FORCEPOINT
POWERED BY Raytheon

FORCEPOINT NGFW

System Engineer Course Data Sheet

FORCEPOINT NGFW

SYSTEM ENGINEER COURSE

Intended audience

- End-User/Customers: System Administrators, network security administrators, IT Staff
- Channel Partners: Consultants, system architects, integrators and planners who help customers with Forcepoint NGFW implementations

Format

- Instructor-Led Training (classroom training)

Duration

- 5 days, 8 hours per day

Pre-requisites

- A working knowledge of networking (TCP, UDP, etc.) and computer security concepts
- General understanding of system administration

Certification requirements

- Completion of all course sessions and lab exercises
- Certification exam (multiple choice and hands-on)

Overview

- During the five sessions, you will learn how to install, configure, administer, and support Forcepoint NGFW. Through instruction, 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 and gain an understanding of how the Forcepoint NGFW fits into the security ecosystem of Forcepoint. 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, under-standing multi-link technology, configuring VPNs, traffic deep inspection, performing common administration tasks including status monitoring and reporting

Course objectives

- Understand system architecture
- Learn how to deploy and configure firewall clustering
- Understand static routing and anti-spoofing
- Understand security policy structure and configuration
- Learn how to use Sidewinder proxies with the NGFW
- Become familiar with and configure Multi-Link for traffic management
- Learn advanced configuration and use cases for IPSec VPNs
- Learn the concept and configuration of Deep Inspection and Regular Expressions
- Learn how to integrate the NGFW with other Forcepoint offerings
- Learn how to configure Dynamic Routing
- Learn how the NGFW can benefit MSSPs and how to configure Virtual Contexts
- Understand the SMC API its use cases
- Learn how to troubleshoot management and engines

Day 1

1) **System Overview and Architecture**
   - SMC and NGFW architecture
   - SMC Sizing and Tuning
   - NGFW Sizing
   - Management and Log Server HA
   - Licensing
2) **Firewall/VPN Role and NGFW Clustering**
   - Network Defense Strategy
   - NGFW Features and Capabilities
   - Clustering Technology
3) **Static Routing and Anti-spoofing**
   - Configuring Static Routing
   - Policy-based Routing
   - Anti-spoofing
4) **NGFW Policy Overview and Templates**
   - Policy Types
   - Hierarchical Policy Structure
   - Special Elements and Actions

Day 2

1) **NGFW Policies - Application Filtering**
   - Packet Processing
   - Application Filtering Methods
   - Protocol Inspection
2) **Sidewinder Proxy Modules**
3) **QoS Overview and Policies**
   - QoS Overview
   - QoS Policies
   - QoS with Multi-Link and VPN
4) **Multi-Link - Outbound Traffic Management**
   - ISP Selection Methods
   - ISP Selection based on QoS
5) **Multi-Link - Inbound Traffic Management**

Day 3

1) **Advanced VPN**
   - Multi-Link VPN Review
   - Hub VPN Configuration
   - Understand Tunnel Selection
2) **Active Directory Integration**
   - Forcepoint DC Agent Installation
   - Forcepoint DC Configuration in the SMC
   - Integrating AD with the SMC
   - Using NPS for Authentication
   - User and Application Usage Reporting
3) **Mobile VPN**
   - IPSec vs. SSL VPN
   - VPN Configuration for Gateway and Client
   - Mobile VPN Troubleshooting Tools
4) **Deep Inspection**
   - Deep Inspection Policy Overview
   - Traffic Inspection Process and Normalization
   - Situations
   - Advanced Evasion Techniques and Mitigation

Day 4

1) **Creating Custom Situations**
   - Situation Types and Context
   - NGFW Regular Expressions
2) **TLS Inspection**
   - Server Protection
   - Client Protection
   - HTTPS Proxy
3) **Event Correlation**
   - Scan Detection
   - SYN Floods and Denial of Service Attacks
   - Correlation Situations
   - Blacklisting
4) **Attack Investigation and Reporting**
5) **IPS and Layer 2 Firewall Roles**
   - Overview of NGFW Roles
   - IPS and Layer 2 Firewall Deployment
   - Clustering with IPS and Layer 2 Firewall
   - Mixed Mode

Day 5

1) **Forcepoint Integration**
   - Web Gateway
   - Advanced Malware Detection
   - URL Filtering
   - McAfee Anti-Malware
2) **Dynamic Routing**
   - Dynamic Routing Configuration in the SMC
   - BGP Peering with ISP(s)
   - Route-based VPN
3) **MSSP and Virtual Contexts**
   - Virtual Contexts
   - SMC Domains
   - Master Engines and Virtual Engines
   - Master Engine Clustering
4) **SMC API**
   - SMC API Overview
   - Configuring the SMC API Service
   - API Requests
5) **Troubleshooting**
   - Troubleshooting Process Overview
   - NGFW Maintenance and Troubleshooting
   - Understanding Log Messages (Advanced)
   - Command Line Tools

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