ProTech "Charting the Course ...
protechtraining.com
... to Your Success!"

Cisco ASA/FirePOWER with Advanced FireSIGHT Administration (ASAFP)

Course Summary

Description

In this three day course, stduents will learn how to use and configure real next-generation Cisco and Sourcefire technology including application control, FireSIGHT, Security Intelligence, Access Control Policies, IPS policies, and URL filtering. Students will also learn to properly tune systems for better performance and greater network intelligence while taking full advantage of powerful tools for more efficient event analysis. Students will acquire the necessary knowledge and skills to manage and tune the FirePOWER product.

This course prepares students to take the Securing Cisco Networks with Sourcefire IPS exam (Exam ID 500-285), but highly concentrates on teaching students how to be an advanced FirePower administrator.

Objectives

By the end of this course, students will be able to:

- Install FirePower on a Cisco ASA
- Install and configure the FirePOWER Services Module and the FireSIGHT Management Center
- Manage the FireSIGHT Manager
- Describe the Cisco and Sourcefire systems infrastructure
- Navigate the user interface and administrative features of the Cisco FirePOWER and Sourcefire systems, including reporting functionality to properly assess threats
- Describe how to deploy and manage Cisco ASA and Sourcefire appliances
- Describe the role FireSIGHT technology plays in the Cisco and Sourcefire systems
- Describe, create, and implement objects for use in Access Control policies
- Describe advanced policy configuration and Sourcefire system configuration options
- Understand how to fine tune IPS policies
- Analyze events

Topics

- What is SourceFire, FirePOWER, and FireSIGHT?
- What is ASA with FirePOWER?
- Installing ASA with FirePOWER
- Configuring and using the FireSIGHT Management Console
- Device Management
- Object Management
- Access Control Policy
- Network-based Malware Detection
- FireSIGHT Technology
- Correlatio Policies
- IPS Policy Basics
- User Account Management
- Reporting

Audience

This course is designed for technical professionals who need to know how to deploy and manage a Cisco ASA with FirePOWER and/or a Sourcefire Appliance system in a network environment.

Prerequisites

In order to fully benefit from this course, it is recommended that students have the following prior to enrolment:

- Technical understanding of TCP/IP networking and basic networking
- Routing and Switching understanding
- Familiarity with the concepts of IPS

Duration

Three days

ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Cisco ASA/FirePOWER with Advanced FireSIGHT Administration (ASAFP)

Course Outline

I. What is SourceFire, FirePOWER, and FireSIGHT?

II. What is ASA with FirePOWER?

III. Installing ASA with FirePOWER

IV. Configuring and using the FireSIGHT Management Console

V. Device Management

VI. Object Management

VII. Access Control Policy

VIII. Network-based Malware Detection

IX. FireSIGHT Technology

X. Correlatio Policies

XI. IPS Policy Basics

XII. User Account Management

XIII. Reporting

XIV. Labs

A. Upgrading the ASA to 9.3 version
B. Downloading the FirePOWER installation file
C. Installing the FirePOWER module on the ASA
D. Verifying the ASA with FirePOWER module and installation
E. Connecting to the inside PC and configuring the FMC
F. Creating Objects
G. Creating an Access Control Policy (Port Inspection)
H. Creating an Access Control Policy (Application Awareness)
I. URL Filtering
J. Including an IPS Policy in Access Control Rules
K. Creating a File Policy
L. Tuning the Network Discover Policy
M. Viewing FireSIGHT Data
N. User Discovery
O. Creating a Correlation Policy Based on Connection Data
P. White Lists
Q. Working with Connection Data and Traffic Profiles
R. Creating an Intrusion Policy
S. Including FireSIGHT Recommendations in an Intrusion Policy
T. Tuning your HTTP_Inspect Preprocessor
U. Applying and Testing your Policy and Variable Set
V. Creating User Accounts and Configuring the User Interface Timeout Value
W. Testing Exempt and Non-exempt Users
X. Permission Escalation
Y. Working with External Accounts
Z. Analysis Lab
AA. Tuning Events
BB. Context Explorer
CC. Comparing Trends with Reports