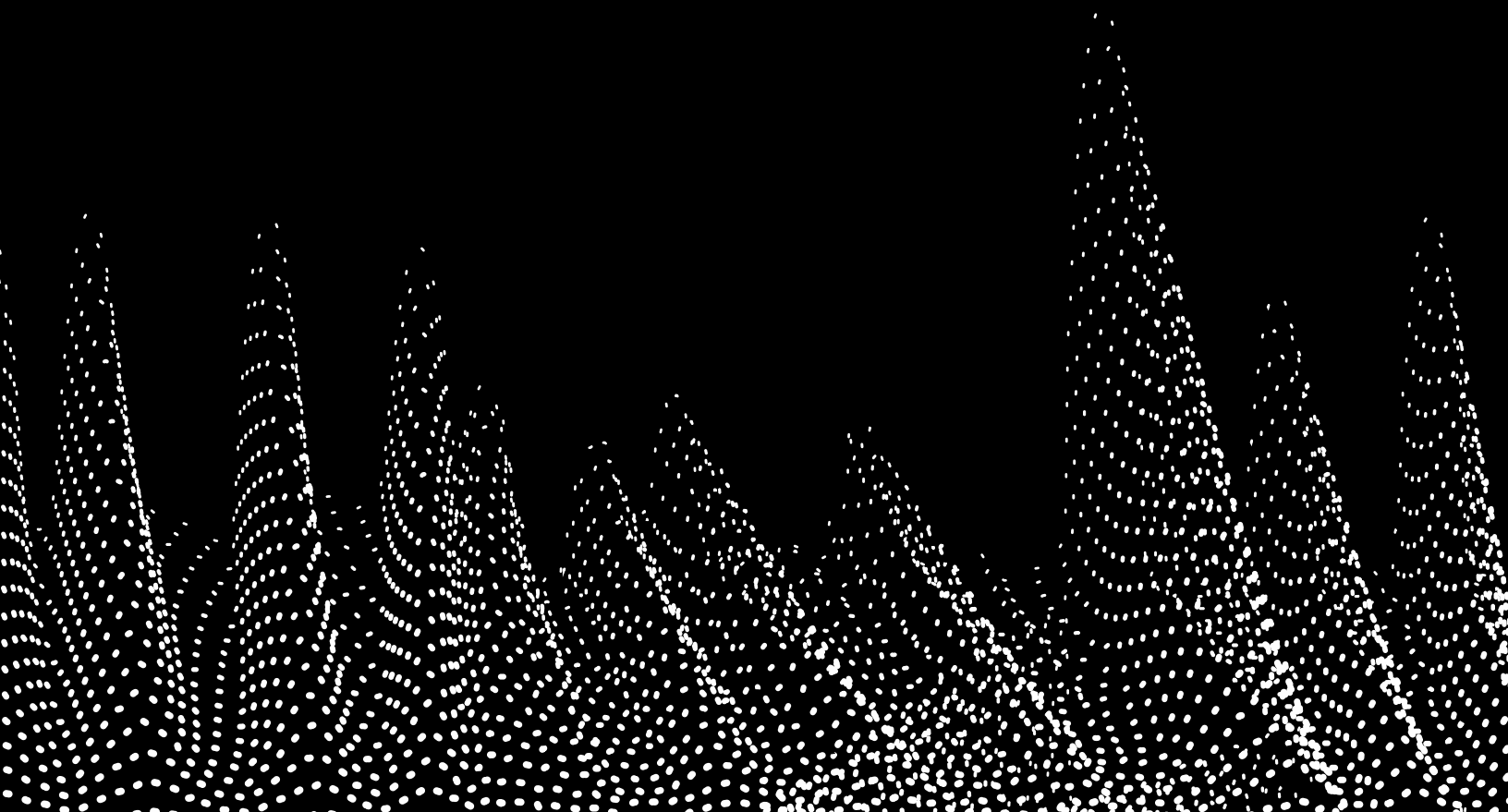
FORCEPOINT
POWERED BY Raytheon

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

Format

- Virtual Instructor-Led training (VILT)
    - Online (remote) training

Duration

- 4 sessions, 4 hours per session
    - Total of 16 hours virtual classroom time

Homework

- Students are required to complete homework activities (outside of class time) to reinforce topics learned and to prepare for the next session
    - Approximately 30-60 min required each day outside of virtual classroom time

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 administer Forcepoint NGFW using the Stonesoft Management Center. Through instruction, demonstrations, and hands-on lab practice exercises, you will learn the requirements and recommendations to successfully manage Forcepoint NGFWs policies and data provided by the systems such as alerts, logs and monitoring statistics. You will develop expertise in creating security rules and policies, managing users and authentication, configuring VPNs, traffic deep inspection and performing common administration tasks.

Course objectives

- Understand the fundamentals of NGFW
- Understand SMC capabilities
- Perform common administration tasks
- Configure security policies and access control
- Understand change control
- Perform traffic inspection
- Manage users and authentication
- Understand VPN
- Configure SSL VPN Portal
- Understand monitoring capabilities
- Configure reporting
- Perform basic troubleshooting

Day 1

0) Introduction
a) Welcome
b) Agenda
c) Virtual Environment Overview
d) NGFW New Features

1) 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

2) NGFW Overview
a) NGFW History & Background
b) Key Benefits and Differentiators
c) Operating Modes
d) Hardware Platforms and Virtualization
e) Installation Methods

3) Getting Started with SMC
a) Management Client Overview
b) System Backups and SMC HA
c) SMC Administrators
d) Policy Change Control
e) Logging and Logs View

Day 2

4) NGFW Policies
a) Policy Types
b) Firewall Templates and Policy Hierarchy
c) NGFW Policies and Policy Editor
d) Traffic Inspection
e) Forcepoint Integration
f) Network Address Translation

5) 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 Rule
h) Advanced Malware Detection
i) File Filtering Policies

6) Alerting and Notifications
a) Alert Escalation Process
b) Alert Policy
c) Alert Chain
d) Alert Notifications

Day 3

7) Users and Authentication

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

8) SSL VPN Portal

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

9) VPN

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

In order to attend this online class, you must have a computer with:

- High-speed Internet connection
- Up-to-date web browser
- Adobe Flash web browser plug-in
- PDF viewer
- Speakers or headphones

A tablet or ebook reader is also recommended.

Test your connection to an Adobe Connect virtual class environment here.

Day 4

10) Using Logs

a) Log Entry Types
b) Visualizing Logs
c) Log Data Pruning
d) Diagnostic
e) Filter Editor
f) Syslog Forwarding

11) Policy Tools

a) Policy Snapshots
b) Rule Search
c) Policy Validation
d) Rule Counter Analysis

12) SMC API

a) SMC API Overview
b) Get Started with SMC API
c) Configuring SMC API service
d) API Requests
e) REST Client
f) Example of Commands

13) 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

14) Troubleshooting

a) Troubleshooting Process
b) Troubleshooting with Logs
c) Capturing Traffic
d) Diagnostics for Support: sgInfo
e) Use Cases: Troubleshooting Management Server and Log Server problem

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