NSE 4 Fortinet Bootcamp

Program Overview :
This training explores firewall policies, the Fortinet Security Fabric, user authentication, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more. These administration fundamentals will provide you with a solid understanding of how to implement basic network security.
The second part of the training includes features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, redundant infrastructure, virtual domains (VDOMs), zero trust network access (ZTNA), SSL VPN, site-to-site IPsec VPN, single sign-on (SSO), and diagnostics.

Course Objectives

I-FortiGate Security:

- Deploy the appropriate operation mode for your network
- Use the GUI and CLI for administration
- Control network access to configured networks using firewall policies
- Apply port forwarding, source NAT, and destination NAT
- Authenticate users using firewall policies
- Understand encryption functions and certificates
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites
- Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
- Fight hacking and denial of service (DoS)
- Collect and interpret log entries
- Identify the characteristics of the Fortinet Security Fabric

II-FortiGate Infrastructure:

- Analyze a FortiGate route table
- Route packets using policy-based and static routes for multipath and load-balanced deployments
- Divide FortiGate into two or more virtual devices, each operating as an independent FortiGate, by configuring virtual domains (VDOMs)
- Understand the fundamentals and benefits of using ZTNA
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices

Target Audience:

- Network Professionals
- IT Security Professionals

Course Duration:
5 days, 40 hours

Programme

Module
Part 1
• **FortiGate Security** 1. Introduction and Initial Configuration 2. Firewall Policies 3. Network Address Translation 4. Firewall Authentication 5. Logging and Monitoring 6. Certificate Operations 7. Web Filtering 8. Application Control 9. Antivirus 10. Intrusion Prevention and Denial of Service 11. Security Fabric
Part 2
• **FortiGate Infrastructure** 1. Routing 2. Virtual Domains 3. Fortinet Single Sign-On 4. ZTNA 5. SSL VPN 6. IPsec VPN