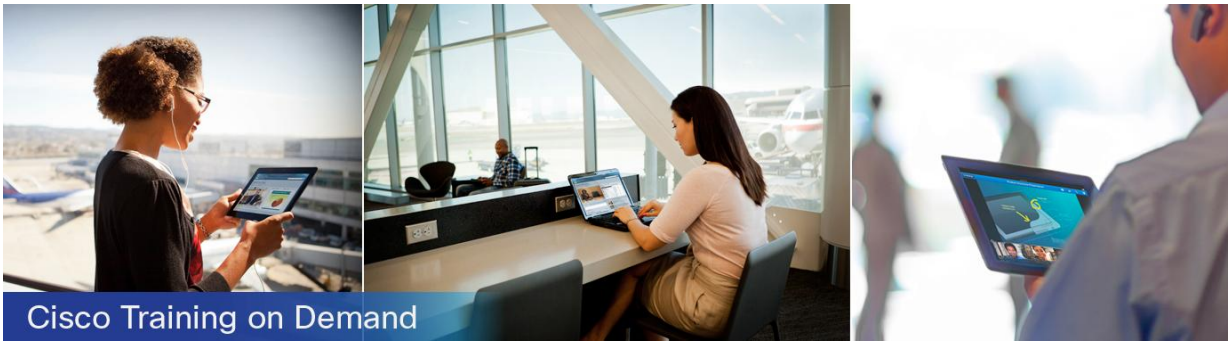
Learning Services

Cisco Training on Demand

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS) Version 2.0



Overview

Securing Cisco® networks with Cisco FireSIGHT™ Intrusion Prevention System (SSFIPS) Version 2.0 Cisco Training on Demand is a lab-intensive course that introduces you to the powerful features of the Cisco FireSIGHT System, including, in-depth event analysis, IPS tuning and configuration, and the Cisco Snort® rules language.

You learn how to use and configure next-generation Cisco IPS technology, including application control, firewall, and routing and switching capabilities. Gain the knowledge and skills needed to tune systems correctly for better performance and greater network intelligence while taking full advantage of powerful tools for more efficient event analysis, including file type and network-based malware detection.

Interested in purchasing this course in volume at discounts for your company? Contact ctod-sales@cisco.com.

Duration

The SSFIPS Training on Demand course consists of 32 lessons, totaling more than 11 hours of video instruction, along with 13 hands-on lab exercises.

Target Audience

SSFIPS is designed for technical professionals who need to know how to deploy and/or manage a Cisco system in a network environment. The primary audience for this course includes security administrators, security consultants, network administrators, system engineers, technical support personnel, and channel partners and resellers.

Objectives

After completing this course, you should be able to:

- Describe the Cisco FireSIGHT system training infrastructure
- Navigate the user interface and administrative features of the Cisco FireSIGHT system, including reporting functionality to assess threats properly
- Describe how to deploy and manage Cisco FireSIGHT devices
- Describe the various detection technologies used in the Cisco FireSIGHT system
- Describe, create, and implement objects for use in access control policies
- Describe advanced policy configuration and Cisco FireSIGHT system configuration options
- Analyze events
- Write and configure basic Cisco Snort rules

Course Prerequisites

Before taking this course, you should have working knowledge and skills about the following:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS

Course Outline

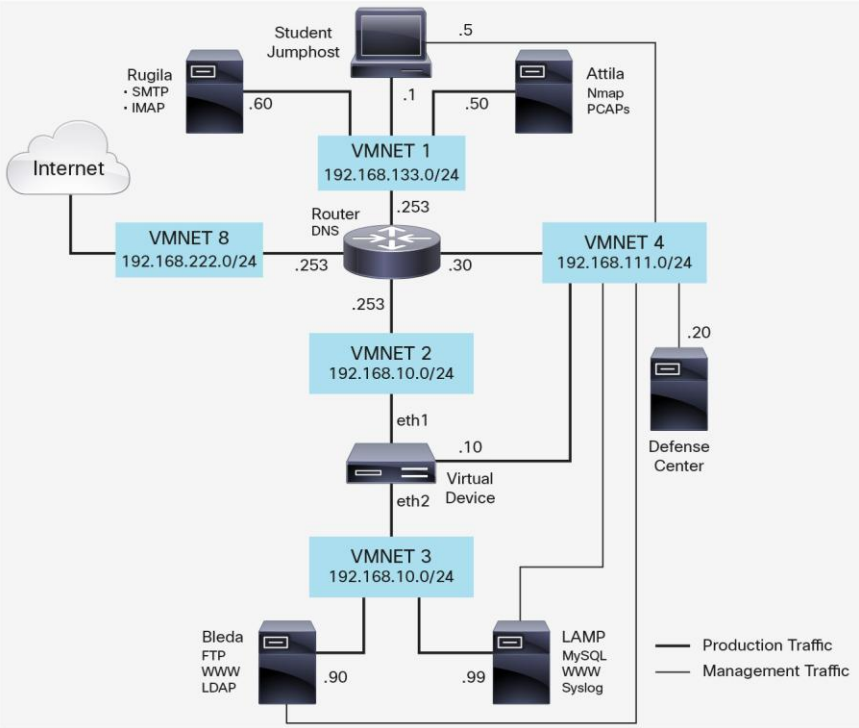
- Lesson 1: Cisco FireSIGHT System Overview and Classroom Setup
- Lesson 2: Hardware Overview and Architecture
- Lesson 3: Device Management
- Lesson 3a: Interface Configuration
- Lesson 3b: Advanced Interface Configuration
- Lesson 3c: Policy-Based Network Address Translation (NAT), Gateway VPN, and Clustered High-Availability State Sharing Overview
- Lesson 4: User Account Management
- Lesson 5: Object Management
- Lesson 5a: Security Intelligence and Variable Sets
- Lesson 6: Access Control Policy
- Lesson 6a: Access Control Policy Rules
- Lesson 7: Cisco FireSIGHT Technology (Hosts)
- Lesson 7a: Cisco FireSIGHT Technology (Hosts)—Demo
- Lesson 7b: Cisco FireSIGHT Technology (Users)
- Lesson 8: Network-Based Malware Detection
- Lesson 8a: Network-Based Malware Detection Analysis
- Lesson 9: Managing SSL Traffic
- Lesson 9a: Managing SSL Traffic Policies
- Lesson 10: IPS Policy Basics

- Lesson 10a: IPS Policy Basics—Advanced Settings
- Lesson 11: Network Analysis Policy
- Lesson 11a: Network Analysis Policy—Demo
- Lesson 12: Event Analysis
- Lesson 12a: Event Analysis—Contest Explorer and Dashboards
- Lesson 13: Reporting
- Lesson 14: Correlation Policies Overview
- Lesson 14a: Correlation Policies Components
- Lesson 14b: Correlation Policies
- Lesson 14c: Correlation Policies Demo
- Lesson 15: Basic Rule Syntax and Usage
- Lesson 15a: Basic Rule Syntax and Usage (continued)
- Lesson 15b: Basic Rule Syntax and Usage Demo

Labs Outline

This course contains 13 hands-on virtual lab exercises, powered by Cisco Learning Labs and Cisco IOL (Cisco IOS® Software on Linux). The topology for all labs is shown in Figure 1.

Figure 1. Topology for All Labs in SSFIPS Course



The labs included in this course are:

- Lab 1: Validating the Environment
- Lab 3: Configuring Inline Interfaces
- Lab 4: User Accounts
- Lab 5: Creating Objects
- Lab 6: Access Control Policies
- Lab 7: Cisco FireSIGHT Technologies
- Lab 8: Advanced Malware Protection
- Lab 10: Intrusion Policies
- Lab 11: Network Analysis Policies
- Lab 12: Event Analysis and Tuning
- Lab 13: Reporting
- Lab 14: Correlation Policies
- Lab 15: Cisco Snort Rule Wiring

Instructor: Paul Azzi

Paul Azzi has almost 20 years of industry experience of which the last 8 years have been focused on security. Having worked for channel partners, he has solid design and deployment experience in Cisco security solutions, which include firewall, IPS, VPN, AAA, Cisco IronPort® technology, and Cisco Integrated Services Engine (ISE). His passion for sharing knowledge has led him to become an education specialist with Cisco for which he travels and delivers security courses.

Supported Configurations

Cisco Training on Demand videos are supported on PCs, Macs, and tablets using one of the following browsers, or later: Mozilla Firefox 30, Google Chrome 35, and Apple Safari 6. The labs are supported on PCs and Macs but not on tablets.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-736285-00 12/15