Name: OpenVPN

## OpenVPN

OpenVPN basiert auf den Sicherheitsfunktionen von OpenSSL. Die Verwendung von SSL/TLSbasierten VPNs hat sich heute als zweite Technologie neben IPsec durchgesetzt, wobei manche Hersteller SSL/TLS-basierte VPNs nur für Remote-Access-VPNs verwenden.
OpenVPN ist unter der GNU GPL lizenziert und steht unter https://openvpn.net/ zum Download für folgende Systeme zur Verfügung:

- Client: Windows, Linux, Android, macOS
- Server: Windows, Linux (RedHat, Fedora, CentOS, Ubuntu, Debian)
- Server: Virtual Appliance (VMware ESXi 5.0 und Microsoft Hyper-V)
- Server: Clouds (Amazon Cloud, Microsoft Azure, Google Cloud)

OpenVPN ist kompatibel mit den Protokollen SSL/TLS, RSA-Zertifikaten, X509-Zertifikaten, NAT, DHCP und TUN/TAP-Interfaces. Es unterstützt jedoch nicht die Protokolle IPsec, IKE, PPTP und L2TP.

① In welchem Netzwerkprotokoll arbeitet OpenVPN hauptsächlich?

- ◯ TCP/IP
- ◯ SMTP
- ◯ FTP
- ◯ HTTP

② Was ist ein Hauptvorteil von OpenVPN?

- ◯ Ermöglicht anonymes Surfen im Internet
- ◯ Bietet umfassende Benutzerauthentifizierungs-und Verschlüsselungsmethoden
- ◯ Reduziert die Internetgeschwindigkeit
- ◯ Ist eine kostenlose Antivirensoftware

③ Verstehen und Analyse von OpenVPN für Fachinformatiker

- Erklären Sie, welche Vorteile OpenVPN im Vergleich zu anderen VPN-Protokollen bietet und in welchen Szenarien es besonders sinnvoll ist, dieses einzusetzen.

**Einrichtung von OpenVPN auf Windows 11 (kurz erklärt)**

Link: https://youtu.be/jiPlad0SJ8c

**YouTube-Video**

**Einrichtung eines eigenen OpenVPN Access Server in unter 30 Minuten**

Link: https://youtu.be/S5m70wmRvgA

**YouTube-Video**