

دوره CCNP Security Pack

دوره کامل و جامع امنیت شبکه سیسکو

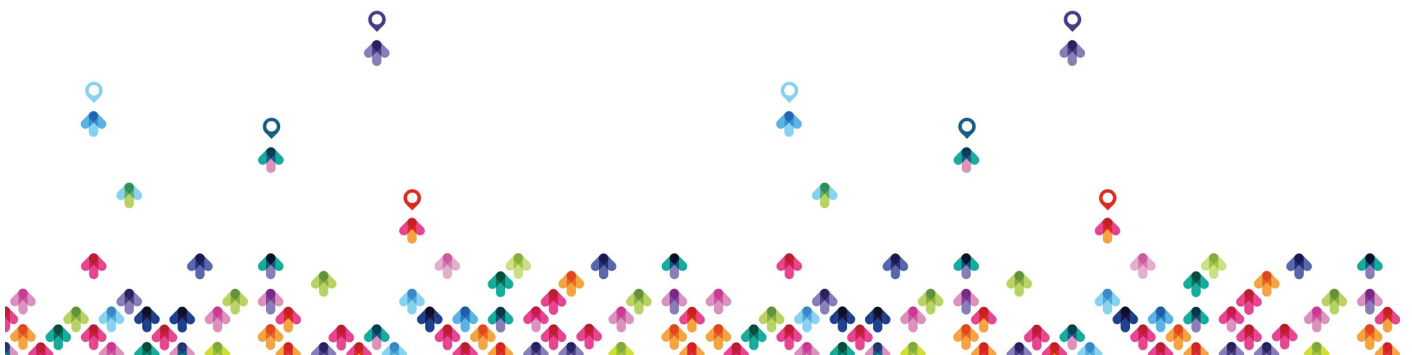
مروری بر دوره

دوره آموزشی **CCNP Security** مختص کسانی طراحی شده است که علاوه بر وظیفه برقراری امنیت تجهیزات شبکه اعم از سوئیچ ها، روترها و تجهیزات و دیوایس های مربوط به شبکه، وظیفه انتخاب، پیاده سازی و پشتیبانی و عیب یابی در فایروال ها، VPN ها و همچنین راهکارهای **IDS/IPS** در محیط های مبتنی بر تجهیزات شبکه را بر عهده دارند. این دوره به صورت **PACK** (جاه برگزار می شود تا نیاز متخصصین امنیت شبکه به دوره های آموزشی امنیت را یکجا پوشش دهد. محتوا و سرفصل های این دوره ترکیبی از دوره **CCNP Security** به نام های زیر می باشد:

- دوره [Implementing Cisco Edge Network Security Solutions \(SENSS\)](#)
- دوره [Implementing Cisco Threat Control Solutions \(SITCS\)](#)
- دوره [Implementing Cisco Secure Access Solutions \(SISAS\)](#)
- دوره [Implementing Cisco Secure Mobility Solutions \(SIMOS\)](#)

