Secure SD-WAN Deployment for Enterprise Networks Training Course

23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO7623_119516

Course Introduction / Overview:

The rapid shift to cloud applications and the increasing mobility of the workforce have rendered traditional WAN architectures inadequate for the modern multi-branch enterprise. This has propelled Software-Defined Wide Area Networking (SD-WAN) from a niche technology to a foundational component of digital transformation. However, this transition introduces a new and complex threat landscape that demands an integrated security approach. This course provides a comprehensive exploration of designing, deploying, and managing a secure SD-WAN infrastructure. We delve into the core principles of SD-WAN architecture, moving beyond basic connectivity to focus on embedding robust security at every layer. As discussed in seminal industry analyses, such as those popularizing the Secure Access Service Edge (SASE) framework, the convergence of networking and security is paramount. This program, offered by BIG BEN Training Center, is meticulously designed to equip participants with the skills to build a resilient, high-performance, and secure network fabric that supports business agility while defending against advanced threats. Participants will learn to implement zero-trust networking principles, configure next-generation firewalls (NGFW), and leverage unified threat management (UTM) within their SD-WAN deployment, ensuring their organization's network is both efficient and secure.

Target Audience / This training course is suitable for:

- Network Architects and Engineers.
- Cybersecurity Analysts and Specialists.
- IT Managers and Directors.
- Network Operations Center (NOC) personnel.
- Solutions Architects and Pre-sales Engineers.
- Infrastructure and Systems Administrators.
- IT professionals involved in network transformation projects.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Retail and E-commerce.
- Manufacturing and Supply Chain.
- Telecommunications and Service Providers.
- Government and Public Sector Agencies.
- Education and Research Institutions.
- Energy and Utilities.

Target Organizations Departments:

- Information Technology (IT) and Infrastructure.
- Cybersecurity and Information Security.
- Network Operations and Engineering.
- Cloud Strategy and Architecture.
- Digital Transformation and Innovation.
- Enterprise Architecture.
- Compliance and Risk Management.

Course Offerings:

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

- Develop a comprehensive SD-WAN strategy aligned with business objectives and security requirements.
- Design a secure and scalable SD-WAN architecture for multi-branch enterprise environments.
- Evaluate and select appropriate SD-WAN vendors and solutions based on technical and security criteria.
- Implement zero-touch provisioning for streamlined and secure branch office deployment.
- Configure and manage advanced security policies, including application-aware routing and NGFW rules.
- Integrate SD-WAN with cloud security services to build a SASE framework.
- Implement robust network segmentation to isolate traffic and minimize attack surfaces.
- Monitor, analyze, and troubleshoot SD-WAN performance and security events effectively.
- Ensure SD-WAN deployments meet industry compliance standards and regulatory requirements.
- Develop an incident response plan tailored to an SD-WAN environment.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can translate theoretical knowledge into real-world skills. This course moves beyond traditional lectures by incorporating a blend of expert-led instruction, detailed case studies of successful multi-branch deployments, and collaborative group workshops. Participants will engage in hands-on simulation exercises that challenge them to design, configure, and secure a virtual SD-WAN environment. These practical sessions are crucial for building confidence and competence in managing complex network security policies. Our approach emphasizes peer-to-peer learning through guided discussions, where participants can share their unique organizational challenges and learn from the experiences of others. Continuous feedback is provided by our expert instructors, who bring years of industry experience in enterprise networking and cybersecurity. The program fosters a dynamic learning environment where complex concepts like SASE and zero-trust networking are demystified through practical application, preparing attendees to lead secure SD-WAN initiatives within their organizations.

Course Agenda (Course Units):

Unit One Foundations of SD-WAN and Enterprise Security

- Introduction to Software-Defined Networking (SDN) and SD-WAN.
- Comparing traditional WAN architectures with SD-WAN.
- Key business drivers and benefits of SD-WAN for multi-branch enterprises.
- Understanding the SD-WAN architecture components: orchestrator, controller, and edge devices.
- Identifying the expanded threat landscape in distributed networks.
- Core security challenges in SD-WAN deployments.
- Introduction to Secure Access Service Edge (SASE) and its core tenets.
- The principles of Zero Trust Networking in an SD-WAN context.

Unit Two Designing a Secure SD-WAN Architecture

- Developing a secure SD-WAN design and deployment strategy.
- Analyzing different SD-WAN topologies: hub-and-spoke, full-mesh, and hybrid models.
- Criteria for selecting SD-WAN vendors and solutions.
- Integrating Next-Generation Firewall (NGFW) capabilities at the WAN edge.
- Planning for Unified Threat Management (UTM) services.
- Designing for high availability, redundancy, and failover.
- Secure integration with public cloud environments (IaaS, SaaS).
- Planning for secure remote access for mobile and remote users.

Unit Three Implementing and Deploying Secure SD-WAN

- Best practices for Zero-Touch Provisioning (ZTP) of branch devices.
- Configuring foundational routing and connectivity policies.
- Implementing application-aware routing and traffic steering policies.
- Establishing secure VPN tunnels and overlay networks.
- Configuring and enforcing network segmentation and micro-segmentation.
- Setting up secure web gateways (SWG) and DNS security.
- Implementing role-based access control (RBAC) for SD-WAN management.
- Validating the deployment through systematic testing and verification.

Unit Four Advanced Security Policies and Threat Management

- Configuring advanced threat protection, including IPS, anti-malware, and sandboxing.
- Integrating threat intelligence feeds into the SD-WAN security fabric.
- Implementing Cloud Access Security Broker (CASB) functionality.
- Developing policies for data loss prevention (DLP).
- Managing encryption and certificate lifecycle for secure communication.
- Creating an effective SD-WAN security incident response plan.
- Conducting security audits and vulnerability assessments of the SD-WAN infrastructure.
- Automating security responses using orchestration tools.

Unit Five Optimizing, Monitoring, and Managing SD-WAN Security

- Key performance indicators (KPIs) for SD-WAN health and security.
- Utilizing SD-WAN analytics for network visibility and forensics.
- Monitoring application performance and user experience.
- Techniques for troubleshooting common SD-WAN connectivity and security issues.
- Managing policy updates and configuration changes across the enterprise.
- Ensuring compliance with standards like PCI-DSS, HIPAA, and GDPR.
- Planning for future scalability and technology evolution.
- Reviewing and optimizing SD-WAN operational costs and total cost of ownership (TCO).

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:

As SD-WAN and SASE converge, how might the traditional roles of network and security teams need to evolve to prevent operational silos and ensure cohesive threat management?

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

This course distinguishes itself by adopting a holistic, security-first approach to SD-WAN deployment, a perspective often fragmented in other training programs. Rather than treating networking and security as separate disciplines, we integrate them from the very first unit, reflecting the industry's shift towards converged frameworks like SASE. Our curriculum is intentionally vendor-agnostic, focusing on the fundamental principles and architectural best practices applicable across any leading platform. This empowers participants with versatile, transferable skills rather than narrow, tool-specific knowledge. Furthermore, the course emphasizes strategic thinking, guiding participants on how to build a business case, design for scalability, and align their SD-WAN strategy with broader digital transformation goals. While other courses may focus heavily on feature-by-feature configuration, we prioritize the "why" behind the "how," using real-world case studies to explore complex decision-making in multi-branch enterprise environments. The program is designed not just to train technicians, but to develop strategic architects who can lead their organizations through a secure and successful network evolution.