Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

ID SFWIPF **Preis** 3.995,– € (exkl. MwSt.) **Dauer** 5 Tage

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Das Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) Training zeigt Ihnen, wie Sie Cisco Secure Firewall Threat Defense für den Einsatz als Firewall der nächsten Generation am Internet-Edge implementieren und konfigurieren. Sie erhalten ein Verständnis für die Architektur und den Einsatz der Cisco Secure Firewall, die Basiskonfiguration, die Paketverarbeitung und die erweiterten Optionen sowie die Fehlerbehebung bei der Secure Firewall-Administration.

Diese Schulung bereitet Sie auf die CCNP Security-Zertifizierung vor, die das Bestehen der Kernprüfung 350-701 Implementing and Operating Cisco Security Core Technologies (SCOR) und einer Konzentrationsprüfung wie der Konzentrationsprüfung 300-710 Securing Networks with Cisco Firepower (SNCF) erfordert. Mit dieser Schulung erhalten Sie außerdem 40 Continuing Education (CE) Credits für die Rezertifizierung.

Wie Sie davon profitieren In dieser Schulung lernen Sie, wie Sie Cisco Secure Firewall Threat Defense für die Bereitstellung implementieren, konfigurieren und verwalten, einschließlich:

- Konfigurieren von Einstellungen und Richtlinien für Cisco Secure Firewall Threat Defense
- Verständnis der Cisco Secure Firewall Threat Defense-Richtlinien und Erklärung, wie verschiedene Richtlinien die Paketverarbeitung durch das Gerät beeinflussen
- Durchführung grundlegender Bedrohungsanalysen und Verwaltungsaufgaben mit dem Cisco Secure Firewall Management Center

Was Sie bei der Prüfung erwartet 350-701 SCOR: Implementing and Operating Cisco Security Core Technologies ist eine 120-minütige Prüfung im Rahmen der CCNP Security Zertifizierung. Das Multiple-Choice-Format testet Wissen und Fähigkeiten im Zusammenhang mit der Implementierung und dem Betrieb von Kernsicherheitstechnologien, einschließlich:

- Sicherheit im Netz
- Sicherheit in der Cloud
- Sicherheit des Inhalts
- Endpunktschutz und -erkennung
- Sicherer Netzzugang
- Sichtbarkeit und Durchsetzung

300-710 SNCF: Securing Networks with Cisco Firepower ist eine 90-minütige Prüfung im Rahmen der CCNP Security-Zertifizierung. Das Multiple-Choice-Format prüft das Wissen über Cisco Firepower® Threat Defense und die virtuellen Appliances der Firepower® 7000- und 8000-Serie, einschließlich:

- Policy Konfigurationen
- Integrationen
- Einsätze

Verwaltung und Fehlerbehebung

Zielgruppe

- Ingenieure für Netzsicherheit
- Verwalter

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Bevor Sie dieses Angebot annehmen, sollten Sie es verstehen:

- TCP/IP
- Grundlegende Routing-Protokolle
- Firewall-, VPN- und IPS-Konzepte

Kursziele

- Beschreiben Sie die Cisco Secure Firewall-Bedrohungsabwehr
- Beschreiben Sie die Bereitstellungsoptionen von Cisco Secure Firewall Threat Defense
- Beschreiben Sie die Verwaltungsoptionen für Cisco Secure Firewall Threat Defense
- Konfigurieren Sie die Grundeinstellungen von Cisco Secure Firewall Threat Defense
- Konfigurieren Sie Hochverfügbarkeit auf Cisco Secure Firewall Threat Defense
- Konfigurieren der grundlegenden Netzwerkadressübersetzung auf der Cisco Secure Firewall Threat Defense
- Beschreiben Sie die Cisco Secure Firewall Threat Defense-Richtlinien und erklären Sie, wie verschiedene Richtlinien die Paketverarbeitung durch das Gerät beeinflussen
- Konfigurieren der Erkennungsrichtlinie auf Cisco Secure Firewall Threat Defense
- Konfigurieren und Erklären von Vorfilter- und Tunnelregeln in der Vorfilterrichtlinie
- Konfigurieren Sie eine Zugriffskontrollrichtlinie für Cisco Secure Firewall Threat Defense
- Konfigurieren Sie Sicherheitsinformationen auf Cisco Secure Firewall Threat Defense
- Konfigurieren Sie die Dateirichtlinie für Cisco Secure Firewall Threat Defense
- Konfigurieren der Intrusion Policy auf Cisco Secure Firewall Threat Defense
- Durchführung grundlegender Bedrohungsanalysen mit dem Cisco Secure Firewall Management Center
- Durchführung grundlegender Verwaltungs- und Systemadministrationsaufgaben für Cisco Secure Firewall Threat Defense
- Durchführung grundlegender Fehlerbehebungen im Verkehrsfluss bei Cisco Secure Firewall Threat Defense
- Verwalten von Cisco Secure Firewall Threat Defense mit Cisco Secure Firewall Threat Defense Manager

Detaillierter Kursinhalt

- Einführung in die Cisco Secure Firewall-Bedrohungsabwehr
- Beschreibung der Bereitstellungsoptionen von Cisco Secure Firewall Threat Defense
- Beschreibung der Verwaltungsoptionen der Cisco Secure Firewall zur Bedrohungsabwehr
- Konfigurieren grundlegender Netzwerkeinstellungen auf der Cisco Secure Firewall Threat Defense
- Konfigurieren der Hochverfügbarkeit auf Cisco Secure Firewall Threat Defense
- Konfigurieren von Auto-NAT auf Cisco Secure Firewall Threat Defense
- Beschreibung der Paketverarbeitung und der Richtlinien von Cisco Secure Firewall Threat Defense
- Konfigurieren der Erkennungsrichtlinie für Cisco Secure Firewall Threat Defense
- Konfigurieren der Vorfilter-Richtlinie auf Cisco Secure Firewall Threat Defense
- Konfigurieren der Zugriffssteuerungsrichtlinie auf Cisco Secure Firewall Threat Defense
- Konfigurieren von Security Intelligence auf Cisco Secure Firewall Threat Defense
- Konfigurieren der Dateirichtlinie auf Cisco Secure Firewall Threat Defense
- Konfigurieren der Intrusion Policy auf Cisco Secure Firewall Threat Defense
- Durchführen einer grundlegenden Bedrohungsanalyse mit dem Cisco Secure Firewall Management Center
- Verwaltung des Cisco Secure Firewall-Bedrohungsabwehrsystems
- Fehlersuche im grundlegenden Verkehrsfluss
- Cisco Secure Firewall Threat Defense Geräte-Manager

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch