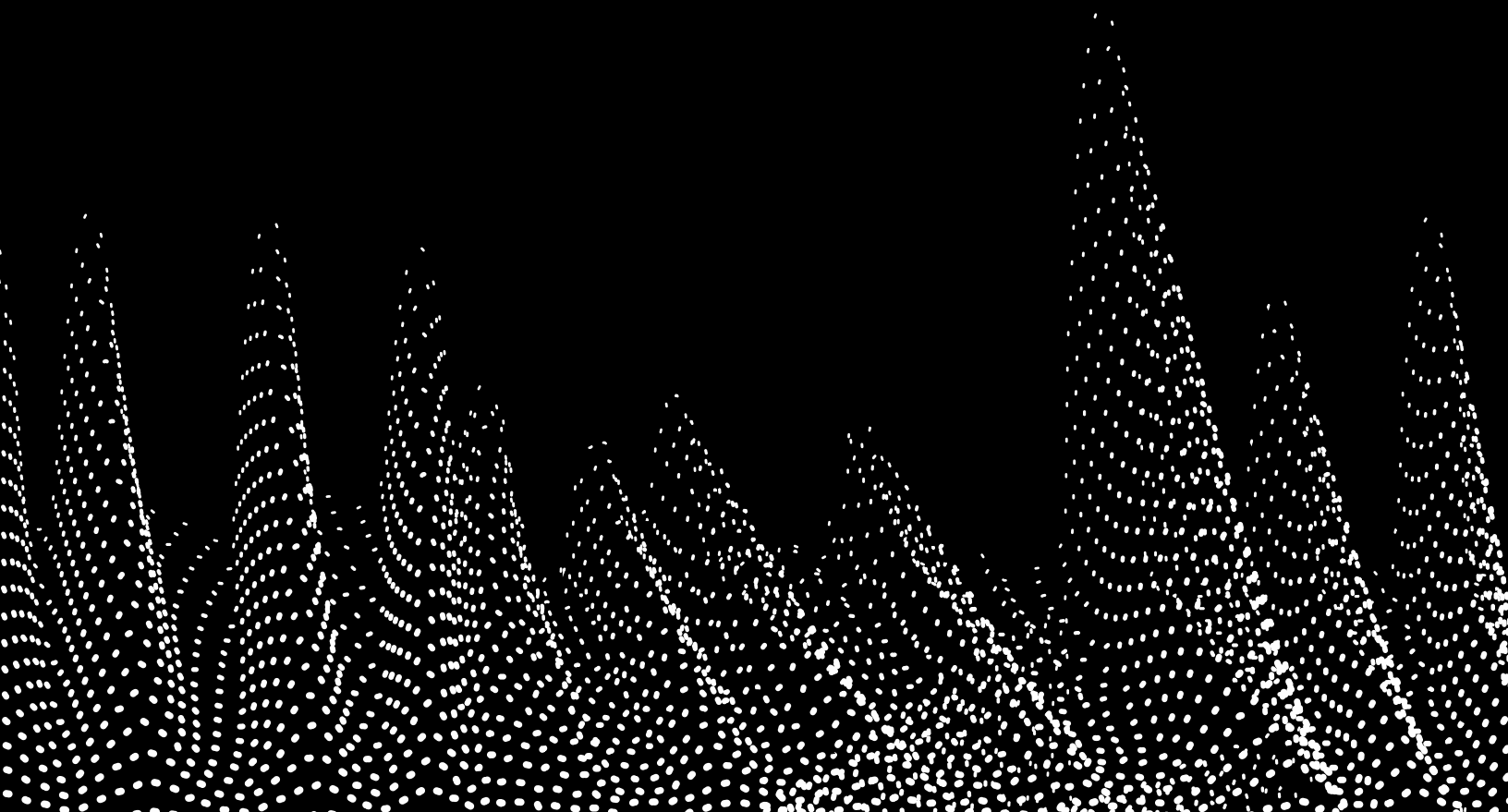
FORCEPOINT
POWERED BY Raytheon

aaa

Forcepoint NGFW

ADMINISTRATOR COURSE

OUTLINE



Forcepoint NGFW

ADMINISTRATOR 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
- **Forcepoint Sales Engineers**: Forcepoint personnel who provide pre-sales and post-sales support for Forcepoint NGFW

Format

- Instructor-Led Training (ILT)

Duration

- 4 Days

Pre-requisites

- Good understanding of networking and computer security concepts
- General understanding of system administration and Internet services

Overview

During the four 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. 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
- Understand different installation methods
- Understand SMC capabilities
- Understand FW/VPN roles and clustering
- Configure routing
- Configure security policies and access control
- Understand Multi-Link technology
- Configure Multi-Link VPNs
- Manage users and authentication
- Configure Mobile VPN
- Configure SSL VPN Portal
- Perform traffic deep inspection
- Perform common administration tasks
- Understand monitoring capabilities
- Configure reporting

Day 1

0) Introduction
a) Participant introductions
b) Logistics
c) Course Objectives
d) NGFW New Features

1) Next Generation Firewall Engine
a) NGFW History & Background
b) Key Benefits and Differentiators
c) Operating Modes
d) Hardware Platforms and Virtualization
e) Installation Methods
f) Licensing

2) SMC Overview
a) NGFW System Architecture
b) SMC Components / Supported Platforms
c) Management & Log Server Properties
d) Web Portal Server Properties
e) Deployment Options
f) Status View / Configuration View
g) Management Client Tools

3) FW/VPN Role and Clustering
a) NGFW FW/VPN Role & Requirements
b) Multi-layer Inspection
c) Single NGFW Overview
d) Clustering Technology
e) Firewall Cluster
f) Additional Firewall Features
g) IPS Serial Clustering
h) Layer 2 Firewall Clustering

4) Routing and Anti-Spoofing
a) Static Routing Configuration
b) Special Routing Conditions
c) Policy Routing
d) Dynamic Routing Overview
e) Anti-Spoofing

Day 2

5) NGFW Policies
a) Policy Types
b) Packet Processing Flow
c) Firewall Templates and Policy Hierarchy
d) NGFW Policies
e) Policy Tools & Rule Options
f) NAT Definition
g) Address Translation Options
h) Proxy ARP and NAT

6) Log Data Management
a) Purpose of Logs
b) Log Entry Types
c) Logging Generation
d) Log Data Pruning
e) Logs View
f) Visualizing Logs
g) Filters
h) Third Party Logs

7) Multi-Link Technology
a) Outbound Traffic Management
b) Link Selection Methods
c) Outbound Multi-Link Configuration
d) Server Pools
e) Multi-Link for Inbound Traffic
f) Configuring Server Pools and
g) Inbound Multi-Link

8) Multi-Link VPN
a) Overview of VPNs
b) VPN Topologies
c) VPN High Availability
d) Policy-Based VPN Configuration
e) VPN Tools
f) Route-Based VPN

Day 3

9) Users and Authentication
a) Managing Users
b) Directory Servers
c) Supported Authentication Methods
d) User Authentication Process
e) Browser Based Authentication
f) User Identification

10) Mobile VPN Client
a) Mobile VPN Connections
b) IPsec VPN vs SSL VPN Tunneling
c) VPN Client Configuration - Gateway Side
d) VPN Client Configuration - Client Side
e) Troubleshooting Tools

11) SSL VPN Portal
a) Client Based and Clientless Access
b) SSL VPN Portal Overview
c) SSL VPN Services
d) Link Translation Methods
e) SSL VPN Portal Configuration

12) Traffic Inspection in Access Rules
a) Traffic Inspection
b) Protocol Agents
c) Sidewinder Proxies
d) Network Applications
e) URL Filtering
f) Anti-Malware
g) Forcepoint Integration
h) TLS Inspection

Day 4

13) Inspection and File Filtering Policies
a) Deep Inspection
b) NGFW Policy Templates
c) Predefined Inspection Policies
d) Situation Concepts
e) Inspection Rules Tree
f) Fine-Tuning Inspection
g) Inspection Exception Rules
h) File Filtering Policies
i) Advanced Malware Detection
j) Packet Inspection Procedure

14) Administration Tasks
a) Role-Based Access Control
b) Alert Process
c) Log Management Tasks
d) Log Forwarding
e) System Upgrades and Backups
f) SMC High Availability
g) Location and Contact Addresses
h) Troubleshooting / Support

15) Monitoring, Statistics and Reports
a) Status Monitoring
b) Overviews
c) Reports
d) Report Designs, Sections, and Items
e) Geolocation Maps
f) Session Monitoring
g) Third-Party Monitoring

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