SFWIPF (FUNDAMENTALS OF CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION) 1.0

Objetivo

â¢ Describe Cisco Secure Firewall Threat Defense. â¢ Describe Cisco Secure Firewall Threat Defense Deployment Options. â¢ Describe management options for Cisco Secure Firewall Threat Defense. â¢ Configure basic initial settings on Cisco Secure Firewall Threat Defense. â¢ Configure high availability on Cisco Secure Firewall Threat Defense. â¢ Configure basic Network Address Translation on Cisco Secure Firewall Threat Defense. â¢ Describe Cisco Secure Firewall Threat Defense policies and explain how different policies influence packet processing through the device. â¢ Configure Discovery Policy on Cisco Secure Firewall Threat Defense. â¢ Configure and explain prefilter and tunnel rules in prefilter policy. â¢ Configure an access control policy on Cisco Secure Firewall Threat Defense. â¢ Configure security intelligence on Cisco Secure Firewall Threat Defense. â¢ Configure file policy on Cisco Secure Firewall Threat Defense. â¢ Configure Intrusion Policy on Cisco Secure Firewall Threat Defense. â¢ Perform basic threat analysis using Cisco Secure Firewall Management Center. â¢ Perform basic management and system administration tasks on Cisco Secure Firewall Threat Defense. â¢ Perform basic traffic flow troubleshooting on Cisco Secure Firewall Threat Defense. â¢ Manage Cisco Secure Firewall Threat Defense with Cisco Secure Firewall Threat Defense Manager.

PÃºblico Alvo

â¢ Security or network professionals seeking knowledge to design, install, configure, operate, and support the Cisco Firepower NGFW Security solution; â¢ Professionals who need to prepare for the Cisco 300-710 certification exam.

PrÃ©-Requisitos

To fully benefit from this course, you should have: â¢ Knowledge of TCP/IP and basic routing protocols; â¢ Desirable familiarity with firewall, VPN, and Intrusion Prevention System (IPS) security concepts.

Carga HorÃ¡ria

40 horas (5 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
â¢ Overview
â¢ Course Goal and Objectives
â¢ Course Flow
â¢ Your Training Curriculum
â¢ Learner Introductions

Introducing Cisco Secure Firewall Threat Defense
â¢ Describe Cisco Secure Firewall Threat Defense
â¢ Introduce firewall concepts and technologies with examples of each type
â¢ Describe traditional network security and how it does not keep up with todayâs modern threats
â¢ Describe Cisco Secure Portfolio
â¢ Cisco Secure Firewall Threat Defense Features Overview
â¢ Cisco Secure Firewall Use Cases
â¢ Cisco Secure Firewall Smart Licensing

Cisco Secure Firewall Threat Defense Deployment Options
â¢ Deployment Modes Overview
â¢ Deployment Cisco Secure Firewall: Firewall modes, IPS interface modes and redundancy options
â¢ Firewall Deployment Mode: Transparent and Routed firewall modes
â¢ Configuring Global Interfaces: supported types of interfaces for management and network traffic
â¢ Configuring IPS Interfaces: role of IPS and how IPS-only interfaces augment IPS deployments
â¢ Resilient and Scalable Design: high availability and clustering configuration options
â¢ High availability for the Cisco Secure Firewall Management Center

Cisco Secure Firewall Threat Defense Management Options
â¢ Describe management options for Cisco Secure Firewall Threat Defense
â¢ Cisco Secure Firewall Threat Defense Management Overview
â¢ Cisco Secure Firewall Management Center (FMC)
â¢ Describe functionalities of Cisco Secure Firewall Management Center
â¢ Cisco Secure Firewall Threat Defense Device Manager (FDM)
â¢ Describe functionalities of Cisco Secure Firewall Device Manager
â¢ Cisco Defense Orchestrator (CDO)
â¢ Describe functionalities of Cisco Defense Orchestrator

Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense
â¢ Configure basic initial settings on Cisco Secure Firewall Threat Defense
â¢ Initial Cisco Secure Firewall Threat Defense Setup
â¢ Cisco Secure Firewall Management Center (FMC) Initial Setup
â¢ Cisco Secure Firewall Threat Defense Registration with Cisco Secure Firewall Management Center
â¢ Cisco Secure Firewall Threat Defense Device Management (FDM)
â¢ Interfaces and Security Zones Configuration
â¢ Static Routing Configuration
â¢ Platform Settings Configuration
â¢ Perform Monitor System Health Using Health Policy
â¢ Configure initial Cisco Secure Firewall Threat Defense device setup

Configuring High Availability on Cisco Secure Firewall Threat Defense
â¢ Introducing high availability on Cisco Secure Firewall Threat Defense
â¢ Active/Standby Failover Overview
â¢ Stateless and Stateful Failover
â¢ Health Monitor Initiated Failover
â¢ Health & Interface Health: Trigger Failover in High Availability Pair
â¢ Active/Standby Failover Configuration
â¢ Verify and Troubleshoot Active/Standby High Availability

