Advanced Firewall Configuration and Management Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern digital perimeter has dissolved, replaced by a complex, multi-cloud environment where the Next-Generation Firewall is the definitive last line of defense. Organizations face an exponential increase in Advanced Persistent Threats and zero-day attacks that bypass legacy security solutions. Advanced Firewall Configuration and Management Training Course is engineered to elevate IT professionals from basic administration to expert-level firewall architect and manager. You?ÇÖll master vendor-neutral and platform-specific methodologies, focusing on high-availability, SD-WAN security integration, and cloud-native firewall deployments. The goal is to fortify your enterprise with a Zero Trust Architecture foundation, ensuring deep packet inspection, SSL decryption, and sophisticated threat prevention are seamlessly integrated into your core security posture.

This advanced training moves beyond simple ACLs and NAT policies to delve into the operational intricacies of a scalable, resilient firewall ecosystem. We will equip you with the practical skills needed for proactive threat hunting, security policy optimization, and centralized security management via tools like Panorama or FortiManager. By focusing on automation and orchestration, SaaS-based security controls, and compliance with critical standards, this course prepares you to be a critical resource in mitigating the global cybersecurity skills gap. Upon completion, you will be proficient in managing the entire firewall lifecycle, transforming it from a mere network filter into a strategic, intelligent component of your organization's overall cyber defense strategy.

Programme Curriculum

Advanced Firewall Configuration and Management Training Course

Introduction

The modern digital perimeter has dissolved, replaced by a complex, multi-cloud environment where the Next-Generation Firewall is the definitive last line of defense. Organizations face an exponential increase in Advanced Persistent Threats and zero-day attacks that bypass legacy security solutions. Advanced Firewall Configuration and Management Training Course is engineered to elevate IT professionals from basic administration to expert-level firewall architect and manager. You?ÇÖll master vendor-neutral and platform-specific methodologies, focusing on high-availability, SD-WAN security integration, and cloud-native firewall deployments. The goal is to fortify your enterprise with a Zero Trust Architecture foundation, ensuring deep packet inspection, SSL decryption, and sophisticated threat prevention are seamlessly integrated into your core security posture.

This advanced training moves beyond simple ACLs and NAT policies to delve into the operational intricacies of a scalable, resilient firewall ecosystem. We will equip you with the practical skills needed for proactive threat hunting, security policy optimization, and centralized security management via tools like Panorama or FortiManager. By focusing on automation and orchestration, SaaS-based security controls, and compliance with critical standards, this course prepares you to be a critical resource in mitigating the global cybersecurity skills gap. Upon completion, you will be proficient in managing the entire firewall lifecycle, transforming it from a mere network filter into a strategic, intelligent component of your organization's overall cyber defense strategy.

Course Duration

5 days

Course Objectives

1. Master Next-Generation Firewall features, including Application-ID and Content-ID.
2. Implement and manage complex Network Address Translation and IPsec VPN tunnels.
3. Design and deploy High Availability and redundancy architectures for maximum business continuity.
4. Configure and troubleshoot SSL/TLS decryption policies to expose hidden threats in encrypted traffic.
5. Implement User-ID and integration with LDAP/Active Directory for granular, user-based access control.
6. Develop and optimize Security Policy Rulebases using the Principle of Least Privilege.
7. Integrate firewalls with Threat Intelligence Platforms and SIEM solutions for real-time visibility.
8. Configure and manage advanced Intrusion Prevention Systems and anti-malware profiles.
9. Secure SD-WAN and multi-cloud environments using distributed firewall policies.
10. Apply best practices for Zero Trust Network Access policy enforcement at the perimeter.
11. Perform security policy optimization and auditing using vendor-specific tools and compliance frameworks
12. Design and deploy Demilitarized Zones and specialized security zones for critical infrastructure.
13. Utilize centralized management platforms for large-scale security orchestration and reporting.

Target Audience

1. Network Engineers and Architects looking to specialize in security.
2. Security Administrators seeking advanced, expert-level firewall skills.
3. Security Operations Center (SOC) Analysts involved in Level 2/3 threat response.
4. IT Managers responsible for compliance and infrastructure security.
5. Candidates preparing for PCNSE, CCSE, or FortiGate NSE 4/5/7 certifications.
6. Cybersecurity Consultants and Auditors requiring deep configuration knowledge.
7. Cloud Engineers focused on securing Hybrid Cloud and multi-cloud network traffic.
8. DevSecOps Engineers integrating security and automation into the network pipeline.

