

# IP VPN

## TLS, IPSec und Wireguard

Virtuelle Private Netze (VPNs) bieten die Möglichkeit, Firmenstandorte über öffentliche IP-Netzwerke zu verbinden, und erlauben mobilen Nutzern die Einwahl in ihr Firmennetz. Hierzu gibt es verschiedene VPN-Konzepte, die in diesem Kurs im Detail betrachtet werden. Ein weiterer Schwerpunkt liegt auf der Absicherung von VPNs. Die Teilnehmer sind nach dem Kursbesuch in der Lage, die Vor- und Nachteile unterschiedlicher Arten IP-basierter VPNs abzuwägen und eigenverantwortlich deren Planung und Implementierung vorzunehmen.

### Kursinhalt

- Site-to-Site VPNs mit IPv4 und IPv6
- GRE und weitere Layer-3-Tunnelprotokolle
- MPLS VPNs
- Layer-2-Tunnelprotokolle für Remote Access VPNs
- Authentisierung und Autorisierung
- Voluntary Tunneling und Compulsory Tunneling
- Sichern von IP VPNs
- Verschlüsselung und Datenintegrität
- IPsec für Site-to-Site VPNs
- Encapsulating Security Payload (ESP) und Authentication Header (AH)
- IKEv2
- IPsec für Remote Access VPNs
- SSL für Remote Access VPNs

**E-Book** Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

### Zielgruppe

Der Kurs wendet sich an Netzwerkadministratoren und -planer, die sich mit der Konzeption und der technischen Realisierung von VPNs auf der Basis unterschiedlicher Tunneling-Technologien in IPv4- und IPv6-Netzen beschäftigen.

### Voraussetzungen

Netzwerk-Know-how, speziell auf dem Gebiet der TCP/IP-Protokollfamilie und der zugehörigen Adressierungs- und Routing-Konzepte, ist erforderlich. Eine gute Vorbereitung ist der Kurs TCP/IP – Protokolle, Adressierung, Routing.

### Kursziel

Der Kurs vermittelt Ihnen die Grundlagen von VPN-Technologien und deren Einsatzmöglichkeiten. Sie lernen, Site-to-Site- und Remote-Access-VPNs sowie sichere Varianten wie IPsec, TLS und WireGuard zu verstehen, Sicherheitsaspekte zu bewerten und VPNs in Ihren Netzwerken effektiv abzusichern.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/IPVP](http://www.experteach.at/go/IPVP)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Stand 26.11.2025

| Training                      |                     | Preise zzgl. MwSt. |           |
|-------------------------------|---------------------|--------------------|-----------|
| <b>Termine in Deutschland</b> | <b>4 Tage</b>       | <b>€ 2.395,-</b>   |           |
| <b>Online Training</b>        | <b>4 Tage</b>       | <b>€ 2.395,-</b>   |           |
| <b>Termin/Kursort</b>         | Kurssprache Deutsch |                    |           |
| 27.04.-30.04.26               | Frankfurt           | 12.10.-15.10.26    | Frankfurt |
| 27.04.-30.04.26               | Online              | 12.10.-15.10.26    | Online    |



