Forcepoint Next Generation Firewall (NGFW): Administrator Virtual Instructor-Led Training

Datasheet

December 2021

Forcepoint

forcepoint.com

Forcepoint Next Generation Firewall (NGFW): Administrator Virtual Instructor-Led Training

NGFWADM

In this 16-hour hands-on virtual instructor-led training (VILT) course, you will learn the skills needed to practice as a system administrator responsible for installation, configuration, administration, and support of Forcepoint NGFW. Through instructional content, demonstrations, and hands-on lab practice exercises, you will learn the requirements and recommendations to successfully deploy Forcepoint NGFW in a variety of network environments. You will develop expertise in creating security rules and policies, managing users and authentication, configuring VPNs, performing deep traffic inspection, and accomplishing common administration tasks including status monitoring and reporting.

Audience

- New and existing customers of Forcepoint NGFW
- Forcepoint channel partners
- Forcepoint NGFW end users

Course Objectives

- Access the virtual training environment, class materials and lab environment.
- Articulate the NGFW System benefits and differentiators.
- Identify the components of the SMC and their roles.
- Administer the SMC components and use them to manage and monitor NGFW firewalls.
- Configure security policies and access control.
- Configure network address translation.
- Configure a Sidewinder Proxy.
- Implement deep inspection through policies and templates.
- Implement file filtering and malware detection.
- Implement alerting and notification.
- Manage users and authentication.
- Configure mobile VPN solutions.
- Configure a site-to-site VPN.
- Manage log collection and storage.
- Utilize monitoring, statistics, and reporting.
- Make use of policy management tools.
- Perform basic troubleshooting of NGFW.

Format:

Virtual Instructor-Led Training

Duration:

16 hours, typically delivered in 4 sessions, 4 hours per session – plus 60-90 minutes of homework each session

Course Price:

$1,150 USD

Exam Price:

One attempt is included

Prerequisites for attendance

- General understanding of system administration and Internet services
- Basic knowledge of networking and computer security concepts
- A computer that meets the requirements noted at the end of this document

Certification exams

This course prepares you for the Certified Forcepoint Next Generation Firewall Administrator exam. One exam attempt is included in the price of the course, but the execution of the exam is not accomplished during the course. A minimum score of 80% on the multiple-choice online exam is required to obtain certification.

Course Outline

Module 0: Introduction

- Prepare to use the virtual training environment.

Module 1: NGFW Overview

- List NGFW benefits and/or differentiators.
- Explain the differences between the operating roles.
- Describe the NGFW engine and appliances.
- Describe at least one of the installation methods.
- Explain the three platforms on which the NGFW can be deployed.

Module 2: SMC Overview

- Describe the Security Management Center and its key features.
- Describe the NGFW system architecture.
- Identify the ports used for communication between SMC components.
- Explain the use of locations and contact addresses.
- Explain the use of SMC Domains.

Module 3: Getting Started with SMC

- Describe the management client and how it works.
- Create system backups.
- Describe SMC high availability options.
- Configure SMC Administrator Access
- Apply configuration to NGFW engines.
- Describe how logs work.

Module 4: NGFW Policies and Templates

- Describe the types of NGFW policies.
- Define firewall policy templates.
- Create a firewall policy hierarchy.
- Describe the benefits of aliases and continue rules.

Module 5: Access Control and NAT

- Explain how traffic is matched in access rules.
- Explain the different types of access rules.
- Describe the actions for processing traffic in access rules.
- Explain the different types of NAT.
- Configure NAT rules.

Module 6: Traffic Inspection.

- Explain the difference between service, service with protocol, and proxy.
- Explain enhanced access control methods.
- Explain different ways to control applications.
- List the detection methods used in the NGFW Inspection.
- Describe AETs and normalization.
- Describe TLS Inspection.
- Configure Snort inspection on the NGFW.
- List the Forcepoint products that integrate with the NGFW.

Module 7: Inspection Policies

- Explain how to send traffic for deep packet inspection.
- Describe Situations and how to use them.
- Define the different type of rules in the inspection policy.
- Tune an inspection policy.

Module 8: Malware Detection and File Filtering Policies

- List the different options for detecting malware.
- Explain how to send traffic for malware detection.
- Configure a file filtering policy.
- Integrate the NGFW with a Data Loss Prevention system

Module 9: Alerting and Notifications

- Explain the alert escalation process in the NGFW system.
- Create an alert policy and alert chain to escalate an alert.

Module 10: Users and Authentication

- Identify supported directory servers and authentication methods.
- Explain the browser-based user authentication mechanism.
- Configure user authentication.
- Differentiate between user authentication and user identification.
- Explain the difference between the Forcepoint FUID and ECA.
- Configure user behavior monitoring

Module 11: Mobile VPN and SSL VPN Portal

- List NGFW Mobile VPN Access options.
- Describe the SSL VPN Portal and the URL Rewrite translation method.
- Configure an SSL VPN Portal.

Module 12: Site-to-Site VPN

- Define the terms used in NGFW VPN Terminology.
- Explain how Site-to-site VPNs work
- Describe Full Mesh, Star and Hub VPN topologies
- List SD-WAN features supported by the NGFW.
- Configure a Policy-Based VPN.
- Describe How a Route-based VPN Works.

Module 13: Using Logs

- Describe the log entry types available in the NGFW.
- Use the interface to interpret and analyze logs.
- Configure and Manage Logs.
- Create permanent filters.
- Analyze how pruning filters affect log data.
- Configure the log server to forward logs to third-party SIEM systems.
- Describe the methods available for managing the space consumed by log data.

Module 14: Monitoring, Statistics, and Reporting

- Describe the benefits of Policy Snapshots.
- Search rules in an NGFW Policy.
- Analyze policy structure and apply tools to optimize the access rules.

Module 15: Policy Tools

- Monitor the system and firewall activity.
- Describe the use of overviews in the SMC user interface.
- Configure and generate reports.
- Monitor third-party components.

Module 16: Troubleshooting

- Explain the troubleshooting process.
- Use the SMC to troubleshoot your systems.
- Explain how to collect diagnostics for Support.
- Resolve common SMC issues.
- Explain how NGFW packet processing works.

Module 17: Single Firewall Installation (classroom only)

- Describe NGFW deployment options.
- List features specific to single firewalls.
- Configure a single firewall in the SMC.
- Configure an NGFW engine for initial contact with the SMC.
- Establish the trust between SMC and a newly installed NGFW engine.

Module 18: What's new in NGFW

- Identify key features new to the NGFW in version 6.10.
- Locate the documentation needed to implement these features.

To attend this virtual online course, you must have a computer with:

- A high-speed internet connection (minimum of 1 MB connection required)
- An up-to-date web browser (Google Chrome recommended)
- PDF viewer
- Speakers and microphone or headset (headset recommended)

A separate tablet or e-book reader is also recommended for the course and lab book delivery

Terms and Conditions

- Virtual Instructor Led Trainings (VILTs) are delivered as live instructor-led training in an online classroom with no on-site delivery element.
- This course is limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint trainings are standard and non-negotiable.
- Forcepoint provides the training "AS IS" and makes no warranties of any kind, express or implied.
- VILT courses must be completed within six months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit https://www.forcepoint.com/services/training-and-technical-certification or contact Forcepoint Technical Learning Services at learn@forcepoint.com.