Course Modules

Module 1: NGFW Architecture and Deployment

- Compare traditional and Next-Generation Firewall capabilities.
- Design and deploy firewall Security Zones and VLAN segmentation.
- Configure initial setup: interfaces, routing, and Virtual Wire/Layer 3 modes.
- Establish High Availability clusters for resiliency.
- Implement secure administrative access using Multi-Factor Authentication and role-based access control.
- Case Study: Migrating from a legacy, port-based firewall to a new App-ID-enabled NGFW in a large corporate network without service interruption.

Module 2: Advanced Security Policy and NAT Configuration

- Master Policy Rulebase Optimization for efficiency and performance.
- Develop granular security policies using Application-ID and user identity
- Configure complex Source and Destination NAT for server access and traffic hiding.
- Implement Inter-Zone and Intra-Zone security policies
- Best practices for creating a "Deny All" final rule and policy cleanup procedures.
- Case Study: Troubleshooting a major e-commerce platform outage due to an incorrectly ordered and conflicting NAT rule that blocked payment gateway traffic.

Module 3: Threat Prevention and IDS/IPS Mastery

- Configure and tune Intrusion Prevention System signatures to minimize false positives.
- Implement Anti-Malware, Anti-Spyware, and Vulnerability Protection profiles.
- Integrate with Cloud Sandboxing to block zero-day malware.
- Customize URL Filtering and DNS Security policies to mitigate phishing and C2 traffic.
- Utilize File Blocking policies to prevent malicious document transmission over permitted applications.
- Case Study: Responding to a high-profile ransomware attack by quickly deploying and tuning custom IPS signatures based on fresh threat intelligence feeds.

Module 4: Decryption and User-ID Integration

- Understand the legal and technical requirements for SSL/TLS Decryption deployment.
- Implement forward and non-forward proxy decryption for inbound and outbound traffic.
- Configure Certificate Management and root certificate deployment for client trust.
- Integrate User-ID with Active Directory, RADIUS, or single sign-on systems.
- Troubleshoot decryption errors and policy-based bypasses for sensitive applications
- Case Study: Designing a Decryption Policy rollout that allowed the security team to identify a massive data exfiltration attempt hidden within encrypted HTTPS traffic.

Module 5: Secure Connectivity

- Configure secure Site-to-Site IPsec VPN tunnels with advanced encryption and authentication
- Deploy and manage Remote Access VPNs using GlobalProtect or FortiClient.
- Implement Tunnel Monitoring and Dead Peer Detection for tunnel stability.
- Enforce Zero Trust Network Access policies based on device posture and user identity.
- Troubleshoot complex VPN issues related to NAT traversal and phase negotiation failures.
- Case Study: Securing a rapid shift to a remote workforce by deploying an MFA-enabled Remote Access VPN solution with granular access policies to internal resources.

Module 6: Logging, Monitoring, and Reporting

- Configure advanced logging profiles and forwarding to an external SIEM solution
- Analyze Threat Logs, Traffic Logs, and URL Logs to identify suspicious activity.
- Utilize firewall diagnostic tools for deep traffic analysis.
- Create custom, executive-level Security Posture Reports and compliance dashboards.
- Establish a Log Retention Policy in compliance with regulatory requirements
- Case Study: Developing an automated threat hunting workflow by correlating firewall logs with endpoint detection data in a centralized SIEM platform.

Module 7: Cloud and SD-WAN Security Integration

- Understand firewall deployment models in Public Cloud environments
- Configure firewalls for SD-WAN deployments, including path selection and quality of service
- Implement Cloud-Native Firewalls and security groups for workload protection.
- Establish centralized policy management across distributed branch office and cloud firewalls.
- Secure IoT/OT networks using specialized segmentation and application control policies.
- Case Study: Designing a unified security policy for a global enterprise connecting 50+ branch offices via SD-WAN and two major public clouds, ensuring consistent policy enforcement.

Module 8: Centralized Management and Automation

- Deploy and manage firewalls at scale using a Centralized Management platform
- Leverage Templates and Device Groups to enforce standardized security policies.
- Utilize firewall APIs and SDKs for configuration automation and scripting
- Perform a Security Policy Audit using Best Practice Assessment tools.
- Understand Disaster Recovery procedures, including backup and restoration of central management configurations.
- Case Study: Automating the deployment of a standardized DMZ Security Policy across 30 production firewalls in a single maintenance window using a REST API script.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com