SFWIPF

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

40 horas | Security & Cybersecurity | Cisco

Cisco Continuing Education Credits

40 CE Credits

INTRODUÇÃO

The goal of the course is to train students how to implement and configure Cisco Secure Firewall Threat Defense at the network edge using software version 7.x.

Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) v1.0 course shows you how to deploy and use Cisco Firepower® Threat Defense system. Beginning with initial device setup and configuration and including routing, high availability, traffic control, and Network Address Translation (NAT). You will learn how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection. You will also learn how to moving on to detailed analysis, system administration, and troubleshooting.

The course is used in these certifications, curricula, specializations, and learning maps.
• CCNP Security (Requires core exam [350-701 SCOR] and one of the concentration exams)
• Exam 300-710 SNCF (This course prepares students for this concentration exam)

OBJETIVO DO CURSO

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

PÚBLICO-ALVO

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

PRÉ-REQUISITOS

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

CONTEÚDO PROGRAMÁTICO

Course Introduction

• Overview
• Course Goal and Objectives
• Course Flow
• Your Training Curriculum
• Learner Introductions

Introducing Cisco Secure Firewall Threat Defense

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

Cisco Secure Firewall Threat Defense Deployment Options

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

Cisco Secure Firewall Threat Defense Management Options

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

Configuring Basic Network Settings on Cisco Secure Firewall Threat Defense

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

Configuring High Availability on Cisco Secure Firewall Threat Defense

• Introducing high availability on Cisco Secure Firewall Threat Defense

• Active/Standby Failover Overview
• Stateless and Stateful Failover
• Health Monitor Initiated Failover
• Health & Interface Health: Trigger Failover in High Availability Pair
• Active/Standby Failover Configuration
• Verify and Troubleshoot Active/Standby High Availability
• Configure and Verify Active/Standby Failover on Cisco Secure Firewall Threat Defense

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

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

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

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

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

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

Configuring File Policy on Cisco Secure Firewall Threat Defense
• File Policy Overview
• Network Malware Protection and File Type Detection Architecture

• File Policy Configuration
• Malware and File Events Analysis
• Implement File Control and Advanced Malware Protection

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

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

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

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

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

Lab outline
• Lab 1: Perform Initial Device Setup
• Lab 2: Configure High Availability
• Lab 3: Configure Network Address Translation
• Lab 4: Configure Network Discovery

- Lab 5: Configure Prefilter and Access Control Policy
- Lab 6: Configure Security Intelligence
- Lab 7: Implement File Control and Advanced Malware Protection
- Lab 8: Configure Cisco Secure IPS
- Lab 9: Detailed Analysis Using the Firewall Management Center
- Lab 10: Manage Cisco Secure Firewall Threat Defense System
- Lab 11: Secure Firewall Troubleshooting Fundamentals
- Lab 12: Configure Managed Devices Using Cisco Secure Firewall Device Manager