

Cisco ASA VPN Konfiguration und Design



Dem Anwender bietet sich mittlerweile ein breitgefächertes Angebot an VPN-Technologien. Der Kurs vermittelt einen Überblick über die verschiedenen Varianten und deren Konfiguration auf der Cisco ASA. Ziel des Kurses ist, dass der Anwender die verschiedenen VPN-Technologien positionieren kann und das notwendige Wissen zur Konfiguration und Wartung von VPN-Tunneln erhält.

Kursinhalt

- VPN-Technologien im Überblick (IPsec, SSL)
- Übersicht aktueller Verschlüsselungstechnologien (Verschlüsselung, Hash und Digitale Signatur)
- IPsec Site-to-Site VPNs
- IPsec Remote Access VPNs
- SSL VPNs (WebVPN und SSL Client)
- Der Adaptive Security Device Manager ASDM

Jeder Teilnehmer erhält ausführliche deutschsprachige Kursunterlagen von ExperTeach, die von Cisco als Derivative Work anerkannt sind.

Zielgruppe

Der Kurs richtet sich an Netzwerker, die bereits praktische Erfahrungen mit der Konfiguration von Cisco Routern gesammelt haben und in diesem Kurs die VPN-Features der Cisco ASA kennenlernen wollen. Des Weiteren richtet sich der Kurs an Netzwerker, die bislang mit dem Cisco VPN-Konzentrator gearbeitet haben und auf die ASA umsteigen wollen.

Voraussetzungen

Dieser Kurs setzt grundlegendes, produktspezifisches Know-how des Cisco IOS sowie Kenntnisse des TCP/IP-Protokolls und Grundlagen der Datenverschlüsselung voraus. Die Teilnehmer sollten außerdem mit den grundlegenden Konzepten von VPN-Technologien vertraut sein.



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.

Cisco ASA VPN

4 Tage € 1.995,00 • CHF 3.595,00 • zzgl. MwSt.

Termin/Kursort

| | | | |
|-----------------|-----------|-----------------|------------|
| 06.08.-09.08.12 | Frankfurt | 29.10.-01.11.12 | Hamburg |
| 24.09.-27.09.12 | München | 10.12.-13.12.12 | Düsseldorf |
| 24.09.-27.09.12 | Wien | | |

Aktuelle Informationen finden Sie auf www.experteach.de ASA2



EXPERTeach



Deutschsprachige
Kurse

IT & TK Training

| | | | |
|----------|--|----------|---------------------------------------|
| 1 | VPN Produkte von Cisco | 5 | IPsec Remote Access VPNs |
| 1.1 | Überblick | 5.1 | Ciscos VPN-Client |
| 1.2 | ASA – Ein Produkt-Überblick | 5.2 | Die Konfiguration auf der ASA |
| 1.3 | ASA – Zahlen | 5.2.1 | Tunnel-Group und Policies |
| 1.4 | ASA – Lizenzen | 5.2.2 | Die Group-Policy |
| 1.5 | Cisco VPN Client | 5.2.3 | Manuelle Konfiguration |
| 1.6 | AnyConnect Client | 5.3 | Kontrolle |
| 1.7 | Secure Desktop Client | 5.4 | Zertifikate |
| 2 | Router und Verschlüsselung | 5.4.1 | Zertifikate beim VPN Client |
| 2.1 | Kleines 1 x 1 der Kryptographie | 5.4.2 | Speziell: Tunnelgruppe und Zertifikat |
| 2.1.1 | Vertraulichkeit – Symmetrische Verschlüsselung | 5.5 | Die Konfiguration im CLI |
| 2.1.2 | Diffie-Hellman – Erzeugen symmetrischer Schlüssel | 5.6 | Hybrid Auth |
| 2.1.3 | RSA – Asymmetrische Verschlüsselung | 6 | SSL VPNs |
| 2.1.4 | Datenintegrität – Hash-Werte | 6.1 | Zugriffsarten |
| 2.1.5 | Authentisierung – Daten und Absender unverfälscht | 6.2 | Full Tunnel Access |
| 3 | VPN Grundlagen | 6.3 | Clientless SSL |
| 3.1 | Die Struktur von IPSec | 6.4 | Zusatzoptionen für WebVPN |
| 3.2 | IPSec – Die Betriebsarten | 6.4.1 | Host Scan |
| 3.3 | Der IPSec Header – Bestandteile von IPSec | 6.4.2 | Cisco Secure Desktop CSD |
| 3.3.1 | Keyed-Hashing for Message Authentication Code – HMAC | 6.4.3 | Dynamic Access Policies DAPs |
| 3.3.2 | Vertraulichkeit – ESP | 6.4.4 | Erweiterte Authentisierungsverfahren |
| 3.3.3 | Aushandlung mit ISAKMP und IKE | 6.5 | VPNs und Redundanz |
| 3.4 | Security Associations | | |
| 3.5 | Main Mode | | |
| 3.6 | Der Quick Mode | | |
| 3.6.1 | Die Methoden der Authentisierung | | |
| 3.7 | Der Aggressive Mode | | |
| 3.8 | IKEv2 | | |
| 3.9 | SSL – Sicherheit für TCP | | |
| 3.9.1 | Der SSL Protokollstapel | | |
| 3.9.2 | SSL-Versionen und TLS | | |
| 3.10 | Der SSL Verbindungsaufbau | | |
| 3.10.1 | Phase 1 – Say Hello | | |
| 3.11 | Sichere Datenübertragung | | |
| 4 | IPsec Site-to-Site VPNs | | |
| 4.1 | Konfiguration der ASA | | |
| 4.2 | Die Tunnelgruppe | | |
| 4.3 | Manuelle Konfiguration | | |
| 4.4 | Die Konfiguration im CLI | | |
| 4.5 | IKEv2 als neue Alternative | | |
| 4.6 | Authentisierung mit Zertifikaten | | |
| 4.6.1 | Stammzertifikat | | |
| 4.6.2 | Identity Zertifikat | | |
| 4.6.3 | Konfiguration im CLI | | |



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