



## F2: FortiGate Security

In diesem dreitägigen Kurs lernen Sie die grundlegenden Funktionen von FortiGate kennen, einschließlich der Sicherheitsprofile. In interaktiven Labors erfahren Sie mehr über Firewall-Richtlinien, Benutzerauthentifizierung, SSL VPN, Einwahl IPsec VPN und wie Sie Ihr Netzwerk mithilfe von Sicherheitsprofilen wie IPS, Antivirus, Webfilterung, Anwendungskontrolle und mehr schützen können. Diese Administrationsgrundlagen vermitteln Ihnen ein solides Verständnis für die Implementierung grundlegender Netzwerksicherheit.

### Listenpreis

1.990,00 € exkl. MwSt

2.368,10 € inkl. MwSt

### Dauer

3 Tage

### Gebühr für Prüfungen/Examen

415,00 € exkl. MwSt / 493,85 € inkl. MwSt

### Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

### Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

### Ihre Ansprechpartnerin



**Gabriela Bücherl**  
Geschäftsführung  
Vertrieb

### Kontakt/Fragen:

[g.buecherl@cbt-training.de](mailto:g.buecherl@cbt-training.de)

Telefon: +49 (0)89-4576918-16

## Inhalte

- Einführung in FortiGate und die Security Fabric
- Firewall-Richtlinien
- Network Address Translation (NAT)
- Firewall-Authentifizierung
- Protokollierung und Überwachung
- Zertifikat-Operationen
- Web-Filterung
- Application Control
- Antivirus
- Intrusion Prevention und Denial of Service
- SSL VPN
- Einwahl IPsec VPN
- Data Leak Prevention (DLP)

**Bitte beachten Sie - Diesen Kurs können Sie zusammen mit dem Fortigate Infrastructure Kurs im vergünstigten "Bundle" buchen.**



## Ziele

- Nach Abschluss dieses Kurses sind Sie zu Folgendem in der Lage:
- Einsatz der für Ihr Netzwerk geeigneten Betriebsart
- Verwendung der GUI und CLI für die Administration
- Die Indikation der Merkmale des Fortinet-Sicherheitsgewebes
- Kontrolle des Netzwerkzugriffs auf konfigurierte Netzwerke mithilfe von Firewall-Richtlinien
- Anwendung von Port Forwarding, Source NAT und Destination NAT
- Authentifizierung von Benutzern mithilfe von Firewall-Richtlinien
- Verstehen von Verschlüsselungsfunktionen und Zertifikaten
- Untersuchung des SSL/TLS-gesicherten Datenverkehrs, um Verschlüsselung zu verhindern, die zur Umgehung von Sicherheitsrichtlinien verwendet wird
- Konfiguration von Sicherheitsprofilen, um Bedrohungen und Missbrauch, einschließlich Viren, Torrents und unangemessene Websites, zu neutralisieren
- Anwendung von Anwendungskontrolltechniken, um Netzwerkanwendungen zu überwachen und zu steuern, die Standard- oder Nicht-Standard-Protokolle und -Ports verwenden
- Bekämpfung von Hacking und Denial of Service (DoS)
- Schutz vor Datenverlusten, indem Sie Dateien mit sensiblen Daten identifizieren und sie daran hindern, Ihr privates Netzwerk zu verlassen
- Bereitstellung eines SSL-VPN für den sicheren Zugriff auf Ihr privates Netzwerk
- Implementierung eines IPsec VPN-Tunnels für die Einwahl zwischen FortiGate und FortiClient
- Sammeln und Interpretieren von Log-Einträgen

---

## Zielgruppe

Netzwerk- und Sicherheitsexperten, die mit Management, Konfiguration, Verwaltung und Überwachung von FortiGate-Geräten befasst sind, die zur Absicherung der Netzwerke ihrer Organisationen eingesetzt werden. Die Teilnehmer sollten alle im FortiGate Security-Kurs behandelten Themen gründlich verstehen, bevor sie den FortiGate Infrastructure-Kurs besuchen.

---

## Voraussetzungen

Kenntnisse von Netzwerkprotokollen und ein grundlegendes Verständnis von Firewall-Konzepten.

---

## Prüfung/Zertifizierung

Dieser Kurs und der Kurs "F3: FortiGate Infrastruktur" bereiten auf die Prüfung NSE 4 vor.  
Prüfung: Fortinet NSE 4 - FortiOS 7.2

Beachten Sie auch unser kostengünstiges Kursbundle "F1: FortiGate Security & Infrastruktur".