Advanced Network Security Architecture and Defense Training Course



19 - 23 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB5303_89383

Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of modern network security architecture and perimeter defense strategies. In an era of sophisticated cyber threats, a reactive security posture is no longer sufficient. This program is designed to equip participants with the forward-thinking skills needed to design, implement, and manage resilient and proactive security infrastructures. Drawing on foundational principles discussed by experts like William Stallings in his work "Network Security Essentials", the course moves beyond basic configurations to instill a deep architectural understanding. Participants will master the principles of defense-in-depth, layered security, and the evolving concept of the network perimeter in the age of cloud computing and remote work. At BIG BEN Training Center, we focus on building a strategic mindset, enabling professionals to create security frameworks that not only defend against current threats but are also adaptable to future challenges. This course covers everything from next-generation firewalls and intrusion prevention systems to advanced concepts like Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE), ensuring a holistic and up-to-date learning experience.

Target Audience / This training course is suitable for:

- Network Security Engineers.
- Cybersecurity Analysts.
- IT Security Managers and Directors.
- Network Architects and Administrators.
- Systems Engineers.
- Security Operations Center (SOC) personnel.
- IT professionals seeking to specialize in network security.
- Information Security Consultants.
- IT Auditors responsible for assessing network security controls.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Government and Public Sector Agencies.
- Energy and Utilities.
- Retail and E-commerce.
- Manufacturing and Industrial Control Systems.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security (InfoSec) Department.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Risk and Compliance Departments.
- Internal Audit Department.
- Infrastructure and Operations Teams.

Course Offerings:

By the end of this course, the participants will have able to:

- Design a robust defense-in-depth security architecture for enterprise networks.
- Evaluate and implement next-generation firewall (NGFW) policies and features.
- Deploy and manage effective intrusion detection and prevention systems (IDS/IPS).
- Apply the principles of the Zero Trust security model to network design.
- Develop secure network segmentation and micro-segmentation strategies.
- Configure and secure virtual private networks (VPNs) for remote access.
- Analyze network traffic to identify and mitigate security threats.
- Integrate various security technologies into a cohesive defense strategy.
- Develop an incident response plan for network-based security breaches.
- Understand and apply security principles for cloud and hybrid network environments.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn theoretical concepts but can also apply them in real-world scenarios. Our approach moves beyond traditional lectures to foster a dynamic learning environment. The course is built upon a foundation of expert-led instruction, where seasoned professionals share their deep industry knowledge and practical insights. This is complemented by a series of hands-on lab simulations, detailed case studies of real security incidents, and collaborative group exercises that encourage problem-solving and critical thinking. Participants will engage in interactive discussions, Q&A sessions, and peer-to-peer knowledge sharing, allowing them to explore complex security challenges from multiple perspectives. Continuous feedback is provided by the instructor to guide learning and reinforce key architectural principles. This blended learning approach ensures that participants leave the course with both the strategic understanding and the practical skills necessary to design and defend complex network infrastructures effectively.

Course Agenda (Course Units):

Unit One Foundations of Modern Network Security Architecture

- Introduction to network security principles and concepts.
- Understanding the modern threat landscape and attack vectors.
- The defense-in-depth and layered security models.
- Exploring security architecture frameworks (e.g., SABSA, TOGAF).
- Conducting security risk assessments and threat modeling.
- Developing and implementing security policies and standards.
- Fundamentals of secure network design and topology.

Unit Two Perimeter Defense and Gateway Security

- The evolution of the network perimeter.
- Deep dive into next-generation firewalls (NGFWs) and their features.
- Configuring firewall policies, rulebases, and access control lists (ACLs).
- Implementing web application firewalls (WAFs) for application security.
- Understanding proxy servers and secure web gateways.
- Strategies for mitigating Distributed Denial-of-Service (DDoS) attacks.
- Securing email with email security gateways and anti-phishing techniques.

Unit Three Intrusion Detection, Prevention, and Network Visibility

- Principles of Intrusion Detection and Prevention Systems (IDS/IPS).
- Signature-based vs. anomaly-based detection techniques.
- Deploying and tuning IDS/IPS for optimal performance.
- Fundamentals of Security Information and Event Management (SIEM).
- Network traffic analysis and flow monitoring for threat hunting.
- Implementing Network Access Control (NAC) solutions.
- The role of deception technologies like honeypots.

Unit Four Advanced Secure Networking and Access Control

- Implementing secure remote access using VPN technologies (IPsec and SSL).
- Introduction to Zero Trust Network Access (ZTNA) principles and architecture.
- Designing network segmentation and micro-segmentation strategies.
- Understanding Secure Access Service Edge (SASE) architecture.
- Securing Software-Defined Networking (SDN) and SD-WAN environments.
- DNS security controls and best practices.
- Data Loss Prevention (DLP) at the network level.

Unit Five Cloud Security and Security Operations

- Architecting security for public cloud environments (IaaS, PaaS).
- Securing hybrid and multi-cloud network connections.
- Managing security in virtualized network environments.
- Developing a network security incident response plan.
- Integrating threat intelligence into security operations.
- Network forensics and incident investigation techniques.
- Future trends in network security and perimeter defense.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Considering the shift towards remote work and cloud services, how does the traditional concept of a network 'perimeter' need to evolve, and what are the primary challenges in securing this new, distributed perimeter?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the strategic and architectural aspects of network security, rather than concentrating solely on the configuration of specific vendor tools. While practical skills are essential, our curriculum is built on the philosophy that a strong architectural foundation is paramount for building resilient and adaptable defenses. We delve deeply into modern paradigms like the Zero Trust model and Secure Access Service Edge (SASE), providing participants with the forward-looking knowledge required to secure today's borderless networks. The content moves beyond reactive measures, emphasizing proactive strategies such as threat modeling and risk-based design. Unlike courses that may offer a fragmented view of security technologies, this program teaches how to integrate disparate solutions from NGFWs and IDS/IPS to cloud-native controls into a cohesive and layered defense-in-depth strategy. The emphasis on case studies and design principles ensures that participants learn not just the 'how' but, more importantly, the 'why' behind critical security decisions, empowering them to think like security architects.