optima
PROFESSIONAL SERVICES

Forcepoint NGFW Administrator Course (ILT) Outline

Forcepoint NGFW

Administrator Course

Intended audience:

- New and existing customers of Forcepoint NGFW
- Forcepoint Channel Partners
- Forcepoint NGFW end users

Format	Duration	Prerequisites	Certification Requirements
Instructor Led-Training (Classroom)	4 Days	• 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	This course prepares you to take and pass the Certified Forcepoint Next Generation Firewall Administrator (NGFW Virtual) Exam. The exam 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.

Overview:

In this instructor led 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.

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's
- Perform common administration tasks
- Manage users and authentication
- Understand monitoring capabilities
- Create and edit reporting of the traffic processed by NGFW's
- Integrate NGFW with other Forcepoint solutions
- Perform basic troubleshooting of NGFW
- Configure and install a single firewall
- Configure security policies and access control

Day1:	**Day 2:**
<u>Module 0: Introduction</u> • Welcome to the course • Understand and prepare to use the virtual training environment <u>Module 1: NGFW Overview</u> • Articulate NGFW key benefits and differentiators from other firewall products • Differentiate the various NGFW operating modes	<u>Module 6: Traffic Inspection</u> • 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 <u>Module 7: Inspection Policies</u>

- 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 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

• Describe SMC High Availability solutions • Understand different SMC Administrator roles and access limitation • Articulate SMC logging approach and how to utilize Logs view <u>Module 4: NGFW Policies and Templates</u> • Describe the types of NGFW policies • Understand firewall policy templates • Explain automatic rules • Understand a firewall policy hierarchy <u>Module 5: Access Control and NAT</u> • 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	
Day 3: <u>Module 10: Users and Authentication</u> • 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 <u>Module 11: Using Logs</u>	

- 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 and dashboards
- 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
- 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

Module 15: Single Firewall Installation

- NGFW Deployment Overview
- NGFW Operating Roles
- Single NGFW Configuration

- NGFW Installation
- Add-Ons Features
- Advanced Configuration Settings

Module 16: What's new in NGFW 6.5

- Describe the new features added in 6.5 to the Forcepoint NGFW