FORCEPOINT

Forcepoint NGFW System Engineer Instructor-led

Datasheet

June 2019

Forcepoint NGFW System Engineer Instructor-led

NGFWIMP

In this Instructor-led course, you will learn how to install, configure, administer, support Forcepoint NGFW. Through instruction, demonstrations, and hands-on lab practice exercises, you will understand the requirements and recommendations to successfully deploy Forcepoint NGFW in a variety of network environments. You will then develop expertise in topics that include, but are not limited to, clustering the NGFW, creating security rules and policies, integrating the NGFW with other Forcepoint technologies, inbound and outbound traffic management, understanding multi-link technology, configuring VPNs, traffic deep inspection, and controlling endpoint activity with the Endpoint Context Agent.

Audience

- End-User/Customers: System Administrators, Network Security Administrators, Network Engineers, IT staff
- Channel Partners: Consultants, System Architects, Integrators and Planners who help customers with Forcepoint NGFW implementations

Course Objectives

- Describe the fundamentals of NGFW
- Detail the Security Management Center (SMC) capabilities
- Plan and deploy the SMC
- Configure and deploy a single firewall and a firewall cluster
- Configure policies for distributed firewall management
- Configure security policies and access control
- Configure and utilize multiple internet connections
- Define Multi-Link Policy-based VPNs
- Manage users and authentication
- Create Mobile VPN
- Monitor user and endpoint activity
- Perform traffic inspection and malware detection
- Create custom network applications
- Configure TLS decryption
- Integrate the NGFW with Forcepoint cloud solutions

Format:
Instructor-led In person*

Duration:
40 hours total - 5 days, 8 hours per day

Language:
English

Course Price:
$3,500 USD

Exam Price:
Included

Prerequisites for attendance

- Completion of the Forcepoint NGFW Administrator Course and certification.
- General understanding of routing and firewall functionality

Certification Exam

This course prepares you to take and pass the Certified Forcepoint NGFW System Engineer Exam.
The System Engineer exam is a two-part exam: Theoretical (multiple choice) and Practical (hands-on). The practical exams will be administered on day 5 of the course. but the execution of the theoretical exam is not accomplished during the course. A minimum score of 80% on the multiple-choice online exam and a 70% of the hands-on exam is required to obtain the System Engineer certification. The System Engineer exam is included in the price of the course.

Course Outline

MODULE 1: SYSTEM ARCHITECTURE OVERVIEW

- Articulate the NGFW System Architecture
- Understand how to size a firewall and management environment
- Understand Management and Log Server high availability
- Become familiar with upgrading Management Server, Log Server, and engines
- Articulate the Forcepoint NGFW license model

MODULE 2: FIREWALL/VPN ROLE AND SINGLE FIREWALL DEPLOYMENT

- Describe basic network defence strategies
- Define the capabilities and key features of the NGFW
- Understand and learn the process of defining and deploy a single firewall
- Identify additional features of the NGFW

MODULE 3: ROUTING AND ANTI-SPOOFING

- Configure static routing
- Describe additional special routing capabilities of the NGFW
- Understand route metrics and route monitoring
- Summarize the origin and function of Anti-spoofing

MODULE 4: NGFW POLICIES

- Describe different NGFW policy types
- Define NGFW policy templates and policy structure
- Identify the anatomy of a security policy and the objects used in policies
- Detail the process of policy installation and activation

MODULE 5: DISTRIBUTED SYSTEM CONFIGURATION

- Describe system communication in a distributed firewall environment
- Identify locations and contact addresses in distributed systems
- Describe system communication between management and engines
- Configure Network Address Translation (NAT)

MODULE 6: FIREWALL/VPN ROLE AND CLUSTERING TECHNOLOGY

- Describe the firewall clustering architecture and theory
- Configure a firewall cluster in the SMC (management)
- Employ NGFW interface options
- Deploy a firewall cluster

MODULE 7: MSSP AND VIRTUAL CONTEXTS

- Describe the SMC Domain Architecture
- Detail the function of the Web Portal Server
- Define Virtual Contexts
- Relate Master Engines and Virtual Engines
- Relate clustering and performance
- Review a configuration and deployment example of an MSSP architecture

