# Design & Setting Up VPNs for Secure Remote Work Training Course

**#NO3392**

# Design & Setting Up VPNs for Secure Remote Work Training Course

## Course Introduction / Overview:

This comprehensive training course is designed to equip IT professionals with the essential skills for designing, implementing, and managing Virtual Private Networks for secure remote work. In a world where remote and hybrid work models are the norm, ensuring secure network access for off-site employees is more critical than ever. This course goes beyond a simple overview of VPNs. It provides a deep dive into various VPN protocols, security considerations, and best practices for creating a reliable and scalable remote access solution. Participants will learn how to select the right VPN technology for their organization, configure servers and clients, and troubleshoot common connectivity issues. We will also cover advanced topics such as multi-factor authentication, network segmentation for remote users, and the integration of VPNs with cloud-based services. Inspired by experts like Eric Geier and his practical approach to network security, this course at BIG BEN Training Center combines theoretical knowledge with hands-on, real-world applications. The curriculum provides a holistic view of modern VPN technology, covering everything from the foundational principles to advanced deployment strategies. By the end of this program, you will have the expertise to build and maintain a secure remote work environment that protects sensitive corporate data and ensures business continuity.

## Target Audience / This training course is suitable for:

- IT and network administrators.
- Cybersecurity analysts.
- System engineers and architects.
- Help desk and technical support staff.
- IT managers.
- Cloud security professionals.
- DevOps engineers.

## Target Sectors and Industries:

- Information Technology and software development.
- Telecommunications.
- Financial services.
- Healthcare.
- Government agencies and defense.
- Education.
- Any organization with a remote or hybrid workforce.

## Target Organizations Departments:

- Information Technology (IT) and Network Operations.
- Cybersecurity and Information Security.
- Technical Support.
- System Administration.
- Human Resources (for managing remote employee access).
- IT Audit and Compliance.
- Data Management.

## Course Offerings:

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

- Design and implement secure VPN solutions for a remote workforce.
- Configure and manage various VPN protocols, including OpenVPN and IPsec.
- Integrate multi-factor authentication (MFA) with VPN access.
- Troubleshoot common VPN connectivity and performance issues.
- Apply best practices for securing remote access to corporate resources.
- Segment networks to enhance security for remote users.
- Manage and monitor VPN connections and user activity.

## Course Methodology:

This training course at BIG BEN Training Center employs a highly practical and hands-on methodology to ensure that participants gain real-world skills in setting up and managing VPNs. The learning experience is a combination of instructor-led presentations, interactive lab exercises, and case studies based on actual remote work security challenges. Participants will have the opportunity to configure a VPN server from scratch and set up clients for different operating systems. Collaborative problem-solving sessions will be a key component, allowing for peer-to-peer learning and the exchange of ideas on complex network security topics. We will use a virtual lab environment for all practical exercises, giving participants a safe space to experiment without affecting a live network. The instructor will provide personalized feedback throughout the course, ensuring that each participant leaves with a solid understanding and the confidence to implement secure remote access solutions. This methodology ensures the course content is directly applicable and provides a comprehensive learning experience that combines rigorous academic knowledge with practical skills development.

## Course Agenda (Course Units):

### Unit One: Fundamentals of VPNs and Remote Access

- The concept of a Virtual Private Network.
- Common VPN protocols and their use cases.
- VPN authentication and encryption methods.
- Remote access vs. site-to-site VPNs.
- Key components of a VPN solution.
- The role of VPNs in modern cybersecurity.
- Understanding client-server communication in a VPN tunnel.

### Unit Two: Configuring OpenVPN

- Installing and setting up an OpenVPN server.
- Generating and managing digital certificates.
- Configuring client-side software.
- Securing OpenVPN with TLS.
- Creating user profiles and access controls.
- Troubleshooting OpenVPN connectivity.
- Advanced server configuration.

### Unit Three: IPsec and Other VPN Technologies

- Introduction to the IPsec protocol suite.
- Configuring a site-to-site IPsec VPN.
- The concept of IKE and ESP.
- Managing IPsec security associations.
- Overview of other protocols, like Wire Guard and L2TP.
- Comparing different VPN solutions.
- Case study: A secure hybrid network deployment.

### Unit Four: Advanced Security and Network Integration

- Implementing multi-factor authentication (MFA).
- Integrating VPNs with Active Directory.
- Network segmentation and access control lists (ACLs).
- Intrusion detection for VPN traffic.
- Monitoring VPN connections and user logs.
- Best practices for securing VPN endpoints.
- Compliance considerations for remote access.

### Unit Five: Troubleshooting and Business Continuity

- Common VPN issues and how to resolve them.
- Diagnosing performance bottlenecks.
- Developing a VPN business continuity plan.
- Security audits and vulnerability scanning.
- The future of remote access and zero trust.
- Final practical project: Building a secure remote work environment.
- Q&A with the instructor.

## 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:

With the rise of zero-trust architectures, how will the traditional role of a VPN as a security perimeter change, and what new skills will be required to manage secure remote access in the future?

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

This course provides a highly focused and practical approach to VPNs that is directly relevant to the demands of modern remote work. Unlike many broad cybersecurity courses that touch on VPNs briefly, this curriculum provides in-depth, hands-on experience in designing, deploying, and managing them. The program emphasizes the specific security challenges posed by a distributed workforce, from securing personal devices to integrating multi-factor authentication for enhanced protection. We go beyond simply teaching how to use a single tool. Instead, we explore various protocols and technologies, enabling participants to make informed decisions for their organization's unique needs. The use of a virtual lab environment ensures that every participant gets hands-on practice in a safe space. This course is built to empower IT professionals to not only set up a VPN, but to create a robust, scalable, and secure remote access solution that stands up to the demands of today's digital threats.