SOPHOS
Security made simple.

XG Firewall: Administrator Course Overview

This course is designed for technical professionals who will be administering Sophos XG Firewall and provides the skills necessary to manage common day-to-day tasks.

The course is available either online or as an instructor-led classroom course.

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
- Perform the initial setup of an XG Firewall and configure the required network settings
- Configure routing, site-to-site connectivity, remote access and wireless
- Protect web applications using web server protection
- Configure firewall rules, policies and user authentication
- Find information using logs, reports and tools

Prerequisites

There are no prerequisites for this course; however, it is recommended that trainees should:

- Have practical knowledge of networking, including subnets, routing, VLANs, and VPNs
- Be familiar with security best practices
- Have 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 become a Sophos Certified Administrator, 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, two XG Firewalls and supporting infrastructure.

Agenda

Module 1: XG Firewall Overview (45 mins)

- Identify the features of the XG Firewall and how the protect against common
- Identify the deployment options available for the XG Firewall
- **Labs (5 mins)**
  - Register for a Sophos Central evaluation

Module 2: Getting Started with XG Firewall (90 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 interfaces and gateways
- Configure static and policy routing
- Manage device access and certificates
- List the types of routing supported on the XG Firewall
- **Labs (85 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 a policy-based route
  - 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 (65 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 (85 mins)**
  - Configure Logging
  - Create Network Firewall Rules
  - Install the SSL CA Certificates
  - Install Sophos Central
  - Publish Servers Using DNAT
  - Configure IPS Policies
  - Enable Advanced Threat Protection
  - Enable DoS (Denial of Service) and Spoof Protection
  - Configure Security Heartbeat

Module 4: Web Server Protection (45 mins)

- Identify the web server protection features and know what they do
- Configure protection policies for a web application
- Publish a web service using the web application firewall

- Use the preconfigured templates to configure Web Server Protection for common purposes, such as Exchange
- Configure SlowHTTP protection
- **Labs (40 mins)**
  - Web Application Firewall
  - Load Balancing with Web Server Protection
  - Web Server Authentication

Module 5: Site-to-Site Connections (55 mins)

- Explain the options available for site-to-site connections
- Configure an IPsec site-to-site VPN
- Implement IPsec VPN failover
- Check and modify route precedence
- Configure an SSL site-to-site VPN
- Explain the deployment modes for RED
- Configure and deploy REDs
- Configure RED tunnels between XG Firewalls
- **Labs (75 mins)**
  - Create an SSL site-to-site VPN
  - Create a Policy-Based Route for an MPLS Scenario
  - Create an IPsec site-to-site VPN
  - Configure IPsec VPN network NAT
  - Configure IPsec VPN failover

Module 6: Authentication (75 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 NTLM authentication for the web proxy
- Configure single sign-on using Synchronized User Identify and STAS
- Install Sophos Authentication for Thin Clients (SATC)
- Create identity-based policies
- Enable and use one-time passwords (OTP)
- **Labs (45 mins)**
  - Create an Active Directory Authentication Server
  - Configure Single Sign-On Using STAS
  - Create User-based policies
  - Configure One Time Passwords

Module 7: Web Protection and Application Control (75 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
- Configure Application Filters
- Detect and categorize applications using Synchronized App Control and Cloud Applications
- **Labs (70 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
  - Categorize Applications using Synchronized Application Control
  - Detect and Categorize Cloud Applications

Module 8: Email Protection (40 mins)

- Explain the differences between the two deployment modes for Email Protection
- 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 Portal
- **Labs (50 mins)**
  - Enable and Configure Quarantine Digests
  - Configure an Email Protection policy
  - Configure Data Control and SPX Encryption
  - User Quarantine Management

Module 9: Wireless Protection (40 mins)

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

Module 10: Remote Access (25 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 (45 mins)**
  - Configure an SSL Remote Access VPN
  - Configure an IPsec Remote Access VPN with Sophos Connect

Module 11: Management, Logging and Reporting (40 mins)

- Manage an XG Firewall in Sophos Central
- Customize and run reports
- Schedule reports
- Configure logging
- **Labs (40 mins)**
  - Run, Customize and Schedule Reports
  - View Sandstorm Activity
  - Use SF Loader tools
  - Connection table
  - Packet capture
  - Dropped packet capture
  - Manage and XG Firewall in Sophos Central

Further information

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