SOPHOS
Cybersecurity evolved.

Sophos Firewall: Engineer Course Overview

This course is designed for technical professionals who will be demonstrating Sophos 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 Partner Portal, or as an instructor-led classroom course. Please contact your CAM or CAE 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.

Objectives

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

- Explain how Sophos 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 a Sophos Firewall and configure the required network settings
- Perform preliminary sizing for a Sophos Firewall

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.

Agenda

Module 1: Sophos Firewall Overview (60 mins)

- Identify the features of the Sophos Firewall and how the protect against common threats
- List the deployment options available for the Sophos Firewall

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

- Configure a Sophos Firewall using the Initial Setup Wizard
- Navigate the WebAdmin and manage objects
- Configure basic networking including zones, interfaces and routing
- Manage device access and certificates
- List the types of routing supported on the Sophos Firewall
- Configure static routing
- **Simulations (30 mins)**
  - Use the Initial Setup Wizard to configure a Sophos Firewall
  - Create IP Host, FQDN Host and Service definitions
  - Configure DNS Request Routes
  - Import the CA certificates
  - Configure Zone and Interfaces
  - Create Static Routes

Module 3: Network Protection (70 mins)

- 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 (ATP)
- **Simulations (55 mins)**
  - Configure Logging
  - Create Network Firewall Rules
  - Install the SSL CA Certificates
  - Install Sophos Central
  - Migrate Linked NAT Rules to Full NAT Rules
  - Publish Servers using Business Application Rules
  - Protect Servers using the Web Application Firewall
  - Configure IPS Policies
  - Enable Advanced Threat Protection
  - Enable DoS (Denial of Service) and Spoof Protection
  - Configure Security Heartbeat

Module 4: 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
- **Simulations (20 mins)**
  - Create an SSL site-to-site VPN
  - Create an IPsec site-to-site VPN
  - Deploy a Remote Ethernet Device

Module 5: Authentication (80 mins)

- List the supported authentication sources and enable them for services on the Sophos Firewall
- Explain the types of user on the Sophos Firewall and know when to use them
- Configure authentication using Synchronized User Identity, NTLM and Kerberos and STAS (Sophos Transparent Authentication Suite)
- Create identity-based policies

- Enable and use one-time passwords (OTP)
- **Simulations (20 mins)**
  - Configure an Active Directory Authentication Server
  - Configure Single Sign-On Using STAS
  - Create User-based policies
  - Configure One Time Passwords

Module 6: Web Protection (60 mins)

- Explain the different deployment and web filtering modes
- Identify the activities that can be used to control web traffic
- Create keyword content filters
- Configure surfing quotas and traffic shaping policies
- Configure web policy overrides and exceptions
- **Simulations (30 mins)**
  - Create a TLS Inspection Rule to decrypt traffic
  - 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 7: Application Control [40 mins]

- Configure Application Filters
- Detect and categorize applications identified by Synchronized Application Control
- Classify and apply traffic shaping to cloud applications
- Create and apply traffic shaping policies to applications
- **Simulations (15 mins)**
  - Create an Application Filter Policy
  - Categorize applications using Synchronized Application Control
  - Detect and categorize cloud applications

Module 8: Email Protection (50 mins)

- Configure global settings including relay settings
- Configure SMTP policies for MTA mode and legacy mode
- Configure policies for client protocols (SMTP, IMAP and POP)
- Create Data Control Lists and use them in policy
- Configure encryption using SPX and data control
- Manage the quarantine using the WebAdmin, email digests and the user portal
- **Simulations (25 mins)**
  - Enable and Configure Quarantine Digests
  - Configure SMTP Routing and Protection
  - Configure Data Control and SPX Encryption
  - User Quarantine Management

Module 9: 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
- **Simulations (15 mins)**
  - Configure an SSL Remote Access VPN
  - Configure an IPsec Remote Access VPN with Sophos Connect

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 and the different types available
- **Simulations (10 mins)**
  - Deploy a Wireless Access Point

Module 11: Logging and Reporting (40 mins)

- Customize reports and create bookmarks
- Schedule reports
- Use the Log Viewer to monitor the Sophos Firewall
- Configure logging
- Configure email and SNMP notifications
- **Simulations (10 mins)**
  - Run, Bookmark and Schedule Reports
  - View Zero-Day Protection Reports

Module 12: Central Management (35 mins)

- Manage a Sophos Firewall in Sophos Central
- Navigate the Sophos Firewall reports and logs in Sophos Central
- Create a zero-touch configuration file in Sophos Central
- Manage backup configuration files in Sophos Central
- **Simulations (10 mins)**
  - Manage a Sophos Firewall in Sophos Central

Further information

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