

Sophos Firewall Administration

Network protection, VPNs, identity policies and operational troubleshooting

FA-0696 · 3 days

Cybersecurity · DevOps, Cloud & Infrastructure

Introduction

This three-day course develops day-to-day Sophos Firewall administration skills through selected configuration labs and troubleshooting exercises. It covers setup, routing, protection policies, identity, VPNs and operational evidence.

The source uses the former XG product naming. Training uses a supported Sophos Firewall deployment rather than end-of-life XG appliances. Features and labs depend on the selected SFOS release, hardware and subscriptions; wireless, endpoint integration, email and web-server protection may use prepared demonstrations. Additional prerequisite preparation should be completed before the course.

Learning outcomes

- Configure selected zones, interfaces, routes, objects, certificates and management access.
- Create and validate firewall, NAT and selected threat-protection policies.
- Explain and configure suitable site-to-site and remote-access VPN examples.
- Integrate a supported authentication source and selected user-based policies.
- Assess web, application, email, wireless and web-server protection options for the chosen deployment.
- Use logs, reports, connection inspection and packet capture to troubleshoot lab scenarios.
- Create and validate configuration backup/recovery procedures.

Prerequisites

- Practical subnet, routing, VLAN and VPN knowledge and experience with security devices.
- Basic Active Directory/LDAP integration, SSH on Linux and security administration.
- A prepared isolated lab with two supported firewall instances, two Windows Server instances and one Linux server.
- Authorised management access and applicable subscriptions; optional access points/endpoints for demonstrated features.

Training outline

1. Day 1 – Platform and initial setup

- Supported deployment options, feature licensing and the XG-to-supported-platform transition.
- Setup assistant, web administration, zones, interfaces, gateways, objects and device-access controls.
- Static and policy routes, DNS request routing and certificate trust.
- Backup/restore compatibility, interface mapping and recovery validation.

2. Day 1 – Network and web-server protection

- Firewall and DNAT rules, logging, IPS, DoS/spoof controls and threat-protection policies.
- Security Heartbeat with suitable endpoint/cloud-service integration; register services rather than installing a cloud portal.
- Web application firewall policies, publishing, supported templates, SlowHTTP protection, load balancing and authentication.
- Selected rule/publishing exercises with controlled test traffic and log review.

3. Day 2 – Site-to-site connections

- IPsec and SSL VPN choices, route precedence, NAT and failover examples.
- Policy-based routing in an MPLS scenario and verification of permitted network reachability.
- RED deployment concepts and release-compatible tunnel configurations; review unsupported legacy modes before upgrades.

4. Day 2 – Authentication and identity policies

- Supported directory/authentication sources, user types and identity-based rules.

- Active Directory integration; supported STAS, Synchronized User Identity, NTLM or thin-client integration options as appropriate.
- One-time-password/MFA configuration and selected positive/negative access tests.

5. Day 2 — Web and application control

- Web policies, custom categories, keyword content filters, activities and quotas.
- Application-filter policies and supported synchronised/cloud-application categorisation.
- Check endpoint integration and subscription requirements, then verify selected permitted and blocked traffic.

6. Day 3 — Email and wireless protection

- Email MTA and legacy-mode concepts, relay controls, SMTP/client policies and data-control lists where supported.
- SPX encryption, quarantine digests and user management in a prepared example.
- Supported wireless access-point deployment, network security modes and hotspots; hardware-dependent demonstration.

7. Day 3 — Remote access

- SSL and IPsec remote-access configurations using suitable supported clients, including Sophos Connect.
- VPN-portal/clientless-access distinctions, mobile-client compatibility and least-privilege access.
- Selected connection and authentication tests with routing and log checks.

8. Day 3 — Management, logging and troubleshooting

- Central/cloud management options, logging and customised/scheduled reports.
- Inspect sandbox-analysis activity where licensed, connection tables and diagnostic tools.
- Capture packets and dropped traffic in the lab; correlate evidence with firewall and VPN rules.
- Periodic lab review and a bounded operational troubleshooting exercise.