durch den internen S-VPN PC; Implementierung von Firewallregeln zum Schutz der S-VPN PCs
- Robuste Lösungsarchitektur durch Einsatz vorkonfigurierter PCs mit Linux-Betriebssystem, RAM-Disk und Autoboot-Funktion (Betriebssystem und Software) via CD-ROM; Konfigurationsdaten sind nicht-flüchtig auf Diskette gespeichert
- Unterstützt (optional) sichere Kommunikationsverbindungen über das öffentliche ISDN
- Unterstützt (optional) die direkte Anbindung von RS232-Systemkonsolenports (Secure Remote Console Funktion)
- Einfache, transparente Integration in (bestehende) Managementumgebungen mit HP OpenView IT/Operations)

Secure Virtual Private Network

Implementierung als Projekt

Die Implementierung sicherheitsrelevanter Hard- und Software innerhalb einer Unternehmensinfrastruktur erfordert immer eine individuelle, kundenspezifische Konfiguration der betroffenen Komponenten.

Eine detaillierte Systemdokumentation und die Einweisung der Systemverantwortlichen in die Funktionsweise und Konfiguration der eingesetzten Lösung bilden die Grundlage für einen stabilen Wirkbetrieb.

Die Implementierung der S-VPN Funktionalität -optional mit Secure Remote Consolen Funktion- erfolgt, unter Berücksichtigung der oben genannten Erfolgsfaktoren, schlüsselfertig als (Festpreis-) Projekt.

Ansprechpartner

Hewlett-Packard GmbH
HP-Consulting
Frank Freihoff
Telefon: 06172 / 16-1704
e-Mail: frank_freihoff@hp.com

Hewlett-Packard GmbH 08/2000
HP Consulting

Leistungsumfang S-VPN:

- Lieferung und Installation der erforderlichen Hardwarekomponenten (S-VPN PCs)
- Lieferung und Installation der bootbaren Betriebssystem-/Software-CD (und Konfigurationsdiskette) für das RAM-basierende Linux S-VPN Betriebssystem.
- Konfiguration der Netzwerkparameter, Erzeugung und Verteilung der Security-Keys zur Authentifizierung sowie Konfiguration der Firewall-Regeln auf den S-VPN PCs.
- Aktualisierung der Konfigurationsdiskette und Erstellung einer Backup-Diskette (Desaster Recovery).
- Funktionstest der kundenspezifischen Implementierung.
- Erstellung einer Projektdokumentation sowie Einweisung in Funktionsweise und Konfiguration der S-VPN Lösung.

Optional: (Secure Remote Console Funktion)

- Lieferung / Installation von Multiplexer und (Adapter-) Kabeln für den RS232-Anschluß.
- Installation der Security-Software und Konfigurationsdateien auf den Client-Systemen.
- Konfiguration der User-spezifischen Systemzuordnung, Parametrisierung der Scripts zum Aufbau der Terminalfenster sowie Erzeugung und Verteilung des Security-Keys auf den Client-Systemen.
- Erzeugung und Verteilung der Security-Keys sowie Konfiguration der User-Autorisierung auf dem S-VPN PC.
- Funktionstest der kundenspezifischen Implementierung (Client-Zugriff, serieller Zugriff).
- Erweiterung der Projektdokumentation und Einweisung in die Bedienung und Konfiguration der Secure Remote Console Funktion.