# Inhaltsverzeichnis

## IP VPN – TLS, IPsec und Wireguard

|   |   |  |
|---|---|--|
| <b>1 VPN-Technologien – eine Einführung</b>             | <b>4.4 Zertifikate</b>                                | <b>7.3.3 Key Exchange</b>                            |
| <b>1.1 Die Umsetzung von VPNs</b>                       | <b>4.4.1 Zertifikate beantragen</b>                   | <b>7.3.4 Phase 4 – Authentisierung und Abschluss</b> |
| <b>1.1.1 Providerlösungen</b>                           | <b>4.4.2 Zertifikate ausstellen</b>                   | <b>7.4 Der Verbindungsaufbau bei TLS 1.3</b>         |
| <b>1.1.2 MPLS VPNs</b>                                  | <b>4.4.3 Authentisierung</b>                          | <b>7.4.1 Cipher Suites bei TLS 1.3</b>               |
| <b>1.1.3 SD-WAN</b>                                     | <b>4.4.4 Certificate Revocation List</b>              | <b>7.4.2 Schlüsselaustausch bei TLS 1.3</b>          |
| <b>1.1.4 VPNs in Eigenregie</b>                         | <b>4.4.5 Infrastruktur</b>                            | <b>7.4.3 Sitzungs-Wiederaufnahme mit 0-RTT</b>       |
| <b>1.1.5 VPNs als Anonymisierungs-Dienstleistung</b>    |   | <b>7.5 Sichere Datenübertragung bei TLS</b>          |
| <b>1.2 IP-VPN-Technologien in Enterprise Netzwerken</b> | <b>5 IPsec für Site-to-Site-VPNs</b>                  | <b>7.5.1 Keys und MACs</b>                           |
| <b>1.2.1 IP Tunnel</b>                                  | <b>5.1 IPsec – Sicherheit für IP</b>                  | <b>7.5.2 DTLS</b>                                    |
| <b>1.2.2 Site to Site VPNs</b>                          | <b>5.2 Die IPsec-Modi</b>                             | <b>7.6 Die Möglichkeiten bei TLS VPNs</b>            |
| <b>1.2.3 Remote Access VPNs</b>                         | <b>5.2.1 Domain Based vs. Route Based</b>             | <b>7.6.1 Clientless TLS VPN</b>                      |
| <b>1.3 VPNs und Sicherheit</b>                          | <b>5.2.2 Sicherung des privaten IP-Paketes</b>        | <b>7.6.2 Application Proxy</b>                       |
| <b>1.3.1 Sicherheit von Provider-VPNs</b>               | <b>5.2.3 GRE-Tunnel mit IPsec sichern</b>             | <b>7.6.3 Nativer Applikations-Zugriff</b>            |
| <b>1.3.2 Sicherheit von Kunden-VPNs</b>                 | <b>5.3 Die IPsec-Header</b>                           | <b>7.6.4 Full Tunnel Lösung</b>                      |
| <b>1.4 VPNs im Netzdesign</b>                           | <b>5.3.1 Der Authentication Header (AH)</b>           | <b>7.7 OpenVPN</b>                                   |
| <b>1.4.1 Router Based VPNs</b>                          | <b>5.3.2 Die Encapsulating Security Payload (ESP)</b> | <b>7.7.1 OpenVPN Server</b>                          |
| <b>1.4.2 Firewalls als VPN Gateway</b>                  | <b>5.4 Tunnel-Aufbau mit IPsec</b>                    | <b>7.7.2 OpenVPN Client</b>                          |
| <b>1.4.3 VPNs und Cloud Lösungen</b>                    | <b>5.4.1 ISAKMP der Transport</b>                     |  |
|   | <b>5.4.2 Internet Key Exchange</b>                    |  |
| <b>2 Layer 3 – Site to Site VPNs</b>                    | <b>5.4.3 Der Security Parameter Index (SPI)</b>       | <b>8 Wireguard</b>                                   |
| <b>2.1 Standortverknüpfung</b>                          | <b>5.5 IKEv1</b>                                      | <b>8.1 Wireguard – Das Konzept</b>                   |
| <b>2.1.1 Full Meshed</b>                                | <b>5.5.1 Der Main Mode</b>                            | <b>8.1.1 Betriebssysteme für Wireguard</b>           |
| <b>2.1.2 Hub and Spoke</b>                              | <b>5.5.2 Der Quick Mode</b>                           | <b>8.1.2 Vorteile von Wireguard</b>                  |
| <b>2.1.3 VPN Routing</b>                                | <b>5.6 Internet Key Exchange v2</b>                   | <b>8.1.3 Einschränkungen</b>                         |
| <b>2.2 Layer-3-Tunneling</b>                            | <b>5.6.1 Kryptographie bei IKEv2</b>                  | <b>8.2 Hintergründe zu Wireguard</b>                 |
| <b>2.2.1 Tunnelinterfaces</b>                           | <b>5.6.2 Tunnelaufbau</b>                             | <b>8.2.1 Wireguard Tunnel</b>                        |
| <b>2.2.2 Routing im Tunnel</b>                          | <b>5.6.3 IKEv2 SA_Init</b>                            | <b>8.2.2 Cryptokey Routing</b>                       |
