McAfee Network Security Platform Administration Course

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
COURSE DESCRIPTION

Agenda at a Glance

Day 1
- Welcome
- Introduction to Network Intrusion Prevention
- Planning
- Getting Started
- User Management
- Administrative Domains
- McAfee Network Security Sensor Overview
- Basic Sensor Management

Day 2
- Virtualization (Sub-Interfaces)
- Policy Configuration
- Policy Customization
- Threat Explorer
- Advanced Malware Protection

Day 3
- Advanced Botnet Detection
- Denial of Service Attacks
- Endpoint Reputation
- Web Server Protection

Day 4
- Firewall Policy Configuration
- Threat Analyzer
- Policy Tuning
- Report Generation
- Operational Status
- Database Maintenance

Course Outline

Module 1: Welcome
- About the Course
- Acronyms and Terms
- Course Logistics
- Locating Resources on McAfee Business Website
- McAfee Product Training
- Foundstone® Security Education
- ServicePortal
- Security Content Release Notes

Module 2: Introduction to Network Intrusion Prevention
- Security Threats: The Increasing Risks
- What are Threats and Attacks?
- Common Attack Types
- Motivation and Contributing Factors for Attacks

Recommended Pre-Work

It is recommended that students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of internet services.
COURSE DESCRIPTION

- Comparing Intrusion Detection and Prevention
- Types of Intrusion Prevention Systems
- Why a Network IPS Is Important
- McAfee Network Security Platform Overview
- New This Release
- Solution Components
- Attack Detection Framework
- Traffic Normalization
- Ten Steps to Using McAfee Network Security Platform
- Beyond Intrusion Prevention

**Module 3: Planning a McAfee Network Security Platform Deployment**

- Choosing a Deployment Option
- Deployment Requirements and Recommendations
- McAfee Network Security Manager Server Requirements
- McAfee Network Security Manager Client Requirements
- Windows Display and Browser Settings
- Virtual Server Minimum Requirements
- Virtual Machine Requirements
- McAfee Network 8X Sensor Support
- McAfee Network Server Ports
- Desktop Firewall Requirements
- Using Antivirus Software with McAfee Network Security Manager
- Wireshark

- Single and Central McAfee Network Security Manager Deployment
- Determining Database Requirements
- Sensor Deployments
- Determining Sensor Placement
- Determining Number of Sensors
- High Availability and Disaster Recovery
- Implementation Process Checklist

**Module 4: Getting Started**

- Logging into Manager Interface
- McAfee Network Security Manager Installation Wizard
- Verifying Access to McAfee Network Security Manager Interface
- Operational Monitors
- Security Monitors
- Navigating McAfee Network Security Manager Interface
- Managing Dashboard Monitors
- Setting up Basic Features
- McAfee Network Security Manager Disaster Recovery (MDR) Overview
- Configuring MDR Pair
- Central Manager Overview
- Defining Trust with Central Manager Proxy Server
- Configuring Proxy Server
- IPS Event Notification Overview
- Viewing Summary of IPS Events
COURSE DESCRIPTION

- Simple Network Management Protocol (SNMP) Overview
- Configuring SNMP Notification
- Syslog Notification Overview
- Configuring Syslog Notification
- Email Server and Notification Overview
- Configuring Email Server and Notification
- Configuring Script Notification
- Fault Notification Overview
- Configuring Fault Notification
- Configuring Common Settings for Faults
- Access Events Notification Overview
- User Activity Overview
- Configuring User Activity: SNMP
- Configuring User Activity: Syslog
- McAfee Global Threat Intelligence (McAfee GTI) Overview
- McAfee GTI Integration Requirements
- Enabling McAfee GTI Integration

Module 5: User Management
- User Management Overview
- Minimum Account Configuration
- Role Assignment Overview
- Viewing Roles and Privileges
- Editing the Default Root Administrator User
- Adding, Editing, and Deleting Users
- Verifying User Credentials
- Creating a Custom Role
- Assigning Domains and Roles
- Managing My Account
- Managing GUI Access
- Viewing User Activity
- Configuring Banner Text and Image
- Configuring Session Controls
- Configuring Password Controls
- Specifying Audit Settings
- Authentication
- Summary of Authentication Configuration
- LDAP External Authentication
- Configuring LDAP (Up to Four Servers)
- Assigning LDAP Authentication
- RADIUS External Authentication
- Configuring RADIUS External Authentication
- Assigning RADIUS Authentication

Module 6: Administrative Domains
- Administrative Domains Overview
- Administrative Domains’ Hierarchical Structure
- How Administrative Domains Work
- Managing Administrative Domains
- Editing the Root Administrative Domain
- Adding a Child Administrative Domain
- Adding Users to a Child Domain
Module 7: McAfee Network Security Platform
Sensor Overview
- M-Series Sensor Portfolio
- NS-Series Sensor Portfolio
- Virtual IPS Series Sensor Portfolio
- Primary Function of Sensor
- Respond
- Inspect
- Classify
- Capture
- Virtualization (Sub-Interfaces)
- Secure Socket Layer (SSL) Decryption
- Acceleration and Operation
- Operating Modes
- Fail-Close and Fail-Open (In-Line Only)
- Multiport Monitoring
- Interface Groups (Port Clustering)
- High Availability
- Large Networks: Perimeter, Core, Internal Placement
- Best Practices