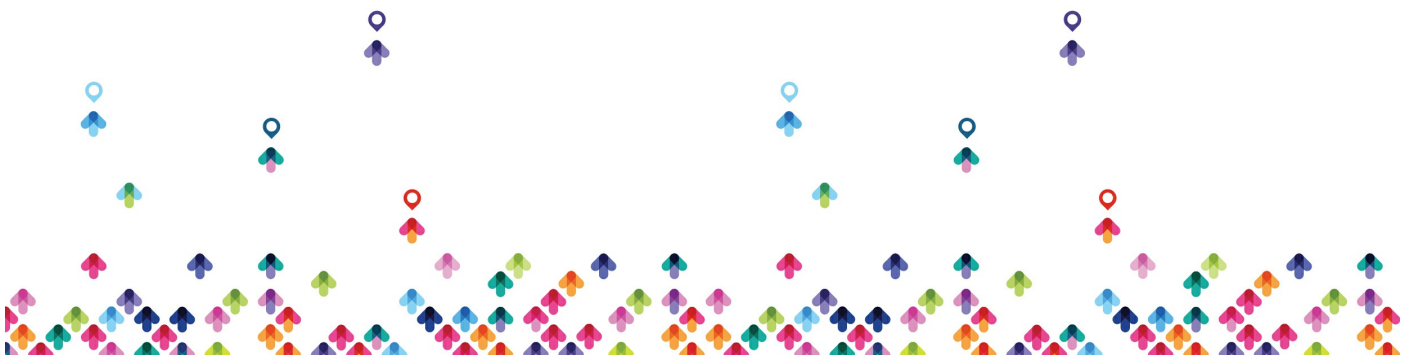
آنچه در این دوره خواهید آموخت

- دورنمای تهدیدات امنیتی
- پیاده سازی معماری امنیت شبکه های ماژولار Cisco مانند SecureX و TrustSec
- راه اندازی مدیریت زیرساخت Cisco و اداره control plane security
- پیکربندی نحوه اداره data plane security در لایه های 2 و 3 Cisco
- پیاده سازی و نگهداری Cisco ASA Network (Address Translations (NAT
- پیاده سازی و نگهداری Cisco IOS Software NAT
- طراحی و راه اندازی راهکارهای دفاعی مقابله با تهدیدات سایبری ارائه شده توسط Cisco در ASA هایی که از



سیاست‌های دسترسی و اپلیکیشن‌ها و شناسایی مبتنی بر inspection استفاده می‌کنند

- پیاده‌سازی فیلتر کننده‌های ترافیک‌های Botnet
- راه‌اندازی Cisco IOS Zone-Based Policy (Firewalls (ZBFW
- پیکربندی و verify کردن Cisco IOS ZBFW
- Application Inspection Policy
- تجهیزات Cisco Web Security
- Cisco Cloud Web Security
- تجهیزات Advanced Malware Protection
- Cisco FirePOWER Next-Generation IPS
- سرویس‌های Cisco ASA FirePOWER
- نوع معماری Cisco ISE و قابلیت‌های مرتبط با کنترل دسترسی (access control)
- معماری، پیاده‌سازی و عملیات مرتبط با پروتکل امنیتی 802.1X
- پیاده‌سازی Extensible Authentication (EAPs) (Protocols) به شکل معمول
- پیاده‌سازی (public key infrastructure (PKI با استفاده از ISE
- پیاده‌سازی پایگاه داده‌های داخلی و خارجی احراز هویت (authentication databases)
- پیاده‌سازی (MAC Authentication Bypass (MAB
- پیاده‌سازی سیاست‌های شناسایی مبتنی بر authorization
- ویژگی‌های Cisco TrustSec
- پیاده‌سازی web authentication و guest access
- پیاده‌سازی خدمات ISE Posture
- پیاده‌سازی ISE Profiling
- (Bring Your Own Device (BYOD و ارتباط آن با ISE
- عیب‌یابی ISE
- انواع فناوری‌های مربوط به VPN و همچنین راه‌اندازی الگوریتم‌های cryptographic و پروتکل‌هایی که



امنیت VPN را فراهم می‌کنند

- پیاده‌سازی و نگهداری راهکارهای site-to-site VPN
- پیاده‌سازی و نگهداری Cisco FlexVPN در VPN های point-to-point و hub-and-spoke
- پیاده‌سازی و نگهداری VPN های clientless SSL شرکت Cisco
- پیاده‌سازی و نگهداری VPN های AnyConnect SSL و IPsec شرکت Cisco
- پیاده‌سازی و نگهداری endpoint security و dynamic access policies (DAP)

