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

دوره CCNP Security-SWSA سیسکو | Securing the Web with Cisco Web Security Appliance v۳.۰

شرح مختصر

دوره آمادگی شرکت در آزمون Concentration exam مدرک ۳۰۰-۷۲۵ SWSA جهت اخذ مدرک CCNP Security

مروری بر دوره

مروری بر دوره

دوره امنیت v۳.۰ (SWSA) Cisco Web Security Appliance Appliance پیاده سازی ، نصب، راه اندازی و نگهداری از فایروال امنیت وب سیسکو (WSA) Cisco® Web Security Appliance با بهره گیری از ساختار Cisco Talos ، محافظت پیشرفته از ایمیل های تجاری و کنترل در مقابل تهدیدات امنیتی وب سایت ها با استفاده از آموزش های تخصصی و عملی ، راه اندازی خدمات پراکسی ، استفاده از سیستم احراز هویت ، اجرای policy های مربوط به دسترسی ها وکنترل ترافیک HTTPS ، اجرای تنظیمات کنترلی و policyها ، استفاده از ویژگی های راهکار anti-malware، پیاده سازی امنیت داده ها و data loss prevention (قابلیت جلوگیری از دست رفتن داده)، مدیریت راهکار Cisco WSA و موارد دیگر را به متقاضیان آموزش می دهد.

این دوره، آمادگی لازم جهت شرکت در آزمون Securing the Web with Cisco Web Security Appliance (SWSA ۷۲۵-۳۰۰) جهت اخذ مدارک CCNP Security و Cisco Certified Specialist - Web Content Security را برای فراگیران فراهم می نماید.

مزایای دوره

توانایی پیاده سازی فایروال Cisco WSA در جهت امنیت گیت وی های وب ، ارائه محافظت در مقابل بدافزارها و استفاده از policyهای کنترلی در جهت حل مشکلات و مقابله با چالش های ایمن سازی و کنترل ترافیک وب

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

کسب مهارتهای عملی پیشرفته برای اخذ مشاغل پر متقاضی حوزه امنیت وب

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- توصیف Cisco WSA
- پیاده سازی سرویس های پروکسی
- بکارگیری سیستم احراز هویت
- توصیف policy های رمزگشایی برای کنترل ترافیک HTTPS از سایر ترافیک ها
- درک policy های differentiated traffic access و پروفایل های شناسایی
- اجرای acceptable use control settings
- مقابله با بدافزارها
- توصیف امنیت داده و data loss prevention
- مدیریت و عیب یابی

سرفصل ها (حضوری)

سرفصل ها

Outline

Describing Cisco WSA

- Technology Use Case
- Cisco WSA Solution
- Cisco WSA Features
- Cisco WSA Architecture
- Proxy Service

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

- Integrated Layer ۴ Traffic Monitor
- Data Loss Prevention
- Cisco Cognitive Intelligence
- Management Tools
- Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
- Cisco Content Security Management Appliance (SMA)

Deploying Proxy Services

- Explicit Forward Mode vs. Transparent Mode
- Transparent Mode Traffic Redirection
- Web Cache Control Protocol
- Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
- Proxy Bypass
- Proxy Caching
- Proxy Auto-Config (PAC) Files
- FTP Proxy
- Socket Secure (SOCKS) Proxy
- Proxy Access Log and HTTP Headers
- Customizing Error Notifications with End User Notification (EUN) Pages

Utilizing Authentication

- Authentication Protocols
- Authentication Realms
- Tracking User Credentials
- Explicit (Forward) and Transparent Proxy Mode

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

- Bypassing Authentication with Problematic Agents
- Reporting and Authentication
- Re-Authentication
- FTP Proxy Authentication
- Troubleshooting Joining Domains and Test Authentication
- Integration with Cisco Identity Services Engine (ISE)

Creating Decryption Policies to Control HTTPS Traffic

- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
- Certificate Overview
- Overview of HTTPS Decryption Policies
- Activating HTTPS Proxy Function
- Access Control List (ACL) Tags for HTTPS Inspection
- Access Log Examples

