Next-Generation Firewall Configuration and Policy Training Course

26 - 30 Oct 2026

Cairo

3700 € (Per Person)

Ref: #NO2213_279031

Course Introduction / Overview:

This comprehensive course provides an in-depth exploration of enterprise firewall configuration and policy management, designed to equip participants with the skills needed to secure modern network infrastructures. In an era of sophisticated cyber threats, a properly configured firewall is the cornerstone of any effective defense-in-depth strategy. This program moves beyond basic setup, delving into the nuances of creating, implementing, and maintaining robust security policies that align with business objectives and compliance requirements. Drawing on principles outlined by leading academics like William Stallings in works such as "Network Security Essentials: Applications and Standards", the curriculum emphasizes a strategic approach to network security. Participants will learn to master Next-Generation Firewall (NGFW) features, including application control, intrusion prevention, and user identity integration. BIG BEN Training Center has developed this course to bridge the gap between theoretical knowledge and practical application, ensuring that attendees can confidently manage complex firewall environments, optimize rule sets for performance, and respond effectively to security incidents. This training is essential for professionals dedicated to protecting critical digital assets against an ever-evolving threat landscape.

Target Audience / This training course is suitable for:

- Network Security Engineers.
- IT Security Administrators.
- Systems Administrators.
- Network Architects.
- Security Analysts.
- IT Managers with security responsibilities.
- Security Operations Center (SOC) personnel.
- Compliance and Audit Officers.
- IT professionals seeking to specialize in network security.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Government and Public Sector Agencies.
- Technology and Software Development.
- Telecommunications Providers.
- E-commerce and Retail.
- Energy and Utilities.
- Education Sector.

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security (InfoSec) Department.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Compliance and Internal Audit Departments.
- Infrastructure and Operations Teams.
- Risk Management Department.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop and implement granular firewall policies based on security best practices.
- Configure and manage core features of Next-Generation Firewalls (NGFWs).
- Integrate user identity and application awareness into security policies.
- Establish and configure secure Virtual Private Network (VPN) tunnels.
- Optimize firewall rule sets to enhance performance and security posture.
- Implement high availability configurations to ensure network resilience.
- Analyze firewall logs to detect and respond to security events.
- Conduct firewall policy audits to ensure compliance with regulatory standards.
- Troubleshoot common firewall configuration and network connectivity issues.
- Understand the principles of network segmentation and Zero Trust architecture.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring participants gain both theoretical knowledge and hands-on competence. This course utilizes a blended learning approach that combines expert-led instruction with practical application. Sessions will feature detailed presentations, real-world case studies of network breaches and successful defenses, and interactive group discussions on security policy design. A significant portion of the course is dedicated to hands-on lab exercises in a simulated enterprise environment, allowing participants to configure firewalls, write policies, and troubleshoot issues without risk to live systems. This immersive experience reinforces learning and builds confidence. The instructor will facilitate collaborative problem-solving activities and provide continuous, constructive feedback. Team-based projects will challenge participants to design a comprehensive firewall policy for a fictional organization, promoting teamwork and strategic thinking. This dynamic and supportive learning environment ensures that participants leave the course with practical skills they can immediately apply in their professional roles.

Course Agenda (Course Units):

Unit One: Fundamentals of Network Firewalls and Security Policies

- Introduction to network security and the role of firewalls.
- Evolution of firewalls from packet filters to Next-Generation Firewalls (NGFW).
- Understanding stateful vs. stateless inspection.
- Core concepts of network address translation (NAT) and port address translation (PAT).
- Principles of effective security policy design.
- The security policy lifecycle from creation to decommissioning.
- Common firewall deployment models and architectures.

Unit Two: Initial Firewall Configuration and Core Policy Implementation

- Performing initial device setup and system configuration.
- Configuring network interfaces, zones, and virtual routers.
- Creating and managing network and service objects.
- Developing fundamental security policies and access control lists (ACLs).
- Implementing source and destination NAT policies.
- Understanding policy processing order and its security implications.
- Best practices for documenting firewall rules and changes.

Unit Three: Mastering Next-Generation Firewall (NGFW) Features

- Configuring Application Identification and Control (App-ID).
- Implementing User Identification (User-ID) for granular policy control.
- Configuring and tuning Intrusion Prevention Systems (IPS).
- Implementing anti-malware and web filtering policies.
- Understanding and configuring SSL/TLS decryption.
- Integrating threat intelligence feeds for enhanced protection.
- Blocking malicious domains and IP addresses using external block lists.

Unit Four: Virtual Private Networks (VPN) and High Availability

- Fundamentals of VPN technology, including IPsec and SSL.
- Configuring site-to-site IPsec VPN tunnels between corporate locations.
- Implementing secure remote access VPNs for mobile users.
- Concepts of firewall high availability (HA).
- Configuring Active/Passive and Active/Active HA clusters.
- Understanding HA link monitoring and failover triggers.
- Testing and verifying HA functionality.

Unit Five: Policy Optimization, Monitoring, and Troubleshooting

- Techniques for analyzing and optimizing the firewall rule base.
- Identifying shadowed, redundant, and overly permissive rules.
- Implementing a structured firewall change management process.
- Configuring logging, monitoring, and reporting features.
- Analyzing firewall logs for security incidents and troubleshooting.
- Common firewall troubleshooting methodologies and tools.
- Preparing for and conducting firewall policy audits for compliance.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As network perimeters dissolve with the rise of cloud and remote work, how must traditional firewall policy management evolve to embrace a Zero Trust security model effectively?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by focusing on the strategic management of security policies rather than just the technical configuration of a specific vendor's device. While many courses teach which buttons to click, this program emphasizes the "why" behind the "how", grounding every technical skill in the broader context of risk management, business enablement, and compliance. It moves beyond foundational setup to address the entire lifecycle of a firewall policy, from initial design and implementation to ongoing optimization, auditing, and eventual decommissioning. The curriculum is uniquely structured to build a strategic mindset, teaching participants how to create policies that are not only secure but also efficient and aligned with organizational goals. By integrating concepts like the Zero Trust architecture and the challenges of securing hybrid environments, the course prepares professionals for the future of network security, not just its present. The emphasis on hands-on labs for policy optimization and troubleshooting real-world scenarios ensures that participants develop practical, critical-thinking skills that are immediately applicable and highly valued in the industry.