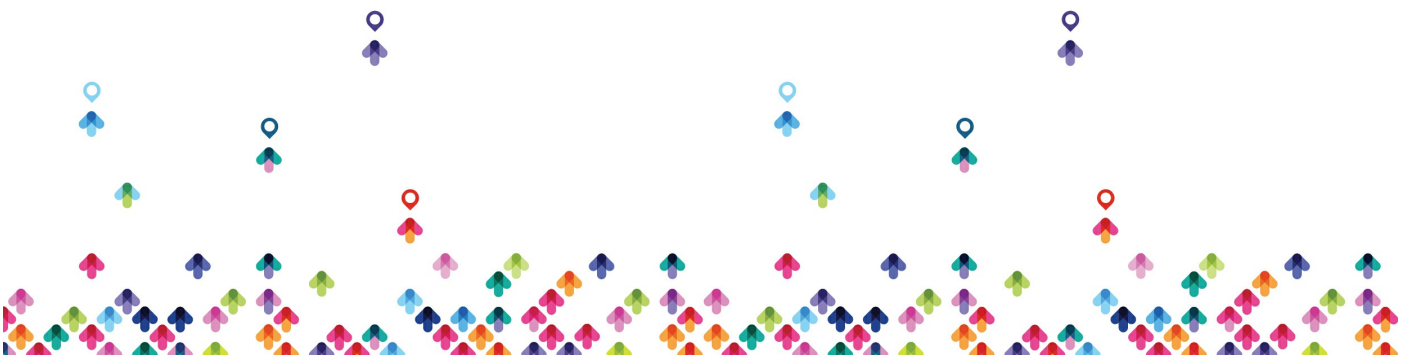
سرفصل‌ها

1. Secure Design Principles

- Course Overview
- Network Security Zoning
- Cisco Module Network Security Architecture
- Cisco SecureX Architecture
- Cisco TrustSec Solution

2. Deploying Network Infrastructure Protection

- Introducing Cisco Network Infrastructure Protection
- Deploying Cisco IOS Control Plane Security Controls
- Deploying Cisco IOS Management Plane Security Controls
- Deploying Cisco ASA Management Plane Security Controls
- Deploying Cisco Traffic Telemetry Methods
- Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls



3. Deploying NAT on Cisco IOS and Cisco ASA

- Introducing Network Address Translation
- Deploying Cisco ASA Network Address Translation
- Deploying Cisco IOS Software Network Address Translation

4. Deploying Threat Controls on Cisco ASA

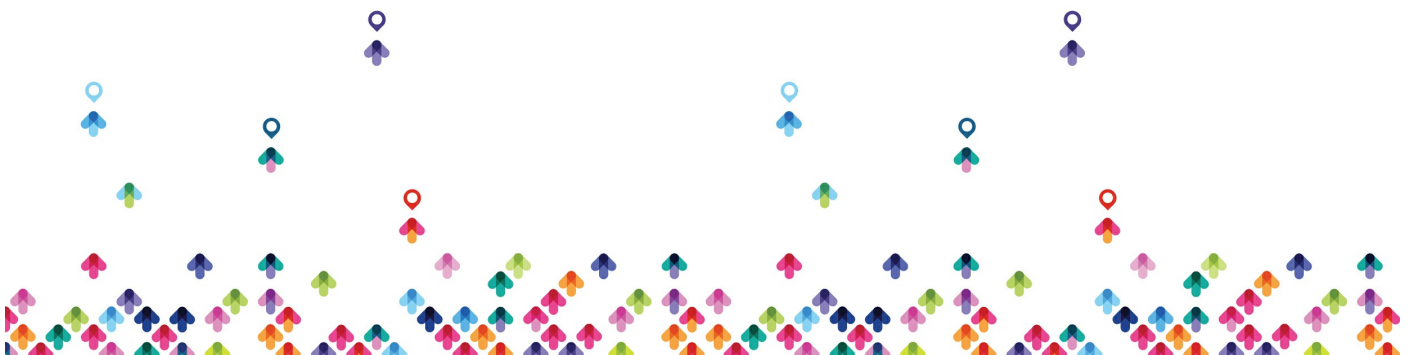
- Introducing Cisco Firewall Threat Controls
- Deploying Basic Cisco ASA Access Policies
- Deploying Advanced Cisco ASA Application Inspection Policies
- Deploying Cisco ASA Botnet Traffic Filtering
- Deploying Cisco ASA Identity Based Firewall

5. Deploying Threat Controls on Cisco IOS Software

- Deploying Basic Cisco IOS Software with Basic Zone-Based Firewall Access Policies
- Deploying Advanced Cisco IOS Software ZBFW with Application Inspection Policies

6. Cisco Web Security Appliance

- Cisco Web Security Appliance (WSA) Solutions
- Integrating the Cisco Web Security Appliance
- Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Configuring Cisco Web Security Appliance Acceptable Use Control



- Configuring Cisco Web Security Appliance Anti-Malware Controls
- Configuring Cisco Web Security Appliance Decryption
- Configuring Cisco Web Security Appliance Data Security Controls

7. Cisco Cloud Web Security

- Cisco Cloud Web Security Solutions
- Configuring Cisco Cloud Web Security Connectors
- Web Filtering Policy in Cisco ScanCenter

8. Cisco Email Security Appliance

- Cisco Email Security Solutions
- Cisco Email Security Appliance Basic Setup Components
- Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies

9. Advanced Malware Protection for Endpoints

- AMP for Endpoints Overview and Architecture
- Customizing Detection and AMP Policy
- IOCs and IOC Scanning
- Deploying AMP Connectors
- AMP Analysis Tools