MODULE 8: OUTBOUND MULTI-LINK TECHNOLOGY

- Describe Outbound Traffic Management and its capabilities
- Explain ISP link selection
- Classify when to use a particular link selection method
- Configure Outbound Multi-Link

MODULE 9: SITE-TO-SITE VPNS

- Define Forcepoint NGFW VPN capabilities
- Define Forcepoint NGFW VPN terminology
- Identify supported VPN topologies
- Relate Multi-Link and VPNs
- Test VPN-related tools in the SMC
- Configure a Multi-Link Policy-Based VPN
- Investigate Route-Based VPNs and when to use them
- Design VPN Hub configuration

MODULE 10: ACTIVE DIRECTORY INTEGRATION

- Define network user management
- Integrate Active Directory with the SMC (management)
- Categorize the role of NPS, LDAP authentication, RADIUS, and TACAC+ in the authentication process
- Deploy Forcepoint User Identification
- Configure and deploy the Endpoint Context Agent
- Monitor network users

MODULE 11: VPN CLIENT

- Describe Mobile VPN connections
- Distinguish IPSec and SSL VPN tunnelling
- Configure an NGFW engine for Mobile VPN connections
- Configure the VPN Client for an endpoint
- Demonstrate tools for Mobile VPN troubleshooting

MODULE 12: TRAFFIC INSPECTION

- Review connection control and the role of Deep Inspection
- Differentiate between Services, Protocol Agents, and Proxy Modules
- Configure a Sidewinder Proxy service
- Establish Network Application Identification
- Differentiate Network Applications and Client Applications

MODULE 13: INSPECTION POLICIES

- Relate firewall and inspection policies
- Illustrate the anatomy of Inspection Policies
- Differentiate the predefined Inspection Policy templates
- Define the concept of Situations
- Define the function of the Inspection Rules tree
- Fine-tune inspection policies
- Analyze the role and function of Inspection Exception rules
- Analyze the use and function of Blacklisting

MODULE 14: MALWARE DETECTION AND FILE FILTERING

- Explain the process of Malware Detection
- Illustrate the anatomy of a File Filtering Policy
- Define the process of using File Reputation services
- Configure built-in Anti-Malware scanning
- Describe the role of Advance Malware Detection

MODULE 15: NGFW INSPECTION TECHNIQUES

- Define techniques used by the NGFW to identify threats
- Detail the traffic inspection process
- Explain the role of Advanced Evasion Techniques and the process of traffic normalization
- Describe misuse detection with Fingerprints
- Describe concept of Situations and their role in traffic inspection
- Analyze Regular Expression syntax
- Review examples of fingerprints

MODULE 16: TLS INSPECTION

- Articulate the purpose of TLS inspection
- Describe TLS inspection exceptions
- Define the process of Server and Client-Side TLS inspection
- Configure the TLS inspection

MODULE 17: NGFW IN LAYER 2 ROLES AND MULTI-LAYER DEPLOYMENT

- Identify NGFW Operating Roles
- Define key features of the IPS and Layer 2 Firewall roles
- Understand the difference between the Firewall and IPS
- Describe a Layer 2 Policy
- Configure and deploy a multi-layer NGFW
- Analyze the role of High Availability in multi-layer deployments

MODULE 18: FORCEPOINT INTEGRATION

- Configure integration with Forcepoint Web Security Cloud
- Detail how to integrate with Forcepoint Advanced Malware Detection
- Review the Malware Detection process
- Understand information exchange using Syslog or other SIEM solutions

MODULE 19: TROUBLESHOOTING

- Detail the NGFW packet inspection process
- Review the troubleshooting process and learn troubleshooting tips
- Define the role of sgInfo in troubleshooting
- Explore how to troubleshooting with logs
- Understand how to troubleshoot a VPN
- Analyze the role of monitoring in troubleshooting
- Troubleshoot the NGFW engine

Terms and Conditions

- Instructor-led trainings limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint training courses are standard and non-negotiable.
- Forcepoint provides the training course “AS IS” and makes no warranties of any kind, express or implied.
- You must register for the course offering within 90 days from purchase or the course may be forfeited.
- Instructor-led courses must be completed within 6 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