

Dieser Kurs vermittelt die Kenntnisse und Fähigkeiten zur Verwendung und Konfiguration der Cisco® Firepower Threat Defense-Technologie mit anfänglicher Geräteeinrichtung und -konfiguration, Routing, Hochverfügbarkeit, Cisco Adaptive Security Appliance (ASA) für die Migration, Verkehrssteuerung und Netzwerkadresse von Cisco Firepower Threat Defense Übersetzung (NAT). Sie lernen, wie Sie Site-to-Site VPN konfigurieren. Standort-VPN, RAS-VPN und SSL-Entschlüsselung, bevor Sie mit der detaillierten Analyse, der System-Administration und der Fehlerbehebung fortfahren.

Kursinhalt

- Cisco Firepower Threat Defense Overview
- Cisco Firepower NGFW Device Configuration
- Cisco Firepower NGFW Traffic Control
- Cisco Firepower NGFW Address Translation
- Cisco Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Site-to-Site VPN
- Remote-Access VPN
- SSL Decryption
- Detailed Analysis Techniques
- System Administration
- Cisco Firepower Troubleshooting

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernoberfläche integriert.

Zielgruppe

- Sicherheitsadministratoren
- Sicherheitsberater
- Netzwerkadministratoren
- Systemingenieure
- Personal des technischen Supports
- Cisco-Integratoren und -Partner

Voraussetzungen

- Kenntnisse über TCP / IP und grundlegende Routing-Protokolle
- Vertrautheit mit Firewall-, VPN- und IPS-Konzepten (Intrusion Prevention System)

Kursziel

This course helps you prepare to take the exam, Securing Networks with Cisco Firepower (300-710 SNCF), which leads to CCNP Security and Cisco Certified Specialist – Network Security Firepower certifications. The 300-710 SNCF exam has a second preparation course as well, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS). You can take these courses in any order.

Bearbeitungszeit

ca. 30 Stunden

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/FIPO

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referentengeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.	
6 Monate Freischaltung	€ 1.000,-

Training	Preise zzgl. MwSt.
Termine in Deutschland	5 Tage € 3.595,-
Online Training	5 Tage € 3.595,-
Terminen auf Anfrage	

Stand 02.03.2024

Inhaltsverzeichnis

SSNGFW – Securing Networks with Cisco Firepower Next Generation Firewall

Cisco Firepower Threat Defense Overview	Implementing an Access Control Policy	System Administration
Examining Firewall and IPS Technology		
Firepower Threat Defense Features and Components	Security Intelligence	Cisco Firepower Troubleshooting
Examining Firepower Platforms	Examining Security Intelligence	Examining Common Misconfigurations
Examining Firepower Threat Defense Licensing	Examining Security Intelligence Objects	Examining Troubleshooting Commands
Cisco Firepower Implementation Use Cases	Security Intelligence Deployment and Logging	Firepower Troubleshooting
	Implementing Security Intelligence	
Cisco Firepower NGFW Device Configuration	File Control and Advanced Malware Protection	Lab outline
Firepower Threat Defense Device Registration	Examining Malware and File Policy	Initial Device Setup
FXOS and Firepower Device Manager	Examining Advanced Malware Protection	Device Management
Initial Device Setup		Configuring High Availability
Managing NGFW Devices	Next-Generation Intrusion Prevention Systems	Migrating from Cisco ASA to Cisco Firepower Threat Defense
Examining Firepower Management Center Policies	Examining Intrusion Prevention and Snort Rules	Implementing QoS
Examining Objects	Examining Variables and Variable Sets	Implementing NAT
Examining System Configuration and Health Monitoring	Examining Intrusion Policies	Configuring Network Discovery
Device Management	Site-to-Site VPN	Implementing an Access Control Policy
Examining Firepower High Availability	Examining IPsec	Implementing Security Intelligence
Configuring High Availability	Site-to-Site VPN Configuration	Implementing Site-to-Site VPN
Cisco ASA to Firepower Migration	Site-to-Site VPN Troubleshooting	Implementing Remote Access VPN
Migrating from Cisco ASA to Firepower Threat Defense	Implementing Site-to-Site VPN	Threat Analysis
	Remote-Access VPN	System Administration
Cisco Firepower NGFW Traffic Control	Examining Remote-Access VPN	Firepower Troubleshooting
Firepower Threat Defense Packet Processing	Examining Public-Key Cryptography and Certificates	
Implementing QoS	Examining Certificate Enrollment	
Bypassing Traffic	Remote-Access VPN Configuration	
	Implementing Remote-Access VPN	
Cisco Firepower NGFW Address Translation	SSL Decryption	
NAT Basics	Examining SSL Decryption	
Implementing NAT	Configuring SSL Policies	
NAT Rule Examples	SSL Decryption Best Practices and Monitoring	
Implementing NAT		
Cisco Firepower Discovery	Detailed Analysis Techniques	
Examining Network Discovery	Examining Event Analysis	
Configuring Network Discovery	Examining Event Types	
	Examining Contextual Data	
Implementing Access Control Policies	Examining Analysis Tools	
Examining Access Control Policies	Threat Analysis	
Examining Access Control Policy Rules and Default Action	System Administration	
Implementing Further Inspection	Managing Updates	
Examining Connection Events	Examining User Account Management Features	
Access Control Policy Advanced Settings	Configuring User Accounts	
Access Control Policy Considerations		