10. Cisco FirePOWER Next-Generation IPS

- Cisco FireSIGHT System
- Configuring and Managing Cisco FirePOWER Devices



- Implementing an Access Control Policy
- Discovery Technology
- Configuring File-Type and Network Malware Detection
- Managing SSL Traffic with Cisco FireSIGHT
- IPS Policy and Configuration Concepts
- Network Analysis Policy
- Creating Reports
- Correlation Rules and Policies
- Basic Rule Syntax and Usage

11. Cisco ASA FirePOWER Services

- Installing Cisco ASA 5500-X Series FirePOWER Services (SFR)

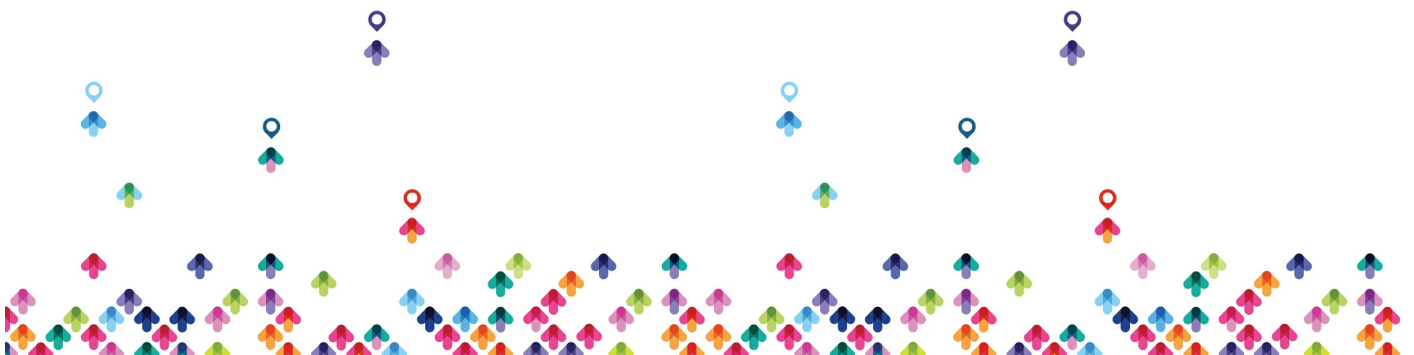
12. Threat Mitigation through Identity Services

- Identity Services
- 802.1X and EAP
- Configure 802.1X Components

13. ISE Fundamentals

- Describe Cisco ISE Features and configure the fundamentals
- Cisco ISE with PKI
- Cisco ISE Authentication
- Cisco ISE with External Authentication

14. Advance Access Control



- Certificate Based User Authentication
- Authorization
- Cisco TrustSec

15. Web Authentication and Guest Access

- Web Authentication
- Guest Access Services

16. Endpoint

- Posture
- Profiler
- BYOD

17. Troubleshooting Network Access Control

- Troubleshooting ISE

18. Fundamentals of VPN Technologies and Cryptography

- The Role of VPNs in Network Security
- VPNs and Cryptography

19. Deploying Secure Site-to-Site Connectivity Solutions

- Introducing Cisco Secure Site-to-Site Connectivity Solutions
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA



- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Deploying Cisco IOS DMVPNs

20. Deploying Cisco IOS Site-to-Site FlexVPN Solutions

- Introducing Cisco IOS Site-to-Site FlexVPN Solutions
- Deploying Point-to-Point IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Hub-and-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Spoke-to-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Basic Cisco Clientless SSL VPN
- Clientless SSL VPN Overview
- Deploying Basic Cisco Clientless SSL VPN on Cisco ASA
- Deploying Application Access in Cisco ASA Clientless SSL VPN
- Deploying Advanced Authentication and Authorization in Clientless SSL VPN

21. Deploying Cisco AnyConnect VPNs

- Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs
- Deploying Cisco AnyConnect IPsec/IKEv2 VPNs

22. Deploying Endpoint Security and Dynamic Access Policies

- Implementing Host Scan



- Implementing DAP for SSL VPNs

مخاطبان دوره

- مهندسين امنيت شبکه

پیش نیازها

- دوره **IINS سیسکو | Implementing Cisco IOS Network Security 3.0**

- دوره **CCNAX v3.0 سیسکو | CCNA Routing and Switching**

