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.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: 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.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**4 Tage**	**€ 2.395,-**
Online Training	**4 Tage**	**€ 2.395,-**
Termin/Kursort		Kurssprache Deutsch
19.08.-22.08.25 Hamburg		19.08.-22.08.25 Online

Stand 07.05.2025

Inhaltsverzeichnis

IP VPN – TLS, IPSec und Wireguard

1 VPN-Technologien – eine Einführung
1.1 Die Umsetzung von VPNs
1.1.1 Providerlösungen
1.1.2 MPLS VPNs
1.1.3 SD-WAN
1.1.4 VPNs in Eigenregie
1.1.5 VPNs als Anonymisierungs-Dienstleistung
1.2 IP-VPN-Technologien in Enterprise Netzwerken
1.2.1 IP Tunnel
1.2.2 Site to Site VPNs
1.2.3 Remote Access VPNs
1.3 VPNs und Sicherheit
1.3.1 Sicherheit von Provider-VPNs
1.3.2 Sicherheit von Kunden-VPNs
1.4 VPNs im Netzdesign
1.4.1 Router Based VPNs
1.4.2 Firewalls als VPN Gateway
1.4.3 VPNs und Cloud Lösungen

2 Layer 3 – Site to Site VPNs
2.1 Standortverknüpfung
2.1.1 Full Meshed
2.1.2 Hub and Spoke
2.1.3 VPN Routing
2.2 Layer-3-Tunneling
2.2.1 Tunnelinterfaces
2.2.2 Routing im Tunnel
2.2.3 VPN-Technologien in Dual-Stack-Netzen
2.3 Multiprotocol VPNs
2.3.1 GRE in Dual Stack Netzen
2.3.2 GRE – Die Optionen
2.3.3 GRE sichern

3 Layer 2 – RA VPNs
3.1 Layer-2-Tunnel für Einwahlclients
3.1.1 Historisch – Die Einwahl
3.1.2 VPDN – Compulsory oder Voluntary Tunneling
3.2 Layer-2-Tunnelprotokolle
3.2.1 PPTP in Microsoft Netzen
3.2.2 L2TP – Der IETF Standard
3.3 Sicherheit bei Layer 2 VPNs
3.3.1 Split Tunneling
3.3.2 Layer 2 VPNs und IPsec
3.3.3 Secure Socket Tunneling Protocol (SSTP)

4 Sicherheit für VPNs
4.1 Symmetrische Verschlüsselung
4.1.1 Lebensdauer der Schlüssel
4.1.2 Schlüsselverteilung
4.2 Datenintegrität durch Hash-Werte
4.2.1 Typische Eigenschaften
4.2.2 Bekannte Verfahren
4.3 Authentisierung und Authentizität
4.3.1 Pre-Shared Key
4.3.2 Public Key Verfahren
4.4 Zertifikate
4.4.1 Zertifikate beantragen
4.4.2 Zertifikate ausstellen
4.4.3 Authentisierung
4.4.4 Certificate Revocation List
4.4.5 Infrastruktur

5 IPSec für Site-to-Site-VPNs
5.1 IPSec – Sicherheit für IP
5.2 Die IPsec-Modi
5.2.1 Domain Based vs. Route Based
5.2.2 Sicherung des privaten IP-Pakets
5.2.3 GRE-Tunnel mit IPsec sichern
5.3 Die IPsec-Header
5.3.1 Der Authentication Header (AH)
5.3.2 Die Encapsulating Security Payload (ESP)
5.4 Tunnel-Aufbau mit IPsec
5.4.1 ISAKMP der Transport
5.4.2 Internet Key Exchange
5.4.3 Der Security Parameter Index (SPI)
5.5 IKEv1
5.5.1 Der Main Mode
5.5.2 Der Quick Mode
5.6 Internet Key Exchange v2
5.6.1 Kryptographie bei IKEv2
5.6.2 Tunnelaufbau
5.6.3 IKEv2 SA_Init
5.6.4 IKE_Auth
5.7 Authentisierungsmöglichkeiten bei IPsec

6 IPsec RA VPNs
6.1 Erweiterungen für IKEv1
6.1.1 Der Aggressive Mode
6.1.2 XAUTH – Erweitere Authentisierung
6.1.3 Hybrid Authentication
6.1.4 IPsec und dynamische IP-Adresszuweisung
6.2 IKEv2 in RA VPNs
6.2.1 Authentisierung mit EAP
6.2.2 Zuweisung interner Adressen
6.3 Probleme mit NAT bzw. PAT
6.3.1 AH verboten
6.3.2 Probleme mit dem Pseudoheader
6.3.3 IP-Adresse als Identifikator
6.3.4 NAT Traversal – NAT-T

7 SSL/TLS VPNs
7.1 TLS VPNs im Einsatz
7.1.1 TLS für RA VPNs
7.1.2 Site to Site VPNs mit TLS
7.2 SSL/TLS – Applikations-Sicherheit
7.2.1 Der TLS Protokollstapel
7.2.2 TLS-Versionen und SSL
7.3 Der Verbindungsaufbau bis TLS 1.2
7.3.1 Phase 1 – Say Hello
7.3.2 Phase 2 und 3 – Zertifikate
7.3.3 Key Exchange
7.3.4 Phase 4 – Authentisierung und Abschluss
7.4 Der Verbindungsaufbau bei TLS 1.3
7.4.1 Cipher Suites bei TLS 1.3
7.4.2 Schlüsselaustausch bei TLS 1.3
7.4.3 Sitzungs-Wiederaufnahme mit 0-RTT
7.5 Sichere Datenübertragung bei TLS
7.5.1 Keys und MACs
7.5.2 DTLS
7.6 Die Möglichkeiten bei TLS VPNs
7.6.1 Clientless TLS VPN
7.6.2 Application Proxy
7.6.3 Nativer Applikations-Zugriff
7.6.4 Full Tunnel Lösung
7.7 OpenVPN
7.7.1 OpenVPN Server
7.7.2 OpenVPN Client

8 Wireguard
8.1 Wireguard – Das Konzept
8.1.1 Betriebssysteme für Wireguard
8.1.2 Vorteile von Wireguard
8.1.3 Einschränkungen
8.2 Hintergründe zu Wireguard
8.2.1 Wireguard Tunnel
8.2.2 Cryptokey Routing
8.3 Protokollabläufe bei Wireguard
8.3.1 Handshake
8.3.2 DoS Mitigation
8.4 Einsatzgebiete
8.4.1 Wireguard RA VPNs
8.4.2 Wireguard in mobilen Netzen

A Lab-Übungen und Lösungen
A.1 Lab Übungen im Kurs
A.1.1 Die Labor-Umgebung
A.1.2 Grundkonfiguration der Router
A.2 Klassische Site to Site VPNs
A.2.1 IPv4 in IPv4-Tunneling
A.2.2 IPv6 in IPv4-Tunneling
A.2.3 Multiprotokoll-Tunnel
A.3 Layer2-Tunneling
A.3.1 PPTP – Der Protokollablauf
A.3.2 L2TP – Der Protokollablauf
A.4 IPsec-VPN
A.4.1 ESP-Tunnel
A.4.2 GRE Tunnel mit IPsec sichern
A.5 Tunnelaufbau mit IKEv1
A.6 Tunnelaufbau mit IKEv2
A.6.1 IKEv2 – Der Protokollablauf
A.6.2 Debugging IKEv2
A.7 TLS/DTLS RA-VPN – Verbindungsaufbau

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at