VSS-01 VPN-Security-Server

In der Internet-Fernwartung wird es immer wichtiger, nicht nur einzelne IP-Adressen „remote“ anzusprechen, sondern ganze IP-Subnetze fernzuwarten. Der VSS-01 löst diese Aufgabe vollständig autark.

Komplettlösung ohne externe Datendienste, da diese immer auch die UnterbrechungdesVPNSchutzesbedeuten. Intern besteht der VSS-01 aus einem konfigurierbaren OpenVPN-Server, der auf einem Schaltschrank-tauglichen 19“-Linux-Server läuft. Über OpenVPN lassen sich bis zu 2.000 VPN-Tunnel aufbauen. Die Fernwartungs-Subnets werden durch spezielle Router realisiert, die Fernwartungs-PCs sind übliche WIN-XP, WIN7 oder Linux PCs. Alle Endgeräte arbeiten als OpenVPN-Clients am VSS-01.

- **Zentrale Verwaltung von mehr als 1.000 Endpunkten**
- **Sichere, verschlüsselte Datenübertragung in einer geschlossenen Benutzergruppe**
- **Integration von IP-Routing und Firewall-Funktionalitäten**
- **Transparente Datenübertragung mit VPN über Routing oder Bridging**
- **Skalierbar in Größen von 50 / 100 / 500 oder größer 1.000 Anwendern/Subnets**
- **Automatische Sicherung der Konfiguration auf einen externen FTP-Server und Redundanz per Hot Standby**
- **Einfaches Webbasierendes Konfigurations-interface**
- **Überwachung per SNMP**

VSS-01 VPN-Security-Server

Funktionen	• Zentrale Verwaltung von mehr als 1.000 Endpunkten • Erstellen und Verwalten von Zertifikaten • Sichere, verschlüsselte Datenübertragung in einer geschlossenen Benutzergruppe • Integration von IP-Routing und Firewall-Funktionalitäten • Transparente Datenübertragung mit VPN über Routing (Layer 3) • Nur PC-Client zu einem oder mehreren Endpunkten (Remote-Wartung) • Nur Außenstation/Filiale zur Zentrale/Leitsystem (Filial-Anbindung) • Alle Endpunkte können miteinander kommunizieren, die Rechtezuweisung erfolgt ausschließlich über die Gruppenzuordnung (Fernwirkbetrieb) • Alle Endpunkte können miteinander kommunizieren ohne Einschränkungen (Transparenter Betrieb / Routing) • Transparente Datenübertragung mit VPN über Bridging (Layer 2) • Im Bridging Betrieb (Layer 2) werden alle Daten inklusive Broadcast- und Multicast-Pakete übertragen. • Alle Endpunkte können miteinander kommunizieren, die Rechtezuweisung erfolgt über die Gruppenzuordnung (Switch-Betrieb mit Zugriffsrechten) • Alle Endpunkte können miteinander kommunizieren ohne Einschränkungen (Switch-Betrieb)
Management	• Einfache Bedienung über eine WEB-Oberfläche • Zentrale Übersicht mit entsprechenden Filterregeln über • Systemfunktionen • Anzahl Endpunkte on-/off-line • Liste Endpunkte on-/off-line, mit Detailübersicht • Gruppenliste • Zentrale Verwaltung von • User-Zugriffsrechten • Zugriffsrechten von Endpunkten • Gruppenregeln • Zertifikaten • Mandantenfähig • SNMP v3 • Email-Versand von Alarmmeldungen oder Zertifikaten
Redundanz	• HotStandBy Modus für bis zu 3 Systeme im Verbund im Master-Slave Betrieb (Master und Slaves können an unterschiedlichen Standorten aufgebaut werden) • Automatisiertes Konfigurations-Backup auf einen FTP/SFTP-Server
Ausführungen	• Hardware-Appliance • 19-Zoll Einbau 1HE • Redundante Spannungsversorgung 230VAC • Intern 2 x 1TB-Festplatte im Raid-System • 4 x 1GB Ethernet Ports, vorkonfiguriert (1xVPN / 1xKonfiguration) • Betriebssystem: Linux (Suse 15) • Virtuelle VPN Appliance • Die VSS-01 VPN-Security-Server-Software 525 ist auch als virtuelles Image erhältlich, um sie auf eigener Server-Hardware zu installieren und zu betreiben.