| <b>2.2.3 VPN-Technologien in Dual-Stack-Netzen</b>      | <b>5.6.4 IKE_Auth</b>                                 | <b>8.3 Protokollabläufe bei Wireguard</b>            |
| <b>2.3 Multiprotocol VPNs</b>                           | <b>5.7 Authentisierungsmöglichkeiten bei IPsec</b>    | <b>8.3.1 Handshake</b>                               |
| <b>2.3.1 GRE in Dual Stack Netzen</b>                   |   | <b>8.3.2 DoS Mitigation</b>                          |
| <b>2.3.2 GRE – Die Optionen</b>                         | <b>6 IPsec RA VPNs</b>                                | <b>8.4 Einsatzgebiete</b>                            |
| <b>2.3.3 GRE sichern</b>                                | <b>6.1 Erweiterungen für IKEv1</b>                    | <b>8.4.1 Wireguard RA VPNs</b>                       |
|   | <b>6.1.1 Der Aggressive Mode</b>                      | <b>8.4.2 Wireguard in mobilen Netzen</b>             |
| <b>3 Layer 2 – RA VPNs</b>                              | <b>6.1.2 XAUTH – Erweitere Authentisierung</b>        |  |
| <b>3.1 Layer-2-Tunnel für Einwahlclients</b>            | <b>6.1.3 Hybrid Authentication</b>                    | <b>A Lab-Übungen und Lösungen</b>                    |
| <b>3.1.1 Historisch – Die Einwahl</b>                   | <b>6.1.4 IPsec und dynamische IP-Adresszuweisung</b>  | <b>A.1 Lab Übungen im Kurs</b>                       |
| <b>3.1.2 VPDN – Compulsory oder Voluntary Tunneling</b> | <b>6.2 IKEv2 in RA VPNs</b>                           | <b>A.1.1 Die Labor-Umgebung</b>                      |
| <b>3.2 Layer-2-Tunnelprotokolle</b>                     | <b>6.2.1 Authentisierung mit EAP</b>                  | <b>A.1.2 Grundkonfiguration der Router</b>           |
| <b>3.2.1 PPTP in Microsoft Netzen</b>                   | <b>6.2.2 Zuweisung interner Adressen</b>              | <b>A.2 Klassische Site to Site VPNs</b>              |
| <b>3.2.2 L2TP – Der IETF Standard</b>                   | <b>6.3 Probleme mit NAT bzw. PAT</b>                  | <b>A.2.1 IPv4 in IPv4-Tunneling</b>                  |
| <b>3.3 Sicherheit bei Layer 2 VPNs</b>                  | <b>6.3.1 AH verboten</b>                              | <b>A.2.2 IPv6 in IPv4-Tunneling</b>                  |
| <b>3.3.1 Split Tunneling</b>                            | <b>6.3.2 Probleme mit dem Pseudoheader</b>            | <b>A.2.3 Multiprotokoll-Tunnel</b>                   |
| <b>3.3.2 Layer 2 VPNs und IPsec</b>                     | <b>6.3.3 IP-Adresse als Identifikator</b>             | <b>A.3 Layer2-Tunneling</b>                          |
| <b>3.3.3 Secure Socket Tunneling Protocol (SSTP)</b>    | <b>6.3.4 NAT Traversal – NAT-T</b>                    | <b>A.3.1 PPTP – Der Protokollablauf</b>              |
|   |   | <b>A.3.2 L2TP – Der Protokollablauf</b>              |
| <b>4 Sicherheit für VPNs</b>                            | <b>7 SSL/TLS VPNs</b>                                 | <b>A.4 IPsec-VPN</b>                                 |
| <b>4.1 Symmetrische Verschlüsselung</b>                 | <b>7.1 TLS VPNs im Einsatz</b>                        | <b>A.4.1 ESP-Tunnel</b>                              |
| <b>4.1.1 Lebensdauer der Schlüssel</b>                  | <b>7.1.1 TLS für RA VPNs</b>                          | <b>A.4.2 GRE Tunnel mit IPsec sichern</b>            |
| <b>4.1.2 Schlüsselverteilung</b>                        | <b>7.1.2 Site to Site VPNs mit TLS</b>                | <b>A.5 Tunnelaufbau mit IKEv1</b>                    |
| <b>4.2 Datenintegrität durch Hash-Werte</b>             | <b>7.2 SSL/TLS – Applikations-Sicherheit</b>          | <b>A.6 Tunnelaufbau mit IKEv2</b>                    |
| <b>4.2.1 Typische Eigenschaften</b>                     | <b>7.2.1 Der TLS Protokollstapel</b>                  | <b>A.6.1 IKEv2 – Der Protokollablauf</b>             |
| <b>4.2.2 Bekannte Verfahren</b>                         | <b>7.2.2 TLS-Versionen und SSL</b>                    | <b>A.6.2 Debugging IKEv2</b>                         |
| <b>4.3 Authentisierung und Authentizität</b>            | <b>7.3 Der Verbindungsaufbau bis TLS 1.2</b>          | <b>A.7 TLS/DTLS RA-VPN – Verbindungsaufbau</b>       |
| <b>4.3.1 Pre-Shared Key</b>                             | <b>7.3.1 Phase 1 – Say Hello</b>                      |  |
| <b>4.3.2 Public Key Verfahren</b>                       | <b>7.3.2 Phase 2 und 3 – Zertifikate</b>              |  |

