

دوره IINS سیسکو | دوره CCNA Security

شرح مختصر

آماده سازی داوطلبین جهت شرکت در آزمون اخذ مدرک - (۲۱۰) CCNA Security IINS (۲۶۰)

مروری بر دوره

مروری بر دوره

در این دوره شما در قالب مثال‌هایی با چگونگی طراحی، پیاده‌سازی و نظارت‌های مربوط به سیاست‌های کلی امنیتی با استفاده از تجهیزات و فناوری‌های امنیتی Cisco IOS، آشنا خواهید شد. شناخت کنترل‌کننده‌های امنیتی دستگاه‌های Cisco IOS و نیز کاربردهای Cisco Adaptive Security Appliance (ASA) از دیگر مطالبی است که در طی این دوره به شما معرفی خواهد شد. این دوره شما را قادر خواهد ساخت که بتوانید از طریق ویژگی‌های امنیتی Cisco IOS، که دسترسی به آنان در Cisco ASA از طریق GUI های مبتنی بر وب و در router ها و switch های Cisco از طریق (CLI) ممکن است را انجام دهید.

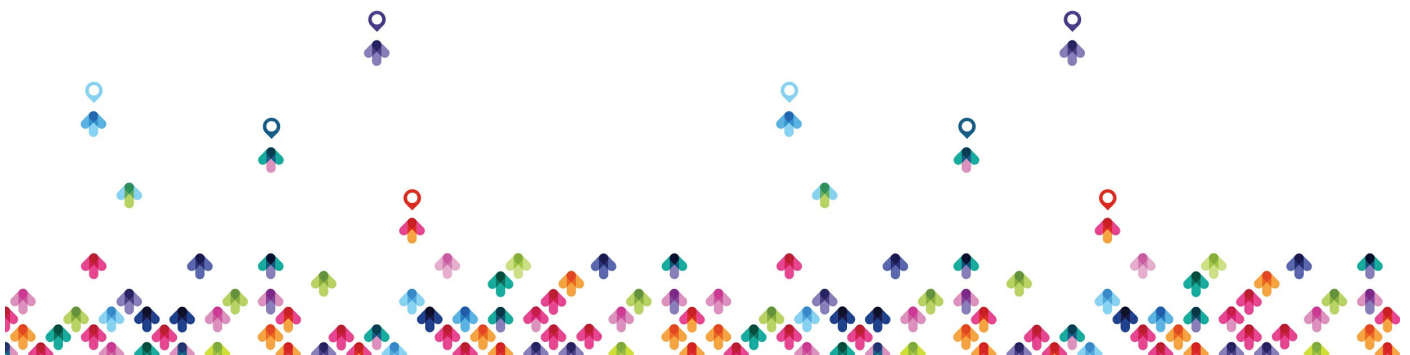
[دانلود نقشه راه سسکو](#)

از دیگر مطالبی که در طی این دوره به شما آموخته خواهد شد می‌توان به چگونگی پیکربندی VPN های Site-to-site در Cisco IOS و Cisco ASA، نمونه‌هایی از malware مدرن و همچنین تکنیک‌های cryptographic با استفاده از hashing و الگوریتم‌های رمزنگاری اشاره کرد.

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

▪ مفاهیم رایج مرتبط با امنیت شبکه



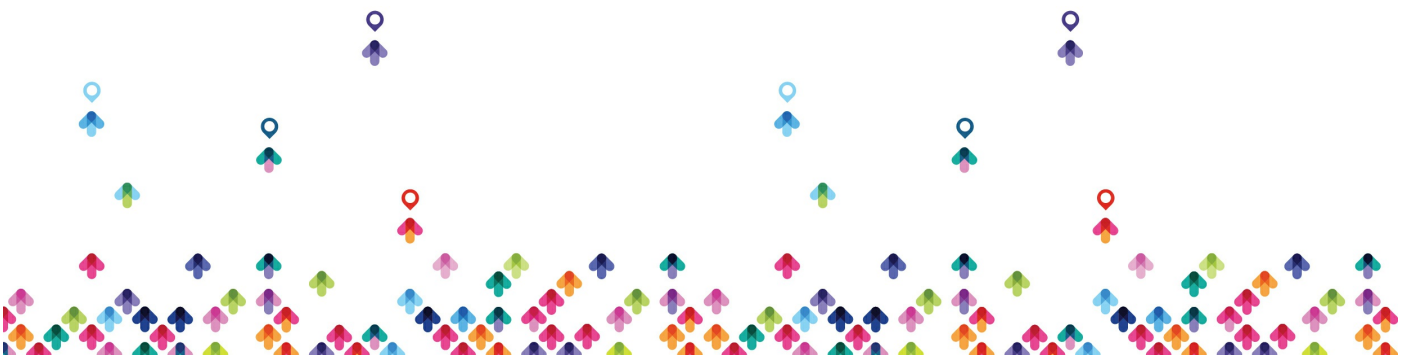
- ایمن‌سازی زیرساخت‌های مربوط به **switching** و **routing**
- راه‌اندازی سرویس‌های اصلی **accounting** و **authentication, authorization**
- راه‌اندازی سرویس‌های اصلی مربوط به **firewall**
- راه‌اندازی سرویس‌های **VPN remote access** و **site-to-site**
- سرویس‌های امنیتی پیشرفته مانند حفاظت در برابر نفوذ، امنیت محتوا و **identity management**
- توسعه سیاست‌های امنیتی جامع در شبکه با هدف مقابله با تهدیدات امنیت اطلاعات
- پیکربندی **router** ها با استفاده از ویژگی‌های نرم‌افزاری **Cisco IOS** شامل مدیریت و گزارش دهی کارکرد
- انجام **Bootstrap** در **Cisco ASA Firewall** به منظور استفاده در **production network**
- پیکربندی **Cisco ASA Firewall** برای دسترسی **remote** به یک **VPN SSL**
- پیکربندی **(Cisco IOS zone-based firewall) (ZBF)** به منظور برقراری عملیات اصلی مربوط به امنیت بر روی شبکه
- پیکربندی **VPN site-to-site** های با استفاده از ویژگی‌های **Cisco IOS**
- پیکربندی مشخصه‌های امنیتی بر روی **IOS** سوئیچ‌ها با هدف حمایت از انواع حملات که به لایه‌های ۲ و ۳ انجام می‌شود
- چگونگی به خطر افتادن شبکه با استفاده از ابزارهای رایگان موجود
- پیاده‌سازی **line password** و فعال‌سازی **password** ها و **secret** ها
- نگاهی به مفاهیم مربوط به **authentication, authorization** و **(AAA) accounting** و ویژگی‌های آن
- با استفاده از **local database** و همچنین **۵.۲ Cisco Secure ACS**
- پیکربندی فیلتر کردن بسته‌ها (**packet filtering**) بر روی **perimeter router**

