**Course Outline**

Forcepoint NGFW Administrator Course

Length 4 Days

## DESCRIPTION

During this four day training course, you will learn how to install, configure, administer, and support Stonesoft NGFW.

Through instruction, demonstrations, and hands-on lab practice exercises, you will learn the requirements and recommendations to successfully deploy Stonesoft 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, deep traffic inspection, performing common administration tasks including status monitoring and reporting.

## PARTICIPANTS

Channel Partners:

- Consultants, system architects, integrators and planners who help customers with Stonesoft NGFW implementations.

Forcepoint Sales Engineers:

- Forcepoint personnel who provide pre-sales and post-sales support for Stonesoft NGFW.

## PREREQUISITES

Working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of Internet services

## OBJECTIVES

Understand the fundamentals of NGFW
- Understand different installation methods
- Understand SMC capabilities
- Understand FW/VPN roles and clustering
- Configure routing
- Configure security policies
- Understand Multi-Link technology
- Configure Multi-Link VPNs
- Manage users and authentication
- Configure IPsec and SSL VPNs
- Perform traffic and deep inspection
- Perform common administration tasks
- Understand monitoring capabilities
- Configure reporting

## PROGRAMME

Day 1

1) Introductions
a) Participant introductions
b) Logistics
c) Course Objectives

2) 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 and Add-ons

3) SMC Overview
a) NGFW System Architecture
b) SMC Components / Supported Platforms
c) Management & Log Server Properties
d) WebPortal Server Properties
e) Deployment Options
f) Status View / Configuration View
g) Management Client Tools
h) Local Manager

4) 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) IPS Serial Clustering
g) Additional Firewall Features
h) NGFW Engine Architecture

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

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

Day 2

7) 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

8) 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

9) 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

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

Day 3

11) IPsec 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

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

13) Traffic Inspection in Access Rules
a) Traffic Inspection
b) Protocol Agents
c) Applications
d) Web Filtering
e) Anti-Virus

f) Anti-Spam
g) GTI and ATD
h) Deep Inspection
i) TLS Inspection

Day 4

14) Inspection and File 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) Rule Options
i) Blacklist
j) Packet Inspection Procedure

15) 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

16) 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