Data Sheet

Learning Services

Cisco Training on Demand

Implementing Cisco Threat Control Solutions (SITCS)

Overview

Implementing Cisco® Threat Control Solutions (SITCS) Version 1.5 is a Cisco Training on Demand course. It prepares you with the knowledge and capabilities to implement and manage security on Cisco ASA firewalls, and provides hands-on experience so that you can deploy Cisco Next Generation Firewall (NGFW), as well as Web Security, Email Security, and Cloud Web Security.

The hands-on experience also assists with configuring various advanced Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall.

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

Duration

The SITCS Training on Demand course is a self-paced course based upon the 5-day instructor-led training version. It consists of 30 sections of instructor video and text totaling more than 18 hours of instruction along with interactive activities, 16 hands-on lab exercises, content review questions, and challenge questions.

Target Audience

The primary audience for this course are those preparing for the 300-210 SITCS exam and network security engineers.

Objectives

After completing this course, you should be able to:

- Describe and implement Cisco Web and Email Security Appliance
- Describe and implement Cloud Web Security
- Describe and implement Cisco ASA (CX) Next-Generation Firewall Services and Cisco Intrusion Prevention Systems

Course Prerequisites

The knowledge and skills recommended before attending this course are:

- Cisco CCNA® certification
- Cisco CCNA Security certification
- Knowledge of Microsoft Windows operating system

Course Outline

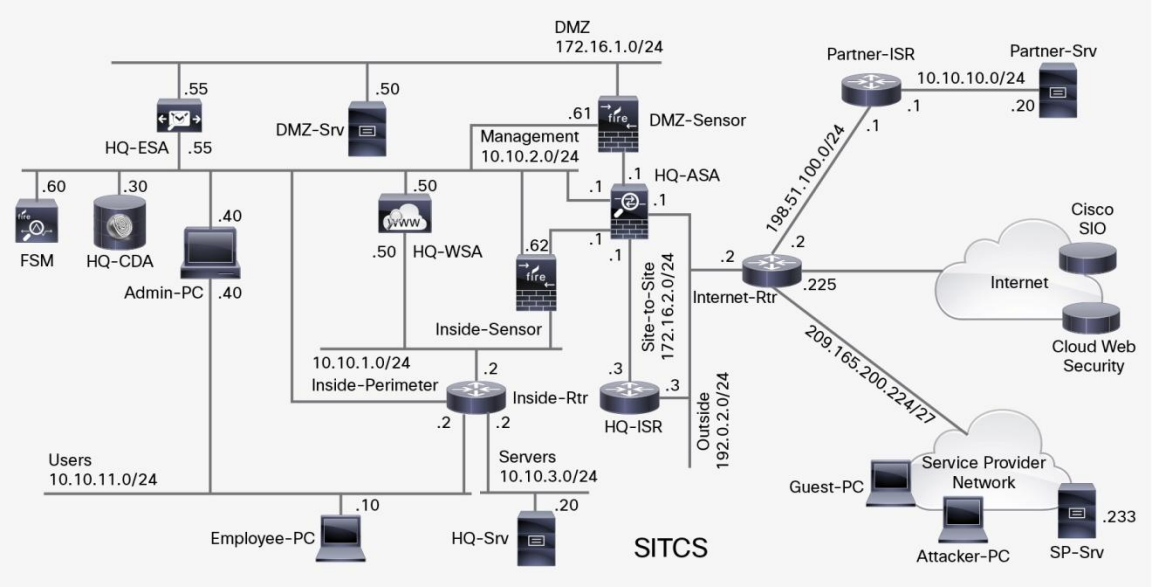
- Course Introduction
- Section 1: Describing the Cisco Web Security Appliance Solutions
- Section 2: Integrating the Cisco Web Security Appliance
- Section 3: Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Section 4: Configuring Cisco Web Security Appliance Acceptable Use Controls
- Section 5: Configuring Cisco Web Security Appliance Anti-Malware Controls
- Section 6: Configuring Cisco Web Security Appliance Decryption
- Section 7: Configuring Cisco Web Security Appliance Data Security Controls
- Section 8: Describing the Cisco Cloud Web Security Solutions
- Section 9: Configuring Cisco Cloud Web Security Connectors
- Section 10: Describing the Web Filtering Policy in Cisco ScanCenter
- Section 11: Describing the Cisco Email Security Solutions
- Section 12: Describing the Cisco Email Security Appliance Basic Setup Components
- Section 13: Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies
- Section 14: AMP for Endpoints Overview and Architecture
- Section 15: Customizing Detection and AMP Policy
- Section 16: IOCs and IOC Scanning
- Section 17: Deploying AMP Connectors
- Section 18: AMP Analysis Tools
- Section 19: Describing the Cisco FireSIGHT® System
- Section 20: Configuring and Managing Cisco FirePOWER™ Devices
- Section 21: Implementing an Access Control Policy
- Section 22: Understanding Discovery Technology
- Section 23: Configuring File-Type and Network Malware Detection

- Section 24: Managing SSL Traffic with Cisco FireSIGHT
- Section 25: Describing IPS Policy and Configuration Concepts
- Section 26: Describing the Network Analysis Policy
- Section 27: Creating Reports
- Section 28: Describing Correlation Rules and Policies
- Section 29: Understanding Basic Rule Syntax and Usage
- Section 30: Installing Cisco ASA 5500-X Series FirePOWER Services Module

Labs Outline

This course contains 16 hands-on lab exercises.

Figure 1. Topology for All Labs in Implementing Cisco Threat Control Solutions



The labs included in this course are:

- Discovery Lab 3.20: Configure Cisco Web Security Appliance Explicit Proxy and User Authentication
- Discovery Lab 6.6: Configure Cisco Web Security Appliance Acceptable Use Controls
- Discovery Lab 13.19: Configure Cisco Email Security Appliance Basic Policies
- Discovery Lab 14.17: Accessing the AMP Public Cloud Console
- Discovery Lab 15.13: Customizing Detection and AMP Policy
- Discovery Lab 16.5: IOCs and IOC Scanning
- Discovery Lab 17.10: Deploying AMP Connectors
- Discovery Lab 18.19: AMP Analysis Tools
- Discovery Lab 20.7: Configure Inline Interfaces and Create Objects
- Discovery Lab 21.12: Create Access Control Policy Rules

- Discovery Lab 22.5: Configure Network Discovery Detection
- Discovery Lab 23.12: Create a File Policy
- Discovery Lab 25.7: Create an Intrusion Policy
- Discovery Lab 26.8: Create a Network Analysis Policy
- Discovery Lab 27.6: Compare Trends
- Discovery Lab 28.13: Create Correlation Policies

Cisco Capital Financing Helps You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx), accelerate your growth, and 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 financing 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 C78-737925-00 10/16