سرفصل‌ها (حضوری)

سرفصل‌ها

۱. Security Concepts

- Threatscape
- Threat defense technologies



- Security policy and basic security architectures
- Cryptographic technologies

۲. Secure Network Devices

- Implementing AAA
- Management protocols and systems
- Securing the control plane

۳. Layer ۲ Security

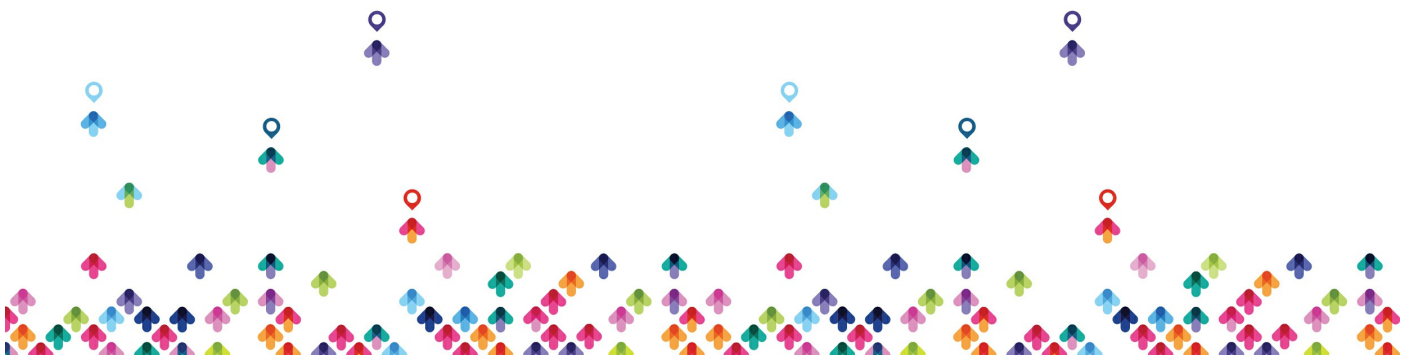
- Securing Layer ۲ infrastructures
- Securing Layer ۲ protocols

۴. Firewall

- Firewall technologies
- Introducing the Cisco ASA v۹.۲
- Cisco ASA access control and service policies
- Cisco IOS zone based firewall

۵. VPN

- IPsec technologies
- Site-to-site VPN
- Client-based remote access VPN
- Clientless remote access VPN



۶. Advanced Topics

- Intrusion detection and protection
- Endpoint protection
- Content security
- Advanced network security architectures

مخاطبان دوره

مخاطبان دوره

- طراحان شبکه
- مهندسين شبکه، سيستم و امنيت
- مديران شبکه و امنيت

پیش نیازها

پیش نیازها

- دانش کار با سیستم عامل ویندوز
- دانش کار با شبکه مبتنی بر Cisco IOS و مفاهیم مربوط به آن

- دوره [ICND1 v3.0 سیسکو | Interconnecting Cisco Networking Devices, Part 1](#)

دوره های مرتبط

دوره های مرتبط

- دوره [SENSS سیسکو | Implementing Cisco Edge Network](#)



Security Solutions

دوره SIMOS سیسکو | Implementing Cisco Secure Mobility Solutions

دوره SISAS سیسکو | Implementing Cisco Secure Access Solutions

دوره SITCS v۱.۵ سیسکو | Implementing Cisco Threat Control Solutions