â¢ Configure and Verify Active/Standby Failover on Cisco Secure Firewall Threat Defense

Configuring Auto NAT on Cisco Secure Firewall Threat Defense
â¢ Configure Network Address Translation on Cisco Secure Firewall Threat Defense
â¢ Explain Network Address Translation & Types of Network Translation
â¢ Configuration for Auto Network Address Translation (Auto-Nat)
â¢ Configure Network Address Translation Steps

Describing Packet Processing and Policies on Cisco Secure Firewall Threat Defense
â¢ Explain How Different Policies Influence Packet Processing Through the Device
â¢ Describe Objects and Explain Usage of Objects in Policies
â¢ Describe Cisco Secure Firewall Threat Defense Policies
â¢ Cisco Secure Firewall Engines and Detailed Packet Processing (Ingress and Egress)

Configuring Discovery Policy on Cisco Secure Firewall Threat Defense
â¢ Discovery Policy Overview
â¢ Network Discovery Policy Configuration
â¢ Discovery Events and Host Profile Analysis
â¢ Configure Network Discovery

Configuring Prefilter Policy on Cisco Secure Firewall Threat Defense
â¢ Explain of Prefilter Policy & Reasons for Using It
â¢ Prefilter Policy Configuration
â¢ Connection Events Analysis
â¢ Analyze Events Produced by Prefilter Rules

Configuring Access Control Policy on Cisco Secure Firewall Threat Defense
â¢ Access Control Policy Overview
â¢ Access Control Policy Rules and Rule Actions
â¢ Access Control Policy Deployment
â¢ Access Control Policy Best Practices
â¢ Configure Prefilter and Access Control Policy

Configuring Security Intelligence on Cisco Secure Firewall Threat Defense
â¢ Security Intelligence Overview
â¢ Security Intelligence Objects
â¢ Configure and Explain: Purpose of Security Intelligence Objects
â¢ IP and URL Security Intelligence Configuration and Verification
â¢ DNS Security Intelligence Configuration and Verification
â¢ Configure Cisco Secure Firewall Threat Defense Security Intelligence Inspection

Configuring File Policy on Cisco Secure Firewall Threat Defense
â¢ File Policy Overview
â¢ Network Malware Protection and File Type Detection Architecture
â¢ File Policy Configuration
â¢ Malware and File Events Analysis
â¢ Implement File Control and Advanced Malware Protection

Configuring Intrusion Policy on Cisco Secure Firewall Threat Defense
â¢ IPS and Snort Introduction
â¢ Intrusion (Snort) Rule Introduction
â¢ Intrusion Policy Fundamentals
â¢ Creating Customizable (User Created) IPS Policies
â¢ Intrusion Event Overview
â¢ Configure Cisco Secure IPS

Performing Basic Threat Analysis on Cisco Secure Firewall Management Center
â¢ Provide an overview of different types of events
â¢ Event Generation & Event Types
â¢ Indications of Compromise
â¢ Context Explorer: Intrusion Events & Indications of Compromise
â¢ Dashboards Overview
â¢ Custom Dashboard Configuration
â¢ Report Overview
â¢ Create a Custom Report Template
â¢ Using the Unified Event Viewer
â¢ Describe the operation of the Unified Event Viewer
â¢ Threat Analysis Example
â¢ Detailed Analysis Using the Firewall Management Center

Managing Cisco Secure Firewall Threat Defense System
â¢ Explain how to implement Cisco Secure Firewall Threat Defense system updates
â¢ Describe the user management options and explain how to configure local user accounts
â¢ Backup of the System
â¢ Configuration Export and Import
â¢ Configuration Rollback
â¢ Manage Cisco Secure Firewall Threat Defense System

Troubleshooting Basic Traffic Flow
â¢ Cisco Secure Firewall Threat Defense CLI
â¢ Traffic Flow Troubleshooting Process and Tools
â¢ Traffic Flow Troubleshooting Examples
â¢ Secure Firewall Troubleshooting Fundamentals

Cisco Secure Firewall Threat Defense Device Manager
â¢ Cisco Secure Firewall Threat Defense Device Manager Initial Configuration
â¢ Cisco Secure Firewall Threat Defense Device Manager Policies Overview
â¢ Configure Managed Devices Using Cisco Secure Firewall Device Manager

Lab outline
â¢ Lab 1: Perform Initial Device Setup
â¢ Lab 2: Configure High Availability
â¢ Lab 3: Configure Network Address Translation
â¢ Lab 4: Configure Network Discovery
â¢ Lab 5: Configure Prefilter and Access Control Policy
â¢ Lab 6: Configure Security Intelligence

â¢ Lab 7: Implement File Control and Advanced Malware Protection
â¢ Lab 8: Configure Cisco Secure IPS
â¢ Lab 9: Detailed Analysis Using the Firewall Management Center
â¢ Lab 10: Manage Cisco Secure Firewall Threat Defense System
â¢ Lab 11: Secure Firewall Troubleshooting Fundamentals
â¢ Lab 12: Configure Managed Devices Using Cisco Secure Firewall Device Manager