خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره CCNP Security-SSNGFW سیسکو | Securing Networks with Cisco Firepower Next Generation Firewall v۱.۰

شرح مختصر

دوره آمادگی شرکت در آزمون Concentration exam مدرک ۳۰۰-۷۱۰ SNCF جهت اخذ مدرک CCNP Security

مروری بر دوره

مروری بر دوره

دوره امنیت شبکه Securing Networks with Cisco Firepower Next Generation Firewall به آموزش استقرار و بکارگیری سیستم جلوگیری از تهدیدات امنیتی Cisco Firepower® Threat Defense می پردازد که در این دوره دانش و مهارت عملی لازم برای استفاده و پیکربندی فایروال Cisco® Firepower Threat Defence شامل تنظیمات اولیه، پیکربندی دستگاه و مسیریابی ، دسترس پذیری بالا ، مهاجرت از فایروال Cisco Adaptive Security Appliance (ASA) سیسکو به فایروال Cisco® Firepower Threat Defence ، کنترل ترافیک و ترجمه آدرس شبکه (NAT)، پیاده سازی ویژگی های امنیتی فایروال های نسل جدید سیسکو Next-Generation Firewall (NGFW) و سیستم جلوگیری از نفوذ نسل جدید سیسکو Next-Generation Intrusion Prevention System (NGIPS) شامل هوش شبکه ای(NI) ، تشخیص نوع فایل ، تشخیص بدافزار مبتنی بر شبکه و بررسی دقیق بسته های شبکه (DPI) و بعلاوه پیکربندی remote-access VPN ، site-to-site VPN و SSL decryption پیش از تجزیه و تحلیل دقیق بسته ها و مدیریت و عیب یابی سیستم ها به متقاضیان آموزش داده شود.

دوره آمادگی لازم جهت شرکت در آزمون (SNCF ۳۰۰-۷۱۰) Securing Networks with Cisco Firepower برای کسب مدارک CCNP Security و Cisco Certified Specialist – Network Security Firepower certifications شامل دو دوره Securing Networks with Cisco Firepower Next Generation Firewall(SSNGFW) v۱.۰ و Securing Networks with Cisco Firepower Next-

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

(SSFIPS) Generation Intrusion Prevention System می باشد که امکان شرکت در دوره های فوق با هر ترتیبی برای متقاضیان امکان پذیر می باشد.

مزایای دوره

پیاده سازی فایروال Cisco Firepower NGFW به منظور محافظت پیشرفته در برابر تهدیدات پیش از حمله، در زمان حمله و پس از حمله

کسب برترین مهارتها و شایستگی های کاری جهت اخذ مشاغل پر متقاضی حوزه امنیت شبکه

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- توصیف مفاهیم کلیدی فناوری های NGFW ، NGIPS ، فایروال Cisco Firepower Threat Defense system و روش های استقرار آنها در شبکه ها
- اجرای تنظیمات اولیه و راه اندازی فایروال Cisco Firepower Threat Defence
- شیوه مدیریت ترافیک و کیفیت خدمات (QoS) با استفاده از Cisco Firepower Threat Defense
- پیاده سازی NAT با استفاده از Cisco Firepower Threat Defence
- اجرای network discovery با استفاده از Cisco Firepower به منظور شناسایی host ها، برنامه های کاربردی و خدمات
- توصیف شیوه های عملکردی و کاربردی اجرای policy های کنترل دسترسی
- توصیف مفاهیم و روشهای اجرای ویژگیهای هوش امنیتی
- توصیف راهکار امنیتی (AMP) Cisco Advanced Malware Protection در کنترل فایل ها و محافظت در مقابل بدافزار های پیشرفته شبکه
- پیاده سازی و مدیریت policy های نفوذ به شبکه(intrusion policies)
- توصیف اجزا و پیکربندی site-to-site VPN
- توصیف و پیکربندی SSL VPN با دسترسی از راه دور با استفاده از Cisco AnyConnect®

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- قابلیت ها و کاربرد رمزگشایی پروتکل امن SSL decryption

سرفصل ها (حضوری)

سرفصل ها

Outline

- Cisco Firepower Threat Defense Overview
- Examining Firewall and IPS Technology
- Firepower Threat Defense Features and Components
- Examining Firepower Platforms
- Examining Firepower Threat Defense Licensing
- Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
- Firepower Threat Defense Device Registration
- FXOS and Firepower Device Manager
- Initial Device Setup
- Managing NGFW Devices
- Examining Firepower Management Center Policies
- Examining Objects
- Examining System Configuration and Health Monitoring
- Device Management
- Examining Firepower High Availability
- Configuring High Availability
- Cisco ASA to Firepower Migration
- Migrating from Cisco ASA to Firepower Threat Defense

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Cisco Firepower NGFW Traffic Control
- Firepower Threat Defense Packet Processing
- Implementing QoS
- Bypassing Traffic
- Cisco Firepower NGFW Address Translation
- NAT Basics
- Implementing NAT
- NAT Rule Examples
- Implementing NAT
- Cisco Firepower Discovery
- Examining Network Discovery
- Configuring Network Discovery
- Implementing Access Control Policies
- Examining Access Control Policies
- Examining Access Control Policy Rules and Default Action
- Implementing Further Inspection
- Examining Connection Events
- Access Control Policy Advanced Settings
- Access Control Policy Considerations
- Implementing an Access Control Policy
- Security Intelligence
- Examining Security Intelligence
- Examining Security Intelligence Objects
- Security Intelligence Deployment and Logging
- Implementing Security Intelligence
- File Control and Advanced Malware Protection

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Examining Malware and File Policy
- Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Examining Intrusion Prevention and Snort Rules
- Examining Variables and Variable Sets
- Examining Intrusion Policies
- Site-to-Site VPN
- Examining IPsec
- Site-to-Site VPN Configuration
- Site-to-Site VPN Troubleshooting
- Implementing Site-to-Site VPN
- Remote-Access VPN
- Examining Remote-Access VPN
- Examining Public-Key Cryptography and Certificates
- Examining Certificate Enrollment
- Remote-Access VPN Configuration
- Implementing Remote-Access VPN
- SSL Decryption
- Examining SSL Decryption
- Configuring SSL Policies
- SSL Decryption Best Practices and Monitoring
- Detailed Analysis Techniques
- Examining Event Analysis
- Examining Event Types
- Examining Contextual Data
- Examining Analysis Tools

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- Threat Analysis
- System Administration
- Managing Updates
- Examining User Account Management Features
- Configuring User Accounts
- System Administration
- Cisco Firepower Troubleshooting
- Examining Common Misconfigurations
- Examining Troubleshooting Commands
- Firepower Troubleshooting

Lab outline

- Initial Device Setup
- Device Management
- Configuring High Availability
- Migrating from Cisco ASA to Cisco Firepower Threat Defense
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

مخاطبان دوره

مخاطبان دوره

- ادمین های امنیت شبکه
- مشاوران امنیت شبکه
- ادمین های شبکه
- مهندسان سیستم
- نیروهای پشتیبانی فنی
- یکپارچه سازان و پارتنرهای سیسکو

پیش نیاز ها

پیش نیازها

- دارا بودن دانش کامل از مدل شبکه TCP / IP و پروتکل های اصلی مسیریابی
- آشنایی با مفاهیم فایروال ، VPN و سیستم جلوگیری از نفوذ (IPS)