FORCEPOINT

FORCEPOINT NGFW

SYSTEM ENGINEER COURSE

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

- NGFW Administrator Certification
- 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, understanding 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 a NGFW in a Distributed environment
- Configure NGFW clustering
- Understand security policy structure and configuration
- Learn how the NGFW can benefit MSSPs and how to configure Virtual Contexts
- Learn how to integrate the system with Active Directory
- Become familiar with and configure Multi-Link for traffic management
- Learn advanced configuration and use cases for IPSec VPNs
- Learn how to use Sidewinder proxies with the NGFW
- Learn the concept and configuration of Deep Inspection and Regular Expressions
- Learn how to integrate the NGFW with other Forcepoint offerings
- 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 Single Firewall

- Network Defense Strategy
- NGFW Features and Capabilities
- Single Firewall Configuration

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) Distributed Architecture

- System Communications and NAT
- Location and Contact Addresses

2) MSSP and Virtual Context

- Virtual Contexts
- SMC Domains
- Master Engines and Virtual Engines
- Master Engine Clustering

3) Clustering Technology

- Firewall Clustering Architecture
- Firewall Cluster Configuration

DAY 3

1) Multi-Link - Outbound Traffic Management

- ISP Selection Methods
- ISP Selection based on QoS
- Multi-Link Configuration

2) Site-to-Site VPN

- Multi-Link VPN Review
- Route Based VPN
- Hub VPN Configuration
- Understand Tunnel Selection

3) Active Directory Integration

- Integrating AD with the SMC
- Using NPS for Authentication
- Forcepoint DC Agent
- Forcepoint ECA Agent
- User and Application Usage

4) Mobile VPN

- IPSec vs. SSL VPN
- VPN Configuration for Gateway and Client
- Mobile VPN Troubleshooting Tools

DAY 4

1) Traffic inspection

- Connection Controls
- Service with Protocol
- Service with Proxy
- Network Applications

2) Deep Inspection

- Deep Inspection Policy Overview
- Situations
- Inspection Policy
- Tuning the Inspection Policy

3) Malware Detection

- Malware Detection Process
- File Filtering Policy
- File Reputation Service
- Anti-Malware Scan
- Advanced Malware Detection

4) Inspection Techniques

- Traffic Inspection Process
- Advanced Evasion Techniques
- Situation Types and Context
- NGFW Regular Expressions

5) TLS Inspection

- Server Protection
- Client Protection
- HTTPS Proxy

DAY 5

1) Layer 2 Deployment

- Overview of NGFW Roles
- IPS and Layer 2 Firewall Deployment
- Multi-Layer Deployment for Firewall/VPN

2) Forcepoint Integration

- Web Gateway
- Advanced Malware Detection
- URL Filtering
- McAfee Anti-Malware

3) Troubleshooting

- Troubleshooting Process Overview
- NGFW Maintenance and Troubleshooting
- Understanding Log Messages (Advanced)
- Command Line Tools

4) Practical Exam

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