Module 1: Deployment

- Recall important information from the Engineer course
- Describe the deployment modes supported by the XG Firewall
- Understand a range of scenarios where each deployment mode would commonly be used
- Use built-in tools to troubleshoot issues
- Labs:
- Register for a Sophos Central evaluation

Module 2: Base Firewall

- Explain how the XG firewall can be accessed
- Understand the types of interfaces that can be created
- Understand the benefits of Fast Path technology
- Configure routing per firewall rule
- Understand best practice for ordering firewall rules
- Explain what Local NAT policy is and known how to configure it
- Labs:
- Activate the Sophos XG Firewalls
- Post-installation configuration
- Bridge interfaces
- Create a NAT rule to load-balance access to servers
- Create a local NAT policy
- Configure routing using multiple WAN links
- Configure policy-based routing for an MPLS Scenario
- Install Sophos Central

Module 3: Network Protection

- Explain what IPS is and how traffic can be offloaded to FastPath
- Demonstrate how to optimize workload by configuring IPS policies
- Examine advanced Intrusion Prevention and optimize policies
- Configure advanced Dos Protection rules
- Demonstrate how the strict policy can be used to protect networks
- Labs:
- Create advanced Dos Rules

Module 4: Synchronized Security

- Explain how Security Heartbeat works
- Configure Synchronized Security
- Deploy Synchronized Security in discover and inline modes
- Understand the advantages and disadvantages of deploying Synchronized Security in different scenarios
- Labs:
- Configure source-based Security Heartbeat firewall rules

- Destination-based Security Heartbeat
- Missing Security Heartbeat
- Lateral Movement Protection

Module 5: Web Server Protection

- Explain how Web Server Protection works
- Describe the protection features
- Configure protection policies for a web application
- Configure web server authentication
- Publish a web service using the Web Application Firewall
- Use the preconfigured templates to configure Web Server Protection for common purposes
- Configure SlowHTTP protection
- Labs:
- Web Application Firewall
- Load balancing with Web Server Protection
- Web Server Authentication and path-specific routing

Module 6: Site-to-Site Connections

- Configure and deploy site-to-site VPNs in a wide range of environments
- Implement IPsec NATing and failover
- Check and modify route precedence
- Create RED tunnels between XG Firewalls
- Understand when to use RED
- Labs:
- Create an IPsec site-to-site VPN
- Configure VPN network NATing
- Configure VPN failover
- Enable RED on the XG Firewall
- Create a RED tunnel between two XG Firewalls
- Configure routing for the RED tunnel
- Configure route-based VPN

Module 7: Authentication

- Demonstrate how to configure and use RADIUS accounting
- Deploy STAS in large and complex environments
- Configure SATC and STAS together
- Configure Secure LDAP and identify the different secure connections available
- Labs:
- Configure an Active Directory authentication server
- Configure single sign-on using STAS
- Authenticate users over a Site-to-Site VPN

Module 8: Web Protection

- Choose the most appropriate type for web protection in different deployment scenarios
- Enable web filtering using the DPI engine or legacy web proxy
- Configure TLS inspection using the DPI engine or legacy web proxy
- Labs:
- Install the SSL CA certificate
- Configure TLS inspection rules
- Create a custom web policy for users

Module 9: Wireless

- Explain how Sophos Access Points are deployed and identify some common issues that may be encountered
- Configure RADIUS authentication
- Configure a mesh network

Module 10: Remote Access

- Configure Sophos Connect and manage the configuration using Sophos Connect Admin
- Configure an IPsec remote access VPN
- Configure an L2TP remote access VPN for mobile devices
- Labs:
- Sophos Connect

Module 11: High Availability

- Explain what HA is and how it operates
- Demonstrate how to configure HA and explain the difference between quick and manual configuration
- List the prerequisites for high availability
- Perform troubleshooting steps and check the logs to ensure that HA is set up correctly
- Explain the packet flow in high availability
- Demonstrate how to disable HA
- Labs:
- Create an Active-Passive cluster
- Disable high Availability

Module 12: Public Cloud

- Deploy XG Firewall in complex network environments
- Explain how XG Firewall processes traffic and use it's information to inform the configuration
- Configure advanced networking and protection features
- Deploy XG Firewall on public cloud infrastructure
- Labs:

- Put a service in debug mode to gather logs
- Retrieving log files
- Troubleshoot an issue from an imported configuration file
- Deploy an XG Firewall on Azure (Simulation)