Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)

ID SFWIPA **Preis** 3.495,– € (exkl. MwSt.) **Dauer** 5 Tage

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

Kursüberblick

Die Schulung **Securing Data Center Networks and VPNs with Cisco Secure Firewall Threat Defense** zeigt Ihnen, wie Sie das Cisco Secure Firewall Threat Defense-System und seine Funktionen als Netzwerk-Firewall für Rechenzentren oder als Internet-Edge-Firewall mit Unterstützung für Virtual Private Networks (VPN) einsetzen und konfigurieren. Sie lernen, wie Sie identitätsbasierte Richtlinien, Secure Sockets Layer (SSL)-Entschlüsselung, Remote-Access-VPN und Site-to-Site-VPN konfigurieren, bevor Sie sich mit der erweiterten Konfiguration des Intrusion Prevention Systems (IPS) und der Ereignisverwaltung, der Integration mit anderen Systemen und der erweiterten Fehlerbehebung beschäftigen. Außerdem lernen Sie, wie Sie die Konfiguration und den Betrieb des Cisco Secure Firewall Threat Defense Systems mithilfe von Programmierbarkeit und Application Programming Interfaces (APIs) automatisieren und wie Sie die Konfiguration von Cisco Secure Firewall Adaptive Security Appliances (ASA) migrieren.

Dieses Training bereitet Sie auf die Prüfung 300-710 Securing Networks with Cisco Firepower (SNCF) vor. Bei Bestehen erhalten Sie die Zertifizierung Cisco Certified Specialist - Network Security Firepower und erfüllen die Anforderung der Konzentrationsprüfung für die Zertifizierung Cisco Certified Networking Professional (CCNP) Security. Mit diesem Training erhalten Sie außerdem 40 Continuing Education (CE) Credits für die Rezertifizierung.

Wie Sie davon profitieren

Diese Schulung wird Ihnen helfen:

- Erweiterte Kenntnisse der Cisco Secure Firewall Threat Defense-Technologie
- Erwerb von Kompetenzen und Fähigkeiten, die für die Implementierung und Verwaltung eines plattformunabhängigen Cisco Secure Firewall Threat Defense-Systems erforderlich sind
- Detaillierte Informationen über die Richtlinienverwaltung, den Verkehrsfluss im System und die Systemarchitektur
- Bereitstellung und Verwaltung vieler der erweiterten Funktionen des Cisco Secure Firewall Threat Defense-Systems
- Erwerb von Kenntnissen über Protokolle, Lösungen und Entwürfe, um Rollen auf Profi- und Expertenebene in Rechenzentren zu übernehmen
- Erwerben Sie 40 CE-Punkte für die Rezertifizierung

Was Sie bei der Prüfung erwartet

300-710 SNCF: Securing Networks with Cisco Firepower ist eine 90-minütige Prüfung, die mit der Cisco Certified Specialist - Network Security Firepower-Zertifizierung verbunden ist und die Voraussetzung für die Konzentrationsprüfung der CCNP Security-Zertifizierung erfüllt.

Das Multiple-Choice-Format testet Ihr Wissen über Cisco Firepower Threat Defense und die virtuellen Appliances der Firepower 7000- und 8000-Serien, einschließlich:

- Policy-Konfigurationen
- Integrationen
- Einsätze
- Verwaltung und Fehlerbehebung

Zielgruppe

- System Installers
- Systemintegratoren
- Systemverwalter
- Netzwerk-Administratoren
- Lösungsdesigner

Empfohlenes Training für die Zertifizierung zum

Cisco Certified Network Professional Security (CCNP SECURITY)

Voraussetzungen

Die Kenntnisse und Fähigkeiten, die Sie vor der Teilnahme an dieser Schulung haben sollten, sind

- Kenntnisse des Übertragungssteuerungsprotokolls/Internetprotokolls (TCP/IP)
- Grundkenntnisse von Routing-Protokollen
- Vertrautheit mit den Inhalten, die in der Schulung Securing Internet Edge with Cisco Secure Firewall Threat Defense erläutert werden

Diese Fähigkeiten können in den folgenden Cisco-Lernangeboten erworben werden:

- Implementing and Administering Cisco Solutions (CCNA) v2.1
- Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

Kursziele

- Beschreiben Sie die Cisco Secure Firewall-Bedrohungsabwehr
- Beschreibung der erweiterten Bereitstellungsoptionen von Cisco Secure Firewall Threat Defense
- Beschreiben der erweiterten Geräteeinstellungen für das Cisco Secure Firewall Threat Defense-Gerät
- Konfigurieren Sie dynamisches Routing auf der Cisco Secure Firewall Threat Defense
- Konfigurieren der erweiterten Netzwerkadressübersetzung auf Cisco Secure Firewall Threat Defense
- Konfigurieren Sie die SSL-Entschlüsselungsrichtlinie auf Cisco Secure Firewall Threat Defense
- Bereitstellung von Remote Access VPN auf Cisco Secure Firewall Threat Defense
- Einsatz von identitätsbasierten Richtlinien auf Cisco Secure Firewall Threat Defense
- Bereitstellung eines IPsec-basierten VPN auf der Cisco Secure Firewall Threat Defense
- Bereitstellung erweiterter Zugangskontroll-Einstellungen auf Cisco Secure Firewall Threat Defense
- Beschreibung der erweiterten Ereignisverwaltung von Cisco Secure Firewall Threat Defense
- Beschreibung der verfügbaren Integrationen mit Cisco Secure Firewall Threat Defense
- Fehlersuche im Datenverkehr mit den erweiterten Optionen von Cisco Secure Firewall Threat Defense
- Beschreiben Sie die Vorteile der Automatisierung von Konfiguration und Betrieb von Cisco Secure Firewall Threat Defense
- Beschreiben Sie die Migration der Konfiguration auf Cisco Secure Firewall Threat Defense

Detaillierter Kursinhalt

- Einführung in die Cisco Secure Firewall-Bedrohungsabwehr
- Beschreibung der erweiterten Bereitstellungsoptionen von Cisco Secure Firewall Threat Defense
- Konfigurieren von erweiterten Geräteeinstellungen auf Cisco Secure Firewall Threat Defense
- Konfigurieren des dynamischen Routings auf der Cisco Secure Firewall Threat Defense
- Konfigurieren von erweitertem NAT auf Cisco Secure Firewall Threat Defense
- Konfigurieren der SSL-Richtlinie auf Cisco Secure Firewall Threat Defense
- Bereitstellung von Remote Access VPN auf Cisco Secure Firewall Threat Defense
- Einsatz von identitätsbasierten Richtlinien auf Cisco Secure Firewall Threat Defense
- Bereitstellen von Site-to-Site VPN auf Cisco Secure Firewall Threat Defense
- Konfigurieren von Snort-Regeln und Netzwerkanalyse-Richtlinien
- Beschreibung der erweiterten Ereignisverwaltung Cisco Secure Firewall Threat Defense
- Beschreiben von Integrationen in Cisco Secure Firewall Threat Defense
- Fehlerbehebung für den erweiterten Datenverkehr auf der Cisco Secure Firewall Threat Defense
- Automatisierung der Cisco Secure Firewall-Bedrohungsabwehr
- Umstellung auf Cisco Secure Firewall Threat Defense

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