Sophos Certified Admininstrator : XG

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 expected to take 5 days to complete, of which approximately half will be spent on the practical exercises.

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

- Recognize the main technical capabilities and how they protect against threats
- Complete common configuration tasks
- Configure the most commonly used features
- View and manage logs and reports
- Identify and use troubleshooting tools

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

- Be knowledge of networking to a CompTIA N+ level
- Be familiar with security best practices
- Experience configuring network security devices

Agenda

Module 1: XG Firewall Overview

Identify the features of the XG Firewall and how the protect against common

Identify the deployment options available for the XG Firewall

Identify the add-ons for central management and reporting

Module 2: Getting Started with XG Firewall

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

Module 3: Network Protection

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

Module 4: Site-to-Site Connections

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

Module 5: Authentication

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)

Module 6: Web Protection and Application Control

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

Module 7: Email Protection

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 Portal

Module 8: Wireless Protection

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

Module 9: Remote Access

Configure remote access using SSL VPN

Configure Clientless Access via the User Portal

Configure remote access for mobile devices

Module 10: Logging, Reporting and Troubleshooting

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