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

Datasheet

September 2020

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 the 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, traffic deep inspection, and performing common administration tasks including status monitoring and reporting.

Audience

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

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

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.

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

- Welcome to the course
- Understand and prepare to use the virtual training environment.

Module 1: NGFW Overview

- Articulate NGFW key benefits and differentiators from other firewall products.
- Differentiate the various NGFW operating modes.
- Describe the NGFW Hardware Platform and Virtualization options.
- Describe different installation methods.
- Understand different NGFW deployment options.

Module 2: SMC Overview

- Articulate the NGFW system architecture.
- Describe the components of the SMC and its supported platforms.
- Identify the properties of the Management & Log server.
- Identify the properties of the Web Portal Server.
- Articulate the SMC Deployment options.
- Understand communication between SMC components and NGFW.
- Understand locations and contact addresses.

Module 3: Getting Started with SMC

- Describe a high-level overview of the functionality of the management client.
- Prepare to perform system backups.
- Describe SMC High Availability solutions.
- Understand different SMC Administrator roles and access limitation.
- Articulate SMC logging approach and how to utilize Logs view.

Module 4: NGFW Policies and Templates

- Describe the types of NGFW policies.
- Understand firewall policy templates.
- Explain automatic rules.
- Understand a firewall policy hierarchy.

Module 5: Access Control and NAT

- Utilize the policy editor to customize NGFW policies.
- Configure Access Control Rules.
- Understand Rules Options.
- Describe the supported types of NAT.
- Configure the Network Address Translation.

Module 6: Traffic Inspection

- Understand the difference between stateful and proxy mode.
- Configure web filtering.
- Explain different ways to control applications.
- Configure Sidewinder Proxy on the NGFW.
- Describe integration with external solutions.

Module 7: Inspection Policies

- Describe the Inspection Policies and Inspection Policy hierarchy.
- Configure the system policies and utilize the template for deep packet inspection.
- Articulate the different inspection policy components and options..
- Modify Inspection rules to react with various traffic.
- Understand how to tune the Inspection Policy.

Module 8: Malware Detection and File Filtering Policies

- Explain the malware detection process in the NGFW.
- Articulate the different options for detecting malware.
- Configure a File Filtering Policy.
- Explain the detection methods used in the NGFW Inspection.

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.
- Configure alert notifications channels.

Module 10: Users and Authentication

- Identify supported directory servers and authentication methods.
- Explain and configure user authentication.
- Comprehend user identification.
- Understand how to integrate active directory interacts with the FUID agent.
- Understand ECA agent integration in windows environments.

Module 11: Mobile VPN and SSL VPN Portal

- Understand client based and clientless remote access.
- Articulate the different Forcepoint options for remote access.
- Perform the SSL VPN Portal configuration.

Module 12: Site-to-Site VPN

- Understand NGFW VPN Terminology.
- Differentiate between policy-based VPN and route-based VPN.
- Understand different site-to-site VPN topologies.
- Configure a policy-based VPN.

Module 13: Using Logs

- Describe the log entry types available in the NGFW.
- Analyze how pruning filters affect log data.
- Create permanent filters.
- Illustrate the analysis and visualization tools for logs.
- Configure log data management tasks.

Module 14: Monitoring, Statistics, and Reporting

- Understand status monitoring views and dashboards.
- Understand Overviews and alert thresholds.
- Create customizable reports from log data.
- Comprehend the different third-party probing methods.

Module 15: Policy Tools

- Understand policy snapshots within the Management Server.
- Run the Rule Search tool available for Access rules, NAT rules, and Inspection Policies.
- Utilize the Policy Validation tool.
- Understand the Rule Counter Analysis.
- Comprehend the Policy Activation process in NGFW.

Module 16: Troubleshooting

- Understand the full troubleshooting process.
- Recognize the different kinds of logs that SMC provides to perform troubleshooting.
- Utilize various logs for troubleshooting and understand their meaning.
- Capture traffic and run diagnostics.
- Learn what to provide support when troubleshooting.
- Apply knowledge through three common problem scenarios.

Module 17: What's new in NGFW

- Describe the new features added in the latest update to the Forcepoint NGFW.

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.

Forcepoint