

## Module 1: XG Firewall Overview (25 mins)

- Identify the features of the XG Firewall and how they protect against common
- Identify the deployment options available for the XG Firewall
- Identify the add-ons for central management and reporting

### Labs (5 mins)

- Register for a Sophos Central evaluation

## Module 2: Getting Started with XG Firewall (45 mins)

- Identify the deployment modes of the XG Firewall
- Configure an XG Firewall using the Initial Setup Wizard
- Navigate the WebAdmin
- Manage objects
- Explain what zones are, and identify the default system zones
- Configure basic networking
- Manage device access and certificates
- Identify the different types of routing supported on the XG Firewall
- Configure static routing

### Labs (50 mins)

- Use the Initial Setup Wizard to configure a Sophos XG Firewall
- Configure a new Sophos XG Firewall by importing a configuration backup
- Navigate the WebAdmin
- Configure Zones and Interfaces
- Create Static Routes
- Create Definitions
- Configure DNS Request Routes
- Import CA Certificates
- Create a Configuration Backup
- Restore a configuration backup to an XG Firewall

## Module 3: Network Protection (35 mins)

- Identify the different types of firewall and understand the purpose of each

- Create and manage firewall rules
- Configure and apply intrusion prevention policies
- Configure DoS & Spoof Protection
- Enable Security Heartbeat and apply restrictions in firewall rules
- Configure Advanced Threat Protection

#### Labs (60 mins)

- Configure Logging
- Create Network Firewall Rules
- Install the SSL CA Certificates
- Install Sophos Central
- Publish Servers Using Business Application Rules
- Configure IPS Policies
- Enable Advanced Threat Protection
- Enable DoS (Denial of Service) and Spoof Protection
- Configure Security Heartbeat

#### Module 4: Site-to-Site Connections (35 mins)

- Explain the VPN options available for site-to-site connections
- Configure an IPsec site-to-site VPN using the wizard
- Configure an SSL VPN
- Explain the deployment modes for RED
- Configure and deploy REDs

#### Labs (30 mins)

- Create an SSL site-to-site VPN
- Create an IPsec site-to-site VPN

#### Module 5: Authentication (35 mins)

- Identify the supported authentication sources and enable them for services on the XG Firewall
- Explain the types of user on the XG Firewall and know when to use them
- Configure NTLM authentication for the web proxy
- Install and configure STAS for single sign-on

- Create identity-based policies
- Enable and use one-time passwords (OTP)

#### Labs (30 mins)

- Create an Active Directory Authentication Server
- Configure Single Sign-On Using STAS
- Create User-based policies
- Configure One Time Passwords

#### Module 6: Web Protection and Application Control (35 mins)

- Configure Web Protection Policies
- Identify the activities that can be used to control web traffic
- Create keyword content filters
- Configure Surfing Quotas
- Configure Traffic Quotas
- Configure Application Filters
- Categorize applications using Synchronized App Control

#### Labs (40 mins)

- Create Custom Web Categories and User Activities
- Create a Content Filter
- Create a Custom Web Policy
- Create a Surfing Quota for Guest Users
- Create an Application Filter Policy

#### Module 7: Email Protection (30 mins)

- Identify the two deployment modes for Email Protection and their differences
- Configure global settings include relay settings
- Configure SMTP policies for MTA mode and legacy mode
- Configure policies for client protocols
- Create Data Control Lists and use them in policy
- Configure encryption using SPX
- Manage the quarantine using digests and the User Porta

### Labs (40 mins)

- Enable and Configure Quarantine Digests
- Configure an Email Protection policy
- Configure Data Control and SPX Encryption
- User Quarantine Management

### Module 8: Wireless Protection (20 mins)

- Identify the access points available and the differences between them
- Configure wireless networks
- Explain the different security modes
- Deploy wireless access points and assign wireless networks
- Configure hotspots for wireless networks

### Labs (10 mins)

- Create a hotspot

### Module 9: Remote Access (20 mins)

- Configure remote access using SSL VPN
- Configure Clientless Access via the User Portal
- Configure remote access for mobile devices

### Labs (15 mins)

- Configure an SSL Remote Access VPN

### Module 10: Logging, Reporting and Troubleshooting (30 mins)

- Customize and run reports
- Schedule reports
- Use the Log Viewer to monitor the XG Firewall
- Configure logging
- Identify and use diagnostic and troubleshooting tools on the XG Firewall

### Labs (40 mins)

- Run, Customize and Schedule Reports
- View Sandstorm Activity

- Use SF Loader Tools
- Connection Table
- Packet Capture
- Dropped Packet Capture