

IP VPN

Tunneling über das Internet

Virtuelle Private Netzwerke (VPNs) stellen heute eine preiswerte Alternative zu klassischen Remote-Access-Szenarien dar, eignen sich aber auch zur Kopplung von Firmenstandorten. Bei der Nutzung des Internets entstehen besonders hohe Anforderungen an eine zuverlässige Authentisierung und Autorisierung der Benutzer sowie an die Datensicherheit. Die Teilnehmer sind nach dem Kursbesuch in der Lage, die Vor- und Nachteile von L2TP, IPsec und SSL/TLS abzuwägen und eigenverantwortlich die Planung und Implementierung von IP-basierten VPNs vorzunehmen.

Kursinhalt

- Layer-2- und Layer-3-Tunnel
- GRE, L2F, L2TP und PPTP
- PPP, PAP, CHAP und RADIUS
- Voluntary Tunneling und Compulsory Tunneling
- Symmetrische und asymmetrische Verschlüsselung (AES, 3DES, RSA)
- Datenintegrität und Replay-Angriffe
- Keyed Hash (MD5, SHA-1)
- Digitale Signaturen und Zertifikate
- Authentisierung
- IPsec: Tunnel Mode und Transport Mode
- Encapsulating Security Payload (ESP) und Authentication Header (AH)
- VPNs mit SSL und TLS
- VPN-Konzentratoren und Home Gateways
- MPLS VPNs vs. IP VPNs

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

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 beschäftigen und hierfür das notwendige Rüstzeug erwerben wollen.

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. Von Vorteil sind weiterhin Kenntnisse des Point-to-Point-Protokolls.



Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf www.experteach.de können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

5 Tage €2.495,00 • CHF 3.795,00 • zzgl. MwSt.

Termin/Kursort

25.06.-29.06.12	Frankfurt	17.09.-21.09.12	Düsseldorf
06.08.-10.08.12	München	05.11.-09.11.12	Hamburg
06.08.-10.08.12	Wien	10.12.-14.12.12	Frankfurt

Aktuelle Informationen finden Sie auf www.experteach.de IPVP





IP VPN – Tunneling über das Internet

1 VPN-Technologien – eine Einführung

- 1.1 Wozu VPNs?
 - 1.1.1 Providerlösungen
 - 1.1.2 Kundendefinierte VPNs
- 1.2 Welche VPN-Technologien werden genutzt?
 - 1.2.1 Frame Relay oder ATM VPNs
 - 1.2.2 VPNs mit MPLS und BGP-4
 - 1.2.3 IP VPNs
- 1.3 Forderungen an die VPN-Lösung
- 1.4 VPN und Sicherheit
 - 1.4.1 Sicherheitsanforderungen
 - 1.4.2 Sicherheit klassischer VPNs
 - 1.4.3 Sicherheit von IP VPNs

2 Vom Tunnel-Protokoll zum VPN

- 2.1 Layer-3-Tunnel für Netze
 - 2.1.1 IP in IP Tunneling
 - 2.1.2 Generic Routing Encapsulation (GRE)
 - 2.1.3 IPsec als Tunnelprotokoll
- 2.2 Layer-2-Tunnel für Einwahlclients
 - 2.2.1 Die Rolle von PPP
 - 2.2.2 VPDN – Compulsory oder Voluntary Tunneling
 - 2.2.3 Layer-2-Tunnelprotokolle
 - 2.2.4 Layer-2 IP VPNs und IPsec

3 Sicherheit für VPNs

- 3.1 Was bedeutet Sicherheit?
- 3.2 Symmetrische Verschlüsselung
 - 3.2.1 Lebensdauer der Schlüssel
 - 3.2.2 Verteilung von Schlüsseln
 - 3.2.3 Asymmetrische Verschlüsselung
- 3.3 Datenintegrität: Hash-Werte
 - 3.3.1 Typische Eigenschaften
 - 3.3.2 Keyed Hash
- 3.4 Data Origin Authentication
 - 3.4.1 Pre-Shared Key
 - 3.4.2 Public Key Verfahren
 - 3.4.3 Zertifikate
 - 3.4.4 PKI und CA
- 3.5 Replay-Angriffe
- 3.6 IPsec und Co. – Ebenen der Sicherheit

4 IPsec VPN

- 4.1 Die Ziele von IPsec
- 4.2 IPsec im Einsatz
 - 4.2.1 Host to Host
 - 4.2.2 IPsec – Gateway-to-Gateway
 - 4.2.3 IPsec und dynamische Einwahl
- 4.3 IPsec – Die Betriebsarten
 - 4.3.1 Der Tunnel Mode
 - 4.3.2 Der Transport Mode
 - 4.3.3 Wogegen IPsec nicht schützen kann

- 4.4 Der grundlegende Aufbau von IPsec
 - 4.4.1 Der Authentication Header (AH)
 - 4.4.2 Encapsulating Security Payload (ESP)
- 4.5 ISAKMP ein Rahmenwerk
- 4.6 Security Associations
- 4.7 Internet Key Exchange
 - 4.7.1 Die Phasen von IKE
 - 4.7.2 Main Mode
 - 4.7.3 Der Aggressive Mode
 - 4.7.4 Der Quick Mode
 - 4.7.5 XAUTH – Erweitere Authentisierung
 - 4.7.6 IPsec und dynamische IP-Adresszuweisung
 - 4.7.7 IKEv2
- 4.8 Problem der Inkompatibilität
- 4.9 IPsec und NAT bzw. PAT
 - 4.9.1 AH verboten
 - 4.9.2 Probleme mit dem Pseudoheader
 - 4.9.3 IP-Adresse als Identifikator
 - 4.9.4 PAT und Schlüsselerneuerung
 - 4.9.5 Probleme mit Anwendungen
 - 4.9.6 NAT Traversal – NAT-T

5 SSL VPN

- 5.1 SSL – Sicherheit für TCP
 - 5.1.1 Der SSL Protokollstapel
 - 5.1.2 SSL-Versionen und TLS
- 5.2 Der SSL Verbindungsaufbau
 - 5.2.1 Phase 1 – Say Hello
 - 5.2.2 Phase 2 und 3 – Zertifikate
 - 5.2.3 Phase 4 – Abschluss des Handshakes
- 5.3 Sichere Datenübertragung
- 5.4 Die Komponenten eines SSL VPNs
 - 5.4.1 Das SSL Gateway
 - 5.4.2 Clientless mit Portal
 - 5.4.3 Der SSL-Client
- 5.5 Konzepte für den Einsatz von SSL VPNs
 - 5.5.1 Anbindung von Filialen mit SSL
 - 5.5.2 SSL für die Anbindung von Teleworkern
 - 5.5.3 SSL für mobile Benutzer
 - 5.5.4 SSL aus dem Internet-Café
- 5.6 Probleme mit SSL VPNs
 - 5.6.1 Schwierigkeiten mit Applikationen
 - 5.6.2 Client-Sicherheit
- 5.7 Produktauswahl
 - 5.7.1 Die Lösungen von Microsoft
 - 5.7.2 Check Point Security Gateway – VPN-1
 - 5.7.3 Die Möglichkeiten bei Cisco
 - 5.7.4 OpenVPN



ExperTeach Gesellschaft für Netzwerkkompetenz mbH

Waldstr. 94 • D-63128 Dietzenbach
 Telefon +49 6074 4868-0 • Telefax +49 6074 4868-109
 info@experteach.de • www.experteach.de

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 12.05.2012