Enterprise Firewall Course

Course Duration: 24 Hrs. **Course Code: ENT-FW-101**

Course Overview

The **Enterprise Firewall** course is designed for network and security professionals responsible for protecting enterprise networks from internal and external threats. This course focuses on deploying, configuring, and managing enterprise-grade firewall solutions, including policy creation, network segmentation, threat prevention, and high availability. Participants will gain hands-on experience in securing complex enterprise networks while preparing for advanced firewall administration and security certifications.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure enterprise firewall solutions
- Implement network segmentation and VLAN policies
- Create and manage security policies, rules, and access control
- Configure NAT, VPNs, and advanced routing
- Monitor network traffic and firewall logs
- Prevent threats including malware, intrusion, and DDoS attacks
- Troubleshoot firewall and network connectivity issues

Target Audience

This course is ideal for:

- Network and Security Engineers
- IT Infrastructure Administrators

- SOC and NOC Teams
- Enterprise Network Designers
- Professionals responsible for firewall deployment and management

Pre-Requisites

Participants should have:

- Basic understanding of networking fundamentals (TCP/IP, LAN/WAN)
- Knowledge of routing, switching, and network protocols
- Prior experience with firewalls or network security devices is recommended

Course Content

Module 1: Enterprise Firewall Architecture and Deployment

- Firewall types and deployment models
- Hardware and software-based firewalls
- High availability and redundancy

Module 2: Security Policy and Access Control

- Creating and managing firewall rules
- VLANs, zones, and network segmentation
- User authentication and access policies

Module 3: Network Address Translation (NAT) and Routing

- NAT configuration and use cases
- Static and dynamic routing integration

- VPN configuration for secure connectivity

Module 4: Threat Prevention and Advanced Security

- Intrusion detection and prevention (IDS/IPS)
- Anti-malware and anti-virus configuration
- DDoS mitigation and traffic inspection

Module 5: Monitoring and Logging

- Firewall logging and event monitoring
- Security analytics and dashboards
- Generating reports and compliance auditing

Module 6: Troubleshooting and Best Practices

- Common firewall and network issues
- Diagnostic tools and techniques
- Operational best practices for enterprise networks