DATASHEET

# Network Security Platform Administration

Education Services Instructor-led Training

## Introduction

The Network Security Platform Administration course is an essential component of implementing a successful intrusion prevention strategy. In hands-on lab sessions, you'll learn how to deploy and configure a Network Security Platform solution to protect against real-world attacks. You can immediately apply your new skills to improve protection for your business and take full advantage of your investment in our McAfee Network Security Platform.

> This course is an essential component of implementing a successful intrusion prevention strategy.

## Audience

System and network administrators, security personnel, auditors, and/ or consultants concerned with network and system security should take this course.

## Course Goals

- Planning the deployment
- Installing and configuring the Manager
- Managing users and resources
- Configuring and managing policies
- Analyzing and responding to threats
- Tuning your security policies for maximum effectiveness

## Agenda At A Glance

Day 1

- Welcome
- Introduction to Network Security Platform
- Planning NSP Deployment
- Getting Started
- Manager Configuration
- User Management

Day 2

- Administrative Domains
- Sensor Overview
- Basic Sensor Setup
- Advanced Sensor Setup
- Policy Configuration
- Policy Customization
- Virtualization (Sub-Interfaces)

Day 3

- Threat Explorer
- Attack Log
- DoS Attacks
- Advanced Malware Detection
- Advanced Callback Detection

Day 4

- Inspection Options Policies
- Web Server Protection
- Firewall Policy Configuration
- Policy Tuning
- Report Generation
- Operational Status
- Database Maintenance

## Course Learning Objectives

### Welcome

The first module provides an overview of course design, logistics, and helpful resources, as well as provides the opportunity for the instructor to learn about you and your training expectations.

### Introduction to Network Security Platform

Describe the key features and benefits of the NSM solution and how to use NSM to enhance security in your or-ganization.

### Planning the NSP Deployment

Describe the deployment planning considerations, such as the deployment options and solution requirements.

### Getting started

Describe the purpose and configuration procedures for various NSP features and components.

### Manager Configuration

Describe the purpose and configuration procedures for various NSP features and components.

### User Management

Describe how to add and configure users and roles in the Network Security Manager (Manager). You will learn about the purpose of role assignments and how to assign predefined roles, as well as create custom roles. You will also learn how to manage GUI login settings.

### Administrative Domains

Describe how to add and configure  admin domains in the Network Security Manager (Manager).

### Sensor Overview

Describe the supported Sensors, their architecture, and deployment options.

### Basic Sensor Setup

Describe how to use the Manager interface for basic setup and management.

### Advanced Sensor Setup

Describe how to use the Manager interface for advanced setup and management.

### Policy Configuration

Describe how to configure and manage IPS policies.

### Policy Customization

Describe how to use the Manager interface for basic setup and management.

### Virtualization

Describe the purpose and benefits of virtualization, how to configure different sub-interface types using the McAfee® Network Security Manager (Manager), and how to assign policies to Network Security Sensor (Sensor) resources.

### Threat Explorer

Describe how to use the Threat Explorer.

### Attack Log

Describe alerts and ignore rules and how to navigate the Attack Log.

### DoS Attacks

Describe how to identify DoS attacks and the configuration of DoS options.

### Advanced Malware Detection

Describe the NSP Advanced Malware features and configuration.

### Advanced Callback Detection

Describe the NSP Advanced Botnet Detection features and configuration.

### Inspection Options Policies

Describe how to identify DoS attacks and the configuration of DoS options.

### Web Server Protection

Identify and configure web server protection.

### Firewall Policy Configuration

Identify and configure a Firewall Policy.

### Policy Tuning

Describe fundamentals about policy tuning, such its purpose and configuration. You will also learn about noise, false positives, and the important of monitoring high-volume attacks.

### Report Generation

Identify, generate, and interpret report types.

### Operational Status

Identify and view the available monitors, and export and generate activity logs.

### Database Maintenance

Describe Network Security Manager (Manager) database maintenance best practices.

Copyright © 2022 Musarubra US LLC