SOPHOS
Security made simple.

XG Firewall:
Architect Course Overview

This course provides an in-depth study of Sophos XG Firewall, designed for experienced technical professionals who will be planning, installing, configuring and supporting deployments in production environments.

The course is intended to be delivered in a classroom setting, and consists of presentations and practical lab exercises to reinforce the taught content. Copies of the supporting documents for the course will be provided to each trainee.

Due to the nature of delivery, and the varying experiences of the trainees, open discussion is encouraged during the training.

The course is expected to take 3 days (24 hours) to complete, of which approximately 8 hours will be spent on the practical exercises.

Objectives

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

- Deploy XG Firewall in complex network environments
- Explain how XG Firewall processes traffic and use this information to inform the configuration
- Configure advanced networking and protection features
- Protect web applications using the web server protection
- Size hardware, virtual and software XG Firewalls for a given set of requirements

Prerequisites

Prior to taking this training you should:

- Have completed and passed the **XG Firewall – Certified Engineer** course and any subsequent delta modules up to **version 17.5**

We recommend students have the following knowledge and experience:

- Experience with Windows networking and the ability to troubleshoot issues
- A good understanding of IT security
- Experience configuring network security devices
- Experience configuring and administering Linux/UNIX systems

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 Architect, 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 3 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 Desktop and three XG Firewalls.

Agenda

Module 1: Engineer Review (60 mins)

- Recall important information from the Engineer course
- **Labs (15 mins)**
  - Register for Sophos Central evaluation

Module 2: Deployment (120 mins)

- Describe the deployment modes supported by the XG Firewall
- Understand the types of interfaces that can be created
- Configured gateways
- Configure policy based and dynamic routing
- **Labs (90 mins)**
  - Activate the Sophos XG Firewalls
  - Post-installation configuration
  - Bridge interfaces
  - Multiple WAN links
  - Create a policy-based route for an MPLS scenario

Module 3: Network Protection (100 mins)

- Understand the benefits of Fast Path technology
- Understand what Strict Policy is
- Examine advanced Intrusion Prevention and optimize policies
- Configure advanced DoS Protection Policies
- Explain what Local NAT policy is and known how to configure it
- Be able to configure routing per firewall rule
- Understand best practice for ordering of firewall rules
- **Labs (30 mins)**
  - Local NAT Policy
  - Advanced DoS Rules

Module 4: Web Server Protection (105 mins)

- Explain how Web Server Protection works
- Describe the protection features
- 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 (60 mins)**
  - Web Application Firewall
  - Load balancing with Web Server Protection
  - Web Server Authentication and path-specific routing

Module 5: Site-to-Site Connections (130 mins)

- Configure and deploy site-to-site VPNs in wide range of environments
- Create RED tunnels between two XG Firewalls
- Understand when to use RED

- **Labs (60 mins)**
  - Create an IPsec site-to-siteVPN
  - 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

Module 6: Authentication (90 mins)

- Configure RADIUS accounting
- Deploy STAS in complex scenarios
- Configure SATC and STAS together
- Configure Secure LDAP
- Explain how to use the Sophos XG API
- **Labs (50 mins)**
  - Configure an Active Directory authentication server
  - Configure single sign-on using STAS
  - Create user-based policies
  - Create custom user-based web policies

Module 7: Synchronized Security (65 mins)

- Explain how Security Heartbeat works
- Understand the advantages and disadvantages of deploying it in different scenarios
- **Labs (40 mins)**
  - Source-based Security Heartbeat
  - Destination-based Security Heartbeat
  - Missing Security Heartbeat
  - Lateral Movement Protection

Module 8: Wireless (40 mins)

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

Module 9: Remote Access (40 mins)

- Modified the configuration profile for Sophos Connect
- Configure an IPsec remote access VPN
- **Labs (20 mins)**
  - Sophos Connect

Module 10: High Availability (85 mins)

- Explain the packet flow in high availability
- List the prerequisites for high availability
- Configure high availability
- **Labs (45 mins)**
  - Active-Active Cluster
  - Active-Passive High Availability

Module 11: Sizing and Troubleshooting (75 mins)

- Size a hardware, software or virtual Sophos XG Firewall appropriately
- Identify factors that can affect sizing
- Perform basic troubleshooting using tcpdump
- Enable debug logging
- Create a Consolidated Troubleshooting Report and explain what information it contains
- **Labs (45 mins)**
  - Debug logging
  - Retrieving log files
  - Troubleshoot an issue from an imported configuration

Further information

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