Module 8: Basic Sensor Management
- Installing Physical Sensors
- Installing Virtual Sensor
- Managing Sensors
- Devices Page: Global Tab
- Devices Page: Device Tab
- Installing Sensors in McAfee Network Security Manager
- Establishing Trust
- Downloading Signature Sets
- Reviewing Device Summary
- Viewing/Editing Physical Ports
- Port Types
- Name Resolution
- Network Time Protocol (NTP)
- Proxy Server
- Activity Reports and Logs Review
- CLI Logging
- IPS Event Logging
- Alerting Options
- Remote Access: TACACS+
- Remote Access: NMS Users and Devices
- Customizing Logon Banner
- Special Configurations
- High Availability
- ATD Integration Overview
- DXL Integration Overview
- Maintenance
- Deploying Pending Changes
- Deploying Device Software
- Troubleshooting
- Performance Monitoring
Module 9: Virtualization
- Virtualization (Sub-Interfaces) Overview
- Valid Interface Types
- Before and After
- VLAN and CIDR Logical Configuration
- Bridge VLAN
- Policy Application
- Determining Direction
- VLAN Tagging
- Double-VLAN Tagging
- CIDR Block Options
- Configuring VLAN Virtual Interface
- Configuring CDIR Virtual Interface
- Configuring Bridge VLAN Virtual Interface
- VLAN Sub-Interface Configuration
- CDIR Sub-Interface Configuration

Module 10: Policies Configuration
- Intrusion Prevention Overview
- What Are Policies?
- Policy Terms and Concepts
- Signatures
- Attack Definitions
- Types IPS Policies
- Policy Assignment
- Inheritance
- How Policies are Applied
- Policy Management Overview
- Adding IPS Policy for Administrative Domain
- Copying or Editing IPS Policy for Administrative Domain
- Deleting IPS Policy for Administrative Domain
- Adding IPS Policy for Interface
- Editing IPS Policy for Interface
- Using IPS Policies Page
- Defining Properties
- Viewing Attack Definitions
- Assigning Policies
- Using Policy Manager
- Interfaces Tab
- Deploying Changes
- Managing Policy Versions
- Deleting Policy
- Policy Import and Export
- Managing Legacy Reconnaissance Policies
- Reconnaissance Attack Settings Merge Utility

Module 11: Policy Customization
- How Attacks Definitions Work
- Traffic Processing and Analysis Attack Definitions Tab
- Attack Categories and Severity
- Attack Protection Categories
- Attack Definitions Tab: Customizing Your View
COURSE DESCRIPTION

- Attack Definitions Tab: Quick Search, Sort, Columns, Groups, Filters, and Detail
- Attacks Detail Pane: Description
- Benign Trigger Probability (BTP)
- Attacks Detail Pane: Settings Tab
- Managing Policy Groups

Module 12: Threat Explorer
- Analyzing Threats
- Customizing Threat Analyzer View
- Analyzing Source and Destination IP Addresses
- Top Attacks
- Top Attackers
- Top Targets
- Top Applications
- Top Attack Executables
- Top Malware
- Guidelines

Module 13: Advanced Malware Protection
- Advanced Malware Detection Overview
- Malware Engines
- Policy Management Overview
- Advanced Malware Policies Configuration Overview
- Using Advanced Malware Policies Page
- Using Policy Manager
- Malware Policy Parameters
- File Types
- Blacklist/Whitelist Engine
- McAfee Threat Intelligence Exchange/McAfee GTI File Reputation Engine
- PDF and Flash Analysis Engines
- Gateway Anti-Malware Engine
- McAfee Advanced Threat Defense Engine
- McAfee Cloud Engine
- Malware Engine Analysis Sequence
- Confidence Level
- Action Thresholds
- Analyzing Malware
- Malware Analysis Overview
- Top Malware Detections Monitor
- Malware Detections Page
- Archiving Malware Files
- Best Practices

Module 14: Advanced Botnet Detection
- Advanced Botnet Detection Overview
- Zero-Day and Targeted Botnet Detection
- Heuristics
- Examples of Implemented Heuristics
- Known Botnet Detection
- C&C Server/Callback Detection
- DNS Response Packet Inspection
COURSE DESCRIPTION

- Whitelisted and Blacklisted Domains Detection
  - Example: Blacklist Domain Detection
- Inspection Options Policies
- How Inspection Option Policies Work
- Policy Management Overview
- Inspection Options Policies Configuration Overview
- Properties Tab
- Inspection Options Tab
- Configuring Traffic Inspection
- Configuring Advanced Botnet Detection
- Advanced Botnet Detection Options
- Legacy Malware Detection Options
- Assigning Policies to Sensor Resources
- Deploying Changes
- Analyzing Botnets
- Top Active Botnets Monitor
- Active Botnets Page: Organization

