Course Introduction

Sophos Certified Engineer (ET80) – Sophos Firewall (XGS)

The Sophos Certified Engineer (ET80) course is a comprehensive technical training program designed to equip IT professionals with the knowledge and practical skills required to deploy, configure, manage, and troubleshoot Sophos Firewall solutions in enterprise environments.

This course provides in-depth coverage of Sophos Firewall architecture, network security policies, VPN technologies, web protection, application control, authentication services, wireless security, centralized management, and advanced threat protection capabilities. Through a combination of instructor-led sessions and hands-on laboratory exercises, participants will gain real-world experience in securing modern network infrastructures using Sophos Firewall XGS platforms.

Upon successful completion of this course, participants will be able to confidently implement Sophos Firewall solutions, enforce security policies, establish secure remote connectivity, and perform effective troubleshooting and maintenance of Sophos security environments.

Who Should Attend

This course is intended for:

- Network Engineers
- Security Engineers
- Firewall Administrators
- Network Administrators
- System Administrators
- Security Analysts
- IT Support Professionals
- SOC Engineers
- Technical Consultants
- Solution Architects
- Managed Security Service Provider (MSSP) Engineers

Prerequisites

Participants should have:

- Basic understanding of TCP/IP networking
- Familiarity with routing and switching concepts
- Knowledge of network security fundamentals
- Basic experience with firewall technologies
- Understanding of VPN concepts is beneficial but not mandatory

Course Duration

- Duration: 4 Days
- Training Hours per Day: 8 Hours
- Total Training Hours: 32 Hours
- Delivery Mode: Instructor-Led Training
- Hands-On Labs: Included Throughout the Course

Learning Outcomes

Upon completion of this course, participants will be able to:

- Deploy and configure Sophos Firewall solutions.
- Implement and manage firewall policies and NAT rules.
- Configure Intrusion Prevention System (IPS) and Advanced Threat Protection (ATP).
- Deploy Site-to-Site and Remote Access VPN solutions.
- Integrate Active Directory, LDAP, and RADIUS authentication services.
- Configure Web Filtering and Application Control policies.
- Manage wireless security using Sophos Access Points.
- Monitor, analyze, and troubleshoot firewall operations.
- Utilize Sophos Central for centralized management and reporting.
- Prepare for the Sophos Certified Engineer (ET80) certification exam.

Sophos Certified Engineer (ET80) – Sophos Firewall (XGS)

Table of Contents (TOC)

4.1 Firewall Rules and Policies

4.2 NAT (Network Address Translation)

4.3 Security Zones

4.4 Business Application Rules

4.5 Policy-Based Routing

4.6 Firewall Best Practices

Module 5: Network Protection

5.1 Intrusion Prevention System (IPS)

5.2 Advanced Threat Protection (ATP)

5.3 DoS and DDoS Protection

5.4 Security Heartbeat Integration

5.5 Threat Intelligence and Reporting

Module 6: Site-to-Site Connectivity

6.1 IPsec VPN Fundamentals

6.2 Site-to-Site VPN Configuration

6.3 VPN Troubleshooting

6.4 High Availability VPN Scenarios

Module 7: Authentication and User Management

7.1 Authentication Methods

7.2 Active Directory Integration

7.3 LDAP and RADIUS Authentication

7.4 Single Sign-On (SSO)

7.5 User and Group Policies

Module 8: Web Protection

8.1 Web Filtering Concepts

8.2 Web Policies and Categories

8.3 HTTPS Inspection

8.4 Malware and Content Scanning

8.5 Safe Browsing Policies

Module 9: Application Control

9.1 Application Visibility and Control

9.2 Application Filtering Policies

9.3 Risk-Based Application Management

9.4 Traffic Monitoring and Reporting

Module 10: Remote Access

10.1 SSL VPN Configuration

10.2 IPsec Remote Access VPN

10.3 VPN Client Deployment

10.4 Remote User Security Policies

Module 11: Wireless Protection

11.1 Wireless Security Overview

11.2 Access Point Integration

11.3 Wireless Networks and SSIDs

11.4 Guest Access Configuration

11.5 Wireless Security Policies

Module 12: Logging and Reporting

12.1 Logging Architecture

12.2 Log Viewer and Analysis

12.3 Reporting Features

12.4 Security Event Investigation

12.5 Compliance Reporting

Module 13: Central Firewall Management

13.1 Sophos Central Overview

13.2 Firewall Registration and Management

13.3 Policy Synchronization

13.4 Centralized Reporting

13.5 Multi-Firewall Administration

Module 14: Monitoring, Maintenance, and Troubleshooting

14.1 System Health Monitoring

14.2 Backup and Restore

14.3 Firmware Upgrades

14.4 Diagnostic Tools

14.5 Troubleshooting Methodology

Module 15: Hands-On Labs

Lab 1: Initial Deployment and Setup

Lab 2: Interface and Zone Configuration

Lab 3: Firewall Rules and NAT

Lab 4: IPS and Threat Protection

Lab 5: Site-to-Site VPN

Lab 6: Authentication Integration

Lab 7: Web Filtering and Application Control

Lab 8: SSL VPN Remote Access

Lab 9: Sophos Central Management

Lab 10: Troubleshooting and Diagnostics