FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint NGFW

CERTIFIED ADMINISTRATOR E-LEARNING COURSE

COURSE DATASHEET

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint NGFW

COURSE OVERVIEW

In this eLearning training course, you will learn how to install, configure, administer, and support 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, understanding multi-link technology, configuring VPNs, traffic deep inspection, performing 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

- Understand the fundamentals of NGFW
- Articulate the NGFW System Architecture
- Differentiate the various NGFW operating modes
- Administer the SMC components and use them to manage and monitor NGFW
- Perform common administration tasks
- Configure security policies and access control
- Manage users and authentication
- Understand monitoring capabilities
- Create and edit reporting of the traffic processed by NGFW
- Integrate NGFW with other Forcepoint solutions
- Perform basic troubleshooting of NGFW

Format:
Computer-based e-Learning

Duration:
8 hours of total content total

Price:
$600 USD non-discountable

Language:
English

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 to take and pass the Certified Forcepoint DLP Administrator Exam. The exam can be purchased separately at a rate of $100. If you would like to take the certification exam following completion of the eLearning course, please contact salestraining@forcepoint.com for purchase details.

COURSE OUTLINE

SESSION 1

Module 0: Introduction

- Welcome to the course
- Understand and prepare to use the virtual training environment
- Describe the new features added in 6.3 to the Forcepoint NGFW

Module 1: 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 2: 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 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
- Define and administer best practices for policy change control
- Articulate SMC logging approach and how to utilize Logs view

SESSION 2

Module 4: NGFW Policies and Access Control

- Describe the types of NGFW Policies
- Understand firewall templates and policy hierarchy
- Describe different policy components
- Utilize the policy editor to customize NGFW policies
- Perform firewall traffic inspection
- Integrate NGFW with other Forcepoint solutions

Module 5: Firewall Policy and Network Address Translation (NAT)

- Describe the supported types of NAT
- Describe proxy ARP and it relevance to the NAT
- Configure the Network Address Translation

Module 6: Inspection and File Filtering 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
- Describe integration with external solutions

Module 7: 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

SESSION 3

Module 8: Users and Authentication

- Identify supported directory servers and authentication methods
- Configure browser based authentication
- Explain how Active Directory and the Logon Collector interact

Module 9: SSL VPN Portal

- Understand client based and clientless remote access
- Describe the mapping of SSL VPN Portal Services
- Perform the SSL VPN Portal configuration

Module 10: 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

SESSION 4

Module 11: 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 12: Monitoring, Statistics, and Reporting

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

Module 13: 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 tool based on information within the Log Server
- Comprehend the Policy Activation process in NGFW

Module 14: 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

**To attend this web based course, you must have a computer with:*
•A high-speed internet connection
•An up to date web browser
•Adobe Flash web browser plug in
•PDF Viewer
•Speakers and microphone or headset

A separate tablet or eBook reader is also recommended for the course and lab book delivery. Test your connection to an Adobe Connect virtual class environment here.

TERMS AND CONDITIONS

- eLearning's are delivered as computer-based training—no onsite delivery element
- eLearning's are limited and may not address all of your unique requirements
- The training services in this course are provided pursuant to the Subscription Agreement
- Forcepoint provides the training "AS IS" and makes no warranties of any kind, express or implied
- eLearning's courses must be completed within 6 months from purchase or the course is forfeited
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions
- Forcepoint trainings are standard and non-negotiable

For more information about other Forcepoint training offerings, please visit our Customer or Partner training page.

Questions about Forcepoint training? Contact Forcepoint Technical Readiness and Training at salestraining@forcepoint.com