Module 15: Denial-of-Service (DoS) Configuration
- DoS Attacks
- Evolution of DoS Attacks
- Types of DoS Attacks
- Volume-Based Attacks
- DoS Learning Mode
- DoS Learning Attacks
- Customizing DoS Learning Attack
- Managing DoS Learning Profiles
- DoS Threshold Mode
- Configuring Thresholds for Volume-Based Attacks
- Connection Limiting Policies
- Adding Connection Limiting Policy
- Rate Limiting (QoS Policies)
- QoS and Rate Limiting Configuration Overview
- Adding QoS Policy
- Configuring Rate Limiting Rules
- Protocol Settings
- Configuring Protocol Settings
- Anti-Spoofing
- Stateful TCP Engine
- DNS Protection Command
- Case Studies

Module 16: Endpoint Reputation
- McAfee GTI Review
- IP Reputation
- Policy Management Overview
- IP Reputation Configuration Overview
- Endpoint Reputation Analysis Options
- Deploying Changes
Module 17: Web Server Protection
- Web Server Protection Overview
- How Web Server Heuristic Analysis Works
- Policy Management Overview
- Heuristic Web Application Server Inspection Configuration Overview
- Prerequisite: SSL Decryption
- Private SSL Certificates
- Prerequisite: Required Attacks
- Configuring Web Server Heuristic Analysis
- DoS Protection for Web Servers
- Layer 7 DoS Protection for Web Servers
- Web Server—DoS Prevention Configuration Overview
- Configuring Web Server—DoS Prevention
- Assigning Policies to Sensor Resources

Module 18: Firewall Policy Configuration
- Firewall Policy Overview
- Managing Firewall Policies
- Prerequisite: SSL Decryption
- Using Firewall Policies Page
- Using Policy Manager
- Rule Objects Overview
- Adding Rule Object
- Stateless Access Rules
- User-Based Access Rules
- Application Identification
- Policy Export and Policy Import
- Firewall Access Logging
- Firewall Access Events
- Firewall Policy Definitions Configuration Report

Module 19: Threat Analyzer
- Threat Analyzer Overview
- Launching Threat Analyzer
- Menu Bar
- Dashboard Page
- McAfee Network Security Platform Health Dashboard
- Viewing Details for Pie Slice
- Deploying Pending Changes
- IPS Dashboard
- Viewing Details for Pie Slice
- Viewing Attacks Over Time
- Viewing Consolidated Attacks
- NTBA Dashboard
- Applications and McAfee GTI View Dashboard
- Adding Dashboards and Monitors
- Customizing the Dashboard Tabs
- Adding a Dashboard
- Adding a Monitor
- Alerts Page
Module 20: Policy Tuning
- What Is Tuning?
- Why Implement Tuning?
- Prior to Tuning
- Two Phases of Policy Tuning
- False Positives and Noise
- Identifying False Positives
- Steps for Reducing False Positives
- Preventing False Positives
- Start with High-Volume Attacks
- Looking for Patterns
- Preventing Future False Positives
- Disabling Attacks and Alerts
- Adding Low-Severity Attacks to Process
- Excessive Alerts
- High-Level Bottom-Up Approach
- Analyzing Event
- Sorting by Attack Name
- Case Studies

Module 21: Report Generation
- Reports Overview
- Role Assignment
- Reporting Preferences
- Configuration Reports Overview
- Running Configuration Report
- Next-Generation Reports Overview
- Running Default Next-Generation Report
- Adding, Duplicating, Editing Next-Generation Report
- Traditional Reports Overview
- Running a Traditional Report
- Adding User Defined Report
- Configuring Report Automation
- Viewing Automatically Generated Reports

Module 22: Operational Status
- Operational Monitors Overview
- Device Summary Monitor
- McAfee Network Security Manager Summary
- Messages from McAfee Monitor
- Running Tasks Monitor
- System Health Monitor
- Managing Faults
- Viewing McAfee Network Security Manager Faults from Dashboard
- Viewing Device Faults from Dashboard
- Viewing Faults from Manage Page
COURSE DESCRIPTION

- Alert Relevance
- Viewing Alert Relevance
- System Log
- Viewing System Log
- Exporting System Log
- Running Tasks
- Viewing User Activity Log

Module 23: Database Maintenance
- Maintenance Overview
- Archiving Malware Files
- Backing Up Data
- Automating Database Backup
- Viewing Scheduler Detail
- Exporting Backup Files
- Deleting Backup Files
- Database Tuning Overview
- Tuning Now
- Automating Tuning
- Enabling and Defining Alert Pruning
- Calculating Maximum Alert Quantity
- Configuring File and Database Pruning
- Data Archiving
- Archiving Data Now
- Automating Archiving Data
- Export Archives
- Restoring Archive

Learn More

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@mcafee.com.