Understanding Differentiated Traffic Access Policies and Identification Profiles

- Overview of Access Policies
- Access Policy Groups
- Overview of Identification Profiles
- Identification Profiles and Authentication
- Access Policy and Identification Profiles Processing Order
- Other Policy Types
- Access Log Examples
- ACL Decision Tags and Policy Groups
- Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications

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

Defending Against Malware
- Web Reputation Filters
- Anti-Malware Scanning
- Scanning Outbound Traffic
- Anti-Malware and Reputation in Policies
- File Reputation Filtering and File Analysis
- Cisco Advanced Malware Protection
- File Reputation and Analysis Features
- Integration with Cisco Cognitive Intelligence

Enforcing Acceptable Use Control Settings
- Controlling Web Usage
- URL Filtering
- URL Category Solutions
- Dynamic Content Analysis Engine
- Web Application Visibility and Control
- Enforcing Media Bandwidth Limits
- Software as a Service (SaaS) Access Control
- Filtering Adult Content

Data Security and Data Loss Prevention
- Data Security
- Cisco Data Security Solution
- Data Security Policy Definitions
- Data Security Logs

Performing Administration and Troubleshooting
- Monitor the Cisco Web Security Appliance
- Cisco WSA Reports

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

- Monitoring System Activity Through Logs
- System Administration Tasks
- Troubleshooting
- Command Line Interface

References

- Comparing Cisco WSA Models
- Comparing Cisco SMA Models
- Overview of Connect, Install, and Configure
- Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
- Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
- Connecting to the Cisco Web Security Virtual Appliance
- Enabling Layer ۴ Traffic Monitor (L۴TM)
- Accessing and Running the System Setup Wizard
- Reconnecting to the Cisco Web Security Appliance
- High Availability Overview
- Hardware Redundancy
- Introducing Common Address Redundancy Protocol (CARP)
- Configuring Failover Groups for High Availability
- Feature Comparison Across Traffic Redirection Options
- Architecture Scenarios When Deploying Cisco AnyConnect® Secure Mobility

Lab outline

- Configure the Cisco Web Security Appliance

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

- Deploy Proxy Services
- Configure Proxy Authentication
- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office ۳۶۵ External Feed
- Validate an Intermediate Certificate
- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

مخاطبان دوره

مخاطبان دوره

- معماران امنیتی
- طراحان سیستم
- ادمین های شبکه
- مهندسان اجرایی
- مدیران شبکه، تکنسین های امنیتی یا شبکه و منهدسان و مدیران امنیت فعال در حوزه امنیت وب
- یکپارچه سازان و پارتنرهای سیسکو

پیش نیاز ها

پیش نیازها

- دارا بودن دانش کامل از سرویس های TCP / IP شامل Domain Name System (DNS)، Secure

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

HTTP ، Simple Network Management Protocol (SNMP)، FTP، Shell (SSH) و HTTPS

- دانش IP routing
- دارابودن یک یا چند مورد از مهارت های پایه ای زیر یا دانش معادل آن:
- اخذ یکی از مدارک سیسکو (CCENT certification یا مدارک در سطوح بالاتر)
- اخذ مدارک مرتبط با حوزه کاری(International Information System Security Certification Consortium ((ISC)۲، +Computing Technology Industry Association (CompTIA) Security، International Council of Electronic Commerce Consultants (EC-Council) ، Global Information Assurance Certification (GIAC)، ISACA).
- اخذ مدرک ۱ ®CCNA (Cisco Networking Academy و ۲ CCNA)
- اخذ مدارک تخصصی سیستم عامل ویندوز: Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA) ، Microsoft Certified Solutions Expert (MCSE) و CompTIA (A+, Network+, Server+)
- استفاده از منابع آموزشی سیسکو در حوزه امنیت وب که از لینک زیر قابل دسترس می باشد:
- https://www.cisco.com/c/m/en_us/products/security/web-security-training.html