SOPHOS
Security made simple.

XG Firewall: Administrator Course Overview

This course is designed for technical professionals who will be administrating Sophos XG Firewall and provides an overview of the product, including an introduction to the major capabilities and core configuration concepts.

The course is available either online via the Sophos Training Portal, or as an instructor-led classroom course. Please contact your Sophos partner to find out more about the availability of classroom courses in your region.
It consists of presentations and practical lab exercises to reinforce the taught content, and electronic copies of the supporting documents for the course will be provided to each trainee through the online portal.

The course is expected to take 3 days (24 hours) to complete, of which approximately half will be spent on the practical exercises.

Objectives

On completion of this course, trainees will be able to:

- Explain how XG Firewall help to protect against security threats
- Configure firewall rules, policies and user authentication
- Demonstrate threat protection and commonly used features
- Perform the initial setup of an XG Firewall and configure the required network settings
- Perform basic troubleshooting, reporting, and management tasks

Prerequisites

We recommend that you have the following knowledge and experience:

- Understand subnetting and routing
- Experience configuring network security devices

If you are uncertain whether you meet the necessary prerequisites to take this course, please email us at globaltraining@sophos.com and we will be happy to help.

Certification

To complete the course, trainees must take and pass an online assessment. The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80% and is limited to 4 attempts.

Lab Environment

Each student will be provided with a pre-configured environment, which simulates a company network with two sites, a head office and a branch office and contains Windows Servers, a Windows client, two XG Firewalls and supporting infrastructure.

Agenda

Module 1: XG Firewall Overview (60 mins)

- Identify the features of the XG Firewall and how the protect against common threats
- List the deployment options available for the XG Firewall
- Define Zero Trust networking
- Introduce troubleshooting for the XG firewall
- **Labs (5 mins)**
  - Register for a Sophos Central evaluation

Module 2: Getting Started with XG Firewall (105 mins)

- Describe the deployment modes of the XG Firewall
- Configure an XG Firewall using the Initial Setup Wizard
- Navigate the WebAdmin and manage objects
- Explain what zones are, and list the default system zones
- Configure basic networking
- Manage device access and certificates
- List the types of routing supported on the XG Firewall
- Configure static routing
- **Labs (80 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 (70 mins)

- Identify the 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 (110 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: Web Server Protection (60 mins)

- 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 (90 mins)**
    - Web Application Firewall
    - Load balancing with Web Server Protection
    - Web Server Authentication and path-specific routing

Module 5: Site-to-Site Connections (80 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 (40 mins)**
    - Create an SSL site-to-site VPN
    - Create an IPsec site-to-site VPN

Module 6: Authentication (80 mins)

- List 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 single sign-on using Synchronized User Identify and STAS
- Create identity-based policies
- Enable and use one-time passwords (OTP)
- **Labs (60 mins)**
    - Create an Active Directory Authentication Server
    - Authenticate using Synchronized User Identity
    - Configure Single Sign-On Using STAS
    - Create User-based policies
    - Configure One Time Passwords

Module 7: Web Protection and Application Control (60 mins)

- Configure Web Protection Policies
- Identify the activities that can be used to control web traffic
- Create keyword content filters
- Configure surfing and traffic quotas
- **Labs (60 mins)**
    - Create Custom Web Categories and User Activities
    - Create a Content Filter
    - Create a Custom Web Policy
    - Delegate Web Policy Overrides
    - Create a Surfing Quota for Guest Users
    -

Module 8: Application Control (30 mins)

- Configure Application Filters
- Detect and categorize applications using Synchronized App Control and Cloud Applications
- **Labs (30 mins)**
    - Create an Application Filter Policy
    - Categorize applications using Synchronized Application Control
    - Detect and categorize cloud applications

Module 9: Email Protection (50 mins)

- Explain the differences between the two deployment modes for Email Protection
- Configure global settings including 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 Portal
- **Labs (55 mins)**
  - Enable and Configure Quarantine Digests
  - Configure an Email Protection policy
  - Configure Data Control and SPX Encryption
  - User Quarantine Management

Module 10: Wireless Protection (45 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 (15 mins)**
  - Create a hotspot

Module 11: Remote Access (55 mins)

- Configure remote access using SSL VPN
- Configure an IPsec remote access VPN with Sophos Connect
- Configure Clientless Access via the User Portal
- Configure remote access for mobile devices
- **Labs (40 mins)**
  - Configure an SSL Remote Access VPN
  - Configure an IPsec Remote Access VPN with Sophos Connect

Module 12: Logging, Reporting and Central Management (50 mins)

- Customize and run reports
- Schedule reports
- Use the Log Viewer to monitor the XG Firewall
- Configure logging
- Manage an XG Firewall in Sophos Central
- **Labs (40 mins)**
  - Manage an XG Firewall in Sophos Central

Further information

If you require any further information on this course, please contact us at globaltraining@sophos.com.