Implementing Secure Solutions with Virtual Private Networks (SVPN)

Course Duration: 40 Hours **Course code: SVPN**

1. Course Overview

The Implementing Secure Solutions with Virtual Private Networks (SVPN) course provides IT professionals with the knowledge and skills necessary to design, implement, configure, and troubleshoot secure site-to-site and remote access VPN solutions using Cisco technologies. This course focuses on using Cisco routers and ASA firewalls to enable VPN services including IPsec, DMVPN, FlexVPN, and SSL VPN. Through a blend of theoretical instruction and hands-on labs, learners will gain the expertise needed to ensure secure communication across public and private networks.

2. What you'll learn?

After completing this course, you will be able to:

- Describe common VPN concepts and components
- Implement and troubleshoot site-to-site IPsec VPN
- Deploy and configure Cisco FlexVPN
- Configure DMVPN Phase 1, 2, and 3
- Implement secure remote access VPN (SSL and IPsec)
- Manage and monitor VPNs using Cisco ASDM and CLI
- Enforce access control and security policies for VPN traffic
- Integrate VPN solutions with authentication servers
- Understand and apply encryption, hashing, and tunneling protocols
- Use advanced troubleshooting tools to resolve VPN issues

3. Target Audience

- Network engineers and administrators
- Security professionals responsible for secure communications
- IT staff involved in implementing remote access solutions

4. Pre-Requisites

Attendees should have:

- Understanding of TCP/IP and basic routing protocols
- Familiarity with Cisco IOS and ASA firewall platforms

Recommended prerequisites:

- CCNA – Implementing and Administering Cisco Solutions
- SCOR – Implementing and Operating Cisco Security Core Technologies

5. Course content

1 – VPN Fundamentals and Architecture

- Introduction to VPNs
- VPN Protocol Comparison (IPsec, SSL, MPLS, GRE)
- Encryption, Hashing, and Authentication Overview
- IPsec Framework and Components
- VPN Topologies and Use Cases
- Security Considerations in VPN Design

2 – IPsec VPN Implementation

- IPsec Protocol Stack (AH, ESP)
- ISAKMP/IKEv1 vs. IKEv2
- Site-to-Site VPN Configuration using Cisco IOS
- Crypto Maps and Transform Sets
- IPsec Tunnel Verification and Troubleshooting
- NAT Traversal and Tunnel Protection

3 – FlexVPN Implementation

- FlexVPN Design Overview
- IKEv2 Tunnel Establishment
- FlexVPN Configuration and Deployment
- Role of Virtual Tunnel Interfaces (VTI)
- EAP Authentication Integration
- Redundancy and High Availability in FlexVPN

4 – Dynamic Multipoint VPN (DMVPN)

- Introduction to DMVPN
- Phase 1, Phase 2, and Phase 3 Architecture
- Hub-and-Spoke Configuration
- NHRP Concepts and Configuration
- IPsec Integration with DMVPN
- Troubleshooting DMVPN

5 – Secure Remote Access VPN

- SSL VPN (Clientless and AnyConnect)
- IPsec Remote Access VPN with IKEv2
- Cisco ASA and Cisco FTD VPN Deployment
- Authentication Integration (RADIUS, LDAP, MFA)
- Group Policies and Tunnel Groups
- Web Portal Customization

6 – Authentication, Authorization, and Accounting (AAA)

- AAA Concepts and Integration
- RADIUS and TACACS+ Setup
- Using Cisco ISE for VPN Authentication
- Certificate-Based Authentication
- Identity-Based Access Control

7 – VPN Policy Control and Access Management

- Traffic Filtering with ACLs
- Split Tunneling and Full Tunnel Modes
- DNS and IP Address Assignment in Remote VPN
- Policy-Based VPNs vs. Route-Based VPNs
- Monitoring VPN Sessions
- Security Logging and Event Tracking

8 – VPN Troubleshooting and Monitoring

- Using CLI Tools and Debug Commands
- Syslog and Event Correlation
- ASA and IOS VPN Troubleshooting Techniques
- Packet Captures and Traffic Analysis
- Real-time Monitoring with ASDM
- Common VPN Issues and Resolutions

9 – Advanced VPN Use Cases and Integration

- VPNs in Hybrid Cloud and Multi-Cloud Environments
- Integrating VPN with SD-WAN
- Mobile VPN Access and BYOD Scenarios
- VPN Automation and Orchestration (Intro)
- Performance Tuning and Best Practices